

THE BASSON BLACKBURN GROUP'S PRIVACY POLICY

IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013

1. OBJECTIVE

1.1. Basson Blackburn Inc., Blackburn Inc., Blackburn Fiduciary Services Pty Ltd and 109 on Main Pty Ltd ("the Basson Blackburn Group" or "the group") are committed to collecting, storing and processing the personal information of our clients in a manner compliant with the Protection of Personal Information Act 4 of 2013 ("POPIA") and the Promotion of Access to Information Act 2 of 2000 ("PAIA").

1.2. Insofar as it is required in terms of POPIA, we will always obtain the written consent of our clients before processing your personal information in any way.

2. DEFINITIONS

2.1. **"Personal Information"**: Information relating to an identifiable, living, natural person and where it is applicable, an identifiable, existing juristic person;

2.2. **"Data Subject"**: The person to whom personal information relates;

2.3. **"Responsible Party"**: For purposes of this Policy, the Responsible Party is the Basson Blackburn Group.

2.4. **"Consent"**: "Voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information."

2.5. **"Processing"**: "Any operation or activity or any set of operations, whether or not by automatic means, concerning personal information."

2.6. **"Record"**: "Any recorded information, regardless of form or medium, in the possession or under the control of a responsible party, whether or not it was created by a responsible party and regardless of when it came into existence."

2.7. **"Regulator"**: "Information Regulator established in terms of Section 39."

- 2.8. **“Special Personal Information”**: Personal information of a data subject relating to their religious or philosophical beliefs; race or ethnic origin; trade union membership; political persuasion; health or sex life; biometric information and criminal behavior (to an extent).

3. GENERAL

- 3.1. The Basson Blackburn Group and its employees undertake to treat client and employee information as strictly confidential.
- 3.2. No personal information regarding a client (or employee) may at any time or by any means be divulged to an unauthorised outsider by an employee.
- 3.3. No employee may request, gather or store any personal information from or regarding a client, unless this is done for business purposes and takes place with the knowledge and consent of the client concerned. The information collected and processed is only used for the specified purpose for which it was intended, as set out at the time of procurement.
- 3.4. We undertake to provide access upon request, to our clients and employees, to their own records, in terms of the provisions of POPIA and PAIA, and where sufficient proof of identity has been shown upon such request.
- 3.5. Where a client wishes to correct/update their records, we request proof of the corrected/updated information before rectifying our documents to reflect the change. Proper record is also kept of the client’s request to amend the details of their record held by us, including the date of the request for the change as well as the change itself.
- 3.6. Where necessary, relevant and in the interest of properly carrying out our instructions and / or mandate, third parties are notified of changes to the details of a client.
- 3.7. There is no fee charged in relation to the request of a data subject for confirmation of whether we hold your personal information.
- 3.8. Where a data subject requests a record or description of the personal information we hold, as well as that information to which third parties have access, we will attend to such a request “within a reasonable time; at a prescribed fee (if any); in a reasonable manner and format; and in a form that is generally understandable.”

4. INFORMATION OFFICER

4.1. The details of our Information Officers and Deputy Information Officer are as follows:

4.1.1. Information Officer: Caryn Rutgers

caryn@bassonblackburn.com

021 871 1401

4.1.2. For 109 on Main Pty Ltd: Magda Nöthnagel

magda@bassonblackburn.com

021 871 1401

4.1.3. Deputy Information Officer: Ginelle van Niekerk

ginelle@bassonblackburn.com

021 871 1401

4.2. For any queries, requests or complaints related to the processing of personal information, please contact our Information Officer/s or Deputy Information Officer.

5. INCIDENT MANAGEMENT PROCESS

5.1. The processing of data, particularly by electronic means, is always accompanied by an inherent amount of risk. Although we do everything in our power to safeguard the integrity of the personal information entrusted to us, security breaches are still a possibility.

5.2. Where we have become aware of a data security breach / have reasonable grounds to believe that there has been a data security breach, this will be reported to the Information Regulator (where necessary), as well as the data subject concerned, as soon as reasonably possible after becoming aware of the compromise / possible compromise, and we will provide enough information to allow the data subject to take action against any potential consequences.

6. RESEARCH REGARDING EMPLOYMENT APPLICATIONS

- 6.1. All employment applicants / prospective employees of the Basson Blackburn Group are required to furnish certain details, within the ambit of the definition of “personal information,” necessary for the consideration of their employment applications, including but not limited to, details of previous employment / work experience, identity numbers and contact details, etc. for the purposes of background and reference checks.
- 6.2. Applicants / prospective employees confirm that the details of any and all references provided to us are so furnished with the express consent of the named person.

7. COOKIES

- 7.1. The Basson Blackburn Group’s website may use cookies and similar technologies to improve the functionality and user experience of the website, as well as to obtain information regarding how visitors use the website.
- 7.2. Cookies are small text files which may be stored on a visitor’s device when visiting the website. Certain cookies may be necessary for the website to function properly, while others may be used for analytical or other purposes.
- 7.3. By using our website, visitors acknowledge that cookies may be used in accordance with this policy. Where required, visitors will be given the opportunity to manage or disable non-essential cookies through the website.

8. INFORMATION SUBMITTED THROUGH THE WEBSITE

- 8.1. Where a visitor to the Basson Blackburn Group’s website voluntarily submits personal information to us, including through a contact form, enquiry form, employment application or other online facility, such information will be treated as confidential and processed in accordance with this policy and applicable legislation.
- 8.2. Personal information submitted through the website will only be collected and processed for the purpose for which it was provided, or for a related purpose that is permitted in terms of POPIA.
- 8.3. Visitors are requested not to submit personal information through the website which is not necessary for the purpose of their enquiry or submission.

- 8.4. Where personal information is submitted through the website for the purposes of an enquiry or potential instruction, the information may be used to respond to the enquiry, communicate with the person concerned and, where applicable, assess and administer the potential instruction.
- 8.5. Where personal information is submitted in connection with an employment application, the provisions of clause 6 of this policy will apply.

9. EMAIL DISCLAIMER

- 9.1. The information contained in the emails sent by an authorised person from the Basson Blackburn Group and/or attachments is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon email correspondence by persons or entities other than the intended recipient is prohibited. If you receive correspondence from us in error, please contact the sender and delete the material from any system and destroy all copies, without any further processing of the information as received. As internet communication cannot be guaranteed to be secure, error and virus free, neither the sender nor receiver will accept any liability for loss or damage sustained as a result of e-mail transmission.

9.2 SPOOFING, WHALING AND PHISHING ALERT

Should you receive an email from us stating that our banking details have changed, please do not act on such notification. We have not changed our banking details. We ask you to be extremely diligent about checking that all information is 100% correct and confirm that the sending email address is correct and from a legitimate person from the Basson Blackburn Group with the @bassonblackburn.com / @blackburninc.co.za / @bbfiduciary.co.za domain. If you are unsure about the banking details you have been provided with, please verify this telephonically with us before making payment.

10. RETENTION OF PERSONAL INFORMATION

- 10.1. The Basson Blackburn Group will retain personal information and records for the periods required by applicable legislation and the rules and requirements of the Legal Practice Council (“LPC”).
- 10.2. In particular, all documents and data relating to the group’s legal matters will be retained for a period of **at least seven years** from date of finalisation of the matter / termination of the mandate, or for such longer period as may be required by applicable legislation, the LPC or the circumstances of the relevant matter.
- 10.3. Personal information will not be retained for longer than is necessary for the purpose for which it was collected, unless a longer retention period is required or permitted by law.

- 10.4. Once the applicable retention period has expired, personal information and records will be securely destroyed or deleted, where appropriate, in accordance with the group's document destruction and data security procedures.

11. EMPLOYEE COGNISANCE OF POLICY & LEGISLATION

- 11.1. Employees of the Basson Blackburn Group, as part of their conditions of employment, receive regular, necessary training centered on dealing with the personal information of our clients in line with the provisions of POPIA.
- 11.2. Each employee, therefore, is aware of the requirements for lawful processing of personal information and has undertaken to treat all client information as strictly confidential, both during and after their employment period.
- 11.3. Our Information Officer is responsible for updating and informing the employees of any relevant new regulations pertaining to POPIA and ensuring that they carry out their duties in line therewith.

12. DOCUMENTS CONTAINING PERSONAL INFORMATION

12.1. COMPUTERS

- 12.1.1. Only authorised employees (attorneys and support staff) have passwords and access to the group's computers, main frame and printers.
- 12.1.2. By virtue of our internal privacy policy, these passwords are not shared with other computer users or divulged to any other person, except the authorised head of division.
- 12.1.3. Passwords and all other forms of access to the group's main frame and information contained therein are immediately removed by the group's IT agents upon an employee's termination of service.

12.2. PRINTERS

- 12.2.1. Documents that are printed in hard copy are immediately removed from the printers and filed in the appropriate file.

12.3. REMOVAL OF DOCUMENTS FROM OFFICE

12.3.1. No files and/or documents containing the personal information of any client or employee may leave the premises without the prior approval of the head of department.

12.3.2. Such approval is only granted where the documents are removed exclusively for work purposes and the head of department is satisfied that the file/document will not fall into the hands of unauthorised persons.

12.3.3. Clauses 12.3.1 and 12.3.2 above also apply to electronic documents and correspondence. No document / information is removed from the office by means of a transportable hard drive or other storage device (e.g. USB stick) without the prior authorization and/or knowledge of the head of department.

12.3.4. Any document that leaves the office building is placed in a sealed envelope with the complete details of the addressee, as well as a return address in the case of non-delivery. These documents are taken to the post office by hand, or by hand to the address of the addressee by an authorised employee of the group.

12.3.5. Where the documents are transported by car, the documents are kept in the boot, which is locked; otherwise appropriately out of sight.

12.3.6. Where documents are sent by courier, the services of a reliable/reputable courier company are utilised and the documents are handed to the courier service in a sealed envelope.

12.3.7. Any document containing personal information of a client / employee is only handed to a person who is not in service of the group where such a person has received a direct instruction to handle the document (e.g. correspondent / sheriff / clerk of the court) or to the person whose information is contained in the document.

12.3.8. Where a client / employee requests that the document be handed to a third party not employed by the group (e.g. a proxy / messenger), a note this effect is made on the relevant file.

12.4. REMOTE COMPUTERS

12.4.1. Where employees are, for any reason, required to work from home / a location that is not the office of one of our branches, remote access is granted to such employees (attorneys and support staff), with the requisite security safeguards (passwords, anti-virus, firewall, etc.) in place to ensure that no unauthorised person gains access to the group's main frame.

12.4.2. Employees are required to obtain prior authorisation from their head of department before removing his/her computer, or any component thereof, from the building/s.

13. RESTRICTION OF ACCESS TO OFFICES

13.1. All documents containing personal information, including all documents created and stored in electronic format, are kept within the premises of our offices, either at Paarl or Durbanville.

13.2. All existing deeds files are kept in a locked safe and all other files are kept in the respective division's filing cabinets.

13.3. Documents in closed files are kept in the archives / storeroom, which is kept locked. The key is kept in a safe place and is only handed to authorised persons.

13.4. When closed files are destroyed after expiry of the prescribed period, the Information Officer ensures that the documents are properly destroyed.

14. ACCESS TO MAIN BUILDINGS (at 109 MAIN ROAD, PAARL & 12 SAN DOMENICO, 10 CHURCH STREET, DURBANVILLE)

14.1. Both the front door and the security gate of both offices are locked when necessary and especially when there is no receptionist to cover and screen incoming visitors to the building. The receptionists only grants access to authorised persons.

14.2. Documents containing personal information are not kept in the foyer, unless necessary and, even then, inside a sealed envelope.

14.3. Non-employees of/visitors to the group are not permitted to leave the foyer area of the office to enter the rest of the building, unless accompanied by an employee of the group, to ensure that the visitor does not gain access to any documents and/or information which does not apply to him/her.

14.4. Outside office hours, the buildings are kept locked at all times and the alarm activated by the last employee to leave the premises.

15. DESTRUCTION OF DOCUMENTS

- 15.1. Any paper on which personal information is printed, which is disposed of during the course of the work day but is not kept in the client file in the usual manner and eventually destroyed, is placed in separate containers from other waste materials.
- 15.2. The filing clerk in each department collects such papers daily to ensure that it is shredded before it may be removed, along with the rest of the day's waste, and destroyed.

16. RISK ANALYSIS

- 16.1. The Information Officer attends, on an annual basis, to an update on the group's risk analysis report and data security safeguards, including the relevant measures pertaining to the group's physical, digital, operational and administrative security.
- 16.2. Where necessary, the relevant aspects of the group's security are updated to ensure that the strongest possible security measures are in place.

17. SUB-CONTRACTORS

- 17.1. There are a number of instances where the group, with the prior consent of the client, must make use of a sub-contractor, for example, where bond documents must be signed in front of a non-employee of the group.
- 17.2. Before the relevant documents are sent to the sub-contractor, electronically or in hard copy, the employee ensures that:
 - 17.2.1. In the case of deeds/conveyancing matters: that the document/s only be sent to the client, or a practicing attorney who is on the panel of the bank concerned. Further, that the document is sent as near as possible to the residential or business address of the client, after the attorney has been contacted telephonically and enquiries made about their willingness to act as correspondent, their fee structure and an agreement from them that they will handle / process the documents and information in accordance with our privacy policy has been obtained; and
 - 17.2.2. In the case of all other matters, including court process and documents: that these documents only be sent to the client, an officer of the court or a practicing attorney after the attorney has been contacted telephonically and enquiries made about their willingness to act as correspondent, their fee structure and

an agreement from them that they will handle the documents and information in accordance with our privacy policy has been obtained.

- 17.3. Other sub-contractors are requested to undertake, in writing, to comply with our privacy and POPIA policies, and to sign a confidentiality agreement with the relevant entity within the group.
- 17.4. Where a sub-contractor handles client information in a manner contrary to the provisions of our privacy and POPIA policies, or there are reasonable grounds to believe that a sub-contractor has handled client information in a manner contrary to the provisions of our privacy and POPIA policies, this will be reported to the data subject concerned, as well as to the Information Regulator, by our Information Officer.

18. BACK-UP SUPPORT

- 18.1. All information stored on the main frame is automatically backed up on a daily basis;
- 18.2. The back-up hardware is kept in the group's vault and is tested monthly by our IT agent to ensure that the information is properly stored; and
- 18.3. A further copy is kept at the offices of the group's IT agent, in a locked cupboard (these copies are taken to the IT agent's office by the IT agent him-/herself, or where necessary, by an employee of the group).



CARYN RUTGERS

Compliance & Information Officer

Dated: SEPTEMBER 2026