VELO CYCLING CLUB COMPLIANCE MANUAL

FOR THE IMPLEMENTATION OF THE

PROTECTION OF PERSONAL INFORMATION ACT OF 2013

1. INTRODUCTION

The Protection of Personal Information Act (POPI) is intended to balance 2 competing interests. These are:

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

1.2 The needs of our society to have access to and to process (work with) our personal information for legitimate purposes, including the purpose of doing business.

This Compliance Manual sets out the framework for our company's compliance with POPI.

2. PROTECTION OF CLIENT INFORMATION

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

2.2 We undertake to process information only for the purpose for which it is intended, to enable us to do our work, as agreed with our clients.

2.3 Whenever necessary, we shall obtain consent to process personal information.

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

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 We shall stop processing personal information if the required consent is withdrawn, or if a legitimate objection is raised.

2.6. We shall collect personal information directly from the client whose information we require, unless:

2.6.1 the information is of public record, or

2.6.2 the client has consented to the collection of their personal information from another source, or

2.6.3 the collection of the information from another source does not prejudice the client, or

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

2.6.5 the information is being collected to comply with a legal obligation, including an obligation to SARS,

2.6.6 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

2.6.7 The information is required to maintain our legitimate interests; or

2.6.8 where requesting consent would prejudice the purpose of the collection of the information; or

2.6.9 where requesting consent is not reasonably practical in the circumstances.

2.7. We shall advise our clients of the purpose of the collection of the personal information.

2.8. We shall retain records of the personal information we have collected for the minimum period as required by law unless the client has furnished their consent or instructed us to retain the records for a longer period.

2.9. We shall destroy or delete records of the personal information (so as to deidentify the client) as soon as reasonably possible after the time period for which we were entitled to hold the records have expired.

2.10. We shall restrict the processing of personal information:

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

2.10.2 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;

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

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

2.11. The further processing of personal information shall only be undertaken:

2.11.1 if the requirements of paragraphs 3; 6.1; 6.4; 6.5 or 6.6 above have been met;

2.11.2 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;

2.11.3 where the information is used for historical, statistical or research purposes and the identity of the client will not be disclosed; or

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

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

2.13. We undertake to retain the electronic file and the electronic data related to the processing of the personal information.

2.14. We undertake to take special care with our client's bank account details, and we are not entitled to obtain or disclose or procure the disclosure of such banking details unless we have the client's specific consent.

3. OUR CLIENT'S RIGHTS

3.1. In cases where the client's consent is required to process their personal information, this consent may be withdrawn.

3.2. 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.

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

4. SECURITY SAFEGUARDS

4.1. In order to secure the integrity and confidentiality of the personal information in our possession, and to protect it against loss or damage or unauthorised access, we must continue to implement the following security safeguards:

4.1.1 Our business premises where records are kept must remain protected by access control, and burglar alarms.

4.1.2 All the user terminals on our internal computer network and our servers must be protected by passwords which must be changed on a regular basis.

4.1.3 Our email infrastructure (currently running on Outlook 365) must comply with industry standard security safeguards, and meet the General Data Protection Regulation (GDPR), which is standard in the European Union.

4.1.4 Vulnerability assessments must be carried out on our digital infrastructure on an annual basis to identify weaknesses in our systems and to ensure we have adequate security in place.

4.1.5 Archived files must be stored behind locked doors and access control to these storage facilities must be implemented.

4.1.6 We must use an internationally recognised Firewall, to protect the data on our local servers, and we must run antivirus protection.

4.1.7 Our staff must be trained to carry out their duties in compliance with POPI, and this training must be ongoing.

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

4.1.9 Employment contracts for staff whose duty it is to process a client's personal information, must include an obligation on the staff member (1) to maintain the Company's security measures, and (2) to notify their manager/supervisor immediately if there are reasonable grounds to believe that the personal information of a client has been accessed or acquired by any unauthorised person.

4.1.10 The processing of the personal information of our staff members must take place in accordance with the rules established in compliance with labour legislation.

4.1.11 The digital work profiles and privileges of staff who have left our employ must be properly terminated.

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

5. SECURITY BREACHES

5.1. Should it appear that the personal information of a client has been accessed or acquired by an unauthorised person, we must notify the Information Regulator and the relevant client/s, unless we are no longer able to identify the client/s. This notification must take place as soon as reasonably possible.

5.2. Such notification must be given to the Information Regulator first as it is possible that they, or another public body, might require the notification to the client/s be delayed.

5.3. The notification to the client must be communicated in writing in one of the following ways:

5.3.1 by mail to the client's last known physical or postal address;

5.3.2 by email to the client's last known email address;

5.3.3 by publication on our website or in the news media; or

5.3.4 as directed by the Information Regulator.

5.4 This 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:

5.4.1 a description of the possible consequences of the breach;

5.4.2 details of the measures that we intend to take or have taken to address the breach;

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

5.4.4 if known, the identity of the person who may have accessed, or acquired the personal information.

6. CLIENTS REQUESTING RECORDS

6.1. On production of proof of identity, any person is entitled to request that we confirm, free of charge, whether or not we hold any personal information about that person in our records.

6.2. If we hold such personal information, on request, and upon payment of a fee of R500.00 plus VAT, we shall provide the person with the record, or a description of the personal information, including information about the identity of all third-parties or categories of third parties who have or have had access to the information. We shall do this within a reasonable period, in a reasonable manner and in an understandable form.

6.3. A client requesting such personal information must be advised of their right to request to have any errors in the personal information corrected, which request shall be made on the prescribed application form.

6.4. In certain circumstances, we will be obliged to refuse to disclose the record containing the personal information to the client. In other circumstances, we will have discretion as to whether or not to do so.

6.5. In all cases where the disclosure of a record will entail 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, and that person shall make their decision having regard to the provisions of Chapter 4 of Part 3 of the Promotion of Access to Information Act.

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

7. THE CORRECTION OF PERSONAL INFORMATION

7.1. A client is entitled to require us to correct or delete personal information that we have, which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or which has been obtained unlawfully.

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

7.3. Any such request must be made on the prescribed form, available upon request.

7.4. Upon receipt of such a lawful request, we must comply as soon as reasonably practicable.

7.5. In the event that a dispute arises regarding the clients rights to have information corrected, and in the event that the client so requires, we must attach to the information, in a way that it will always be read with the information, an indication that the correction of the information has been requested but has not been made.

7.6. We must notify the client who has made a request for their personal information to be corrected or deleted what action we have taken as a result of such a request.

8. SPECIAL PERSONAL INFORMATION

8.1. Special rules apply to the collection and use of information relating to a person's religious or philosophical beliefs, their race or ethnic origin, their trade union membership, their political persuasion, their health or sex life, their biometric information, or their criminal behaviour.

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

8.3. Having regard to the nature of our work, it is unlikely that we will ever have to process special personal information, but should it be necessary the guidance of the Information Officer, or his delegate, must be sought.

9. THE PROCESSING OF PERSONAL INFORMATION OF CHILDREN

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

10. INFORMATION OFFICER

10.1. Our Information Officer is designated to be our Chief Executive Officer whose responsibilities include:

10.1.1 Ensuring compliance with POPI.

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

10.1.3 Working with the Information Regulator in relation to investigations.

10.2. Our Information Officer must designate in writing as many Deputy Information Officers as are necessary to perform the tasks mentioned in paragraph 1 above.

10.3. Our Information Officer and our Deputy Information Officers must register themselves with the Information Regulator prior to taking up their duties.

10.4. In carrying out his duties, our Information Officer must ensure that:

10.4.1 our compliance manual is developed, implemented, monitored and maintained;

10.4.2 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.

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

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

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

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

11. CIRCUMSTANCES REQUIRING PRIOR AUTHORISATION

11.1. In the following circumstances, we will require prior authorisation from the Information Regulator before processing any personal information:

11.1.1 In the event that we intend to utilise any unique identifiers of clients (account numbers, file numbers or other numbers or codes allocated to clients for the purposes of identifying them in our business) for any purpose other than the original intention, or to link the information with information held by others;

11.1.2 if we are processing information on criminal behaviour or unlawful or objectionable conduct;

11.1.3 if we are processing information for the purposes of credit reporting;

11.1.4 if we are transferring special personal information or the personal information of children to a third party in a foreign country, that does not provide adequate protection of that personal information.

11.2. The Information Regulator must be notified of our intention to process any personal information as set out above prior to any processing taking place and we may not commence with such processing until the Information Regulator has made a decision in our favour. In the event that the Information Regulator does not make a decision within the stipulated time periods, we can assume that the decision is in our favour and commence processing the information.

12. DIRECT MARKETING

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

12.1.1 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

12.1.2 they did not object then or at any time after receiving any such direct marketing communications from us.

12.2. We may only approach clients using their personal information, if we have obtained their personal information in the context of providing cycling related services to them, and we may then only market cycling related services to them.

12.3. We may only carry out direct marketing (using any form of electronic communication) to other people if we have received their consent to do so.

12.4. 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.

12.5. 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.

12.6. 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. TRANSBORDER INFORMATION FLOWS

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

13.1.1 the client consents to this, or requests it; or

13.1.2 such third party is subject to a law, binding corporate rules or a binding agreement which protects the personal information in a manner similar to POPI, and such third party is

governed by similar rules which prohibit the onward transfer of the personal information to a third party in another country; or

13.1.3 the transfer of the personal information is required for the performance of the contract between us and the client; or

13.1.4 the transfer is necessary for the conclusion or performance of a contractor the benefit of the client entered into between us and the third-party; or

13.1.5 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.