HC hahn collections
DEBT RECOVERY

COMPLIANCE MANUAL

FOR THE IMPLEMENTATION OF THE

PROTECTION OF PERSONAL INFORMATION ACT NO 4 OF 2013

CONTENTS:

1. INTRODUCTION

The Protection of Personal Information Act 4 of 2013 (POPI) gives effect to the right of privacy, by introducing measures to ensure that the personal information of an individual (data subject) is safeguarded when it is processed by responsible parties. The Act also aims to balance the right to privacy against other rights, particularly the right to access to information, and to generally protect important interests, including the free flow of information within and across the borders of the Republic. Therefor the Act intents to balance two competing interests, namely:

1.1 Our constitutional right to privacy (which requires our personal information to be protected); and

1.2 The need to have access to and to process our personal information for legitimate purposes.

In this Compliance Manual we set out the framework for our company's compliance with POPI.

Where reference is made to "Processing" means any operation or activity or any set of operations, whether or not by automatic means, concerning Personal information, including:

- The collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- Dissemination by means of transmission, distribution or making available in any other form; or
- Merging, linking, as well as restriction, degradation, erasure or destruction of information,

and **"Process", "Processes"** and **"Processed"** have the corresponding meanings.

2. SECURITY SAFEGUARDS

In order to secure the integrity and confidentiality of the personal information in our possession, and to protect against loss or damage or unauthorized access, we continue to implement the following security measures:

2.1 Our business premises where records are kept are and remain protected by access control, burglar alarms and armed response.

2.2 All computers are password protected and such passwords are changed on a regular basis.

2.3 Our email infrastructure must comply with industry standard security safeguards, and meet the General Data Protection Regulation (GDPR), which is standard in the European Union.

2.4 Assessments must be carried out on our digital infrastructure vulnerability at least on an annual basis to identify weaknesses and to ensure we have adequate security in place.

2.5 All our archived files are stored behind locked doors, no unauthorized third party has access to the archived files.

2.6 The antivirus protection automatically runs in the background to ensure our computers are kept updated with the latest patches.

2.7 Our staff is trained to carry out their duties in compliance with POPI, and such training must be ongoing.

2.8 It is a term of our employment contract with every staff member that they must maintain full confidentiality in respect of all of our clients' affairs, including our clients' personal information.

2.9 Employment contracts for staff whose duty it is to process our client's personal information, includes an obligation on the staff member to (a) comply with the terms of the POPI manual, (b) maintain the confidentiality of all our client's and colleagues' personal information and affairs, and (c) to notify the Principal or a Director immediately if there are reasonable grounds to believe that the personal information of a client has been accessed by an unauthorized person.

2.10 The processing of our staff members personal information takes place in accordance with the rules contained in the relevant labor legislation.

2.11 The personal information of clients and staff will be destroyed timeously in a manner that de-identifies the person.

2.12 The security safeguards will be verified on a regular basis to ensue effective implementation and must continually be updated in response to new risks.

3. SECURITY BREACHES

3.1 In the unfortunate event that the personal information of a client has been accessed or acquired by an unauthorized person, we shall notify the Information Regulator and the relevant client, unless we are no longer able to identify the client. This notification must take place as soon as reasonably possible.

3.2 The notification to the client will be communicated in writing in one of the following ways, with a view to ensue that the notification reaches the client:

3.2.1 to clients last know email address;

3.2.2 to clients last know physical or postal address;

3.2.3 as may be directed by the Information Regulator.

3.3 The notification to the client must give sufficient information to enable the client to protect themselves against the potential consequences of the security breach, and must include the following:

3.3.1 information of the possible consequences of the breach;

3.3.2 the measures we have or intent to take to address the breach;

3.3.3 recommendation of what the client could do to mitigate the adverse effects of the breach; and

3.3.4 if know the identity of the person who may have accessed the personal information.

4. CORRECTION OF CLIENTS PERSONAL INFORMATION

4.1 A client is entitled to request us to correct or delete personal information in regard to that client, which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or acquired unlawfully.

4.2 A client is also entitled to require us to destroy or delete records of personal information about the client that we are no longer authorized to retain.

4.3 Any such request must be made on the prescribed Form 2 in the Regulations.

4.4 Upon receipt of such lawful request of the abovementioned Form 2, we must as soon as reasonably practicable comply with such request.

4.5 In the event that a dispute arises regarding the clients right to have the information corrected, and the client so requires, we must attach to the information, an indication that the correction of the information has been requested but has not been made.

4.6 The client who made such request for their personal information to be corrected or deleted must be notified of the action we have taken to such request.

5. CLIENTS REQUESTING RECORDS

5.1 Any person is entitled to request that we confirm, free of charge and on production of proof of identity, whether or not we hold personal information about **that** person in our records.

5.2 If we hold such personal information, upon payment of a fee of our applicable tariff at the time plus VAT (if applicable), we shall provide the person requesting the information with the record, or a description of the personal information, including information about the identity of all third parties who have or had access to the information. We shall do this within a reasonable time.

5.3 A client requesting their personal information must be advised of their right to request to have any errors in their personal information corrected, which request must be done on the prescribed Form 2 in the Regulations.

5.4 In all cases where the disclosure of a record entails the disclosure of information that is additional to the personal information of the person requesting the record, the written consent of the Information Officer (or

his delegate) will be required, which person shall make their decision with regard to the provisions of Chapter 4 of Part 3 of the Promotion of Access to Information Act 2 of 2000.

5.5 If a request for personal information is made and part of the request is refused, every other part must still be disclosed.

6. SPECIAL PERSONAL INFORMATION

6.1 In terms of Section 26 of the Act special rules apply to the collection and processing of personal information relating to a person's religious or philosophical beliefs, race or ethic origin, trade union membership, political persuasion, health or sex life or biometric information or criminal behavior 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 or the disposal of such proceedings.

6.2 However, in terms of Section 27 of the act, the prohibition on processing personal information, as referred to in Section 26, does not apply if the –

(a) processing is carried out with the consent of a data subject referred to in Section 26;

(b) processing is necessary for the establishment, exercise or defence of a right or obligation in law;

(c) processing is necessary to comply with an obligation of international public law;

(d) processing is for historical, statistical or research purposes to the extent that –

(i) the purpose serves a public interest and the processing is necessary for the purpose conserved; or

(ii) it appears to be impossible or would involve a disproportionate effort to ask for consent,

And sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent;

(e) information has deliberately been made public by the data subject; or

(f) provisions of section 28 to 33 are, as the case may be, complied with.

….

6.3 We shall not process any of the Special Personal Information without the clients consent, or where this is necessary for the establishment, exercise or defence of a right or an obligation in law.

7. PROCESSING OF PERSONAL INFORMATION OF CHILDREN

7.1 We may only process the personal information of a child if we have the consent of the child's parent's or legal guardians.

8. CIRCUMSTANCES REQUIRING PRIOR AUTHORISATION

8.1 The circumstances which require prior authorization from the Information Regulator before processing any personal information are set out in Section 57 and 58 of the Act.

8.2 Should the need arise for the processing of such personal information we shall follow the requirements set out in Section 57 and 58 of the Act.

9. TRANSBORDER INFORMATION

9.1 We may not transfer a client's personal information to a third party in a foreign country, unless:

9.1.1 the client consents thereto, alternatively requests it; or

9.1.2 the transfer of the personal information is required for the performance of the contract between ourselves and the client; or

9.1.3 the transfer is necessary for the conclusion or performance of a contract for the benefit of the client in terms of our mandate; or

9.1.4 the transfer is necessary for the conclusion or performance of a contract for the benefit of the client entered into between ourselves and the third party; or

9.1.5 the transfer of the personal information is for the benefit of the client and it is not reasonably possible to obtain their consent and that if it were possible the client would be likely to give such consent.

10. OUR UNDERTAKINGS TO OUR CLIENTS

10.1 We undertake to follow POPI at all relevant times and to process personal information lawfully and reasonably, in order not to infringe unnecessarily on the privacy of our clients.

10.2 We undertake to process information only for the purpose for which it is intended, to enable us to do our work as mandated by our clients.

10.3 If necessary, we shall obtain consent to process personal information, which consent shall be in writing.

10.4 Where we do not seek consent, the processing of our client's personal information will be following a legal obligation placed upon us, or to protect a legitimate interest that requires protection.

10.5 We shall stop processing personal information if the required consent is withdrawn, or if a legitimate objection is raised.

10.6 We shall collect personal information directly from the client whose information we require, unless;

10.6.1 the information is of public record; or

10.6.2 the client has consented to the collection of their personal information from another source; or

10.6.3 the collection of the information from another source does not prejudice the client; or

10.6.4 the information to be collected is necessary for the maintenance of law and order or national security; or

10.6.5 the information is being collected to comply with a legal obligation; or

10.6.6 the information collected is required for the conduct of proceedings in any court or tribunal, where these proceedings have commenced or are reasonably contemplated; or

10.6.7 the information is required to maintain our legitimate interests; or

10.6.8 where requesting consent is not reasonably practical.

10.7 We shall retain records of the personal information we have collected for the minimum period as required by law unless the client has specifically instructed and has furnished their consent for us to retain such records for a longer period. Whereafter we shall destroy or delete the client's personal information (so as to de-identify the client) as soon as reasonably possible after the time period for which we were entitled to hold the records have expired.

10.8 We shall restrict the processing of personal information:

10.8.1 where the accuracy of the information is contested, for a period sufficient to enable us to verify the accuracy of the information;

10.8.2 where the purpose for which the personal information was collected has been achieved and where the personal information is being retained only for the purposes of proof;

10.8.3 where the client requests that the personal information is not destroyed or deleted, but rather retained; or

10.8.4 where the client requests that the personal information be transmitted to another automated data processing system.

10.9 The processing of further personal information shall only be undertaken:

10.9.1 where the further processing is necessary because of a threat to public health or public safety or to the life or health of the client, or a third person;

10.9.2 where this is required by the Information Regulator appointed in terms of POPI.

10.10. We ensure that the personal information which we collect and process is complete, accurate, not misleading and up to date.

10.11. We retain the physical file and the electronic data related to the processing of the personal information.

10.12. We are not entitled to disclose our client's bank account details, unless we have the client's specific consent.

10.13. A information letter shall be send alternatively handed to every client when we accept a mandate from such client, such letter informs the client of our duty to them in terms of POPI.

11. CLIENTS RIGHTS

11.1 Where a client's consent is required to process their personal information, such consent may be withdrawn.

11.2 In cases where we process personal information without consent to protect a legitimate interest, to comply with the law or to pursue or protect our legitimate interests, the client has the right to object to such processing.

11.3. All clients are entitled to lodge a complaint regarding our application of POPI with the Information Regulator.

11.4. Form 2 (clients consent to process personal information) must be completed by each client when we accept a mandate, to obtain the client's consent to process their personal information while we do our work for them, unless such consent has been obtained within another document signed by the client.

12. DIRECT MARKETING (if applicable to the business)

12.1. We may only carry out direct marketing (using any form of electronic communication) to clients if:

12.1 they were given an opportunity to object to receiving direct marketing material by electronic communication at the time that their personal information was collected; and

12.2 no objection was received at the time the personal information was collected or at any time after receiving any such direct marketing communications.

12.2 We may only approach clients using their personal information, if we have obtained their personal information in the context of providing services associated with our business to them, and we may then only market such services to them.

12.3 We may approach a person to ask for their consent to receive direct marketing material only once, and we may not do so if they have previously refused their consent.

12.4. A request for consent to receive direct marketing must be made in the prescribed manner and form. The prescribed form of this request and consent is an annexure to this Compliance Manual, Form 4 of the Regulation.

12.5. All direct marketing communications must disclose our identity and contain an address or other contact details to which the client may send a request that the communications cease.

13. INFORMATION OFFICER

13.1 Our Information Officer is Graham Dudley Powell who is our Chief Executive Officer/Managing Director or someonein a senior management position nominated and authorised by our Chief Executive Officer/Managing Director in writing. Such authorisation shall be made on Annexure C (of the Guidance Notes issued on 1 April 2021, annexed to Compliance Manual.

Our Information Officer's responsibilities include:

13.2 Ensuring compliance with POPI.

13.3 Dealing with requests which we receive in terms of POPI.

13.4 Working with the Information Regulator in relation to investigations.

13.5. Our Information Officer must designate in writing as many Deputy Information Officers as are necessary to perform the tasks mentioned above. Such designation shall be done by the completion of the prescribed form which is Annexure B (of the Guidance Notes issued on 1 April 2021) annexed to this Compliance Manual.

13.6. Our Information Officer and our Deputy Information Officers must register themselves with the Information Regulator prior to taking up their duties on the Regulators online portal to effect registration kindly do the following:

- On Google type in – Information regulator online registration, then
- Click on – Information officers Registration Portal – Department of Justice, then
- Go to – follow this link to open the ONLINE REGISTRATION FORM,

  And register.

see Annexure A (of the Guidance Notes issued on 1 April 2021) annexed to this Compliance Manual to fill out the Information and Deputy Information Officers details for your records.

13.7 In carrying out their duties, our Information Officer must ensure that:

13.7.1 this Compliance Manual is implemented;

13.7.2 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;

13.7.3 that this Compliance Manual is developed, monitored, maintained and made available;

13.7.4 that internal measures are developed together with adequate systems to process requests for information or access to information;

13.7.5 that internal awareness sessions are conducted regarding the provisions of POPI, the Regulations, codes of conduct or information obtained from the Information Regulator; and

13.7.6 that copies of this manual are provided to persons at their request, hard copies to be provided upon payment of a fee (to be determined by the Information Regulator).

13.8. Guidance notes on Information Officers have been published by the Information Regulator (on 1 April 2021) and our Information Officer and deputy Information Officers must familiarize themselves with the content of these notes.

14 OFFENCES AND PENALTIES

14.1 POPI provides for serious penalties for the contravention of its terms. For minor offences, a guilty party can receive a fine or be imprisoned for up to 12 months. For serious offences, the period of imprisonment rises to a maximum of 10 years. Administrative fines for the company can reach a maximum of R10 million.

14.2. Breaches of this Compliance Manual will also be viewed as a serious disciplinary offence.

14.3. It is therefore imperative that we comply strictly with the terms of this Compliance Manual and protect our client's personal information in the same way as if it was our own.

15. SCHEDULE OF ANNEXURES AND FORMS

15.1. Information letter to client. (Form 1)

15.2. Client's consent to process personal information. (Form 2)

15.3. Objection to the Processing of Personal Information. (Form 3) (Form 1 of the Regulations).

15.4. Request for correction or deletion of personal information. (Form 4) (Form 2 of the Regulations).

15.5. Application for consent to direct marketing. (Form 5) (Form 4 of the Regulations)

15.6 Addendum to our Employment Contract/ letter of appointment. (Form 6)

15.7. Information Officer's registration form. (Form 7) (Annexure A)

15.8. Designation and delegation to Deputy Information Officer. (Form 8) (Annexure B)

15.9. Authorisation of Information Officer. (Form 9) (Annexure C)

15.10 Security Implementation checklist.

15.11 Guidance note on Information officers and Deputy Information officers.

Hahn Collections (Pty) Ltd