von Lieres, Cooper & Barlow Attorneys
Attorneys, Notaries & Conveyancers

PRIVACY POLICY OF VON LIERES COOPER & BARLOW ("VLCB")

IN TERMS OF THE PROTECTION OF INFORMATION ACT NO.4 OF 2013

("POPIA)

INTRODUCTION:

- VLCB recognises the importance of privacy and is committed to safeguarding the information held by it.

- This policy seeks to give effect to right to privacy in respect of all individuals with whom VLCB may transact, regulate the manner in which personal information is processed and provide those individuals with their rights and remedies to protect their personal information in terms of POPIA.

DEFINITIONS FOR PURPOSES OF THIS POLICY:

- Data Subject: The person to whom personal information relates (client/other individual/party to a transaction).

- FICA: The Financial Intelligence Centre Act No 38 of 2001, as amended.

- Information Officer: The head of VLCB, being a private body.

- LPA: The Legal Practice Act 28 of 2014

- Operator: A person who processes personal information for a Responsible Party in terms of a contract.

- PAIA: Promotion of Access to Information Act 2 of 2000, as amended.

- Personal information: The information relating to an identifiable, living, natural person and where it is applicable, an identifiable, existing juristic person.

- Processing: Any operation or activity concerning personal information including the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use thereof. This also includes dissemination by means of transmission, distribution or making available the information in another form, or merging and linking, as well as restriction, degradation, erasure or destruction of information.

- Responsible Party: A private body which determines the purpose of and means for processing personal information.

- Restriction: to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information.

1. ACCOUNTABILITY:

1.1 As the Responsible Party, VLCB's details are as follows:

Address: 6th Floor
71 Loop Street
Cape Town
8000
Tel: 021 422 1870
Email: reception@vlcb.co.za
Website: www.vlcb.co.za

1.2 VLCB has appointed Nevashni Moodley as its Information Officer and her details are as follows:

Address: 6th Floor
71 Loop Street
Cape Town
8000
Tel: 021 422 1870
Email: nevashni@vlcb.co.za

The information officer has been registered in accordance with POPIA under registration number: 1529/2021-2022/IRRTT

1.3 VLCB has appointed Jesica Barnardo as its Deputy Information officer and her details are as follows:

Address: 6th Floor
71 Loop Street
Cape Town
8000
Tel: 021 422 1870
Email: jesica@vlcb.co.za

1.4 VLCB has appointed Cidac Computers CC as its Operator, and their details are as follows:

Address: 78 Punters Way
Claremont
Cape Town
7708
Tel: 021 683 1667

Email: caryn@cidac.co.za

2. PURPOSE SPECIFICATION:

2.1 As firm offering legal services, VLCB collects various personal information on data subjects in order to comply with various legislative and regulatory requirements as well as to carry out our mandate in terms of which the data subject has instructed us.

2.2 VLCB collects personal information from data subjects for various purposes, including, but not limited to:

- 2.2.1 billing of a data subject including payment information and VAT registration numbers;
- 2.2.2 VLCB'S obligations in terms of FICA;
- 2.2.3 VLCB'S obligations to comply with any other legislative or regulatory obligations
- 2.2.4 in order to give effect to its mandate and carry out instructions efficiently;
- 2.2.5 when permitted by law to do so, and;
- 2.2.6 when any other information is necessary in order to provide a data subject with the best possible service but only for legitimate business purposes.

2.3 The means of collection of personal information from data subjects are the following:

- 2.3.1 from the data subject directly;
- 2.3.2 by visiting our browser or website;
- 2.3.3 by making use of any of our online and social media platforms;
- 2.3.4 when submitting an enquiry to us, contacting us or requesting that we contact a data subject;
- 2.3.5 by submitting an enquiry on our website;
- 2.3.6 by emailing us directly;
- 2.3.7 by contacting us telephonically;
- 2.3.8 by visiting or consulting one of our professionals or employees at our premises or elsewhere, and;
- 2.3.9 by conducting Deeds Office searches through online programs such as Search Works, Windeed and Transunion.

2.4 Retention and restriction of records:

2.4.1 In terms of the LPA and its regulations, a law firm is required to retain information on all its clients for a period of seven (7) years before destroying same. All provisions in this policy are subject to the LPA and its regulations.

2.4.2 Personal information on data subjects will not be retained for longer than required to achieve its purpose, unless:

2.4.2.1 the retention as required by law or any relevant code of conduct;

2.4.2.2 VLCB requires the information for related functions;

2.4.2.3 the information is required in terms of a contract between the parties;

2.4.2.4 consent is obtained where the data subject is a minor, and;

2.4.2.5 for statistical purposes and will not be used for any other purpose.

2.4.3 VLCB shall destroy and/or delete records of personal information if it no longer has the authority by the data subject to retain it. VLCB undertakes to destroy or delete the personal information in such a way as to prevent reconstruction thereof.

2.4.4 VLCB will restrict the processing of personal information if:

2.4.4.1 the accuracy thereof is contested by the data subject, and until VLCB can verify the personal information;

2.4.4.2 VLCB no longer needs the personal information for the purpose for which it was collected, but is needed or maintained for proof;

2.4.4.3 the processing of the personal information is unlawful and the data subject objects to deletion or destruction, but requests that the personal information be restricted instead, and;

2.4.4.4 the data subject requests that the personal information be transmitted to another automated processing system.

2.4.5 The processing of personal information that has been restricted, can only be processed for purposes of proof with consent from the data subject, or offers protection to another individual or public interest.

2.4.6 Where the processing of personal information has been restricted, VLCB will inform the data subject before lifting any such restriction.

3. <u>PROCESSING LIMITATION:</u>

3.1 VLCB undertakes to only process personal information if it is done so lawfully and in a reasonable manner that does not infringe on the privacy of the data subject, and that is not excessive for the purposes of which it is obtained.

3.2 <u>Consent, justification and objection:</u>

3.2.1 Personal information will only be processed if:

3.2.1.1 consent has been obtained;

3.2.1.2 it is necessary to carry out functions to conclude or perform actions in terms of a contract to which the data subject is party to;

3.2.1.3 it is necessary to carry out the mandate in terms of which the data subject and/or third party has instructed VLCB;

3.2.1.4 it is imposed by law;

3.2.1.5 it protects the legitimate interest of the data subject;

3.2.1.6 it is necessary for the performance of a duty by a public body, or;

3.2.1.7 it is in the pursuit of a legitimate interest of VLCB/third party to whom the information is supplied.

3.2.2 The data subject can withdraw consent at any time provided the above-mentioned circumstances are not present (3.2.1.2 – 3.2.1.6).

3.2.3 VLCB shall bear the burden of proof for consent.

3.2.4 A data subject is entitled to object to processing personal information if:

3.2.4.1 reasonable grounds exist, unless legislation provides for processing, or;

3.2.4.2 there has been direct marketing.

3.2.5 Once a data subject has objected to the processing of personal information, VLCB will no longer process that personal information, subject to legislative and other lawful requirements.

3.3 Collection of information:

3.3.1 All personal information will be collected directly from the data subject unless:

3.3.1.1 it is public record or made public;

3.3.1.2 the data subject consented to the personal information being obtained from another source. The collection from another source may not prejudice the legitimate interest of the data subject;

3.3.1.2.1 The collection of personal information from another source will be necessary:

3.3.1.2.1.1 to avoid prejudice to the maintenance of law and that prevents the execution and prosecution of offences;

3.3.1.2.1.2 is imposed by law in respect of any SARS legislation/regulations;

3.3.1.2.1.3 if the proceedings are before a court or tribunal;

3.3.1.2.1.4 if it is a matter of national security, and;

3.3.1.2.1.5 to maintain the legitimate interest of VLCB/third party to whom the information has been supplied.

3.3.1.3 compliance thereof will prejudice a lawful purpose, and;

3.3.1.4 compliance thereof will not be practical in this case.

4. FURTHER PROCESSING LIMITATION:

4.1 The further processing of personal information will always be in accordance with the purpose for which it was collected.

4.2 To determine whether further processing is compatible with the original purpose, VLCB will take into account:

4.2.1 the relationship between further processing and the original collection;

4.2.2 the nature of the personal information;

4.2.3 the consequences of intended further processing;

4.2.4 the manner in which the personal information was collected, and;

4.2.5 the contractual rights/obligations between the parties.

4.3 The processing of further information will be allowed if:

4.3.1 the consent is obtained for further processing;

4.3.2 is available on public record;

4.3.3 is necessary:

4.3.3.1 to avoid prejudice and maintenance of the law, and to prevent, prosecute and execute an offence,

4.3.3.2 to comply with obligations imposed by SARS, or;

4.3.3.3 in the interest of national security.

4.3.4 to mitigate public health and safety, or;

4.3.5 for historical, statistical/research purposes and VLCB ensures that it is carried out solely for that purpose and in an unidentifiable form.

5. INFORMATION QUALITY

5.1 VLCB will take reasonable steps to ensure:

5.1.1 the personal information collected is complete;

5.1.2 the personal information is accurate;

5.1.3 the personal information is not misleading, and;

5.1.4 the personal information is updated if and when necessary.

5.2 VLCB will always take into account the purpose for the collection/further processing of personal information.

5.3 VLCB will verify information collected against documentation requested from data subjects and from third parties such as Searchworks, WinDeed and/or Transunion.

5.4 VLCB will give data subjects an opportunity to verify the personal information collected should the personal information change at any stage whilst VLCB is in possession of it.

5.5 VLCB will update the personal information when it becomes aware of any changes.

6. OPENNESS:

6.1 When collecting personal information VLCB will ensure that the data subject is aware of the following:

6.1.1 the information being collected and where it is collected from;

6.1.2 the name and address of VLCB;

6.1.3 the purpose for which it is collected;

6.1.4 whether the supply of information by the data subject is voluntary or mandatory;

6.1.5 the consequences of failure to provide the information;

6.1.6 any law or authority that requires the information to be collected;

6.1.7 if the information is to be transferred to third party party/international organisation and the level of protection offered by that third party/international organisation;

6.1.8 further information:

6.1.8.1 who is the recipient of the information/category of recipients;

6.1.8.2 what is the nature and category of the information;

6.1.9 the existence of the right to access and right to rectify the information collected;

6.1.10 the right to object to the processing of personal information if:

6.1.10.1.1 it is not required by legislation

6.1.10.1.2 is collected as a result of direct marketing;

6.1.11 the right to lodge a complaint with the Information Regulator and the contact details of the information regulator.

6.2 <u>VLCB will ensure that it complies with the above-mentioned requirements if:</u>

6.2.1 the personal information is collected directly from the data subject and is prior to the information being collected.

6.2.2 in any other case, prior to the information being collected, or as soon as reasonably possible thereafter.

6.3 <u>VLCB does not need to comply with clause 6.1 above if:</u>

6.3.1 the data subject or competent person acting for a child has consented to non-compliance;

6.3.2 non-compliance would not prejudice the data subject in terms of POPIA;

6.3.3 non-compliance is necessary:

6.3.3.1 to avoid prejudice and maintain the law, including to prevent/detect/investigate/prosecute/execute an offence;

6.3.3.2 to comply with obligations imposed by law or SARS;

6.3.3.3 for the conduct of proceedings in any court/tribunal, or;

6.3.3.4 in the interest of national security

6.3.4 compliance will prejudice a lawful purpose of the collection of personal information;

6.3.5 compliance is not reasonably practical in the circumstances, or;

6.3.6 the information will:

6.3.6.1 not be used in a form in which the data subject may be identifiable, and/or;

6.3.6.2 be used for historical, statistical and/or research purposes.

7. <u>SECURITY SAFEGUARDS:</u>

7.1 <u>VLCB undertakes to ensure the integrity and confidentiality of personal information in its possession/under its control by taking appropriate, reasonable, technological and organisational measures to prevent:</u>

7.1.1 the loss of, damage to and/or unauthorised destruction of personal information, and;

7.1.2 the unlawful access to and/or processing of personal information

7.2 <u>VLCB has taken and will regularly take reasonable measures to:</u>

7.2.1 identify all reasonable foreseeable internal and external risks to the personal information collected;

7.2.2 establish and maintain appropriate safeguards against risk identified;

7.2.3 regularly verify safeguards and ensure that they are effectively implemented, and;

7.2.4 ensure safeguards are continually updated in response to new risks and/or deficiencies in previously implemented safeguards.

7.3 VLCB will give due regard to the generally accepted information security practices in the legal industry.

7.4 <u>All VLCB staff and employers shall ensure the following:</u>

7.4.1 no USB's are to be utilised on company owned computer equipment unless authorisation from a partner has been obtained;

7.4.2 no personal information regarding data subjects will be stored on the desktop of staff or employer computers and/or laptops;

7.4.3 all staff and employers shall maintain and/or change their passwords regularly in order to ensure that their computers/laptops cannot bear accessed by unauthorised persons;

7.4.4 when working remotely, they will only do so through the secure VPN program loaded by the operator onto all laptops;

7.4.5 all personal information and data subjects will be saved onto Ghost Practice or the server which is protected by a high level hardware firewall with an antivirus program in Lock mode; and

7.4.6 all email communication with data subjects are stored on the cloud through Office 365.

7.5 Information processed by an operator:

7.5.1 VLCB's operator will:

7.5.1.1 process information only with the knowledge and authorisation of VLCB, and;

7.5.1.2 treat the information with confidentiality and not disclose the personal information unless required by law and/or in the process of carrying out duties.

7.6 Security measures regarding information processed by operator:

7.6.1 VLCB has an agreement in terms of which the operator establishes and maintains the security measures referred to in 7.1, 7.2 and 7.3 above.

7.6.2 The operator shall notify VLCB immediately where there are reasonable grounds to believe that personal information of a data subject has been accessed and/or acquired by an unauthorised person.

7.7 Notification of security compromises:

7.7.1 Where there are reasonable grounds to believe that personal information has been accessed/acquired by an unauthorised person, VLCB will:

7.7.1.1 notify the information regulator, and;

7.7.1.2 notify the data subject, unless notification will impede a criminal investigation by a public body.

7.7.2 VLCB will notify the information regulator and data subject as soon as possible, taking into account the need to establish the data subject, scope of the compromise, law enforcement and restoring the integrity of the system.

7.7.3 VLCB will notify the data subject in the following ways:

7.7.3.1 by mailing the data subject at his/her last known physical/postal address;

7.7.3.2 by emailing the data subject at his/her last known email address;

7.7.3.3 by placing the notice in a prominent position on VLCB's website;

7.7.3.4 by publishing the notice in news media, and/or;

7.7.3.5 as directed by the information regulator.

7.7.4 The notice will provide sufficient information in order for the data subject to take protective steps against potential consequences, including:

7.7.4.1 the description of the possible consequence of the security compromise;

7.7.4.2 description of the measures that VLCB intends to take and/or has taken to address the compromise;

7.7.4.3 a recommendation with regards to measures to be taken by the data subject to mitigate possible adverse effects of the compromise, and;

7.7.4.4 if known by VLCB, the identity of the unauthorised person who accessed/acquired the personal information.

7.8 Measures and Standards of security adopted by VLCB:

7.8.1 VLCB is a small firm with approximately 15 staff members at any given time. The measures put in place to protect personal information and data subjects are appropriate to the size of the firm, the type of business offered and the information processed by it.

7.8.2 Server- the server is protected by a high level antivirus and hardware firewall.

7.8.3 Emails- only emails are operated through the cloud via Office 365. Emails are password protected. There is an administration portal which requires two phase access prior to granted access to office 365.

7.8.4 GhostPractice- this is VLCB'S accounting and file management system. One cannot be granted access to GhostPractice unless they are an active user utilising a VLCB machine. Furthermore, one must be logged into the server before being granted access to GhostPractice. The server protection as mentioned in clause 7.8.1 above will also be effective in this instance.

7.8.5 Third-party programs utilised by VLCB such as WebConvey, LexisNexis and E4 have their own security measures and protection policies in place. If a staff member logs onto these third-party programs, it utilises their server and VLCB does not put its cyber security infrastructure at risk.

7.8.6 VLCB has put in place all possible measures to protect personal information and data subjects as mentioned in paragraphs 7.8.2 to 7.8.4 above. It is therefore unlikely that an external breach can take place, however, this can never be ruled out.

7.8.7 VLCB has put in place measures to immediately be aware of attempted breach into its server. Should any attempted breach occur, the firewall shall go into lockdown mode. As soon as this occurs, VLCB's operator will be notified.

7.8.8 In respect of remote access, secure VPN programs have been installed on all laptops which are password protected.

7.8.9 In respect of internal risks, it is staff policy not to allow any USB's to be used on VLCB computer equipment unless authorised by a partner; no client information is to be stored on a desktop; all staff and employers shall maintain and/or change their passwords regularly in order to ensure that their computers/laptops cannot bear accessed by unauthorised persons; when working remotely, they will only do so through the secure VPN program loaded by the operator onto all laptops; all personal information and data subjects will be saved onto Ghost Practice or the server which is protected by a high level hardware firewall with an antivirus program in Lock mode; andall email communication with data subjects are stored on the cloud through Office 365.

7.8.10 All authorised emails generated through VLCB's IP address goes through Clickit, which will present with VLCB's banners and signature. If there is an unauthorised email, it will not have the banners and signature.

7.8.11 VLCB furthermore utilises Sendmarc, a program that blocks spam emails and email addresses that use a different IP address to the email address itself.

7.8.12 When a new employee is employed by VLCB, he/she will be provided with passwords from the Operator. The employee will not be authorised to change these passwords unless prior consent has been obtained from a Partner of the firm. Upon termination of the employee's employment, all passwords and computer equipment will be handed back to the Operator and the Operator will be responsible for resetting all passwords and computer settings.

7.8.13 In respect of devices such as cellular phones, the phones need to be password protected in order to have access to emails.

7.8.14 In those circumstances where VLCB has been instructed to destroy personal information on a data subject, such information will be wiped from the system in terms of the NIST800-88 wiping standard. This will ensure that information cannot be reconstructed.

7.8.15 Data is encrypted in both WAN and LAN environments.

7.8.16 All backups conducted are encrypted.

7.8.17 VLCB'S Wi-Fi is protected and have prevention technologies in place. There is a Guest mode established which limits the risk of access to the server by unauthorised individuals.

7.8.18 An internal audit will be conducted together with the Operator annually to assess internal and external risks, adopt this policy and security programs, and maintain the standards stipulated in this policy.

8. DATA SUBJECT PARTICIPATION:

8.1 Access to personal information:

8.1.1 A data subject has the right to:

8.1.1.1 request that VLCB confirm, free of charge, whether it holds any personal information on the data subject, and/or;

8.1.1.2 request from VLCB the record and/or description of the personal information on the data subject that is held, including details of all third parties who may have had access to the information:

8.1.1.2.1 within a reasonable time;

8.1.1.2.2 at a prescribed fee, if any;

8.1.1.2.3 in a reasonable manner and format, and;

8.1.1.2.4 in a form that is generally acceptable.

8.1.2 In response to the request, a data subject will be made aware that he/she has a right to correct the personal information stored.

8.1.3 If the data subject is required to pay a fee, VLCB undertakes to give the data subject a cost estimate prior to providing the service, and may require a deposit.

8.1.4 VLCB must refuse to disclose any information to the data subject if Chapter 4 PAIA applies (if the grounds for refusal of a public body to disclose personal information exists then VLCB must also refuse to disclose the information).

8.1.5 If only part of the personal information on the data subject falls within paragraph 8.1.4 above, then the remaining information must be disclosed to the data subject.

8.2 <u>Correction of information:</u>

8.2.1 A data subject may request VLCB to:

8.2.1.1 correct and/or delete personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading and/or obtained unlawfully.

8.2.1.2 destroy and/or delete personal information that VLCB is no longer authorised to retain, subject to the provisions of the LPA and its regulations.

8.2.2 On request by the data subject, VLCB must, as soon as reasonably possible:

8.2.2.1 Correct the personal information;

8.2.2.2 destroy and/or delete the personal information, subject to the LPA and its regulations;

8.2.2.3 provide the data subject, to his or her satisfaction, credible evidence in support of the personal information, or;

8.2.2.4 where VLCB and the data subject cannot agree, attach to the information a comment that a request has been made by the data subject, but that such a request has not been granted.

8.2.3 If VLCB has taken steps in respect of paragraph 8.2.2 above, and any such information has been previously disclosed to third parties, VLCB will report, as soon as possible, the changes in personal information to those parties.

9. PROCESSING OF SPECIAL PERSONAL INFORMATION:

9.1 VLCB will not process special personal information concerning:

9.1.1 Religion, philosophical beliefs, race, ethnic origin, trade union membership, political persuasion, health, sex life and/or biometric information of a data subject, and;

9.1.2 criminal behaviour of the data subject to the extent that such information:

9.1.2.1 relates to an alleged commission of an offence, and/or;

9.1.2.2 a proceeding in respect of any alleged offence or disposal thereof.

Unless the processing of the special personal information is necessary to carry out its mandate.

9.2 The prohibition mentioned in paragraph 9.1 above shall not apply if:

9.2.1 the processing of special personal information is carried out with the consent of the data subject;

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

9.2.3 it is necessary to comply with an obligation of international public law;

9.2.4 it is used for historical, statistical and/or research purposes to the extent:

9.2.4.1 that its purpose serves a public interest, and/or;

9.2.4.2 it is impossible or disproportionate to ask for consent,

and there are sufficient safeguards in place to ensure there is no adverse effect on the privacy of the data subject.

9.2.5 the data subject has deliberately made information public.

9.3 The Information Regulator may authorise VLCB to process special personal information if it is in the public interest and there are appropriate safeguards in place.

10. <u>CONSENT BY DATA SUBJECTS:</u>

10.1 VLCB has developed a consent in compliance with the provisions of POPIA which shall be provided to each and every data subject VLCB transacts with.

10.2 The consent, as far as reasonably possible, must be signed and dated by the data subject prior to any information being collected.

11. <u>REVIEW OF POPIA POLICY:</u>

11.1 VLCB shall review the provisions of this policy annually in conjunction with the Information Officer, Deputy Information Officer and Operator.

11.2 In addition to the above, should VLCB become aware of any internal and/or external risks, it will immediately take steps to mitigate that risk and amend this policy accordingly, if needs be.

12. <u>TRAINING:</u>

12.1 Training of all staff and employers on this policy and the provisions of POPIA shall be concluded within three months of implementation of this policy by VLCB.

12.2 Each employee shall sign a declaration confirming that they have familiarise themselves with the provisions of this policy and POPIA.

_____

N MOODLEY
INFORMATION OFFICER
22 JUNE 2021