Protection of Personal Information Act 4 of 2013
EXTERNAL PRIVACY POLICY - JULY 2021

COMPANY DETAILS:
Company Name including the trading name: Kashalay Trading 112 (PTY) Ltd t/a Gordon Cumming Body Repairs
Company Registration Number: 2019/186550/07
Company Representative details: Kyla Clarke
Physical address: 15 Motor City, Bonza Bay Road, Beacon Bay, East London, 5241
Postal address: PO Box 7026, East London, 5200
Information Officer appointed for the business: Kyla Clarke (ID: 9307090064080)

"hereinafter referred to as the BUSINESS"

INDEX

DEFINITIONS

"**child**": means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself;
"competent person": means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child;
"data subject": for purposes of this Policy and in context of the BUSINESS will include, but not be exclusively limited to:

- Customers in the automotive industry;

- Insurers;
- Employees of the BUSINESS;
- Suppliers of parts, components, equipment and other operational materials;
- Industry regulators;
- Professional service providers;
- General operational service providers;

"direct marketing": means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of –

- Promoting or offering to supply, in the ordinary course of business of the BUSINESS; or
- Requesting the data subject to make a donation of any kind for any reason;

"electronic communication": means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient;

"filing system": means any structured set of personal information which in the case of the BUSINESS consist of physical files kept in the offices of the BUSINESS together with the data filed on the various software systems used by the BUSINESS;

"GDPR": means The General Data Protection Regulation 2016/679 which is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It addresses the transfer of personal data outside the EU and EEA areas and it imposes obligations onto organizations anywhere, if they target or collect data related to personal information from individuals in the EU. The regulation was put into effect on May 25, 2018.

"operator": for purposes of this Policy means a person or juristic person who processes personal information for a responsible party, which in this Policy will mean the BUSINESS in terms of a contract or mandate, without coming under the direct authority of that party;

"person": means a natural person or a juristic person;

"Personal information": means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

- Information relating to the education or the medical, financial, criminal or employment history of the person;
- Any identifying number, symbol, e-mail address, telephone number, location information, online identifier or other particular assignment to the person;
- The biometric information of the person;
- The personal opinions, views or preferences of the person;
- Correspondence sent by the person that would reveal the contents of the original correspondence if the message is of a personal or confidential nature;
- The views or opinions of another individual about the person; and
- The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;

''private body'' means—

(a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity;

(b) a partnership which carries or has carried on any trade, business or profession; or

(c) any former or existing juristic person, but excludes a public body

"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, organisation, 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;

"Promotion of Access to Information Act": means the Promotion of Access to Information Act (PAIA), 2000 (Act No. 2 of 2000);

"public record": means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body.

"record": means any recorded information regardless of form or medium, including any of the following:

- Writing on any material;
- Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
- Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
- Book, map, plan, graph, or drawing;
- Photograph, film, negative, tape or other device in which one or more visuals images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced; b) In the possession or under the control of a responsible party; and c) Regardless of when it came into existence;

"Regulator": – means the Information Regulator established in terms of Section 39 of the POPIA;

"responsible party": means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;

"restriction": means 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;

"RMI": means the Retail Motor Industry Organisation which is a motor industry organisation which serves the needs of its members and plays a key role in enabling motor trades to deliver its service to motoring consumers.

"special personal information": means personal information as referred to in Section 26 of the POPIA which includes Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

"this Act": means the Protection of Personal Information Act, No. 4 of 2013.

"unique identifier": means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

1. INTRODUCTION

The BUSINESS operates as a motor body repair business from its premises. As part of its operations, it deals with individual customers, collective customers who may belong to a fleet, insurers who refer repairs to the BUSINESS, SAMBRA, its service suppliers and support, the RMI and other industry Associations from time to time.

In performing its services to its customer base, the BUSINESS collects, processes and shares personal and special personal information. The BUSINESS acknowledges that most of its communications (both on the part of the BUSINESS of companies and on the part of their customers) are done electronically via the internet, per email and other electronic methods and should data subjects' information be collected manually, the information is inserted into the digital systems of the BUSINESS, processed both manually and digitally as a result and shared electronically if necessary.

2. OBJECTIVE

Although is not possible to ensure 100% mitigation against data breaches, the objective of this Policy is to ensure adherence of the BUSINESS and all its employees to the provisions within POPIA read together with its Regulations where necessary aimed at:

- Protecting BUSINESS'S South African data subjects from harm,
- To ensure that data subjects' Consent is obtained by the BUSINESS as provided for in POPIA,
- To ensure that data subjects' information is not unlawfully shared with third parties unless Consent for such sharing is obtained,
- To stop identity fraud;
- To create awareness amongst employees in respect of the cyber risks and
- Generally, to protect privacy.

The BUSINESS takes its responsibilities in terms of POPIA seriously and intends to continue developing its internal and external processes. This Policy constitutes the EXTERNAL SET OF PRIVACY RULES applicable to the information collected and processed by the BUSINESS and sets out the standard for suitable protection of personal information as required by POPIA. A variety of operational document changes have been implemented in support of the terms contained within this Policy.

3. POPIA CORE PRINCIPLES

In its quest to ensure the protection of data subjects' privacy as far as it is possible, the BUSINESS commits to the following:

3.1. To continue developing and maintaining reasonable protective measures against the possibility of risks such as loss, unauthorised access, destruction, use, alteration or revelation of personal information.

3.2. To regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information;

3.3. To ensure that the requirements of the POPIA legislation are upheld within the BUSINESS. In terms of sections 8, 17 and 18 of POPIA, the BUSINESS confirms that it adheres to an approach of transparency of operational procedures that controls collection and processing of personal information and subscribes to a process of accountability and openness throughout its operations.

3.4. In terms of the requirements set out within sections 9, 10, 11, 12, 13 14 and 15 of POPIA, the BUSINESS undertakes to collect personal information in a legal and reasonable way, for a specific reason and only if it is necessary for its operations and to process the personal information obtained from customers, clients, employees, visitors and services suppliers only for the purpose for which it was obtained in the first place.

3.5. Processing of personal information obtained from customers, clients, employees, service and product suppliers will not be undertaken in an insensitive, derogative discriminatory or wrongful way that can intrude on the privacy of the particular data subject.

3.6. In terms of the provisions contained within sections 23 to 25 of POPIA, all data subjects of the BUSINESS will be allowed to request access to certain personal information and may also request correction or deletion of personal information within the specifications of the POPIA. Data subjects should refer to FORMS 1 & 2 attached hereto for these purposes.

3.7. To not request or process information related to race, religion, medical situation, political preference, trade union operative within the BUSINESS, sexual certitude or criminal record unless this is lawfully required and unless the data subject has expressly consented. The BUSINESS will also not process information of children unless the specific consent provisions contained within POPIA have been complied with.

3.8. In terms of the provisions contained within section 16 of POPIA**,** the BUSINESS confirms its commitment that data subjects' information is recorded and retained accurately.

3.9. To not provide any documentation to a third party or service provider without the express consent of the data subject except where it is necessary for the proper execution of the service as expected by the data subject.

3.10. To keep effective record of personal information and undertakes not to retain information for a period longer than required.

3.11. In terms of sections 19 to 22 of POPIA, the BUSINESS undertakes to secure the integrity and confidentiality of personal information in its possession. The BUSINESS undertakes further to provide the necessary security of data and keep it in accordance with prescribed legislation.

4. CONSENT

When data subjects' information is collected, processed or shared by the BUSINESS during the process of it fulfilling its contractual service delivery obligations, the BUSINESS recognizes its obligations to explain the reasons for the collection of information from the particular data subject/s and to obtain the required Consents to process and where required the sharing of the information pursuant to such explanation.

If personal information is used for any other reason than the original reason of it being collected, the specific Consent for such purpose must be obtained from the data subject. The BUSINESS do not intend using data subjects' information for other reasons other than the reason for which it was collected.

If SPECIAL PERSONAL INFORMATION is collected, processed and stored for any reason from any of BUSINESS'S data subjects, a specific Consent for such collection must first be obtained unless:

4.1. Processing is carried out with a prior consent of the data subject;

4.2. Processing is necessary for the establishment, exercise or defense of a right or obligation in law;
4.3. Processing is for historical, statistical or research purposes.

5. COLLECTION, PROCESSING AND SHARING OF INFORMATION

The BUSINESS collects and processes personal and special personal information from its data subjects for a variety of reasons and in a variety of ways.

When clients/customers engage with the BUSINESS in respect of the repair of a motor vehicle or any other related services (such as the replacement of a part for instance), the client/customers are expected to complete a variety of information, including banking particulars, in order for a customer account to be created with the BUSINESS. In addition, employees are required to supply personal and banking information when they are employed by the BUSINESS and employees' information may be shared with third parties in terms of statutory requirement. Employees are expected to sign a POPIA DECLARATION as part of their employment contract. The BUSINESS's product suppliers and other service providers are also requested to supply certain information in order to facilitate the services and products being delivered to the BUSINESS'S customers.

Data subjects who subscribe to the various services and products of the BUSINESS and who complete personal information are guided by the BUSINESS through the provisions of POPIA, why information is required, how the information will be processed and with whom the information will be shared.

Sharing of information supplied is often required but not essential for all of the BUSINESS'S operations but by submitting such information, all data subjects acknowledge the following:

5.1. Personal information collected by BUSINESS will be collected directly from the data subject, unless –
5.1.1. The information is contained or derived from a public record or has deliberately been made public by the data subject;
5.1.2. Collection of the information from another source would not prejudice a legitimate interest of the data subject;
5.1.3. Collection of the information from another source is necessary -
  5.1.3.1. To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
  5.1.3.2. To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue;
  5.1.3.3. For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;
  5.1.3.4. In the interest of national security;
  5.1.3.5. To maintain the legitimate interests of the BUSINESS or of a third party to whom the information is supplied;
  5.1.3.6. Compliance would prejudice a lawful purpose of the collection;
  5.1.3.7. Compliance is not reasonably practicable in the circumstances of the particular case.
5.1.4. Personal information is collected for a specific, explicitly defined and lawful purpose related to a function or activity of the BUSINESS;
5.2. Steps will be taken to ensure that the data subject is aware of the purpose of the collection of the information.
5.3. The BUSINESS will take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary, having regard to the purpose for which the personal information is collected and further processed.
5.4. Where personal information is collected form a data subject directly, BUSINESS will take reasonably practicable steps to ensure that the data subject is aware of: -
5.4.1. The nature of the information being collected and where the information is not collected from the data subject, the source from which it is collected;
5.4.2. The name and address of the BUSINESS;
5.4.3. The purpose for which the information is being collected;
5.4.4. Whether or not the supply of the information by the data subject is voluntary or mandatory;
5.4.5. The consequences of failure to provide the information;
5.4.6. Any particular law authorising or requiring the collection of the information.

The BUSINESS collects only the essential information from its data subjects as is required for the purposes of facilitating the motor body repair or replacement or installation of a motor part.

6. STORAGE OF INFORMATION

The BUSINESS stores data subjects' information on its electronic database in addition to the physical files and forms which it keeps at its offices. The BUSINESS has adopted formal document control rules as part of its business practices which relate specifically to: where data subject's documents are kept, who controls such documents, who is responsible for management of such documents as well as general rules regarding the copying, filing and distribution of data subjects' documents.

The management and employees of the BUSINESS acknowledge the risks facing data subjects in respect of the storage of personal and special personal information within physical files or on the BUSINESS'S software system/s. To ensure that its best attempts are made to minimize data subjects from suffering loss of personal information, misuse or unauthorised alteration of information, unauthorized access or disclosure of personal information generally, the BUSINESS will:

6.1. Store personal information in databases that have built-in safeguards and firewalls to ensure the privacy and confidentiality of your information.
6.2. Constantly monitor the latest internet developments to ensure that the systems evolve as required. The BUSINESS tests its systems regularly to ensure that our security mechanisms are up to date.
6.3. Ensure that safeguards exist with regards to physical files.
6.4. Continue to review its internal policies and third party agreements where necessary to ensure that these are also complying with the POPIA and Regulations in line with BUSINESS'S Policy rules.

7. DISPOSAL OF DATA SUBJECTS' INFORMATION

The BUSINESS undertakes to ensure that records no longer needed or of no value are disposed of at the proper time. References to the time and manner of disposal of BUSINESS'S data subject files are contained within its internal document control rules. These rules, together with the below general rules apply to all documents which are collected, processed or stored by the BUSINESS and include but are not limited to documents in paper and electronic format, for example, e-mail, web and text files, PDF documents etc.

The BUSINESS does not automatically discard or dispose of the telephone numbers, email addresses of or electronic communications (such as emails) with data subjects with whom it has previously dealt but will do so on request by the data subject.

The directors and employees of BUSINESS acknowledge that electronic devices, on which contact names, number and communication are stored can hold vast amounts of information, some of which can linger indefinitely and undertake to remove contact particulars and other personal information from these devices also if requested by a data subject. Data subjects are referred to the FORMS hereto attached in respect of the request herein mentioned**.**

When physical files are designated for disposal, the relevant responsible persons within the BUSINESS will ensure that:

7.1. Under no circumstances will paper documents or removable media (CD's, DVD's, discs, etc.) containing personal or confidential information be simply binned or deposited in refuse tips.
7.2. All electrical waste, electronic equipment and data on disk drives be physically removed and destroyed in such a way that the data will by no means be able to be virtually retrievable.
7.3. All paper documents that should be disposed of, be shredded locally and then be recycled where practically possible.
7.4. In the event that a third party is used for data destruction purposes, the Information Officer will ensure that such third party will also comply with these rules and any other applicable legislation.
7.5. The BUSINESS may suspend the destruction of any record or document due to pending or reasonably foreseeable litigation, audits, government investigations or similar proceedings. Management of the BUSINESS undertakes to notify employees of applicable documents where the destruction has been suspended to which they have access to.
7.6. In the event that a document and/or information is no longer required to be stored in accordance with this policy and relevant legislation, it should be deleted and destroyed.
7.7. The Information Officer should be consulted where there is uncertainty regarding the retention and destruction of a document and/or information.

8. INTERNET AND CYBER TECHNOLOGY

In recognition of the cyber risk associated with digital collection, processing, storing and sharing of information, the BUSINESS has implemented specific rules applicable to all users of its systems, email and internet and will continue to upgrade and assess the digital risk inherent to its operations.

8.1. Acceptable use of BUSINESS'S Internet Facilities & standard Anti-Virus rules

The repercussions of misuse of the BUSINESS IT and email systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g. computer viruses), legal and financial penalties for data leakage and lost productivity resulting from network downtime. In order to ensure that the BUSINESS'S IT systems are not misused, everyone who uses or has access to the BUSINESS'S systems have received training and internal guidelines in order to meet the following five high-level IT Security requirements:

8.1.1. Information will be protected against any unauthorized access as far as possible;
8.1.2. Confidentiality of information will be assured as far as possible;
8.1.3. Integrity of information will be preserved as far as possible;
8.1.4. Availability of information for business processes will be maintained;
8.1.5. Compliance with applicable laws and regulations to which the BUSINESS is subject will be ensured by the Information Officer as far as possible.

Every user of the BUSINESS's IT systems undertakes responsible for exercising good judgment regarding reasonable personal use.

8.2. IT Access Control

Management, in collaboration with the IT support person/s of the BUSINESS undertake to ensure that logging into the IT system and software packages is password controlled and shall exercise all caution in allowing unauthorized access to the password. It further undertakes that the password/s shall be reviewable from time to time but in particular where GOOGLE based products are used and linked (such as Facebook, Whatsapp and GMAIL based domains).

8.3. The BUSINESS'S Email Rules

The BUSINESS acknowledges that most of its communications are conducted via email and instant messaging (IM). Given that email and IM may contain sensitive and confidential information, the information involved must be appropriately protected.

In addition, email and IM are potential sources of spam, social engineering attacks and malware, so the database of the BUSINESS must be protected as completely as possible from these threats. The misuse of email and IM can pose many legal, privacy and security risks, so it is important for users to be aware of the appropriate use of electronic communications. Awareness amongst employees within the BUSINESS of companies is a priority for management and training in respect hereof will regularly be arranged.

It is of use to note that all users of the BUSINESS's email system are prohibited from using email to:

8.3.1. Send, receive, solicit, print, copy, or reply to text, images, or jokes that disparage others based on their race, religion, colour, gender, sex, sexual orientation, national origin, veteran status, disability, ancestry, or age.
8.3.2. Send, receive, solicit, print, copy, or reply to messages that are disparaging or defamatory.
8.3.3. Spread gossip, rumours, or innuendos about employees, clients, suppliers, or other outside parties.
8.3.4. Send, receive, solicit, print, copy, or reply to sexually oriented messages or images.
8.3.5. Send, receive, solicit, print, copy, or reply to messages or images that contain foul, obscene, disrespectful, or adult-oriented language.
8.3.6. Send, receive, solicit, print, copy, or reply to messages or images that are intended to alarm others, embarrass BUSINESS negatively impact productivity, or harm morale.

The purpose of these rules is to ensure that information sent or received via the BUSINESS'S IT systems is appropriately protected, that these systems do not introduce undue security risks to the BUSINESS and that users are made aware of what the management of the BUSINESS deems as acceptable and unacceptable use of its email and IM.

8.4. **The BUSINESS'S Rules related to handheld devices**

Many users do not recognize that mobile devices represent a threat to IT and data security. As a result, they often do not apply the same level of security and data protection as they would on other devices such as desktop or laptop computers. These rules outline the BUSINESS'S requirements for safeguarding the physical and data security of mobile devices such as smartphones, tablets, and other mobile devices that PC's and Notebooks but only as far as such devices are supplied to the data subject by the BUSINESS for usage by such data subject in fulfilment of a function related to or associated with the BUSINESS.

8.4.1. The BUSINESS'S users of handheld devices are expected to diligently protect their devices from loss and disclosure of private information belonging to or maintained by the BUSINESS.
8.4.2. In the event of a security incident or if suspicion exists that the security of the BUSINESS'S systems has been breached, the Information Officer and employee shall be obliged to notify the IT support of the group of companies immediately especially when a mobile device may have been lost or stolen.

8.5. **Anti-virus rules**

8.5.1. Management of the BUSINESS is responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into the BUSINESS'S programs (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited.
8.5.2. Users are discouraged from attempting to remove viruses themselves. If a virus infection is detected, users are expected to disconnect from the BUSINESS'S networks, stop using the infected computer immediately and notify the IT support.
8.5.3. It is further worth noting that the BUSINESS'S users are encouraged to be cautious of e-mail attachments from an unknown source as viruses are often hidden in attachments and that the BUSINESS confirms that all employees have received and will continue to receive internal training in respect of such virus and how to identify them If a virus is suspected, the attachment must not be opened or forwarded and must be deleted immediately.

8.6. **Physical access control**

All of the BUSINESS'S premises that include computers and other types of information technology resources will be safeguarded against unlawful and unauthorized physical intrusion, as well as fire, flood and other physical threats. This includes but is not limited to; security doors, key entry areas, external doors that are locked from closing until opening of the building, locked and/or barred windows, security cameras, registration of visitors at entrances, security guards, and fire protection.

8.7. **Usage Data**

Usage Data is collected automatically when using the internet services of the BUSINESS, in particular its website. Usage Data may include information such as data subjects' device's internet protocol address (e.g. IP address), browser type, browser version, details of the pages of the BUSINESS'S website that are visited by data subjects, the time and date of the website visit, the time spent on those pages, unique device identifiers and other diagnostic data. When data subjects access the website services of the BUSINESS by or through a mobile device, the BUSINESS may collect certain information automatically, including, but not limited to, the type of mobile device used by the data subject, unique ID, the IP address of the mobile device, the mobile operating system, the type of mobile Internet browser used, unique device identifiers and other diagnostic data. The BUSINESS may also collect information that the user's browser sends whenever the BUSINESS'S website is visited.

8.8. **Tracking Technologies and Cookies**

Cookies and similar tracking technologies are used to track the activity on the BUSINESS'S website, should this be applicable, and store certain information. Tracking technologies used are beacons, tags, and scripts to collect and track information and to improve and analyze the efficiency of the website. The technologies which may be used to track may include:

8.8.1. Cookies or Browser Cookies. A cookie is a small file which may be placed on a data subject's device. Data subjects can instruct their browser to refuse all Cookies or to indicate when a Cookie is being sent. However, if this function of the BUSINESS'S website is not accepted, data subjects may not be able to use some parts of the website and unless the browser settings have been adjusted, the BUSINESS'S website may use Cookies.
8.8.2. Flash Cookies. Certain features of the website may use local stored objects (or Flash Cookies) to collect and store information about data subjects' preferences or activity on the website. Flash Cookies are not managed by the same browser settings as those used for Browser Cookies. For more information on how Flash Cookies can be deleted the following process can be followed: "Where can I change the settings for disabling, or deleting local shared objects?" available at https://helpx.adobe.com/flashplayer/kb/disable-local-shared-objects;
8.8.3. Web Beacons. Certain sections of the website and emails may contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) that permit the BUSINESS for example, to count users who have visited those pages

or opened an email and for other related website statistics (for example, recording the popularity of a certain section and verifying system and server integrity).

8.8.4. Cookies can be "Persistent" or "Session" Cookies. Persistent Cookies remain on data subjects' personal computer or mobile device even when offline, while Session Cookies are deleted as soon as data subjects' web browsers are closed.

9. THIRD PARTY OPERATORS

The BUSINESS recognizes that, in fulfilling certain of its contracts with its customers and in order to operate efficiently in fulfilling such contracts, it is necessary at times to share data subjects' personal and special personal information with third parties for specific reasons related to the BUSINESS'S service delivery.

As referenced in clauses 5 and 6 above, the BUSINESS will obtain the necessary Consent where required from the particular data subject.

The BUSINESS shall moreover and where possible enter into an OPERATORS' AGREEMENT with the relevant third party with which BUSINESS shares data subjects' information in order to ensure that the third party operator treats the personal information of BUSINESS'S data subjects responsibly and in accordance with the provisions contained in the Act and Regulations thereto. BUSINESS shall, where possible request copies of the third party operators' POPIA Policy, rules, internet rules and details of the third party's Information Officer.

10. BANKING DETAILS

It is a known fact that electronic transmission of banking details poses a particular cyber risk threat which the BUSINESS recognizes. Businesses who share banking details electronically are particular targets for email interceptions and in particular the interception of banking details for purposes of payment in respect of the transaction. The BUSINESS'S data subjects are open to large amounts of damages and losses if emails are intercepted and banking details are fraudulently amended without the data subject's knowledge.

To mitigate the risk of internet and email interceptions of banking details, the BUSINESS has implemented clear warnings within all its correspondences (emails and physical letters) warning data subjects of the risks of email hacking and interceptions. In the event that banking details are physically sent to data subjects or received from data subjects per email or instant messaging platforms for purposes of payment, the banking details will be confirmed with a telephone call and a follow up whatsapp. It is recorded that, in certain instances, data subjects' bank details are to be shared with relevant third parties but in such event, all care shall be taken to ensure encryption of emails.

11. DIRECT MARKETING

The BUSINESS understand its obligations to its data subjects in relation to its direct marketing communications. From time to time, the BUSINESS may send emails for the purposes of marketing new products or specials. In the event that the BUSINESS sends out such emails, it undertakes to ensure that the necessary UNSUBSCRIBE or OPTING OUT options are made available to its data subjects and recipients of such communication.

The BUSINESS is furthermore committed to not share data subjects' information with third parties for the sole purpose of such third party marketing to such data subjects. In the event that any associated third party using the data subjects' information shared by BUSINESS with such third party in the fulfilment of its customer orders, BUSINESS takes no responsibility for any consequences suffered by the data subject which may have been caused by the third party's actions.

12. DATA CLASSIFICATION

All of the BUSINESS'S employees share in the responsibility for ensuring that the BUSINESS'S information assets receive an appropriate level of protection as set out hereunder:

12.1. Managers of the BUSINESS are responsible for assigning classifications to information assets according to the standard information classification system presented below.

12.2. Where practicable, the information category shall be embedded in the information itself.

12.3. All employees of the BUSINESS shall be guided by the information category in their security-related handling of its information. All information of the BUSINESS and all information entrusted to the BUSINESS from third parties fall into one of three classifications in the table below, presented in order of increasing sensitivity.

Information Description	Examples	Category
Unclassified Public	Information is not confidential and can be made public without any implications for the BUSINESS	Product brochures widely distributed Information widely available in the public domain, including publicly available web site areas of the BUSINESS Sample downloads of the BUSINESS'S software that is for Sale. Financial reports required by regulatory authorities. Newsletters for external transmission
Proprietary	Information is restricted to management approved internal access and protected from external access. Unauthorized access could influence the BUSINESS'S operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital.	Passwords and information on corporate security procedures Know-how used to process client information Standard Operating Procedures used in all parts of BUSINESS'S activities All software codes developed by the BUSINESS, whether used internally or sold to clients
Client Confidential Data	Information collected and used by the BUSINESS in the conduct of its business to	Salaries and other personnel data

	employ people, to log and fulfil client mandates, and to manage all aspects of corporate finance. Access to this information is very restricted within the BUSINESS. The highest possible levels of integrity, confidentiality, and restricted availability are vital. Children's personal and special personal information.	Accounting data and internal financial reports Confidential customer business data and confidential contracts Non-disclosure agreements with clients\vendors Company business plans

13. RIGHTS OF THE DATA SUBJECT- FORMS 1 & 2 ATTACHED

13.1. The data subject or competent person where the data subject is a child, may withdraw his, her or its consent to procure and process his, her or its personal information, at any time, providing that the lawfulness of the processing of the personal information before such withdrawal or the processing of personal information is not affected.

13.2. A data subject may object, at any time, to the processing of personal information–

- In writing, on reasonable grounds relating to his, her or its particular situation, unless legislation provides for such processing; or
- For purposes of direct marketing other than direct marketing by means of unsolicited electronic communications.

13.3. A data subject, having provided adequate proof of identity, has the right to –

- Request the BUSINESS of companies to confirm, free of charge, whether or not the BUSINESS holds personal information about the data subject; and
- Request from the BUSINESS of companies a record or a description of the personal information about the data subject held by the group of companies, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information – within a reasonable time, at a prescribed fee as determined by the Information Officer, in a reasonable manner and format and in a form that is generally understandable.

13.4. A data subject may, in the prescribed manner, request that the BUSINESS of companies

- Correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or
- Destroy or delete a record of personal information about the data subject that the BUSINESS are no longer authorised to retain.

13.5. Upon receipt of a request referred to in clause 14.4, the BUSINESS will, as soon as reasonably practicable –

- Correct the information;
- Destroy or delete the information;
- Provide the data subject, to his, her or its satisfaction, with credible evidence in support of the information; or
- Where an agreement cannot be reached between the BUSINESS and the data subject, and if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made.

13.6. The BUSINESS will inform the data subject, who made a request as set out in clause 14.5, of the action taken as a result of the request.

14. COVID 19

The BUSINESS has implemented and continue to apply its Workplace Risk Assessment measures in line with accepted Occupational Health and Safety Guidelines issued by the Departments of Labour and Health and in terms of the Regulations and Directions to the Disaster Management Act. With reference to these assessment measures, the BUSINESS is and will remain entitled to oblige employees to complete a Covid 19 Risk Assessment form upon entering the BUSINESS offices, workshops or factories and any other of its premises and before such employees are despatched to a customer's premises for installation or maintenance provided that the personal and special personal information required to be completed are necessary and limited to the purposes of assessing the risk of Covid 19 exposure.

The BUSINESS may also, where required by statute, share the information with the Departments of Labour and Health especially in the event of someone testing positive and/or where a significant increase of risk exists in the workplace and offices.

The BUSINESS take no responsibility for the Covid 19 protocols which may or may not be followed by customers at their premises. Data subjects who engage with these customers are encouraged to check that protocols are followed to the satisfaction of the data subject.

15. **INFORMATION OFFICER**

15.1. **The general responsibilities of Information Officers for the BUSINESS include the following:**

15.1.1. The encouragement of compliance, by the BUSINESS, with the conditions for the lawful processing of personal information;
15.1.2. Managing requests made to the BUSINESS pursuant to POPIA;
15.1.3. Working with the Regulator in relation to investigations conducted pursuant to prior authorisation required to process certain information of POPIA in relation to the business.
15.1.4. Continuously perform data backups, store at least weekly backup offsite, and test those backups regularly for data integrity and reliability.
15.1.5. Review policy rules regularly, document the results, and update the policy as needed.
15.1.6. Continuously update information security policies and network diagrams.
15.1.7. Secure critical applications and data by patching known vulnerabilities with the latest fixes or software updates.
15.1.8. Perform continuous computer vulnerability assessments and audits

15.2. **The data breach responsibilities of the Information Officers for the BUSINESS include the following:**

15.2.1. Ascertain whether personal data was breached;

15.2.2. Assess the scope and impact by referring to the following:

15.2.2.1. Estimated number of data subjects whose personal data was possibly breached

15.2.2.2. Determine the possible types of personal data that were breached

15.2.2.3. List security measures that were already in place to prevent the breach from happening.

15.2.3. Once the risk of the breach is determined, the following parties need to be notified within 72 hours after being discovered:

15.2.3.1. The Information Regulator

15.2.3.2. Communication should include the following:

- Contact details of Information Officer
- Details of the breach,
- Likely impact,
- Actions already in place, and those being initiated to minimise the impact of the data breach.
- Any further impact is being investigated (if required), and necessary actions to mitigate the impact are being taken.

15.2.4. Review and monitor

15.2.4.1. Once the personal data breach has been contained, BUSINESS will conduct a review of existing measures in place, and explore the possible ways in which these measures can be strengthened to prevent a similar breach from reoccurring.

15.2.4.2. All such identified measures should be monitored to ensure that the measures are satisfactorily implemented.

16. GDPR

16.1. In addition to the provisions contained within POPIA, GPDR rules apply in particular to the BUSINESS in respect of controlling and processing of personal data of any data subject residing in the EU as stated in the General Data Protection Regulation.

16.2. For ease of reference throughout this clause 16 and only for purposes of the applicability of the GDPR in respect of EU resident individual data subjects, the following terms will mean:

16.2.1. **Data Controller**: the entity that determines the purposes, conditions and means of the processing of personal data.

16.2.2. **Data Processor**: the entity that processes data on behalf of the data controller, with or without the use of automated systems, to collect, store, organize, retain, modify, query, use, forward, transmit, disseminate or combine and compare data. This also includes disposing of, deleting and blocking data and data storage media.

16.2.3. **Data Subject**: a natural person whose personal data is processed by a data controller or data processor.

16.3. **Personal Data**: any information related to a natural person or data subject, that can be used to directly or indirectly identify the person.

16.4. The BUSINESS fully supports and complies with the 6 (Six) protection principles of the GDPR related to data subjects of THE BUSINESS who fall within the scope of the GDPR and which are summarised below:

16.4.1. **Lawfulness, fairness and transparency**: The personal information of the European citizens will be processed lawfully, fairly and in a transparent manner in relation to the data subject.

16.4.2. **Purpose limitation:** The personal information of the European citizens will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purpose.

16.4.3. **Data Minimisation**: The personal information of the European citizens will be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

16.4.4. **Accuracy**: The personal information of the European citizens will be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purpose for which it is processed, is erased or rectified without delay.

16.4.5. **Storage Limitation**: The personal information of the European citizens will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR, subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

16.4.6. **Integrity and Confidentiality**: The personal information of the European citizens will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

16.5. **External EU service providers**

In order to avoid duplication, any EU service provider that have already signed an Agreement with the BUSINESS, does not need to sign another Consent form with the BUSINESS. Any other External EU service provider must sign an Agreement and Consent declaration, whereby confirming commitment to this policy

17. AVAILABILITY AND REVISION

A copy of this Policy will be made available on the website of the BUSINESS if applicable or at the physical offices/premises of the BUSINESS. This policy will continually be updated to comply with legislation, thereby ensuring that personal information will be secure.

FORM 1

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013) REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 2]

Note:

1. *Affidavits or other documentary evidence as applicable in support of the objection may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*
3. *Complete as is applicable.*

A	**DETAILS OF DATA SUBJECT**
Name(s) and surname/ registered name of data subject:	
Unique Identifier/ Identity Number	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname/ Registered name of responsible party:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/ E-mail address:	
C	**REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) to (f)** *(Please provide detailed reasons for the objection)*

Signed at ..... this ..... day of .....20……..

..... *Signature of data subject/designated person*

FORM 2

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013) REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 3]

Note:

1. *Affidavits or other documentary evidence as applicable in support of the request may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*
3. *Complete as is applicable.*

Mark the appropriate box with an "x".

Request for:

☐ Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.

☐ Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

A	**DETAILS OF THE DATA SUBJECT**
Name(s) and surname/ registered name of data subject:	
Unique identifier/ Identity Number:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname/ registered name of responsible party:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/ E-mail address:	
C	**INFORMATION TO BE CORRECTED/DELETED/ DESTRUCTED/ DESTROYED**

D	**REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(a) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY ; and or** **REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(b) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN.** *(Please provide detailed reasons for the request)*

Signed at ..... this ..... day of .....20……..

.....
Signature of data subject/ designated person

FORM 3

APPLICATION FOR THE CONSENT OF A DATA SUBJECT FOR THE PROCESSING OF PERSONAL INFORMATION FOR THE PURPOSE OF DIRECT MARKETING IN TERMS OF SECTION 69(2) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013) REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018 [Regulation 6]

TO: _____
_____
_____

FROM: *(Name of data subject)*

_____
_____
_____
_____

Contact number(s): _____
Fax number: _____
E-mail address: _____
(Name, address and contact details of responsible party)

Full names and designation of person signing on behalf of responsible party:

_____

.....
Signature of designated person

Date: _____

PART B

I,_____*(full names of data subject)* hereby:

☐ Give my consent.

To receive direct marketing of goods or services to be marketed by means of electronic communication.

SPECIFY GOODS or SERVICES:
SPECIFY METHOD OF COMMUNICATION: FAX:
E - MAIL:
SMS:
OTHERS – SPECIFY:

Signed at ..... this ..... day of .....20.....
.....*Signature of data subject*