POPI COMPLIANCE POLICY

1. INTRODUCTION

1.1 This POPI Compliance Policy was prepared in accordance with section 51 of the Promotion of Access to Information Act, 2000 (PAIA) and to address requirements of the Protection of Personal Information Act, 4 of 2013 (POPIA).

1.2 This Protection of Personal Information POPI Compliance Policy integrates the PAIA and POPI Acts into one Compliance Policy, due to the interrelationship of both legislations. The one requires the other to work, which means that we will first address the PAIA and thereafter the POPI.

1.3 This POPI Compliance Policy applies to BATTLE BEAR (PTY) LTD with the company number of 2019/566806/07, hereafter BATTLE BEAR "we", "us", "our" and to the prospective and existing client hereafter, "you", "yours".

2. DEFINITIONS

In this POPI Compliance Policy, the following words bear the meaning set out below:

2.1 ''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;

2.2 "client" means a natural or juristic person in the form of a prospective client who has shown interest in a product or service or an existing client who received a product or service and have provided a name, and contact details to be contacted;

2.3 ''consent'' means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;

2.4 ''data subject'' refers to any person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity;

2.5 ''de-identify'', concerning the personal information of a data subject, means to delete any information that, identifies the data subject; can be used or manipulated by a reasonably foreseeable method to identify the data subject; or can be linked by a reasonably foreseeable method to other information that identifies the data subject, and;

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

2.6.1 promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or

2.6.2 requesting the data subject to make a donation of any kind for any reason;

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

2.8 “employee” means any person who works for or provides services to us, and receives or is entitled to receive remuneration;

2.9 ‘‘filing system’’ means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria;

2.10 ‘‘information matching programme’’ means the comparison, whether manually or using any electronic or other devices, of any document that contains personal information about ten or more data subjects with one or more documents that contain personal information of ten or more data subjects, to produce or verify information that may be used to take any action regarding an identifiable data subject;

2.11 ‘‘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;

2.12 ‘‘person’’ means a natural person or a juristic person;

2.13 ‘‘personal information’’ means information relating to an identifiable, living, natural person, and where it is applicable and identifiable, existing juristic person, including, but not limited to:

2.13.1 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;

2.13.2 information relating to the education or the medical, financial, criminal or employment history of the person;

2.13.3 any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignments to the person;

2.13.4 the biometric information of the person;

2.13.5 the personal opinions, views or preferences of the person;

2.13.6 correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

2.13.7 the views or opinions of another individual about the person; and

2.13.8 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;

2.14 ‘‘private body’’ means:

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

2.14.2 a partnership which carries or has carried on any trade, business or profession; or

2.14.3 any former or existing juristic person, but excludes a public body;

2.15 ‘‘processing’’ means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

2.15.1 the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

2.15.2 dissemination using transmission, distribution or making available in any other form; or

2.15.3 merging, linking, as well as restriction, degradation, erasure or destruction of information;

2.16 ‘‘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;

2.17 ‘‘record’’ means any recorded information, regardless of form or medium, including any of the following:

2.17.1 Writing on any material;

2.17.2 information produced, recorded or stored using any tape-recorder, computer equipment, whether hardware or software or both, or other devices, and any material subsequently derived from information so produced, recorded or stored;

2.17.3 label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

2.17.4 book, map, plan, graph or drawing;

2.17.5 photograph, film, negative, tape or other devices in which one or more visual images are embodied to be capable, with or without the aid of some other equipment, of being reproduced;

2.17.6 in the possession or under the control of a responsible party;

2.17.7 whether or not it was created by a responsible party; and

2.17.8 regardless of when it came into existence;

2.18 ‘‘Regulator’’ means the Information Regulator established in terms of section 39;

2.19 ‘‘re-identify’’, concerning the personal information of a data subject, means to resurrect any de-identified information, that:

2.19.1 identifies the data subject;

2.19.2 can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

2.19.3 can be linked by a reasonably foreseeable method to other information that identifies the data subject and

2.20 "requester" means any person or entity requesting access to a record that is under our control;

2.21 ''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;

2.22 ''unique identifier'' means any identifier that is assigned to a data subject and is used by a responsible party for the operations of that responsible party and that uniquely identifies that data subject concerning that responsible party.

3. OUR UNDERTAKING

3.1 We undertake to follow this POPI Compliance Policy at all relevant times and to process personal information lawfully and reasonably, so as not to infringe unnecessarily on the privacy of our clients.

3.2 We undertake to process information only for the purpose for which it is intended, to enable us to do our work, as agreed with clients.

3.3 Whenever necessary, we shall obtain consent to process personal information.

3.4 Where we do not seek consent, the processing of our client's personal information will be following a legal obligation placed upon us, or to protect a legitimate interest that requires protection.

3.5 We shall stop processing personal information if the required consent is withdrawn, or if a legitimate objection is raised.

3.6 We shall collect personal information directly from the client whose information we require, unless:

3.6.1 the information is a public record, or

3.6.2 the client has consented to the collection of their personal information from another source, or

3.6.3 the collection of the information from another source does not prejudice the client, or

3.6.4 the information to be collected is necessary for the maintenance of law and order or national security, or

3.6.5 the information is being collected to comply with a legal obligation, including an obligation to SARS, or

3.6.6 the information collected is required for the conduct of proceedings in any court or tribunal, where these proceedings have commenced or are reasonably contemplated; or

3.6.7 the information is required to maintain our legitimate interests; or

3.6.8 where requesting consent would prejudice the purpose of the collection of the information; or

3.6.9 where requesting consent is not reasonably practical in the circumstances.

3.7 We shall advise the Client of the purpose of the collection of the personal information.

3.8 We shall retain records of the personal information we have collected for the minimum period as required by law unless the client has provided their consent or instructed us to retain the records for a longer period.

3.9 We shall destroy or delete records of the personal information (to de-identify the client) as soon as reasonably possible after the time period for which we were entitled to hold the records have expired.

3.10 We shall restrict the processing of personal information:

3.10.1 where the accuracy of the information is contested, for a period sufficient to enable us to verify the accuracy of the information;

3.10.2 where the purpose for which the personal information was collected has been achieved and where the personal information is being retained only for proof;

3.10.3 where the client requests that the personal information is not destroyed or deleted, but rather retained; or

3.10.4 where the client request that the personal information is not be transmitted to another automated data processing system.

3.11 The further processing of personal information shall only be undertaken:

3.11.1 if the requirements of paragraphs 3.6.1; 3.6.4; 3.6.5 or 3.6.6 above have been met;

3.11.2 where the further processing is necessary because of a threat to public health or public safety or the life or health of the client, or a third person;

3.11.3 where the information is used for historical, statistical or research purposes and the identity of the client will not be disclosed; or

3.11.4 where this is required by the Information Regulator appointed in terms of POPI.

3.12 We undertake to ensure that the personal information which we collect, and the process is complete, accurate, not misleading and up to date.

3.13 We undertake to retain the electronic data related to the processing of personal information.

4. OUR CLIENT'S RIGHTS

4.1 In all cases, we require a client's consent through a web form on our website to provide and process their personal information. This is done based on a statement on a webpage where clients indicate their consent to be contacted, via an email, telephone call or SMS or any other form of electronic communication.

4.2 In cases where we process personal information without consent to protect a legitimate interest, to comply with the law or to pursue or protect our legitimate interests, the client has the right to object to such processing.

4.3 All clients are entitled to complain about our application of the POPIA with the Information Regulator.

5. SECURITY SAFEGUARDS

5.1 To secure the integrity and confidentiality of the personal information in our possession, and to protect it against loss or damage or unauthorised access, we must continue to implement the following security safeguards:

5.1.1 our business premises where records are kept must remain protected by access control, burglar alarms and armed response;

5.1.2 archived files must be stored behind locked doors and access control to these storage facilities must be implemented;

5.1.3 all the user terminals on our internal computer network and our servers are protected by passwords;

5.1.4 our email infrastructure must comply with industry-standard security safeguards, and meet the general data protection regulations;

5.1.5 vulnerability assessments must be carried out on our digital infrastructure at least on an annual basis to identify weaknesses in our systems and to ensure we have adequate security in place;

5.1.6 we must use an internationally recognised firewall;

5.1.7 our staff is trained to carry out their duties in compliance with the POPIA, and this training is ongoing.

5.1.8 it is a term of the contract with every staff member that they must maintain full confidentiality in respect of all of our client's affairs, including our clients' personal information.

5.1.9 employment contracts for staff whose duty it is to process a client's personal information include an obligation on the staff member to:

5.1.9.1 maintain the company's security measures, and to

5.1.9.2 notify the Information Officer immediately if there are reasonable grounds to believe that the personal information of a client has been accessed or acquired by any unauthorised person, by email.

5.1.10 the processing of the personal information of our staff members is taking place under the rules contained in the relevant labour legislation;

5.1.11 the digital work profiles and privileges of staff who have left our employment are properly terminated as required by law;

5.1.12 the personal information of clients and staff are destroyed timeously in a manner that de-identifies the person.

5.2 These security safeguards are verified regularly to ensure effective implementation, and these safeguards are continually updated in response to new risks or deficiencies.

6. SECURITY BREACHES

6.1 Should it appear that the personal information of a client has been accessed or acquired by an unauthorised person, we will notify the Information Regulator and the relevant clients, unless we are no longer able to identify the clients. This notification must take place as soon as reasonably possible.

6.2 Such notification must be given to the Information Regulator first as it is possible that they, or another public body, might require the notification to the client/s be delayed.

6.3 The notification to the client must be communicated in writing in one of the following ways, to ensure that the notification reaches the client:

6.3.1 by email to the client's last known email address;

6.3.2 by publication on our website or in the news media; or

6.3.3 as directed by the Information Regulator.

6.4 This notification to the client must give sufficient information to enable the client to protect themselves against the potential consequences of the security breach, and must include:

6.4.1 a description of the possible consequences of the breach;

6.4.2 details of the measures that we intend to take or have taken to address the breach;

6.4.3 the recommendation of what the client could do to mitigate the adverse effects of the breach; and

6.4.4 if known, the identity of the person who may have accessed, or acquired the personal information.

7. RECORDS AVAILABLE WITHOUT A REQUEST

7.1 Records of a public nature, typically those disclosed on our website, maybe accessed without the need to submit a formal application.

7.2 Other non-confidential records, such as statutory records maintained at CIPC, may also be accessed without the need to submit a formal application.

8. RECORDS AVAILABLE ONLY ON REQUEST

8.1 This section provides more information of records available only on request to access basis in terms of the PAIA section 51(1) (e).

8.2 Note that the accessibility of the records may be subject to the grounds of refusal set out in section 10 of this POPI Compliance Policy. Amongst other, records deemed confidential on the part of a third party will require permission from the third party concerned, in addition to normal requirements, before we will consider access.

8.3 The records are classified and grouped as follows:

Category	Records
Companies Act Records	• Documents of Incorporation • Memorandum of Incorporation • Minutes of meetings of the Board of Directors • Register of directors' shareholdings • Share certificates • Special resolutions/Resolutions passed • Records relating to the appointment of, Auditors and Company Secretary
Financial Records	• Accounting Records • Annual Financial Reports • Annual Financial Statements • Asset Registers • Bank Statements • Banking details and bank accounts
Personnel documents & records	• Job descriptions • Training Records
Procurement records	• Terms and Conditions • Contractor, client, and supplier agreements • Policies and Procedures
Marketing and sales records	• Marketing & sales records • Lead and customers records • Client transactional records • Client and lead email correspondence • Client training records • Client databases
Information technology records	• Information technology systems and user manuals • Software licensing • System documentation and manuals

9. METHOD OF REQUESTING RECORDS

9.1 On provision of proof of identity, a client is entitled to request that we confirm, free of charge, whether or not we hold any personal information about a client in our records.

9.2 If we hold such personal information, on request, and upon payment of a fee of R 550-00 plus VAT, we shall provide the client with the record, or a description of the personal information, including information about the identity of all third parties or categories of third parties who have or have had access to the information. We shall do this within a reasonable time, in a reasonable manner and understandable format.

9.3 A client requesting such personal information must be advised of their right to request to have any errors in the personal information corrected, which request shall be made on the prescribed application form. Use FORM 1 in Section 21.

9.4 In certain circumstances, we will be obliged to refuse to disclose the record containing the personal information to the client. In other circumstances, we will have discretion as to whether or not to do so.

9.5 In all cases where the disclosure of a record will entail the disclosure of information that is additional to the personal information of the client requesting the record, the written consent of the Information Officer will be required, and that person shall make their decision having regard to the provisions of Chapter 4 of Part 3 of the Promotion of Access to Information Act (PAIA).

9.6 If a request for personal information is made and part of the requested information may, or must be refused, every other part must still be disclosed.

10. REFUSAL OF ACCESS TO RECORDS

10.1 We are entitled to refuse a request for information.

10.2 The main grounds we could refuse a request for information relates to the:

10.2.1 mandatory protection of the privacy of a third party who is a natural person or a deceased person (section 63) or a juristic person, as included in the Protection of Personal Information Act 4 of 2013, which would involve the unreasonable disclosure of personal information of that natural or juristic person;

10.2.2 mandatory protection of personal information and for disclosure of any personal information to, in addition to any other legislative, regulatory, or contractual agreements, comply with the provisions of the Protection of Personal Information Act 4 of 2013;

10.2.3 mandatory protection of the commercial information of a third party in terms of section 64 if the record contains:

- trade secrets of the third party;

- financial, commercial, scientific, or technical information which disclosure could likely cause harm to the financial or commercial interests of that third party;
- information disclosed in confidence by a third party to us, if the disclosure could put that third party at a disadvantage in negotiations or commercial competition;
- mandatory protection of confidential information of third parties in terms of section 65, if it is protected in terms of any agreement;
- mandatory protection of the safety of individuals and the protection of property in terms of section 66;
- mandatory protection of records that would be regarded as privileged in legal proceedings in terms of section 67.

10.3 Our commercial activities in terms of section 68, may include:

- our trade secrets;
- our financial, commercial, scientific, or technical information which disclosure could likely cause harm to the financial or commercial interests of our company;
- the information which, if disclosed could put our company at a disadvantage in negotiations or commercial competition;
- a computer program which is owned by us, and which is protected by copyright;
- the research information in terms of section 69 of our company or a third party, if its disclosure would disclose the identity of our researchers, marketers or the subject matter of the research and would place the research at a serious disadvantage.

10.4 Requests for information that are silly or annoying, or which involve an unreasonable diversion of resources shall be refused.

10.5 All requests for information will be assessed on their own merits and per the applicable legal principles and legislation.

10.6 If a requested record cannot be found or if the record does not exist, the Information Officer shall, by way of an affidavit or affirmation, notify the requester that it is not possible to give access to the requested record. Such notice will be regarded as a decision to refuse a request for access to the record concerned for the purpose of the PAIA. If the record should later be found, the requester shall be given access to the record in the manner stipulated by the requester in the prescribed form, unless the Information Officer refuses access to such record.

11. THE CORRECTION OF PERSONAL INFORMATION

11.1 A client is entitled to require us to correct or delete personal information that we have, which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or which has been obtained unlawfully.

11.2 A client is also entitled to require us to destroy or delete records of personal information about the client that we are no longer authorised to retain.

11.3 Any such request must be made on the prescribed FORM 3 in Section 21.

11.4 Upon receipt of such a lawful request, we must comply as soon as reasonably practicable.

11.5 If a dispute arises regarding the client's rights to have the information corrected, and if the client so requires, we must attach to the information, in a way that it will always be read with the information, an indication that the correction of the information has been requested but has not been made, and a reason why it was not corrected.

11.6 We must notify the client who has made a request for their personal information to be corrected or deleted what action we have taken as a result of such a request.

12. SPECIAL PERSONAL INFORMATION

12.1 The Personal Information provided initially by you may consist of your first name, last name and email address. You may need to provide additional information later during a consultation session.

12.2 As mentioned above, BATTLE BEAR may be provided with additional information that could be regarded as Special Personal Information either through our Website or the consultation session.

12.3 Special information includes religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health, sex life, biometric information, or criminal behaviour. BATTLE BEAR limits access to this type of information and do have policies and procedures in place designed to safeguard the information.

12.4 We do not collect any unnecessary personal data from you and do not process your information in any way, other than as specified in this Privacy Policy.

12.5 You may object to us processing your information by using this FORM 2 in Section 21.

13. THE PROCESSING OF PERSONAL INFORMATION OF CHILDREN

13.1 The Website is not intended for children 18 years and younger, and BATTLE BEAR does not intentionally collect or maintain personal information about any person under this age.

14. CIRCUMSTANCES REQUIRING PRIOR AUTHORISATION

14.1 In the following circumstances, we will require prior authorisation from the Information Regulator before processing any personal information:

14.1.1 In the event that we intend to utilise any unique identifiers of clients (account numbers, file numbers or other numbers or codes allocated to clients to identify them in our business) for any purpose other than the original intention, or to link the information with information held by others;

14.1.2 if we are processing information on criminal behaviour or unlawful or objectionable conduct;

14.2 The Information Regulator must be notified of our intention to process any personal information as set out in par. 14.1 above before any processing taking place and we may not commence with such processing until the Information Regulator has decided in our favour. The Information Regulator has 4 weeks to decide but may decide that a more detailed investigation is required.

14.3 In this event, the decision must be made in a period as indicated by the Information Regulator, which must not exceed 13 weeks. If the Information Regulator does not decide within the stipulated time periods, we can assume that the decision is in our favour and commence processing the information.

15. DIRECT MARKETING

15.1 We may only carry out direct marketing (using any form of electronic communication) to clients if:

15.1.1 they were allowed to object to receiving direct marketing material by electronic communication at the time that their personal information was collected; and

15.1.2 they did not object then or at any time after receiving any such direct marketing communications from us.

15.2 We may only approach clients using their personal information, if we have obtained their personal information in the context of providing services associated with our marketing efforts to them, and we may then only market program information or coaching services to them.

15.3 We may only carry out direct marketing (using any form of electronic communication) to other people if we have received their consent to do so.

15.4 We may approach a person to ask for their consent to receive direct marketing material only once, and we may not do so if they have previously refused their consent, using FORM 5 in Section 21.

15.5 A request for consent to receive direct marketing must be made in the applicable Web Form and our Contact Page on the Website or the prescribed hard copy form, see FORM 8 and FORM 9 in Section 21.

15.6 All direct marketing communications must disclose our identity and contain an address or other contact details to which the client may send a request that the communications cease.

15.7 All emails communications have the option to unsubscribe at the footer of the email.

16. TRANSBORDER INFORMATION FLOWS

16.1 We may not transfer a client's personal information to a third party in a foreign country, unless:

16.1.1 the client consents to this, or requests it; or

16.1.2 such third party is subject to a law, binding corporate rules or a binding agreement which protects the personal information in a manner similar to POPI, and such third party is governed by similar rules which prohibit the onward transfer of the personal information to a third party in another country;

16.1.3 or the transfer of the personal information is required for the performance of the contract between us and the client; or

16.1.4 the transfer is necessary for the conclusion or performance of a service for the benefit of the client entered into between us and the third party; or

16.1.5 the transfer of the personal information is for the benefit of the client, and it is not reasonably possible to obtain their consent and that if it were possible the client would be likely to give such consent.

16.1.6 The Client can also be requested to complete FORM 4 in Section 21, where the Web Form was not completed for whatever reason.

17. OFFENCES AND PENALTIES

17.1 The POPIA provides for serious penalties for the contravention of its terms. For minor offences, a guilty party can receive a fine or be imprisoned for up to 12 months. For serious offences, the period of imprisonment rises to a maximum of 10 years. Administrative fines for the company can reach a maximum of R10 million.

17.2 Breaches of this POPI Compliance Policy will also be viewed as a serious disciplinary offence.

17.3 It is therefore imperative that we comply strictly with the terms of this POPI Compliance Policy and protect our client's personal information in the same way as if it was our own.

18. INFORMATION OFFICER

18.1 Our Managing Director has appointed and authorised Cameryn Gardner as Information Officer to oversee the application of the PAIA and POPIA within our company. Such designation is done by the completion of the prescribed form, see FORM 6 Section 21. Our

18.2 Information Officer's responsibilities include:

18.2.1 Ensuring compliance with this POPI Compliance Policy and with the POPIA.

18.2.2 Dealing with requests which we receive in terms of POPI.

18.2.3 Working with the Information Regulator concerning investigations.

18.3 Our Information Officer must register with the Information Regulator before taking up their duties, see FORM 7 in Section 21.

18.4 In carrying out their duties, our Information Officer must ensure that:

18.4.1 this POPI Compliance Policy is implemented;

18.4.2 a Personal Information Impact Assessment is done to ensure that adequate measures and standards exist to comply with the conditions for the lawful processing of personal information;

18.4.3 that this POPI Compliance Policy is developed, monitored, maintained and made available;

18.4.4 that internal measures are developed together with adequate systems to process requests for information or access to information;

18.4.5 that internal awareness sessions are conducted regarding the provisions of POPI, the Regulations, codes of conduct or information obtained from the Information Regulator; and

18.4.6 that copies of this POPI Compliance Policy are provided to persons at their request, hard copies to be provided upon payment of a fee (to be determined by the Information Regulator).

18.4.7 Guidance notes on Information Officers have been published by the Information Regulator and our Information Officer is familiar with the content of these notes.

18.5 Contact Details of BATTLE BEAR Information Officer.

Managing Director	Mr Cameryn Gardner
Registered Address	13A Oxford Road, Bedford Gardens, Gauteng
Email Address	admin@battlebearmarketing.com
Telephone	
Website	https:\\battlebearmarketing.com\contact\

19. HUMAN RIGHTS COMMISSION

This section provides more information about the Guide of SA Human Rights Commission in terms of section 51(1) (b))

19.1 The PAIA grants a requester access to records of a private body, if the record is required for the exercise or protection of any rights. If a public body lodges a request, the public body must be acting in the public interest.

19.2 Requests in terms of the PAIA shall be made in accordance with the prescribed procedures, at the rates provided.

19.3 Requesters are referred to the Guide in terms of Section 10 which has been compiled by the South African Human Rights Commission, which will contain information for the purposes of exercising Constitutional Rights. The Guide is available from the SAHRC.

The contact details of the Commission are:

Contact Body	The South African Human Rights Commission
Registered Address	PAIA Unit, 29 Princess of Wales Terrace, Cnr York and Andrew, Streets, Parktown
Postal Address	Private Bag 2700, Houghton 2041
Email Address	PAIA@sahrc.org.za
Telephone	+27 11 877 3600
Website	www.sahrc.org.za

20. CONTACT US

If there are any questions about this policy, please contact BATTLE BEAR by using our "Contact Us" page or contact our Information Officer directly for support.

Our address is 13A Oxford Road, Bedford Gardens, Gauteng.

21. SCHEDULE OF ANNEXURES AND FORMS

If you need access to any of the forms, please click on the link and download form, and follow the procedure as described above. Once the form is completed, please upload the completed form on our contact page or email it to admin@battlebearmarketing.co.za in a PDF format duly signed.

21.1 Form 1 – Request for Access to Records

21.2 Form 2 – Objections to Processing Information

21.3 Form 3 - Request for Correction or Deletion of Personal Information

21.4 Form 4 – Consent to Process Personal Information

21.5 Form 5 - Consent for Direct Marketing

21.6 Form 6 - Designation of the Information Officer

21.7 Form 7 – Duties of the Information Officer

21.8 Form 8 Advertise my Business – Web Form

21.9 Form 9 – Contact Us – Web Form