

DATA PROTECTION POLICY

1. INTRODUCTION

1.1 The Protection of Personal Information Act, 4 of 2013 (POPIA), is a law, which regulates the processing of Personal Information, which is owned by persons and legal entities, known as Data Subjects, in and outside South Africa.

1.2 POPIA, inter alia, requires that the person who is processing a Data Subject's Personal Information, known as a Responsible Party, complies with certain data privacy principles and conditions, including:

1.2.1 obtaining consent to use a Data Subject's Personal Information;

1.2.2 informing a Data Subject why one requires the use of the Data Subject's Personal Information and the parties who the Responsible Party will be sharing such Personal Information with;

1.2.3 the responsible and secure use, dissemination and storage of Personal Information, which use must at all times be purpose specific; and

1.2.4 ensuring the permanent destruction of a Data Subject's Personal Information once the purpose for which the Personal Information was required has come to an end, subject to any legal retention periods.

1.3 In order to perform our operations we process Personal Information on a regular basis.

1.4 We as a Responsible Party are obligated to comply with the provisions of POPIA and to this end must ensure that mechanisms and processes are in place for the lawful processing of Personal Information.

1.5 We have developed a Personal Data Privacy Policy which sets out how all directors, employees, and where applicable its representatives, agents, vendors, customers, clients and / or service providers must lawfully process a Data Subject's Personal Information, the provisions of which policy is are set out hereunder.

2. DEFINITIONS

2.1 The following words and or phrases shall bear the corresponding meanings as assigned to them, unless the context where the word or phrase is used indicates a contrary meaning:

2.1.1 "The Vendor" means the proprietor as described on the "Home" / "Landing" page of this website ("the vendor"). Any reference to "we", "our" or "us" includes, the employees of the proprietor's employees, officers, directors, representatives, agents, shareholders, affiliates, subsidiaries, holding companies, related entities, advisers, sub-contractors, service providers, successors, assigns and suppliers.;

2.1.3 "The Confidential Policy" means the Confidentiality Policy and Protocol;

2.1.4 "The Personal Data Policy" means the Personal Data Protection Policy and Protocol set out hereunder;

2.1.5 "Consent" means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of Personal Information;

2.1.6 "Contractors" means any representatives, agents, contractors, subcontractors, service providers, suppliers and / or vendors who perform for or carry out work or services for or on behalf of the Vendor;

2.1.7 "Data Subject" means the person to whom the Personal Information relates, who owns and will provide the Vendor or its Operator (s) with its Personal Information;

2.1.9 "employee(s)" means a person employed by the Vendor, including fixed term and part time employees;

2.1.10 "Operator" means a natural person or a juristic person who processes a Data Subject's Personal Information on behalf of the Vendor in terms of a contract or mandate, without coming under the direct authority of the Vendor;

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

2.1.12 "Personal Information" means information relating to any identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, namely the a person or entity whose Personal Information is being processed, (Data Subject), including, but not limited to (a)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; (b)information relating to the education or the medical, financial, criminal or employment history of the person; (c)any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; (d)the biometric information of the person; (e)the personal opinions, views or preferences of the person; (f)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; (g)the views or opinions of another individual about the person; and (h) 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;

2.1.13 "process / 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; (d)sharing with, transfer and further processing, to and with such information.

2.1.14 "POPIA" refers to the Protection of Personal Information Act (No 4 of 2013);

2.1.15 "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; (c)whether or not it was created by a responsible party; and (d)regardless of when it came into existence;

2.1.16 "Responsible Party" means the party who is to process a Data Subject's Personal Information.

3. PURPOSE AND OBJECTIVES

3.1 The purpose of the Personal Data Policy is to describe the provisions which apply to the Personal Information which the Vendor processes from time to time and to set out how the Vendor's directors, employees and / or the Professionals are to process Personal Information when operating in the Vendor's environment.

3.2 The primary objectives of the Personal Data Policy are to provide standards, guidelines and useful instruments on how Personal Information is to be processed, safeguarded and protected, as is required under POPIA.

3.3 The Personal Data Policy includes, on the one side, the rights on data protection that must be respected by the Vendor and, on the other side, the legal guidelines that must be followed by it in relation to the protection of Personal Information which it will process from time to time.

4. SCOPE AND APPLICATION

4.1 Internally

4.1.1 The requirements outlined in the Personal Data Policy apply to all the Vendor's directors and employees regardless of their hierarchical position within the organization or their professional qualification.

4.1.2 All the Vendor's directors and employees are prohibited from processing Personal Information other than in terms of the principles, standards and procedures set out and prescribed under the Personal Data Policy.

4.2 Externally

4.2.1 The requirements outlined in this Personal Data Policy apply to all Contractors who the Vendor's directors and its employees may engage with from time to time.

4.2.2 In order to give effect to the principles of the Personal Data Policy, the Vendor will ensure that the contents of this policy are included and referenced in

all trading documents which the Vendor may provide to, or exchange with the Contractors.

4.2.3 In accordance with the Vendor's professional obligation to act in the best interest of the company and all Professionals are prohibited from using or dealing with another's Personal Information, directly or indirectly, other than in terms of the principles, standards and procedures set out and prescribed under the Personal Data Policy.

5. POPIA PROCESSING CONDITIONS AND RELATED CONTROLS

5.1 General undertaking to comply with processing conditions

5.1.1 The Vendor's Professionals do, and will on an ongoing basis, process Personal Information, which belongs to Data Subjects.

5.1.2. In order to comply with the provisions of POPIA read with the processing conditions found thereunder, the Vendor as an accountable and Responsible Party has implemented and will maintain the POPIA processing controls and procedures detailed below, which without exception, will apply to the Vendor's Professionals when they process Personal Information.

5.2 Accountability

5.2.1 The Vendor will remain the Responsible Party for all Personal Information processed under its control and authority, even where an Operator on behalf of the Vendor processes such Personal Information.

5.2.2 For the purposes of ensuring compliance with POPIA and the Personal Data Policy, the Vendor has:

5.2.2.1 established and implemented a privacy governance structure and a formal privacy reporting structure;

5.2.2.2 defined and embedded within their organization, data privacy roles and responsibilities to give effect to and implement the aforementioned privacy structures and related processes;

5.2.2.3 appointed an Information Officer (IO) which position will be responsible for addressing all privacy related queries, including queries relating to POPIA, it's processing activities and the Personal Data Policy;

5.2.2.4 established a formal data privacy training awareness programme which training is presented to all the Vendor's directors and employees and which training will form part of the induction training programme.

5.3 Lawfulness of Processing

5.3.1 The Vendor will ensure that:

5.3.1.1 Personal Information is processed in a lawful manner, which does not unlawfully infringe upon the rights of Data Subjects;

5.3.1.2 processing of Personal Information will not be excessive;

5.3.1.3 only adequate and required Personal Information will be collected from a Data Subject, which will thereafter only be used by the Vendor for the required and stated purpose;

5.3.1.4 Personal Information is processed only with the necessary consent of the Data Subject, save where no consent is required as per the provisions of POPIA, and the Vendor has a legitimate business requirement to process such Personal Information;

5.3.1.5 where for whatsoever reason, consent from the Data Subject which is required as per POPIA, is not received, then the person processing the Personal Information will consult with the Information Officer to determine if such Personal Information can be processed;

5.3.1.6 a valid justification for the processing of Personal Information will be provided to all Data Subjects;

5.3.1.7 where a Data Subject objects to the processing of his or her Personal Information, the Vendor will, subject to the provisions of POPIA, stop processing the Personal Information, unless it is lawfully required to do so in terms of legislation or for legitimate business purposes;

5.3.1.8 all Data Subjects will be informed of their respective rights to data privacy as per the provisions of POPIA and their corresponding right to ask for any Personal Information which the Vendor may have of theirs, their right to update such information and the right to object to the processing of their Personal Information and the consequences of such objection; and

5.3.1.9 other than within the lawful exceptions defined by POPIA, Personal Information will be collected directly from a Data Subject.

5.4 Purpose specification

5.4.1 The Vendor will ensure that:

5.4.1.1 all Personal Information processed by it will be processed for a specific, explicitly defined and lawful purpose related to a function, operational or business activity of the Vendor;

5.4.4.2 all Data Subjects whose Personal Information is collected and processed, will be made aware of the purpose of the collection and processing of their Personal Information, under the Vendor's standards section 18 informed consent documentation.

5.5 Further processing limitation

5.5.1 The Vendor will ensure that:

5.5.1.1 further processing of a Data Subject's Personal Information will only be permitted if this processing is compatible with the original purpose of collection and processing;

5.5.1.2 prior to any further processing, a Further Information Processing Assessment (FIPA) will be performed by the Information Officer or its deputy to assess whether further processing of Personal Information is compatible with the original purpose of collection and processing;

5.5.1.3 if Personal Information is to be used for further processing, that the affected Data Subjects will be informed of such further processing and where applicable, will be asked to provide their consent for such further processing.

5.6 Information Quality

5.6.1 The Vendor will ensure that:

5.6.1.1 all Personal Information held by it, is complete, accurate, and not misleading;

5.6.1.2 all Data Subjects will be given the opportunity to update and correct their Personal Information, which is processed by the Vendor, on a regular basis.

5.7 Openness

5.7.1 The Vendor will ensure that:

5.7.1.1 before it processes any Data Subject's Personal Information, it will provide the Data Subject with a detailed processing notice, known as a section 18 notice, which notice sets out why the Personal Information and the related processing thereof is required, how the Personal Information will be used, who it will be shared with, and how it will be stored and destroyed once the purpose for the processing has come to an end;

5.7.1.2 the PAIA Manual includes details of all of the Vendor's processing operations with regard to Personal Information.

5.8. Processing of Personal Information

5.8.1. Following the above and in order to operate its business and achieve its objectives, including achieving its operation and commercial, legal and contractual obligations, the Vendor will:

5.8.1.1 process Personal Information of employees and where applicable, Personal Information of employee relatives, dependants or acquaintances;

5.8.1.2 process Personal Information of the Vendor's representatives, public officials, agents, vendors, contractors, subcontractors, service providers and where applicable, Personal Information of the owners, shareholders or directors of the aforementioned;

5.8.1.3 process Personal Information of customers or clients, including potential customers and clients and where applicable, Personal Information of the owners of the customers or clients, their clients and / or family members and acquaintances;

5.8.1.4 process Personal Information of third parties;

5.8.1.5 share some of the above-mentioned Personal Information, depending on the purpose for which it was collected with the Vendor's representatives, public officials, agents, vendors, contractors, subcontractors, and customers / clients;

5.8.1.6 send some of the abovementioned Personal Information, depending on the purpose for which it was collected, across South African borders, which sharing includes:

(a) sending the Personal Information to centralized platforms and other company affiliates;

(b) making use of Cloud Computing Solutions which may entail the processing and cross-border transfer of some of the abovementioned Personal Information, depending on the purpose for which it was processed.

5.8.2 Where the Vendor receives Personal Information from a Data Subject that belongs to another, the Data Subject providing the said Personal Information must have permission from the owner thereof to provide to the Vendor the said Personal Information, and any employee processing said information must ensure that this consent is in place.

5.8.3 All Personal Information provided to the Vendor by a Data Subject will only be processed for the purposes as stated in the applicable section 18 POPIA informed consent notice.

5.8.4 The Vendor regularly hosts internal and external marketing and related events which are attended by directors, employees, representatives, public officials, agents, vendors, contractors, subcontractors, and customers / clients,

(hereinafter referred to as “attendees”) where photographs and video footage may be taken and attendees may be interviewed or requested to submit information, comments or opinions. In addition, the Vendor publishes or causes to be published articles, photographs, video footage, comments, information, opinions and interviews involving Data Subjects in their publications as well as external media publications and platforms, both locally and internationally. These photographs, video footage, comments and personal interviews constitute Personal Information. Following this all persons who attend these events and / or submit to photographs or video footage and agree to give interviews, comments and opinions must, prior to engaging with the Vendor to give their consent for the use and publication of their Personal Information.

5.8.5 All of the processing referred to under clause 5.8.1- 5.8.4 above, must without exception be done in accordance with:

- this Policy;
- the standard and applicable section 18 POPIA informed consent notices;
- any related POPIA guidelines and procedures as well as any applicable laws on data privacy;

5.9 Processing of Personal Information by the Vendor’s Operators

5.9.1 In order to operate its business and achieve its objectives, including achieving its legal and contractual obligations, the Vendor will from time to time ask other parties to process Personal Information on its behalf, including without detracting from the generality thereof:

- Pension / provident fund and medical aid administrators;
- Employment agencies;
- Regulators such as the National Credit Regulator, Consumer Commission, and the Department of Labour;
- Advertising and Promotional Agencies;
- IT Service providers; and
- Credit Bureau,

(hereinafter referred to as an “Operator”)

5.9.2 Where the Vendor receives Personal Information from a Data Subject that is to be processed on its behalf by an Operator, the Vendor must ensure that the Data Subject is made aware of the fact that said Personal Information is to be processed by an Operator and that the Operator is provided with a written mandate to process the Personal Information on behalf of the Vendor which mandate must set out:

- the reasons for the processing of the Personal Information by the Operator;
- the scope of the processing;
- that such processing may only be for the purposes as stated in the written mandate; and
- that the Personal Information processed must be kept confidential and secure.

5.10 Use and deletion of Personal Information

5.10.1 The Vendor will ensure that:

5.10.1.1 Personal Information will only be used and processed for as long as the Personal Information is required to achieve the stated purpose;

5.10.1.2 once the purpose for the processing has come to an end, the Vendor, in line with their Retention Guidelines, archive and retain the Personal Information for only as long as it is lawfully required to retain such records;

5.10.1.3 on expiration of the legal retention period, referred to under 5.10.1.2 above, all records containing the particular Personal Information will be permanently deleted or destroyed, which destruction or deletion will be performed in a manner that prevents its reconstruction in an intelligible form as per the Safe Data Destruction Guidelines which describe the Vendor's approved destruction procedure and related techniques.

5.11 Security safeguards

5.11.1 The Vendor will ensure that:

5.11.1.1 the integrity of Personal Information in their possession or under its control is safeguarded which will be done through the implementation and application of appropriate, reasonable, technical and organisational measures,

duly employed in order to minimize and / or to prevent, loss, damage and / or the unauthorised destruction of such Personal Information;

5.11.1.2 on going Privacy Impact Assessment (PIA) will be performed by the Information Officer over all electronic systems and / or applications as well as any manual processes or procedures which involve the processing of Personal Information, including any potential or new electronic systems and / or applications in order to ensure that such processing of Personal Information complies with the required and prescribed POPIA security standards.

5.11.2 The Vendor will ensure that where Personal Information is processed by Operators acting on its behalf, that such processing will only take place under the following conditions:

5.11.2.1 all processing will take place with the knowledge and under the authorization of the Vendor as per a written mandate, which mandate will be concluded as between the Vendor and the Operator prior to the processing taking place;

5.11.2.2 all processing carried out by an Operator will be strictly in accordance with the written mandate;

5.11.2.3 Personal Information processed by an Operator will be treated as confidential;

5.11.2.4 the Operator must ensure that reasonable security safeguards are implemented in respect of all Personal Information which it processes and holds on behalf of the Vendor;

5.11.2.5 the Operator is under a legal and contracted duty to ensure the confidentiality, security and integrity of the Personal Information whilst under its possession and control and to indemnify and hold the Vendor harmless should this undertaking and requirement be breached, howsoever such breach occurs;

5.11.2.6 there will be a process in place to monitor and report Operator compliance and conformance with the written mandate and / or agreement;

5.11.2.7 the Operator will have a duty to notify the Vendor immediately in the case of any breach of the Operator mandate or any loss or unauthorized use of or access to the Personal Information under its possession and / or control.

5.11.3 All electronic devices, such as PC's, Laptops, smart phones and tablets, and portable data storage devices which hold and / or store Personal Information must be without exception password protected and sufficiently encrypted so that in the event of a person gaining unauthorized or unlawful access to such device, that such person or others gaining unauthorized or unlawful access to such device is unable to access and or use, read or download the Personal Information stored or held thereon.

5.11.4 No Personal Information may be left unattended within the Vendor's offices, including workspaces, reception areas, meeting rooms, desks, printers, shredders and other office equipment.

5.11.5 All Personal Information housed in hard copy format, i.e. on paper or in files must when not in use, be kept under lock and key and adequate security controls must be implemented and be in place to guard against unauthorized or unlawful access.

5.11.6 Where there has been a suspected breach of security in respect of any Personal Information under the control of the Vendor or where Personal Information has been accessed by an unauthorised party, the person who has discovered said breach or unauthorized access must immediately inform the Information Officer, which notification will be done in accordance with the Personal Information Breach Procedure.

5.11.7 The Vendor shall implement security measures in respect of the processing of Personal Information, which measures shall be implemented according to the security level required for each type of File as follows:

5.12 Data Subject participation

5.12.1 All formal requests for records containing Personal Information must be lodged in accordance with the information provided in the Promotion of Access to Information Act (PAIA) Manual.

5.12.2 Upon a reasonable request from a Data Subject, using the procedure set out under the PAIA Manual, the Vendor will, as soon as is reasonably practical under the circumstances, provide the requesting Data Subject with access to its requested Personal Information.

5.12.3 The Vendor will take the necessary steps to validate the identity of the Data Subject prior to providing them with access to the requested Personal Information.

5.13 Special Personal Information

5.13.1 Provided there is compliance with the provisions set out under POPIA, we may process the following Special Personal Information:

5.13.1.1 Personal Information which belongs to a child, provided that permission to process such Personal Information is obtained from the child's parent or guardian; or

5.13.1.2 Personal Information pertaining to a Data Subject which concerns the Data Subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, or criminal behaviour, where the Vendor receives the explicit consent of the Data Subject or alternatively where the Vendor has a legitimate reason to process this Special Personal Information.

5.13.2 All the Vendor's directors and employees must prior to the processing of the above-mentioned Special Personal Information consult with the Information Officer or its deputy in order to determine whether the processing of this Special Personal Information is permitted.

5.14 Direct marketing

5.14.1 The Vendor will only be allowed to send direct market communications to Data Subjects that have provided their prior consent to the receipt of such direct marketing communications and related materials.

5.14.2 In order to obtain a Data Subject's permission to send them direct marketing material, the Vendor will provide all Data Subjects who it is desirous of sending direct marketing communications to, with an opt-in option for which the Data Subject will be required to complete.

5.14.3 Once a Data Subject consents via an "opt- in" to receiving direct marketing communication and related materials, will ensure that it provides the Data Subject under every contact with such Data Subject an opportunity to opt-out of receiving further direct marketing communications.

5.14.4 In the event of the Data Subject electing to “opt out” of further direct marketing communications, the Vendor should remove that Data Subject from its direct marketing mailing list and stop sending that Data Subject any further direct marketing material.

5.15 Trans-border Personal Information flows

5.15.1 The Vendor may not transfer a Data Subject’s Personal Information to a third party in a foreign country unless:

5.15.1.1 the third party is within the Vendor’s group, which exchange is done under the standard set of binding corporate rules;

5.15.1.2 the Data Subject has provided its consent to its Personal Information being set outside South Africa;

5.15.1.3 the third party is located in a foreign country which country has adequate data protection legislation which is equivalent or similar to POPIA ;

5.15.1.4 the transfer of the Personal Information is necessary for the performance of a contract; or

5.15.1.5 in the case of a child’s Personal Information, the written consent of the parent or guardian has been provided.

5.15.2 Employees are required to consult with the Information Officer or its deputy before any trans-border flows of Personal Information is performed.

6. STATUTORY APPOINTMENTS

6.1 Information Officer

6.1.1 POPIA compels the Vendor to appoint an Information Officer, who will be responsible for the following:

6.1.1.1 ensuring adequate compliance with the conditions for the lawful processing of Personal Information;

6.1.1.2 providing guidance to the organisation and its employees for adequate disclosure of Personal Information, when Special Personal Information can be processed, and providing guidance on Trans-border Flows of Personal Information;

6.1.1.3 identifying training requirements and developing a training curriculum in line with legislative and employee requirements;

6.1.1.4 dealing with Data Subject access requests made in terms of POPIA and PAIA;

6.1.1.5 developing a privacy strategy;

6.1.1.6 monitoring and measuring privacy compliance and enforcement;

6.1.1.7 responding to breaches and Personal Information incidents;

6.1.1.8 reporting to management and stakeholders;

6.1.1.9 performing privacy risk assessments and data inventories;

6.1.1.10 developing and implementing privacy policies and guidance; and

6.1.1.11 administering privacy roles and responsibilities.

7. COMPLAINT PROCEDURE

7.1 The Information Officer has established an internal complaints department.

7.2 Where any Data Subject or someone acting on their behalf, feels that their Personal Information has or is not being processed with the necessary level of privacy and confidentiality, or who wish to enquire or complain about or object to

the use of their Personal Information, such person must be asked to submit their query, complaint or objection to the Information Officer using the “contact us” tab.

PRIVACY POLICY

Your privacy is important to us. It is the our policy to respect your privacy regarding any information we may collect from you across our apps, websites and other platforms we own and operate.

We only ask for personal information when we truly need it to provide a service to you. We collect it by fair and lawful means, with your knowledge and consent. We also let you know why we’re collecting it and how it will be used.

We only retain collected information for as long as necessary to provide you with your requested service. What data we store, we’ll protect within commercially acceptable means to prevent loss and theft, as well as unauthorized access, disclosure, copying, use or modification.

We don’t share any personally identifying information publicly or with third-parties, except when required to by law.

Our website may link to external sites that are not operated by us. Please be aware that we have no control over the content and practices of these sites and cannot accept responsibility or liability for their respective privacy policies.

You are free to refuse our request for your personal information, with the understanding that we may be unable to provide you with some of your desired services.

Your continued use of our website will be regarded as acceptance of our practices around privacy and personal information and your consent to the processing of your personal information. If you have any questions about how we handle user data and personal information, feel free to contact us. This policy is effective as of 15 February 2019.

SECTION 18 POPI NOTICE

INFORMED CONSENT DOCUMENT

INTRODUCTION

AJP Group Holdings (Pty) Ltd together with all of its subsidiaries (“AJP Group”) is committed to protecting your privacy and recognizes that it needs to comply to statutory requirements in the collection, processing and distribution of personal information.

Section 14 of the Constitution of the Republic of South Africa, 1996, provides that everyone has the right to privacy; furthermore the Protection of Personal Information Act, 4 OF 2013(POPI) further reiterates that the right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information.

According to section 18 of the Act, if personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is made aware of the information being collected and where the information is not collected from the data subject, the source from which it is collected, subject to certain exceptions, including those where the collection of information is required for a contractual or legal purpose and / or is required for the purpose of protecting the legitimate interests of the Company.

SECTION 18 DETAILS

Following this the AJP Group would like to acquire Informed Consent from you (the “Data Subject”) before it collects from you, any of your personal information. In terms of Section 18 of POPI the Company is obliged to provide you with the following information when collecting personal information from you:

- Type of information collected: All information as is required to process a Data Subject’s order, to provide its services to the Data Subject and to provide marketing materials to the Data Subject, including but not limited to bank account details, identity or registration numbers, e-mail address, physical and postal address, telephone and contact numbers, location information, and other required identifiers pertaining to the Data Subject from time to time;
- Nature or category of the information: All information shall be stored on properly secure servers owned by the vendor and/or its third party affiliates;
- Purpose: All information collected is done so for the purposes of processing the orders of Data Subjects, to provide its services to the Data Subject and to market the Vendor’s services and/or products to them;
- Source: all information will only be sourced from the Data Subject;

- Voluntary or mandatory: A Certain portion of the information required is mandatory in terms of the laws of the Republic of South Africa however certain information is voluntary in order that the Data Subject's orders and purchases may be properly processed;
- Legal requirement: the Vendor is statutorily obliged by Financial Intelligence Centre Act 38 of 2001(FICA) and/or Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (RICA) to collect personal information;
- Contractual requirement: Certain of the Data Subject's Personal Information is mandatory in order that the sale between the parties may be properly concluded;
- Responsible party details: The Responsible party, the Vendor including without detracting from the generality thereof, its directorate and officials, management, executives, and employees and operators who need to process the Data Subject's Personal Information. The details of which can be found in the PAIA Manual at the following link
<https://www.ajpg.net/policies/Access%20to%20Information.pdf>
- Consequences of not providing: Should the Data Subject fail to provide the Personal Information, the Vendor shall be unable to provide its services to the Data Subject as the information is vital to the provision of said services. Further to this any such failure or the provision of any false information shall be in breach of FICA and/or RICA and other related laws, statutes and regulations which will render the Data Subject's transaction invalid and may result in the Data Subject's profile on the website being terminated;
- Cross border transfer: The Data Subject's Personal Information will be transferred to servers outside the borders of the Republic of South Africa. All such servers are and shall remain properly secure against hacking and other forms of tampering;
- Recipients of information: The Vendor its Directors, employees, agents and third party affiliates (for the purposes server storage and/or delivery) shall be the only recipients of the Personal Information and in such instances only as much of the information shall be divulged so as to allow the aforementioned to properly perform their duties ;
- Access and right to amend: The Data Subject shall at all times have the right to access his/her/its Personal Information and shall further have the right to amend same;
- Right to object: The Data Subject shall at all times have the right to object to the processing of personal information as referred to in section 11(3); and
- Complaints: The Data Subject shall have the right to lodge any complaints with the Information Regulator of South Africa at complaints.IR@justice.gov.za or P.O Box 31533, Braamfontein, Johannesburg, 2017.

CONSENT

By utilising the website and/or the AJP Group's services, and based on the above, I hereby agree to provide AJP Group Holdings (Pty) Ltd and all of its subsidiaries with my personal information.

I further agree that:

- I am supplying this information voluntarily and without any undue influence from any party
- I am supplying this information because it is mandatory to supply this information to properly process any transaction on the website;
- Failure to provide this information will result in me not being able to purchase any goods and/or services from the website.

I am aware that I have the following rights with regard to my personal information being collected: I have the right to access my information and to rectify any information that is collected from me. I may object to the processing of your personal information. I may lodge a complaint to the Information Regulator as set out by the POPI Act

I have read and understood this notice and consent to the collection of my personal information.