



Protection of Personal Information Act 4 of 2013

EXTERNAL PRIVACY POLICY

BRAND HUBB

JUNE 2021

INDEX

1.	Definitions	1
2.	Introduction	3
3.	Objective of the Policy	3
4.	POPIA Core Principles	3
5.	Consent	4
6.	Collection, Processing and Sharing	4
7.	Storage of Information	5
8.	Disposal of Information	5
9.	Internet and Cyber Technology	6
10.	Third Party Operators	8
11.	Banking details	8
12.	Direct Marketing	9
13.	Classification of Information	9
14.	Data Subjects' Rights	9
15.	Covid 19	10
16.	Information Officer and Duties	10
17.	Promotion of Access to Information	11
18.	Availability and Revision	11
	ANNEXURES	
	Form 1: Objection to Processing	12
	Form 2: Request for Correction or Deletion	13
	Form 3: Consent of Data Subject	15

1. DEFINITIONS

“biometrics”: means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition;

“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”: means the person to whom personal information relates and for the purposes of BRAND HUBB, this will include but not be limited to – visitors to the various BRAND HUBB websites, customers who have previously bought goods via BRAND HUBB, employees, external service suppliers, suppliers of products and all associates of BRAND HUBB;

“direct marketing”: means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of – a) Promoting or offering to supply, in the ordinary course of business of BRAND HUBB, legal services to the data subject; or b) Requesting the data subject to make a donation of any kind for any reason;

“deputy information officers”: means **CHARNE LUYANE GIBSON**;

“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 BRAND HUBB consist of physical files kept in the offices of BRAND HUBB together with the data filed on the various software systems used by BRAND HUBB;

“BRAND HUBB”: for purposes of this Policy document means the company registered as BRAND HUBB (PTY) LTD, Registration Number 2015/181834/07 which includes various shops within the BRAND HUBB brand such as, but not limited to ShopCandy, ShopAcer, 3dStore, DJI, Fittime with operational offices situated at the district office park, 8 Kikuyu Rd Sunninghill, 2157;

“Information officer”: of BRAND HUBB will mean **JD O’CONNOR**;

“operator”: means a person who processes personal information for a responsible party 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 – a) The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; b) Dissemination by means of transmission, distribution or making available in any other form; or c) 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 – a) Regardless of form or medium, including any of the following: I. Writing on any material; II. 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; III. Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; IV. Book, map, plan, graph, or drawing; V. Photograph, film, negative, tape or other device in which one or more visual 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;

“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.

2. INTRODUCTION

BRAND HUBB operates within the ONLINE SHOPPING space where customers can purchase third party goods via the BRAND HUBB website, make payment of such purchases online and where after BRAND HUBB arranges for delivery of the goods to the customer.

BRAND HUBB deals with many role players in the online shopping space and in delivering its online services to its customers, always collects personal information from such customers and shares such information with third party suppliers of BRAND HUBB.

BRAND HUBB acknowledges that most of its communications with customers, product suppliers and services suppliers are done electronically via the internet, per email and other electronic methods. In recognizing the international risk of data breach and also to ensure that lawful conditions exist surrounding its data subject’s information, BRAND HUBB accepts that all its South African based data subjects’ Constitutional Right to Privacy is of utmost importance. BRAND HUBB further accepts that its data subjects based in other parts of the world are entitled to equal rights to privacy in terms of Regulations applicable to such data subjects in the countries in which they are based. As such, BRAND HUBB is committed to comply with South Africa’s POPIA. BRAND HUBB is further committed to the education of its data subjects in respect of their rights to privacy and will make all operational amendments necessary.

3. OBJECTIVE

Although is not possible to ensure 100% mitigation against data breaches, the objective of this Policy is to ensure adherence of BRAND HUBB to the provisions within POPIA together with its Regulations aimed at protecting all BRAND HUBB’s data subjects from harm as wide as possible by protecting their personal information, to ensure that data subjects’ Consent is obtained 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 and generally to protect privacy. BRAND HUBB 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 BRAND HUBB and sets out the standard for suitable protection of personal information as required by POPIA.

4. POPIA CORE PRINCIPLES

In its quest to ensure the protection of data subjects’ privacy, BRAND HUBB fully commits as follows:

- 4.1. 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.
- 4.2. 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;
- 4.3. To ensure that the requirements of the POPIA legislation are upheld within BRAND HUBB. In terms of sections 8, 17 and 18 of POPIA, BRAND HUBB 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.
- 4.4. In terms of the requirements set out within sections 9, 10, 11, 12, 13 14 and 15 of POPIA, BRAND HUBB 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 clients, employees, visitors and services suppliers only for the purpose for which it was obtained in the first place.

- 4.5. Processing of personal information obtained from owners, occupiers, visitors and service suppliers will not be undertaken in an insensitive, derogative discriminatory or wrongful way that can intrude on the privacy of the particular data subject.
- 4.6. In terms of the provisions contained within sections 23 to 25 of POPIA, all data subjects of BRAND HUBB 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.
- 4.7. To not request or process information related to race, religion, medical situation, political preference, trade union membership, sexual certitude or criminal record unless this is lawfully required and unless the data subject has expressly consented. BRAND HUBB will also not process information of children unless the specific consent provisions contained within POPIA have been complied with.
- 4.8. In terms of the provisions contained within section 16 of POPIA, BRAND HUBB is committed that data subjects' information is recorded and retained accurately.
- 4.9. 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.
- 4.10. To keep effective record of personal information and undertakes not to retain information for a period longer than required.
- 4.11. In terms of sections 19 to 22 of POPIA, BRAND HUBB will secure the integrity and confidentiality of personal information in its possession. BRAND HUBB will provide the necessary security of data and keep it in accordance with prescribed legislation.

5. CONSENT

When data subjects' information is collected, processed or shared online or manually by BRAND HUBB during the process of BRAND HUBB delivering its online shopping services, BRAND HUBB recognizes its obligations to explain the reasons for the collection of information from the particular data subject/s and obtains the required Consents to process and where required the sharing of the information pursuant to such explanation and using the information for limited marketing purposes.

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. SPECIAL PERSONAL INFORMATION may be collected from data subjects without specific Consent if:

- 5.1. Processing is carried out with a prior consent of the data subject;
- 5.2. Processing is necessary for the establishment, exercise or defense of a right or obligation in law;
- 5.3. Processing is for historical, statistical or research purposes.

BRAND HUBB has amended its standard documentation and online terms with references to the Act and will obtain all clients' general Consent in each transaction.

6. COLLECTION, PROCESSING AND SHARING OF INFORMATION

BRAND HUBB collects and processes personal information from its data subjects for a variety of reasons and in a variety of ways. Customers who wish to place orders via the BRAND HUBB online platform may register as members or may purchase items as a guest of BRAND HUBB. In both instances, customers are obliged to complete necessary information to successfully register. In this way, personal and special information are collected from data subjects who place online orders via the BRAND HUBB website and the information is then shared with the relevant delivery suppliers of BRAND HUBB in order to arrange delivery of the orders.

By submitting personal and special personal information details to BRAND HUBB, all data subjects acknowledge the following:

- 6.1. Personal information collected by BRAND HUBB will be collected directly from the data subject, unless –
 - 6.1.1. The information is contained or derived from a public record or has deliberately been made public by the data subject;
 - 6.1.2. Collection of the information from another source would not prejudice a legitimate interest of the data subject;
 - 6.1.3. Collection of the information from another source is necessary -
 - 6.1.3.1. To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
 - 6.1.3.2. To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue;

- 6.1.3.3. For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;
 - 6.1.3.4. In the interest of national security;
 - 6.1.3.5. To maintain the legitimate interests of BRAND HUBB or of a third party to whom the information is supplied;
 - 6.1.3.6. Compliance would prejudice a lawful purpose of the collection;
 - 6.1.3.7. Compliance is not reasonably practicable in the circumstances of the particular case.
- 6.1.4. Personal information is collected for a specific, explicitly defined and lawful purpose related to a function or activity of BRAND HUBB;
 - 6.2. Steps will be taken to ensure that the data subject is aware of the purpose of the collection of the information.
 - 6.3. BRAND HUBB 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.
 - 6.4. Where personal information is collected from a data subject directly, BRAND HUBB will take reasonably practicable steps to ensure that the data subject is aware of: -
 - 6.4.1. 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;
 - 6.4.2. The name and address of BRAND HUBB;
 - 6.4.3. The purpose for which the information is being collected;
 - 6.4.4. Whether or not the supply of the information by the data subject is voluntary or mandatory;
 - 6.4.5. The consequences of failure to provide the information;
 - 6.4.6. Any particular law authorising or requiring the collection of the information.

7. STORAGE OF INFORMATION

BRAND HUBB acknowledges the risks facing data subjects with the storage of personal and special personal information on the BRAND HUBB's software systems as well as filing copies of the physical information sheets containing personal information physically in an office. 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, it will:

- 7.1. Store personal information in databases that have built-in safeguards and firewalls to ensure the privacy and confidentiality of your information.
- 7.2. Constantly monitor the latest internet developments to ensure that the systems evolve as required. BRAND HUBB tests its systems regularly to ensure that our security mechanisms are up to date.
- 7.3. 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 BRAND HUBB's Policy rules.

8. DISPOSAL OF DATA SUBJECTS' INFORMATION

BRAND HUBB is responsible to ensure that necessary records and documents of their data subjects are adequately protected and maintained to ensure that records that are no longer needed or are of no value are disposed of at the proper time. These rules apply to all documents which are collected, processed or stored by BRAND HUBB and include but are not limited to documents in paper and electronic format, for example, e-mail, web and text files, PDF documents etc.

BRAND HUBB does not discard or dispose of the telephone numbers, email addresses of data subjects and electronic communications with data subjects with whom it has previously dealt but will do so on request by the data subject..

Secure disposal maintains data security and supports compliance with this BRAND HUBB policy. BRAND HUBB acknowledges that electronic devices and media can hold vast amounts of information, some of which can linger indefinitely.

- 8.1. 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.
- 8.2. BRAND HUBB undertakes to ensure that 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.
- 8.3. BRAND HUBB will ensure that all paper documents that should be disposed of, be shredded locally and then be recycled.
- 8.4. 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 this policy and any other applicable legislation.
- 8.5. BRAND HUBB may suspend the destruction of any record or document due to pending or reasonably foreseeable litigation, audits, government investigations or similar proceedings. BRAND HUBB undertakes to notify employees of applicable documents where the destruction has been suspended to which they have access to.

- 8.6. 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.
- 8.7. The Information Officer should be consulted where there is uncertainty regarding the retention and destruction of a document and/or information.

9. INTERNET AND CYBER TECHNOLOGY

The following clauses constitute a summary of the terms contained in the INTERNAL IT/EMAIL/CYBER SECURITY POLICY which applies to all employees when using the BRAND HUBB internet and email services.

9.1. Acceptable use of BRAND HUBB's Internet Facilities & standard Anti-Virus rules

The repercussions of misuse of BRAND HUBB 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 BRAND HUBB's IT systems are not misused, everyone who uses or has access to BRAND HUBB's systems have received training and internal guidelines in order to meet the following five high-level IT Security requirements:

- 9.1.1. Information will be protected against any unauthorized access as far as possible;
- 9.1.2. Confidentiality of information will be assured as far as possible;
- 9.1.3. Integrity of information will be preserved as far as possible;
- 9.1.4. Availability of information for business processes will be maintained;
- 9.1.5. Compliance with applicable laws and regulations to which BRAND HUBB is subject will be ensured by the Information Officer as far as possible.

Every user of BRAND HUBB's IT systems takes responsible for exercising good judgment regarding reasonable personal use.

9.2. IT Access Control

BRAND HUBB undertakes 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 is a further undertaking 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).

9.3. BRAND HUBB's Email Rules

BRAND HUBB acknowledges that most of its communications are conducted via email and instant messaging (IM). Given that email and IM may contain extremely sensitive and confidential FIRM information, the information involved must be appropriately protected. In addition, email and IM are potentially sources of spam, social engineering attacks and malware, so BRAND HUBB must be protected as completely as possible from these threats. The misuse of email and IM can post many legal, privacy and security risks, so it is important for users to be aware of the appropriate use of electronic communications.

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

- 9.3.1. 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.
- 9.3.2. Send, receive, solicit, print, copy, or reply to messages that are disparaging or defamatory.
- 9.3.3. Spread gossip, rumours, or innuendos about employees, clients, suppliers, or other outside parties.
- 9.3.4. Send, receive, solicit, print, copy, or reply to sexually oriented messages or images.
- 9.3.5. Send, receive, solicit, print, copy, or reply to messages or images that contain foul, obscene, disrespectful, or adult-oriented language.
- 9.3.6. Send, receive, solicit, print, copy, or reply to messages or images that are intended to alarm others, embarrass BRAND HUBB negatively impact productivity, or harm morale.

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

9.4. BRAND HUBB'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. This

policy outlines BRAND HUBB'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.

- 9.4.1. BRAND HUBB's users of handheld devices are expected to diligently protect their devices from loss and disclosure of private information belonging to or maintained by BRAND HUBB.
- 9.4.2. In the event of a security incident or if suspicion exists that the security of BRAND HUBB's systems has been breached, BRAND HUBB shall be obliged to notify the IT support immediately together with the Information Officer or Deputy Information Officer should the Information Officer not be available especially when a mobile device may have been lost or stolen.

9.5. **Anti-virus rules**

- 9.5.1. Management of BRAND HUBB 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 BRAND HUBB's programs (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited.
- 9.5.2. It is worth noting that users are discouraged from attempting to remove viruses themselves. If a virus infection is detected, users are expected to disconnect from BRAND HUBB's networks, stop using the infected computer immediately and notify the IT support.
- 9.5.3. It is further worth noting that BRAND HUBB'S users are encouraged to be cautious of e-mail attachments from an unknown source as viruses are often hidden in attachments and BRAND HUBB 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.

9.6. **Physical access control**

- 9.6.1. All of BRAND HUBB'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.

9.7. **Usage Data**

Usage Data Usage Data is collected automatically when using the internet services of BRAND HUBB. 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 BRAND HUBB'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 BRAND HUBB by or through a mobile device, BRAND HUBB 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. BRAND HUBB may also collect information that the user's browser sends whenever BRAND HUBB's website is visited.

9.8. **Tracking Technologies and Cookies**

Cookies and similar tracking technologies are used to track the activity on BRAND HUBB's website 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:

- 9.8.1. 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 BRAND HUBB's website is not accepted, data subjects may not be able to use some parts of the website. Unless the browser settings have been adjusted BRAND HUBB's website may use Cookies.
- 9.8.2. 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>;
- 9.8.3. 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 BRAND HUBB 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).

9.8.4. 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.

9.9. **BRAND HUBB'S website**

Data subjects who use the BRAND HUBB website will be subject to the general website terms and conditions available on the website landing page. Customers who register on the BRAND HUBB online platforms confirm that they have read through and understand the terms and conditions associated with the usage of the website.

10. **THIRD PARTY OPERATORS**

BRAND HUBB recognizes that, in fulfilling its service offering to its customer base and in order to operate efficiently, it is necessary at times to share data subjects' personal and special personal information with third parties for specific reasons related to BRAND HUBB's service delivery. As referenced in clauses 5 and 6 above, BRAND HUBB will obtain the necessary Consent where required from the particular data subject.

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

11. **BANKING DETAILS**

When orders are placed, customers have a choice of payment methods available to them for payment of their order/s via EFT, debit/credit card payments or paygate options such as Payfast, PayU, Payflex, Walletdoc. Customers are subject to the terms and conditions related to their personal and special personal information which they complete on these payment platforms of such platform suppliers and cannot hold BRAND HUBB liable for a data breach which may occur on any one of these payment platforms.

12. **DIRECT MARKETING**

BRAND HUBB is 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 BRAND HUBB with such third party in the fulfilment of its legal services, BRAND HUBB takes no responsibility for any consequences suffered by the data subject which may have been caused by the third party's actions.

BRAND HUBB sends out regular bulk emails to its database of existing customers. These bulk emails contain new product offerings and other relevant information related to the BRAND HUBB service. These bulk emails will always contain the required OPTING OUT/UNSUBSCRIBE options which allow the recipients of the emails to request a removal of their details from these bulk emails.

13. **DATA CLASSIFICATION**

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

- 13.1. Managers of BRAND HUBB shall be responsible for assigning classifications to information assets according to the standard information classification system presented below.
- 13.2. Where practicable, the information category shall be embedded in the information itself.
- 13.3. All employees of BRAND HUBB shall be guided by the information category in their security-related handling of BRAND HUBB's information. All information of BRAND HUBB and all information entrusted to BRAND HUBB 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 BRAND HUBB	Product brochures widely distributed ☐ Information widely available in the public domain, including publicly available web site areas of BRAND HUBB Sample downloads of BRAND HUBB' 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 BRAND HUBB' 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 BRAND HUBB' activities All software codes developed by BRAND HUBB , whether used internally or sold to clients
Client Confidential Data	Information collected and used by BRAND HUBB in the conduct of its business to employ people, to log and fulfil client mandates, and to manage all aspects of corporate finance. Access to this information is very restricted within BRAND HUBB. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	Salaries and other personnel data Accounting data and internal financial reports Confidential customer business data and confidential contracts Non-disclosure agreements with clients\vendors Company business plans

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

- 14.1. 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.
- 14.2. A data subject may object, at any time, to the processing of personal information– a) In writing, on reasonable grounds relating to his, her or its particular situation, unless legislation provides for such processing; or b) For purposes of direct marketing other than direct marketing by means of unsolicited electronic communications.
- 14.3. A data subject, having provided adequate proof of identity, has the right to – a) Request BRAND HUBB to confirm, free of charge, whether or not BRAND HUBB holds personal information about the data subject; and b) Request from BRAND HUBB a record or a description of the personal information about the data subject held by BRAND HUBB, 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.
- 14.4. A data subject may, in the prescribed manner, request BRAND HUBB to – a) 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 b) destroy or delete a record of personal information about the data subject that BRAND HUBB is no longer authorised to retain.
- 14.5. Upon receipt of a request referred to in clause 14.4, BRAND HUBB will, as soon as reasonably practicable – a) correct the information; b) destroy or delete the information; c) provide the data subject, to his, her or its satisfaction, with credible evidence in support of the information; or d) where an agreement cannot be reached between BRAND HUBB 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.
- 14.6. BRAND HUBB 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.

15. COVID 19

BRAND HUBB has implemented and continues 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, BRAND HUBB is and will remain entitled to oblige employees and other visitors to complete a Covid 19 Risk Assessment form upon entering the BRAND

HUBB offices 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. BRAND HUBB 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. BRAND HUBB's delivery service providers will follow their own Covid 19 protocols when making delivery of an order and BRAND HUBB will not be liable for implementation and enforcement of such third party measures.

With the implementation of the BRAND HUBB Workplace Vaccination program, further employee and other relevant data subjects' personal and medical information may be collected and processed by BRAND HUBB and may be shared with Regulated third parties and internally if the sharing of the information complies with the provisions for the BRAND HUBB Vaccination program Policies.

16. INFORMATION OFFICER

16.1. Appointed Information Officer:

INFORMATION OFFICER: **JD O'Connor**

Contact details 083 456 7671 / 010 020 8600

Email jd@brandhubb.com

Postal Address: PO Box 2295, Sunninghill, 2157

Street Address: The District Office Park, 8 Kikuyu Road, Sunninghill, 2191

DEPUTY INFORMATION OFFICERS: Charne Luayne Gibson

Contact details 010 020 8600

Email charne@brandhubb.com

Postal Address: PO Box 2295, Sunninghill, 2157

Street Address: The District Office Park, 8 Kikuyu Road, Sunninghill, 2191

16.2. The general responsibilities of BRAND HUBB's Information Officer and Deputy Information Officer/s where delegated include the following:

- 16.2.1. The encouragement of compliance, by BRAND HUBB, with the conditions for the lawful processing of personal information;
- 16.2.2. Managing requests made to BRAND HUBB pursuant to POPIA;
- 16.2.3. 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.
- 16.2.4. Continuously perform data backups, store at least weekly backup offsite, and test those backups regularly for data integrity and reliability.
- 16.2.5. Review policy rules regularly, document the results, and update the policy as needed.
- 16.2.6. Continuously update information security policies and network diagrams.
- 16.2.7. Secure critical applications and data by patching known vulnerabilities with the latest fixes or software updates.
- 16.2.8. Perform continuous computer vulnerability assessments and audits

16.3. The data breach responsibilities of BRAND HUBB's Information Officer and Deputy Information Officer/s where delegated include the following:

- 16.3.1. Ascertain whether personal data was breached;
- 16.3.2. Assess the scope and impact by referring to the following:
 - 16.3.2.1. Estimated number of data subjects whose personal data was possibly breached
 - 16.3.2.2. Determine the possible types of personal data that were breached
 - 16.3.2.3. List security measures that were already in place to prevent the breach from happening.
- 16.3.3. Once the risk of the breach is determined, the following parties need to be notified within 72 hours after being discovered:
 - 16.3.3.1. The Information Regulator
 - 16.3.3.2. 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.

16.3.4. Review and monitor

16.3.4.1. Once the personal data breach has been contained, BRAND HUBB 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.

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

17. AVAILABILITY AND REVISION

A link to this Policy is made available on BRAND HUBB company website www.brandhubb.com

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) <i>(Please provide detailed reasons for the objection)</i>

Signed at this day of20.....

..... *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 / DESTROYED / 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. <i>(Please provide detailed reasons for the request)</i>

Signed at this day of20.....

.....
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 of20.....

.....*Signature of data subject*

