POLICY STATEMENT AND MANUAL OF:

PROTECTION OF PERSONAL INFORMATION AND THE RETENTION OF DOCUMENTS FOR

Giflo Holdings (Pty) Ltd

and all its subsidiaries (“the company”)

(Registration number: 1971/006528/07)

Updated: June 2021

1. Introduction

Giflo Holdings (Pty) Ltd and its subsidiaries (hereafter referred to as "Giflo") focuses on developing commercial and medical property. Businesses needing office space to rent can engage with the company about their specific requirements, securing their property goals in partnership with Giflo. Giflo's relationships with tenants are valuable attributes. Continuous interaction, constant availability and uncompromising service excellence differentiates our company.

Giflo is obligated to comply with *The Protection of Personal Information Act (4 of 2013)*. The POPIA requires the company to inform its tenants (first line customers), staff, suppliers (of services) and visitors as to the manner in which their personal information is collected, rationale or purpose, used, disclosed, stored and destroyed. The company guarantees its commitment to protecting its individual's privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

The Privacy Policy is made available on the company's website www.giflogroup.co.za and by request from the company's head office.

2. Collection and use of personal data

2.1 We will only collect, use or disclose your personal data with your consent, where the company's legitimate interest applies, or as authorized by applicable national and/or local laws and regulations. The personal data collected may include:

- Full Name
- Gender
- Date of Birth
- Passport #
- Home Address / Delivery Address
- Email Address
- Contact Telephone/ Cell or Mobile #
- National ID #
- Banking Details
- Children's names
- Firearm licences
- Vehicle details
- FAIC details
- CIPC details
- Tenant financial data
- Biometric data (fingerprints and facial recognition)

2.2 By signing an agreement with us (whether tenant, supplier or staff), you consent to our collection, use and disclosure of your personal data for any or all purposes specified below:

- Administer your contract with us,
- Provide the services required from us (and for all other matters relating to such contract),
- Verify and carry out financial transactions in relation to payments made from us,
- Managing, investigating or responding on feedback, requests, claims or complaints provided or made by you,
- Audit the provision of data from our systems,
- Improve or customize the functionality of our systems,
- Identify visitors to our premises, and
- Identify visitors to our website.

2.3 We collect personal data directly from you (or from your authorized representatives) in the following ways:

- When you complete the Contract and associated Credit Profile detail,
- When you apply (and are appointed) for any position as advertised,
- When you perform and supply any suppliers' services or products as requested by a RFQ and RFP, and
- When you interact with any of our social media platforms to give a feedback or submit an inquiry.

2.4 With your consent, we may collect, use and disclose your personal data for any or all the purposes specified below:

- Administer the appropriate service contract,
- Investigate or respond to a query or feedback submitted via the electronic or online contact form,
- Comply with any relevant national and/or local law or regulation,
- Conduct market surveys, research or data mining to enable us to understand client preferences and demographics to develop marketing programmes in relation to our services, and
- Inform you of updates to the website.

Your consent will always be obtained through a written agreement or by administering the 'opt-in' and 'opt-out' function associated with the request.

2.5 Your personal data will be retained by us and will be accessible to our staff and 3rd parties engaged by us for any of the purposes stated in this Privacy Policy. You authorize us to (a) disclose all or any of your personal data to such 3rd parties, and (b) collect your personal data from any other sources available to us (including credit referral agencies and commercial banks).

2.6 Insufficient or incorrect personal data provided to us by you may result in delays or failure in providing the services requested by you.

3. Confidentiality of personal data

3.1 Personal data provided to us by tenants, staff, suppliers or visitors will be kept confidential and will only be disclosed for the purposes stated in this Privacy Policy. We may disclose personal data to 3rd parties who perform certain tasks relating to the provision of our services to our tenants, staff, suppliers and visitors. All such 3rd parties are required by us to use the personal data strictly to provide the services and are required to maintain the confidentiality of the personal data.

3.2 Any questions, comments, suggestions, or information (other than personal data) submitted or posted by tenants, staff, suppliers or visitors will be deemed voluntarily provided to us on a non-confidential and non-proprietary basis. We may use, reproduce, disclose, or transmit such information in connection with the development, auditing, and marketing of services, to meet the needs of our tenants, staff, suppliers or visitors or for any other purpose.

3.3 We will only disclose your personal data without notice to you if required to do so by law, or in the good faith belief that such disclosure is necessary to:

- Comply with legal process, or under compulsion of an order of court or governmental agency,
- Protect our rights, property or safety, its tenants, staff, suppliers and visitors or others.

3.4 This Privacy Policy applies only to personal data collected via contracting. We are not responsible for the privacy practices or policies of other contracts (e.g. services provided to tenants by outside contractors).

4. Information collected by cookies

Our Website and Services use “cookies” to help personalize your online experience. A cookie is a text file that is placed on your hard disk by a web page server. Cookies cannot be used to run programmes or deliver viruses to your computer. Cookies are uniquely assigned to you and can only be read by a web server in the domain that issued the cookie to you.

We may use cookies to collect, store and track information for statistical purposes to operate the Website and Services. You have the ability to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. If you choose to decline cookies, you may not be able to fully experience the features of the Website and Services.

5. Collection of computer data

5.1 When you interact electronically with the company or visit our website, our company servers automatically records information that your browser sends. This information may include:

- Your computer's IP address
- Browser type
- Websites visited before our website
- Pages visited within our website (including time spent on those pages)
- Other items and information searched for on our website, access times and dates etc.

5.2 This information is collected for security, auditing, analysis and evaluation to help us improve our systems and the services we provide. *This information will not be used in association with any personal data.*

6. Disclosure of Information

The company may disclose a tenant's, supplier's or staff's personal information to any associate company and/or approved product- or 3rd party service providers whose services tenants and staff elect to use. The company has agreements in place to ensure that compliance with confidentiality and privacy conditions. The company may also share tenant's, supplier's and staff's personal information with and obtain information about tenants, suppliers and staff from 3rd parties for the reasons already discussed above. The company may also disclose a tenant's, supplier's or staff's information where it has a duty or a right to disclose in terms of applicable legislation, the law, or where it may be deemed necessary to protect the company's rights.

7. Access request; Withdrawal of consent; Updating of personal data

7.1 All tenant, supplier and staff information must be dealt with in the strictest confidence and may only be disclosed, without fear of redress, in the following circumstances (also see clause 7.2 below):

7.1.1 where disclosure is under compulsion of law;

7.1.2 where there is a duty to the public to disclose;

7.1.3 where the legitimate interests of the Company require disclosure; and

7.1.4 where disclosure is made with the express or implied consent of the tenant or employee.

7.2 Disclosure to 3rd parties: All staff have a duty of confidentiality in relation to the Company, tenants and suppliers. In addition to the provisions of clause 7.1 above, the following are also applicable:

7.2.1 Information on tenants and staff: Our tenants' and staff' right to confidentiality is protected in the Constitution and in terms of ECTA *(Electronic and Communications Act, 25 of 2002)*. Information may be

given to a 3rd party if the tenant, or employee has consented in writing to that person receiving the information.

7.2.2 Requests for company information:

7.2.2.1 These are dealt with in terms of PAIA, which gives effect to the constitutional right of access to information held by the company, that is required for the exercise or protection of rights. Private bodies, like the company, can however refuse access to records if disclosure would constitute an action for breach of the duty of secrecy owed to a 3rd party.

7.2.2.2 In terms hereof, requests must be made in writing on the prescribed form to the company's Information Officer in terms of PAIA. The requesting party must state the reason for wanting the information and must pay a prescribed fee.

7.2.2.3 The company's manual in terms of PAIA, which contains the prescribed forms and details of prescribed fees, is referenced in Annexure A.

7.2.3 Confidential company information may not be disclosed to 3rd parties as this could constitute industrial espionage. The affairs of the company must be always kept strictly confidential.

7.3 The company views any contravention of this Privacy Policy very seriously and employees who are guilty of contravening the policy will be subject to disciplinary procedures, which may lead to the dismissal of any guilty party.

7.4 You may contact us via email (josias@giflogroup.co.za) or by telephone (021 863 0605) to,

a) request for access to your personal data,
b) withdraw your consent to our use or disclosure of your personal data, or
c) terminate your (data) profile with us.

7.5 Request to withdraw your consent to use or disclose your personal data may result in delays or failure to provide you with the services requested or purchased from us.

8. Storage of documents

8.1 Hard copies

8.1.1 Documents are stored in an archive and a vault.

8.2 Electronic copies

8.2.1 Documents are stored on business computers and our cloud-based server.

9. Security of personal data

9.1 Personal data collected by us will be,

a) safely and securely stored, and

b) disposed when no longer needed by us for business or legal purposes.

9.2 The following procedures are in place to protect personal information:

9.2.1 The Information Officer is **Josias de Kock** (contact details in Annexure A) and he is responsible for the compliance with the conditions of the lawful processing of personal information and other provisions of POPIA;

9.2.2 This policy has been put in place throughout the company and training on this policy and the POPIA has already taken place as part of the company's compliance function;

9.2.3 Each new employee will be required to sign an employment contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPIA;

9.2.4 Every employee currently employed within the company will be required to sign an addendum to their employment contracts containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPIA;

9.2.5 The company archived tenant information is stored on site, which is also governed by POPIA, and access to these areas are limited to authorized personal.

9.2.6 Company suppliers, insurers and other 3rd party service providers will be required to sign an SLA (Service Level Agreement) guaranteeing their commitment to the Protection of Personal Information; this is however an ongoing process that will be evaluated as needed.

9.2.7 All electronic files or data are backed up by our cloud server provider who is also responsible for system security that protects 3rd party access and physical threats (see relevant Cybercrimes clause).

9.3 Electronic storage:

9.3.1 The internal procedure requires that electronic storage of information (relevant to tenant, suppliers and staff) is performed as follows:

a) important documents and information are stored electronically,

b) access is controlled through user ID and password allocation,

c) storage and retrieval are based on access criteria as specified by the IO,

d) department heads together with the IO will determine any storage off-site or of hard copies where this is required for security purposes or business continuation.

9.3.2 Scanned documents: If documents are scanned, the hard copy must be retained for as long as the information is used or for 1 year after the date of scanning, except for documents pertaining to personnel. Any document containing information on the written particulars of an employee, including: employee's name and occupation, time that each employee worked, remuneration and date of birth, must be retained for a period of 3 years after termination of employment.

9.3.3 Sec. 51 of the Electronic Communications Act (No 25 of 2005) requires that personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates, processes or stores the information and a record of any 3rd party to

whom the information was disclosed must be retained for a period of 1 year or for as long as the information is used. It is also required that all personal information which has become obsolete must be destroyed.

9.4 Destruction of documents

9.4.1 Documents may be destroyed after the termination of the retention period as required by the legislations specified in Annexure "A" hereto.

9.4.2 Each department is responsible for attending to the destruction of its documents, which are done on a regular basis. Files are checked to make sure that they may be destroyed and to ascertain if there are important original documents in the file(s). Original documents are returned to the holder thereof, failing which, they should be retained by the company pending such return.

9.4.3 After completion of the process in 9.4.2 above, the department head shall, in writing, authorise the removal and destruction of the documents in the authorisation document. These records will be retained by the IO.

9.4.4 The documents are then made available for collection by the removers (or deputized employee) of the company's documents, who also ensure that the documents are shredded before disposal. This also helps to ensure confidentiality of information.

9.4.5 Documents may also be stored off-site, in storage facilities approved by the Company.

10. Cybersecurity

Giflo warrants that it has policies and procedures reasonably designed to detect, prevent and respond to cyberattacks, including providing training to its employees with respect to cybersecurity and monitoring compliance with its cybersecurity policies and procedures. Further, Giflo agrees that it will promptly notify the Regulator of any cybersecurity breach where this has been detected.

11.Bring your own device (BYOD)

For purposes of this Policy, a BYOD is any electronic device or peripheral used for storing, accessing, or transmitting electronic data and includes, but is not limited to data such as email on personal devices, flash drives, external hard drives, and other electronic storage devices; cell phones; smartphones; tablets; smart watches. Connection of any of these devices to the company's Wi-Fi or intranet will require compliance with the Policy.

12.Transfer of Information Outside the EU

Giflo Holdings (Pty) Ltd and its subsidiaries is a company based in the Republic of South Africa. All our facilities, affiliates, tenants, suppliers, and 3rd party providers are primarily located in South Africa. Please note that if you are communicating electronically or accessing our website from the European Union ('EU"), it is likely that your information will leave the EU for use in South Africa as described in this Privacy Policy. If personal data of EU residents is transferred or processed outside the EU Area, we will take all necessary steps to maintain the security of such personal data.

13.Changes to Privacy Policy

We may change this Privacy Policy at any time without prior notice to our customers and tenants, suppliers or visitors. Any changes to this Privacy Policy will be published on our website.

14.Contact Us

If you have any questions about our data protection policy or practices, you may contact our Information Officer via email (josias@giflogroup.co.za) or by telephone (021 863 0605).

15.General Disclaimer

The information contained in the Policy is for information purposes only. While we endeavour to keep the information up to date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to the information, products, services, or related graphics contained on the website or related materials for any purpose. Any reliance you place on such information is therefore strictly at your own risk. In no event will we be liable for any loss or damage including, without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits relating to, or in connection with, the use of the website or related materials.

Every effort is made to keep the website up and running smoothly. However, Giflo takes no responsibility for, and will not be liable for, the website being temporarily unavailable due to technical issues beyond our control. The content on this website is owned and copyrighted by Giflo, its licensors or others with all rights reserved. You may not use the content without the prior written permission of Giflo. All trademarks, trade names and logos and all related product names, design marks and slogans that appear on this website are either the trademarks or service marks (registered or unregistered) of Giflo or its licensors unless otherwise stated herein. Giflo and its licensors expressly reserve all intellectual property rights in all content on this website. No license is granted to you in connection with such content. In our sole discretion, we or our licensors may seek to fully enforce our intellectual property rights. By accessing and using this website you accept each of the foregoing terms and conditions without limitation. If you do not accept each of these terms and conditions, you should exit the website.

16.Email Disclaimer

Any email and files/attachments transmitted with it are confidential and are intended solely for the use of the individual or entity to whom they are addressed. If this message has been sent to you in error, you must not copy, distribute, or disclose of the information it contains as it is strictly prohibited and may be unlawful. Please notify Giflo immediately and delete the message from your system.

Annexure A

ACCESS TO INFORMATION ACT
Compiled in terms of Section 51 of the Promotion of Access to Information Act, 2 of 2000 (PAIA)

Responsible senior managers company:
Josias de Kock (Financial Manager) to deal with requests.

Postal address:
PO Box 608, Suider-Paarl, 7624

Street address:
57 Main Road, Paarl, 7646

Telephone number:
021 863 0605

Fax number:
N/A

E-mail address of authorised body: josias@giflogroup.co.za

Website: http//www.giflogroup.co.za

Latest notice in terms of Section 52(2) regarding records that are automatically available (Section 51(1)(c))

Descriptions of categories of records have not been submitted to the Minister in terms of Section 52(1) and therefore no notice has been published in the Government Gazette.

Records held in terms of other applicable legislation (Section 51(1)(d)).

Records of the company which are available in accordance with legislation other than the PAIA are:

1. Companies Act 71 of 2008 – Founding documents, statutory records and returns, minute books and registers, books of account, accounting records and statements, supporting documents and vouchers, in material and electronic format.
2. Income Tax Act 58 of 1962 – Returns of income, assessments, objections, records and supporting vouchers, appointment of public officer, and correspondence with revenue authorities.
3. Value Added Tax Act 89 of 1991 – Returns, assessments, receipts and correspondence.
4. Basic Conditions of Employment Act 75 of 1997 – Returns, statutory records, correspondence.
5. Employment Equity Act 55 of 1998 – Plan, annual reports and income differentials.
6. Skills Development Act 97 of 1998 – Workplace skills plan and report.

7. Skills Development Levies Act 9 of 1999 – Returns for payment of levy.
8. Unemployment Insurance Fund Contributions Act 4 of 2002 – Returns for payment of contributions.
9. Unemployment Insurance Fund Act 63 of 2001 – Returns for payment of contributions.
10. Labour Relations Act 66 of 1995 – Recruitment records, disciplinary records.
11. Occupational Health and Safety Act 85 of 1993 – Appointments and designations of committees and persons, health and safety policies. Minutes of meetings, reports, risk assessments, correspondence.
12. Compensation for Occupational Injuries and Diseases Act 190 of 1993 – Accident registers and reports, returns.

Records held as a matter of standard practice (Section 51(1)(e))

In addition to information available in terms of the above statutes, the company has such information as is required for the daily running of its business, including internal telephone and address lists, company policies, minutes of meetings, correspondence, directives, contracts, employee's records, requisitions, applications, memoranda, project evaluations, approvals, consents and general administrative information.

Requests for access to records (Chapter 3 of the PAIA)

Requests for access to records of this company must be made in the prescribed manner, i.e., must correspond substantially with Form C of Annexure B to Regulations R187 of 15 February 2002 published in the Government Gazette number 23119.

Fees

The IO of the company will notify the requester (other than a personal requester) by notice, requiring the requester to pay the prescribed fee (if any) before further processing the request. A personal requester does not pay such a fee.

Fees are set out in the Regulations R187 of 15 February 2002, in Government Gazette number 23119.