DATA PRIVACY POLICY

Document Number	:	POPIA-002
Revision	:	00
Status	:	Active

CONFIGURATION CONTROL AND APPROVAL

Document History

Rev.	Date	Preparer	Changes
00	2021/07/01	Legal	N/A

Document Approval

Action	Name	Designation	Signature
Prepared	Trudi Maré	Legal	
Approved	Wayne Pollak	Chief Executive Officer	

DATA PRIVACY POLICY

BIDVEST SERVICES (PTY) LTD T/A BIDVEST STEINER

(REGISTRATION NUMBER: 2000/011155/07)

Statement from the Bidvest Group Ltd Board of Directors

"*The Bidvest Group Limited (hereinafter referred to as the "Group") has a long and proud tradition of conducting business with the highest ethical standards and in compliance with all applicable laws.*

The Group values of accountability, honesty, integrity and respect finds true application in the committed approach of the Group to data privacy.

This Data Protection Policy ("Policy") was developed to provide clear guidance to all directors, employees and those who process personal information on behalf of all the divisions and companies in the Group to ensure a lawful, transparent and consistent approach to the processing of personal data.

The Bidvest Group Board of Directors is committed to conducting business in line with the Group values and we expect your strict adherence to this Data Protection Policy and we thank you for your commitment hereto.

Any violation of this Policy will result in swift corrective action and violators will be held accountable."

1. PURPOSE

This Policy seeks to ensure that the *Company*:

1.1 complies with, and the manner in which it intends to comply therewith, legal standards and best practices applicable in the *RSA* for the *Processing* of *Personal Information* belonging to *Data Subjects.* For purposes hereof includes all *Personnel*, clients and third party vendors (e.g. operators or services providers) *Processing Personal Information* on behalf of the *Company*;

1.2 protects the privacy rights of all *Data Subjects* with whom it engages;

1.3 is transparent in relation to the *Processing* of *Personal Information*, especially in relation to what *Personal Information* it *Processes*, the reasons for such *Processing* and the manner in which it is done;

1.4 familiarise itself with the risks involved in relation to the *Processing* of *Personal Information* including data breaches and unlawful access as well as the protection controls available to manage the identified risks;

1.5 establishes appropriate data protection procedures and standards for the *Processing* of *Personal Information*.

2. DEFINITIONS AND INTERPRETATION

2.1 For purpose of this Policy an italicised word or phrase indicates that the word or phrase is defined in the glossary attached hereto as Annexure "**A**".

3. APPLICATION AND SCOPE OF THIS POLICY

3.1 This Policy applies to:

3.1.1 the following persons:

(a) all *Personnel*;

(b) all third parties acting for or on behalf of the *Company*, including *Operators*, service providers, contractors and agents, provided they have been made aware of this Policy;

3.1.2 all *Personal Information Processed* by the *Company* in an *Automated* or non-*Automated* manner, and regardless of how stored or recorded i.e. stored electronically, digitally, on paper or on other materials or through other methods.

3.2 All *Personnel Processing Personal Information* is:

3.2.1 expected to comply with the *Company*'s legal obligations in so far as they relate to the *Processing* of *Personal Information*, which has to be done in order to protect the *Company* from the risk of non-compliance, and the consequences of such non-compliance, including loss of *Personal Information*, investigations, administrative penalties, criminal charges and fines, civil claims and damages, as well as reputational risk;

3.2.2 required to read, understand and comply with this Policy when *Processing Personal Information* in the course of performing their tasks and must observe and comply with all *Personal Information* controls, standards, practices and training to ensure such compliance.

3.3 This Policy must be read in conjunction with other related *Company* policies and procedures especially those issued under direction of the internal Information Technology ('IT') unit.

3.4 Any breach of this Policy and related policies and procedures may result in disciplinary action and other necessary corrective action.

4. LAWFUL *PROCESSING* OF *PERSONAL INFORMATION*

4.1 The lawful *Processing* of *Personal Information* is based on the *8 Processing Conditions*. The *Company* must observe and comply with the aforesaid set of core principles at all times from the moment that *Personal Information* is collected until it is archived, deleted or destroyed.

5. RIGHTS OF *DATA SUBJECTS*

5.1 The *Company* acknowledges the right of every *Data Subject* to the lawful *Processing* of his/her/its *Personal Information* and the *Company* will maintain appropriate measures and procedures to give effect to a *Data Subject's* aforesaid right such as:

5.1.1 to be notified that:

(a) *Personal Information* about him/her/it is being collected;

(b) his/her/its *Personal Information* has been accessed or acquired without authorisation;

5.1.2 to establish whether the *Company* holds *Personal Information* of him/her/it and to request access thereto;

5.1.3 to request, where necessary, the correction, destruction or deletion of his/her/its *Personal Information*;

5.1.4 to object, on reasonable grounds relating to his/her/its situation, to the *Processing* of his/her/its *Personal Information*;

5.1.5 to object to the *Processing* of his/her/its *Personal Information* at any time for direct marketing or not to have his/her/its *Personal Information Processed* (or to have the *Processing* thereof ceased) for purposes of direct marketing via unsolicited electronic communication;

5.1.6 not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated *Processing* of his/her/its *Personal Information* intended to provide a profile of the *Data Subject*;

5.1.7 to submit a complaint with the *Information Regulator* including the alleged interference with the protection of his/her/its *Personal Information* and/or to institute civil proceedings concerning the alleged interference.

6. PROTECTION PRINCIPLES

6.1 The *Company* will ensure that it has adequate resources, systems and processes in place to demonstrate compliance with its *Processing* obligations, including:

6.1.1 appointing a suitably qualified and experienced *Information Officer* and providing the person with adequate support and resources;

6.1.2 ensuring that at the time of deciding how the *Company* will *Process Personal Information*, and throughout its *Processing*, implementing appropriate technical and organisational measures that are designed to ensure compliance with *Personal Information* protection principles (known as 'protection by design');

6.1.3 ensuring that, by default, only *Personal Information* that is necessary for each specific purpose is processed both in relation to the nature, extent and volume of such *Personal Information*, the period of storage and the accessibility of the *Personal Information* (known as 'protection by default');

6.1.4 ensuring that where any intended *Processing* presents a high risk to the rights of a *Data Subject*, the *Company* has carried out a risk assessment and is taking steps to mitigate those risks;

6.1.5 integrating the protection of *Personal Information* into the *Company*'s internal procedures and documents, by way of policies, rules, standards and instructions;

6.1.6 continuous training of the *Company*'s *Personnel* and, where necessary, those who *Process Personal Information* on behalf of the *Company* on *POPIA*, this Policy and the *Company*'s related policies and procedures, and maintaining a record of all such training; and

6.1.7 regularly testing the measures implemented by the *Company* and conducting periodic reviews to assess the adequacy and effectiveness of this Policy, and the *Company*'s related *Personal Information* policies and procedures which are applicable to the *Company*.

7. CONDITIONS FOR *PROCESSING*

7.1 The *Company* will only *Process Personal Information* in a lawful, fair and in a transparent manner, for a specified, explicit and legitimate purpose and that *Personal Information* which is *Processed* by it is adequate, relevant and limited to what is necessary in relation to the purpose for which it is to be *Processed.*

7.1.1 A *Data Subject* has the right to be told that his/her/its *Personal Information* is being *Processed*, including what type of *Personal Information* will be *Processed*, the reason for the *Processing*, who the *Personal Information* will be shared with and whether such information will be sent outside the territory where it is being *Processed*, and how the *Personal Information* will be safeguarded.

7.2 Consent to *Process* under certain circumstances:

7.2.1 In order to *Process Personal Information* for any specific purpose, the *Company* must always have a lawful basis and purpose for doing so.

7.2.2 Consent to *Process* a *Data Subject*'s *Personal Information* will not always be required and the *Company* in terms of *POPIA* will be allowed to lawfully *Process* a *Data Subject*'s *Personal Information* without the *Data Subject*'s consent under the following circumstances:

(a) the *Processing* is necessary for the conclusion of and performance under a contract to which the *Data Subject* is a party (for instance a contract of employment or registration with the *Company* as a vendor);

(b) the *Processing* is necessary in order for the *Company* to comply with certain legal obligations (for instance, to comply with the labour laws);

(c) the *Processing* is in order to protect the legitimate interests of the *Data Subject*, or of the *Company* or a third party (e.g. a situation where the *Processing* is necessary to protect a life); or

(d) the *Processing* is in order to perform a public duty or to perform tasks carried out in the public interest or the exercise of official authority.

7.2.3 If the *Processing* of a *Data Subject*'s *Personal Information* is required for purposes which are not detailed under clause 7.2.1 above, then in such circumstances, in order to legitimise and ensure that such *Processing* is lawful, the *Data Subject* has to agree to such *Processing* i.e. it has to provide consent to the *Processing* of its *Personal Data*. In this regard it is important to note that consent can be implied i.e. consent can be done by way of a gesture or simple indication of agreement. Consent must however at all times be freely and genuinely given.

7.2.4 Where a third party provides the *Company* with a *Data Subject*'s *Personal Information* (for example, a curriculum vitae containing a job applicant's *Personal Information* provided by a recruitment agent or credit bureau records containing *Personal Information* about a debtor which is provided by a credit bureau in relation to a *Data Subject*'s credit worthiness) the *Company* must obtain confirmation that it was collected by the third party in accordance with all applicable *Data Privacy and Security Laws*, that such *Personal Information* was lawfully *Processed*, and that the sharing of the *Personal Information* with the *Company* was clearly explained to the *Data Subject* by such third party and where required, permission to *Process* including the passing on or the sharing of information was obtained from the *Data Subject*.

7.2.5 *Data Privacy and Security Laws* distinguish between general *Personal Information* and special or sensitive *Personal Information*. Special *Personal Information* concerns the *Data Subject*'s race, ethnicity, politics, religion, trade union membership, genetics, biometrics, health, sex life or sexual orientation.

(a) In accordance with *POPIA*, in order to *Process* special *Personal Information*, being the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a *Data Subject*; or the criminal behaviour of a *Data Subject* to the extent that such information relates to the alleged commission by a *Data Subject* of any offence; or any proceedings in respect of any offence allegedly committed by a *Data Subject* or the disposal of such proceedings, the following has to be shown in relation to such processing:

(i) the *Processing* is carried out with the consent of a *Data Subject*;
(ii) the *Processing* is necessary for the establishment, exercise or defence of a right or obligation in law;
(iii) the *Processing* is necessary to comply with an obligation of international public law;
(iv) the *Processing* is for historical, statistical or research purposes, to the extent that the purpose serves a public interest and the *Processing* is necessary for the purpose concerned;

(v) getting the necessary consent appears to be impossible or would involve a disproportionate effort to acquire, and sufficient guarantees are provided for to ensure that the *Processing* does not adversely affect the individual privacy of the *Data Subject* to a disproportionate extent;

(vi) the information has deliberately been made public by the *Data Subject*;

(vii) permission has been received from the *Information Regulator* to *Process* special *Personal Information* if such *Processing* is in the public interest and appropriate safeguards have been put in place to protect the *Personal Information* of the *Data Subject*;

(viii) where the *Processing* concerns religious or philosophical beliefs, and such *Processing* has been done and is necessary to protect the spiritual welfare of the *Data Subjects*, unless they have indicated that they object to the *Processing*, and provided that such information is not supplied to third parties without the consent of the *Data Subject*;

(ix) where the *Processing* concerns race or ethnic origin, and such *Processing* is carried out to identify *Data Subjects* and only when this is essential for that purpose; and to comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination;

(x) where the *Processing* concerns trade union membership, and such *Processing* is carried out by the trade union because it is necessary to achieve the aims of the trade union or trade union federation and provided that such information is not supplied to third parties without the consent of the *Data Subject*;

(xi) where the *Processing* concerns the *Data Subject*'s health, and such *Processing* is carried out by:

(aa) medical professionals, healthcare institutions or facilities or social services, if such *Processing* is necessary for the proper treatment and care of the *Data Subject*, or for the administration of the institution or professional practice concerned;

(bb) insurance entities, medical schemes, medical scheme administrators and managed healthcare organisations;

(cc) administrative bodies, pension funds, the *Company* as employer or institutions working for them, if such *Processing* is necessary for: the implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health life of the *Data Subject*; or the reintegration of or support for *Personnel* entitled to benefit in connection with sickness or work incapacity, and provided that such information is kept confidential;

(xii) where the *Processing* concerns a *Data Subject*'s criminal behaviour or biometric information, such *Processing* is carried out by bodies charged by law with applying criminal law or by responsible parties who have obtained that information in accordance with the law, and where the *Processing* concerns *Personnel* such *Processing* is done in accordance with the rules established in compliance with labour legislation;

(xiii) where the *Processing* concerns a *Data Subject* under the age of 18, such *Processing*:

(aa) is carried out with the prior consent of a competent person;

(bb) is necessary for the establishment, exercise or defence of a right or obligation in law;

(cc) is necessary to comply with an obligation of international public law;

(dd) for statistical purposes to the extent that: the purpose serves a public interest and the *Processing* is necessary for the purpose concerned;

or it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the *Processing* does not adversely affect the individual privacy of the child to a disproportionate extent;

(ee) concerns sensitive *Personal Information* which the child has deliberately made public with the consent of a competent person.

7.3 Purpose specific:

7.3.1 The *Company*, including *Personnel* and third parties *Processing Personal Information* on behalf of the *Company,* must only *Process Personal Information* for specified, explicit and legitimate purposes that have been communicated to *Data Subjects* before the *Personal Information* is collected or during the collection thereof.

7.3.2 When *Processing* a *Data Subject*'s *Personal Information*, the *Company*, including its *Personnel* and third parties *Processing Personal Information* on behalf of the *Company*, have a duty to inform the *Data Subject* why the information is required and what will be done with it whilst under the *Company*'s control. Without a lawful basis and purpose for *Processing*, such *Processing* will be unlawful and unfair and may also have an adverse impact on the *Data Subject* concerned. No *Data Subject* should be unaware that their *Personal Information* is or has been *Processed* by the *Company*. In other words, any *Processing* of a *Data Subject*'s *Personal Information* must be purpose specific, and the *Data Subject* must be informed about such *Processing* and how such *Personal Information* will be used, before the intended use thereof.

7.3.3 The *Company*, it's *Personnel* and third parties *Processing Personal Information* on behalf of the *Company,* must ensure that they do not *Process* any *Personal Information* obtained for one or more specific purposes for a new purpose that is not compatible with the original purpose. If the *Company*, or its *Personnel* and third parties *Processing Personal Information* on behalf of the *Company,* want to *Process Personal Information* for a new or additional purpose for which the *Personal Information* was collected, then they will have to provide the *Data Subject* with the details of such *Processing* and the reason(s) why the *Personal Information* has to be *Processed*, and where necessary, if required, obtain the *Data Subject*'s consent to such *Processing*.

7.4 Direct marketing:

7.4.1 The *Company* and its *Personnel* and/or third parties who *Processes Personal Information* on behalf of the *Company,* will ensure that before they send direct marketing to customers for the first time, that they have given the customer the opportunity in an informal manner to agree or disagree to the receipt of direct marketing material.

7.4.2 The *Company* and its *Personnel* and/or third parties who *Process Personal Information* on behalf of the *Company, will* ensure that before they send direct marketing to non-customers that they receive appropriate opt in consents in a manner and form that aligns with any *Data Privacy and Security Laws*.

7.4.3 The *Company* and its *Personnel* and/or any third party who *Process Personal Information* on behalf of the *Company,* must ensure that when a *Data Subject* exercises their right to object to direct marketing, in the form of an opt out, that such opt out is recorded and honoured.

7.4.4 The *Company* must develop a direct marketing policy and guideline and all *Personnel* or third parties who *Process Personal Information* on behalf of the *Company*, need to familiarise themselves with these documents and ensure that they understand and comply with these obligations in relation to direct marketing before embarking upon any direct marketing campaign.

7.5 Profiling:

7.5.1 The *Company* may from time to time, use *Personal Information* for profiling purposes which is done via “cookies” on its website.

7.5.2 *Personnel* or third parties who *Process Personal Information* on behalf of the *Company*, will ensure that when *Personal Information* is used for profiling purposes, that the following takes place:

(a) clear information explaining the profiling is provided to *Data Subjects*, via privacy notices, cookie opt ins and cookie notices, including the significance and likely consequences of the profiling;

(b) appropriate mathematical or statistical procedures are used;

(c) technical and organisational measures are implemented to minimise the risk of errors. If errors occur, such measures must allow the errors to be easily corrected; and

(d) all *Personal Information Processed* for profiling purposes shall be secured to prevent discriminatory effects arising out of profiling.

7.6 *Personal Information* minimisation:

7.6.1 The *Personal Information* that the *Company,* its *Personnel* and third parties *Process* on behalf of the *Company,* must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be *Processed*.

7.6.2 *Personnel* and third parties *Processing Personal Information* on behalf of the *Company,* must only *Process Personal Information* that is absolutely necessary for the performance of the required purpose and related duties and tasks and not for any other purposes. Accessing excessive *Personal Information* that is unnecessary or which one is not authorised to access, or that one has no reason to access, may result in disciplinary action and in certain circumstances, may constitute a criminal offence, give rise to civil liability or administrative penalties.

7.7 Accuracy:

7.7.1 The *Personal Information* that the *Company,* it’s *Personnel* and third parties *Processing Personal Information* on behalf of the *Company,* collect and *Process* must be accurate and, where necessary, kept up-to-date and must be corrected and deleted without delay when the *Company* or its *Personnel* and third parties *Processing Personal Information* on behalf of the *Company* discover, or are notified, that the *Personal Information* is inaccurate.

7.7.2 *Personnel* and third parties *Processing Personal Information* on behalf of the *Company,* must ensure that they have procedures in place to ensure that the *Personal Information* on record is kept updated, especially where one becomes aware that *Personal Information* is inaccurate. Where appropriate, any inaccurate or out-of-date records should be deleted or destroyed.

7.8 Security, integrity and confidentiality:

7.8.1 The *Personal Information* that the *Company*, its *Personnel* and third parties *Processing Personal Information* on behalf of the *Company, Process* must be secured by appropriate technical and organisational measures which guard against accidental loss, destruction or damage, and against unauthorised or unlawful *Processing*.

7.8.2 The *Company* will develop, implement and maintain appropriate technical and organisational measures for the *Processing* of *Personal Information* taking into account the nature, scope, context and purposes for such *Processing*, the volume of *Personal Information Processed* and the likelihood and severity of the risks of such *Processing* for the rights of *Data Subjects* and

has procedures in place to ensure that it regularly evaluates and tests the effectiveness of such measures to ensure that they are adequate and effective.

7.8.3 *Personnel* and third parties *Processing Personal Information* on behalf of the *Company,* must ensure that they:

(a) observe and comply with all the *Company*'s information security policies, especially those pertaining to *Personal Information* security at all times;

(b) do not attempt to circumvent any administrative, physical or technical measures the *Company* has implemented as doing so may result in disciplinary action and in certain circumstances, may constitute a criminal offence, give rise to civil liability or administrative penalties;

(c) ensure that the confidentiality and security of *Personal Information* is maintained at all times;

(d) ensure that they only store *Personal Information* on *Company* servers which are protected by approved security software, and one or more firewalls under the direction of the internal Information Technology unit and where transferred or uploaded to cloud computing services from computers, devices and applications, that these services have been approved by said unit;

(e) ensure that prescribed security measures and controls are implemented, or where instructed, followed to prevent unauthorised access to *Personal Information*, the accidental deletion of *Personal Information* or the exposure of *Personal Information* to malicious hacking attempts;

(f) ensure that all devices where *Personal Information* is stored, are password protected and that passwords are not written down or shared, irrespective of seniority or department which passwords must be strong passwords which are changed regularly. If a password is forgotten, it must be reset using the applicable method;

(g) ensure that all hard copies of *Personal Information*, along with any electronic copies stored on physical or removable media is stored securely in a locked box, drawer, cabinet, or similar, and that such data is not removed from the *Company* premises unless with prior approval from the *Data Subject*'s supervisor and when so removed, that such data is encrypted if it is on a removable media device;

(h) ensure that all *Personal Information* stored electronically is regularly backed up using the *Company*'s provided systems and applications and in accordance with backup protocols. Such backups will be tested regularly in line with the *Company*'s standard backup procedures and protocols under the direction of the internal IT unit;

(i) ensure that no *Personal Information* is stored on any mobile device (including, but not limited to, laptops, tablets, smartphones or data sticks), whether such device belongs to the *Company* or otherwise, without the formal written approval of the supervisor concerned and, in the event of such approval, the *Personal Information* is stored or held strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary when so stored, that such *Personal Information* is encrypted;

(j) ensure that where *Personal Information* is stored on paper, that it is not left in places where persons can view the content, e.g. on a printer, but instead is kept in a secure place where an unauthorised person cannot access or see it, such as in a locked drawer, safe or cabinet and that when no longer required, that same is shredded;

(k) ensure that when any *Personal Information* is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed),

it should be securely deleted and disposed of. For further information on the deletion and disposal of *Personal Information*, please refer to the relevant *Company*'s data retention and destruction policy;

(l) ensure that all device screens, when not in use, are always locked especially when left unattended;

(m) ensure that all *Personal Information* transferred within the *Bidvest Group*'s network and infrastructure is only transmitted over secure networks, including wireless and wired networks;

(n) ensure that *Personal Information* is not shared informally and when shared that there is a lawful or business reason for such sharing. When sending emails which contain *Personal Information*, ensure that they are marked "confidential", do not contain the *Personal Information* in the body of the email, whether sent or received, but rather placed in an attachment, which email is then encrypted before being transferred electronically;

(o) ensure that *Personal Information* is not transferred or sent to any entity not authorised directly to receive it;

(p) ensure that *Personal Information* is not being kept in a form that identifies a *Data Subject* for longer than is necessary in relation to the purposes for which it was collected (except in order to comply with any legal, accounting or reporting requirements);

(q) ensure that where *Personal Information* is to be sent by facsimile/electronic transmission, ensure that the recipient has been informed in advance of the transmission and that he or she is either waiting by the fax machine to receive the information or implemented a security measures to ensure confidentiality is maintained upon receipt;

(r) ensure that where *Personal Information* is transferred physically, whether in hardcopy form or on removable electronic media, that it is passed directly to the recipient or sent using recorded delivery services and housed in a suitable container marked "confidential";

(s) ensure that generally all *Personal Information* is handled with care at all times, kept confidential, and that it is not left unattended or on view to unauthorised *Personnel*; and

(t) ensure that all software (including, but not limited to, applications and operating systems) used in connection with the *Company* are installed on *Company* owned computers or devices and which have been installed by and with the prior approval of the internal IT unit, which software must at all times be kept up-to-date.

7.9 Retention of *Personal Information*:

7.9.1 Storing *Personal Information* for longer than necessary may increase the severity of a *Personal Information* breach and may also lead to increased costs associated with such storage. In order to manage these risks the *Company* will maintain policies and procedures to ensure that *Personal Information* is deleted, destroyed or anonymised after a reasonable period of time following expiry of the purpose for which it was collected.

7.9.2 Where appropriate, *Personnel* and third parties processing *Personal Information* on behalf of the *Company,* must take all reasonable steps to delete or destroy any *Personal Information* that the *Company* no longer requires in accordance with the relevant *Company*'s records management policies and data retention and destruction policy.

7.10 Sharing *Personal Information*:

7.10.1 The transfer of any *Personal Information* to an unauthorised third party will give rise to and constitute a breach of the lawfulness, fairness and transparency principle and, where caused by a security breach, will give rise to and constitute a *Personal Information* breach.

7.10.2 *Personnel* and third parties *Processing Personal Information* on behalf of the *Company,* are not permitted to share *Personal Information* with other persons, unless:

(a) there is a legitimate *Company* need to share the *Personal Information*;

(b) the fact that the *Personal Information* will be shared with another has been communicated to the *Data Subject* in a privacy notice or processing notice beforehand; and

(c) the person receiving the *Personal Information* has either agreed to keep the *Personal Information* confidential and to use it only for the purpose for which it was shared, or where acting as an *Operator* (i.e. such person will be *Processing* the *Personal Information* on behalf of the *Company*), has concluded an agreement with or mandate from the C*ompany*, before receipt of the *Personal Information*.

7.11 Transfers outside of the *RSA*:

7.11.1 *POPIA* prohibits the transfer of the *Personal Information* outside of the *RSA,* including transmitting, sending, viewing or accessing *Personal Information* in or to a different country, unless:

(a) the *Data Subject* consents to such *Processing*; or

(b) the country where the *Personal Information* is being transferred to provides the same level of protection for the *Data Subject*(s) as housed under the *Data Privacy and Security Laws* applicable in the *RSA*.

7.11.2 *Personnel* and third parties *Processing Personal Information* on behalf of the *Company,* are not permitted to transfer *Personal Information* to areas outside the *RSA*, unless at least one of the following controls and safeguards are in place:

(a) the *Information Regulator* has issued an “adequacy decision” confirming that the territory or country to which the *Company* proposes transferring the *Personal Information* to, has adequate *Personal Information* protection laws in place which will ensure that such *Personal Information* remains protected as it was in the *RSA*;

(b) the *Bidvest Group* has an approved set of standard binding corporate rules which apply to *Personal Information* which is transferred as between its own subsidiaries which make up the *Bidvest Group*, which subsidiaries are located in a territory or country which falls outside the *RSA*, which rules set out how the *Personal Information* will be protected as it was in the country or territory from where it came;

(c) the *Company* has a standard *Personal Information* transfer agreement, mandate or clause for incorporation in any agreement in place which will be concluded with the third party recipient of the *Personal Information* prior to them receiving *Personal Information* and which agreement or mandate incorporates the requirements to be followed by the third party in order to ensure that such *Personal Information* remains protected as it was in the *RSA*;

(d) the *Company* has an approved code of conduct in place which has been approved by the *Information Regulator*, which allows such transfers;

(e) the *Data Subject* has given its express and explicit consent to the proposed transfer, having been fully informed of any potential risks;

(f) the transfer is necessary to perform a contract between the *Company* and a *Data Subject*, for reasons of public interest, to establish, exercise or defined legal claims or to protect the legitimate interests of the *Data Subject* in circumstances where the *Data Subject* is incapable of giving consent; or

(g) the transfer is necessary, in limited circumstances to protect the parties' legitimate interests.

7.11.3 Whenever *Personnel* and/or any third party *Processing Personal Information* on behalf of the *Company*, need to transfer *Personal Information* to areas outside the *RSA,* it has a duty to ensure one of the controls and safeguards detailed above are in place.

7.12 Transparency and *Processing* notices:

7.12.1 The *Company* has a duty to show that it has dealt with a *Data Subject* in a transparent manner. To demonstrate transparency, the *Company* must provide all *Data Subjects* with appropriate notices before it collects and processes their *Personal Information*.

7.12.2 The *Data Privacy and Security Laws* provides for information to be contained in all privacy notices and processing notices, including:

(a) the types of *Personal Information* collected;

(b) the purposes for which they will be *Processed*;

(c) the lawful basis relied upon for such *Processing*;

(d) the period for which the *Personal Information* will be retained;

(e) who the *Company* may share the *Personal Information* with; and

(f) if the *Company* intends to transfer *Personal Information* to countries outside the *RSA*, the mechanism relied upon for such transfer as well as the respective rights of the *Data Subject*.

7.12.3 *Personnel* and or any third party *Processing Personal Information* on behalf of the *Company*, must ensure that a *Data Subject* is made aware of the information set out below:

(a) the types of *Personal Information* collected and the purpose or reason for the collection;

(b) the lawful basis relied upon for such *Processing* or whether consent is required for the *Processing*;

(c) the period for which the *Personal Information* will be retained;

(d) who the *Company* will be sharing the *Personal Information* with, including external transfers and the mechanism relied upon for such transfer;

(e) the security measures which are in place to protect the *Personal Information*; and

(f) the respective rights of the *Data Subject*.

7.12.4 *Personnel* and/or any third party who *Processes Personal Information* on behalf of the *Company*, should ensure that all documents and/or records where *Personal Information* is recorded and/or incorporated or which calls for or sets out that *Personal Information* is required, incorporate a *Personal Information Processing* clause which records or states in such document or *Record*, that the *Company* will have to, in order to deal with the *Data*

Subject, *Process* the *Data Subject*'s *Personal Information* and that such *Processing* is subject to:

(a) the provisions of the relevant *Data Privacy and Security Laws*; or

(b) the *Company*'s *Processing* mandate and requirements.

7.13 *Operator*:

7.13.1 The Company will conclude a *Personal Information* transfer agreement with or have an arrangement or mandate in place with all *Operators* prior to them receiving and or *Processing Personal Information* on behalf of the *Company*, which agreement, arrangement or mandate incorporates requirements which will have to be followed by the *Operator* in order to ensure that such *Personal Information* is *Processed* and protected in accordance with the *Data Privacy and Security Laws* and security procedures and standards acceptable to the *Company*.

7.12.3 Personnel or third parties who *Process Personal Information* on behalf of the *Company*, will ensure that when they appoint an *Operator*, that clauses 6.13.2 is given effect to.

7.13 Protection Impact Assessments:

7.13.1 A Data Protection Impact Assessment ('DPIA'), also known as a Privacy Impact Assessment, is a process to help identify and minimise the *Personal Information* protection risks involved in processes and activities involving the *Processing* of *Personal Information*.

7.13.2 In order to assess the impact of the *Data Privacy and Security Laws*, and what the *Company* needs to do in order to comply with these laws, an initial base line DPIA will be conducted by the *Company* and which will form the basis of the *Company*'s *Personal Information* privacy framework.

7.13.3 Further DPIA's will be carried out when new technologies or new systems, solutions and research studies are implemented or where *Personal Information Processing* is likely to result in high risk to both the *Data Subjects* and to the *Company*.

7.13.4 A DPIA will:

(a) describe the nature, scope, context and purposes of the *Processing*;

(b) assess necessity, proportionality and compliance measures;

(c) identify and assess risks to the *Data Subject*; and

(d) identify any additional measures to mitigate those risks.

7.13.5 All DPIA's will be assessed and signed off by the *Information Officer* and the internal IT unit. All *Personnel* and/or third parties who *Process Personal Information* on behalf of the *Company* must familiarise themselves with the requirement to conduct a DPIA and ensure where one is required that it is conducted in accordance with the relevant *Company*'s DPIA Policy.

7.14 Training:

7.14.1 The *Company* will conduct training sessions on a continuous basis covering the contents of the *Data Privacy and Security Laws* and the *Company*'s related *Personal Information Processing* policies and procedures, which will be available to all *Personnel* and/or third parties who *Process Personal Information* on behalf of the *Company*.

7.14.2 All *Personnel* and/or third parties who *Process Personal Information* on behalf of the *Company*, will ensure that they acquire the necessary training, that they understand the *Data Privacy and Security Laws* and the *Company* related *Personal Information Processing* policies

and procedures, and that importantly all *Processing* of *Personal Information* is done in accordance with the *Data Privacy and Security Laws*, the training, the related policies and procedures and/or any guidelines issued by the *Company* from time to time.

7.15 Record-keeping:

7.15.1 The *Company* must keep full and accurate records of all its *Processing* activities in accordance with the *Data Privacy and Security Laws* and related requirements including:

(a) the name and details of the *Information Officer* and any deputies as appointed;

(b) all *Operators* who *Process Personal Information* on behalf of the *Company*;

(c) the purposes for which the *Company Processes Personal Information*;

(d) details of the categories of *Personal Information Processed* by the *Company*;

(e) details of any transfers of *Personal Information* to territories outside *RSA,* including all mechanisms and security safeguards details of all retention periods in respect of *Personal Information* as per the *Company's* data retention and destruction policy; and

(f) detailed descriptions of all technical and organisational measures taken by the *Company* to ensure the security of *Personal Information.*

7.16 Archiving and destruction of *Personal Information*:

7.16.1 The *Company* will, in order to facilitate the correct creation, use, storage, archive, retrieval and ultimate destruction of *Records,* developed a *Record* management and retention policy and retention schedule.

7.16.2 *Personnel* and third parties *Processing Personal Information* on behalf of the *Company* will ensure that when they *Process Personal Information,* that such information is *Processed* in strict compliance with the *Company*'s records management and retention policy and retention schedule.

7.16.3 *Personnel* and third parties *Processing Personal Information* on behalf of the *Company,* will furthermore ensure that when *Personal Information* is no longer needed for the specific purposes for which it was collected, that such *Personal Information* is archived for the legally required retention period and thereafter deleted, destroyed or anonymised, which must be done in strict compliance with any *Company*'s retention policy and records retention schedule.

7.17 Reporting *Personal Information* breaches:

7.17.1 In the event of a *Personal Information* breach, the *Company* has a duty to give notice of such breach to the *Information Regulator* and to the affected *Data Subjects*.

7.17.2 The *Company* will maintain appropriate procedures to deal with any *Personal Information* breach and will notify the *Information Regulator* and/or the *Data Subjects* when it is legally required to do so.

7.17.3 All cyber and or *Personal Information* breaches are strictly private and confidential.

7.17.4 All *Personal Information* breaches must be reported immediately to the *Company*'s *Information Officer* which report must include the following details:

(a) categories and approximate number of *Data Subjects* concerned;

(b) categories and approximate number of *Personal Information* records concerned;

(c) the likely cause of the consequences of the breach; and

(d) details of the measures taken, or proposed to be taken, to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

7.17.5 Only the *Company*'s *Information Officer* with the approval of the *Company*'s Board has the right to report any *Personal Information* or security breach to the *Information Regulator* and/or the affected *Data Subjects*, as the case may be.

7.17.6 *Personnel* and/or any third party who *Processes Personal Information* on behalf of the *Company,* must familiarise themselves with, observe and comply with the *Company*'s *Personal Information* breach procedure and to this end has a duty to immediately report through to the *Company*'s *Information Officer*, any known or suspected *Personal Information* breach and to take all appropriate steps to preserve evidence relating to the breach.

8. MEASURES FOR DATA SUBJECT TO GIVE EFFECT TO THE PROTECTION OF HIS/HER/ITS *PERSONAL INFORMATION*

8.1 A *Data Subject* has the right at any time to ask any person (natural or juristic) who holds its *Personal Information*, including the *Company*, for access to his/her/its *Personal Information*, including finding out more about the *Personal Information* which the *Company* holds about the *Data Subject*, what it is doing with that *Personal Information*, and why it is *Processing* the *Personal Information*.

8.1.1 The *Data Subject* may request access via the procedure provided for in the *Company PAIA* manual. If any *Personnel* and/or any other third party who *Processes Personal Information* on behalf of the *Company* is asked for any *Personnel Information* which pertains to a *Data Subject* or to the *Company*, such person making the request must be referred firstly to the *Company Information Officer* for further assistance.

8.2 A *Data Subject* has the right to *Personal Information* portability i.e. to receive or request the *Company* to transfer to a third party, a reproduction or copy of the *Data Subject*'s *Personal Information*.

8.2.1 The *Data Subject* may request such portability via the procedure provided for in the *Company PAIA* manual. If any *Personnel* and/or any other third party who *Processes Personal Information* on behalf of the *Company* is asked for any *Personnel Information* which pertains to a *Data Subject* or to the *Company*, such person making the request must be referred firstly to the *Company Information Officer* for further assistance.

8.3 A *Data Subject* may object to the *Processing* of *Personal Information* by the *Company* (inclusive for direct marketing purposes), on reasonable grounds relating to his/her/its particular situation, unless *Data Privacy and Security Laws* or other legislation requires such *Processing*. A *Data Subject* has the right to object to decisions creating legal effects or significantly affecting the *Data Subject* which were made solely by automated means, including profiling, and the right to request human intervention. The *Data Subject* also has the right to ask for the reasons why a decision was made and the underlying methodology which was used to make the decision.

8.3.1 The *Data Subject* lodge an objection via the procedure provided for in the *Company PAIA* manual. If any *Personnel* and/or any other third party who *Processes Personal Information* on behalf of the *Company* is asked for any *Personnel Information* which pertains to a *Data Subject* or to the *Company*, such person making the request must be referred firstly to the *Company Information Officer* for further assistance.

8.4 A *Data Subject* may request the *Company* to:

8.4.1 correct or delete its *Personal Information* in the *Company*'s possession or under the *Company*'s control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or

8.4.2 destroy or delete a *Record* of *Personal Information* about the *Data Subject* that the *Company* is no longer authorised to retain,

and such request will be dealt with in accordance with the procedure provided for in the *Company PAIA* manual. If any *Personnel* and/or any other third party who *Processes Personal Information* on behalf of the *Company* is asked for any *Personnel Information* which pertains to a *Data Subject* or to the *Company*, such person making the request must be referred firstly to the *Company Information Officer* for further assistance.

8.5 In instances where the Data Subject withdraws his/her/its consent, the *Company* will cease to *Process* the *Data Subject*'s *Personal Information* from the date of such withdrawal and so it will be important to advise the *Data Subject* of the consequences of the withdrawal, i.e. that the *Company* will not be able to continue its relationship with the *Data Subject*;

8.6 A Data Subject may submit a complaint with the *Information Regulator* including concerning the alleged interference with the protection of his/her/its *Personal Information*.

8.6.1 Details regarding the procedure and forms may be obtained from the office of the *Information Regulator*.

9. GOVERNANCE

9.1 The *Company Information Officer* will be responsible for the following:

9.1.1 developing, constructing and once prepared, implementing and overseeing the various *Personal Information Processing* policies and procedures, including this Policy;

9.1.2 monitoring compliance with this Policy, the various *Personal Information Processing* policies and the *Data Privacy and Security Laws*;

9.1.3 arranging and implementing relevant training to all *Personnel* and where applicable, other persons who *Process Personal Information* on behalf of the *Company*;

9.1.4 providing ongoing guidance and advice on *Personal Information Processing*;

9.1.5 conducting DPIA's when required, including base line risk assessments of all the *Company's Personal Information Processing* activities;

9.1.6 ensuring that all operational and technological *Personal Information* protection standards are in place and are complied with;

9.1.7 working closely with IT in order to ensure that appropriate technological and operational measures have been implemented in order to ensure the safety and security of all *Personal Information* which the *Company* holds;

9.1.8 receiving and considering reports from IT about compliance with all technological and operational *Personal Information* protection standards and protocols;

9.1.9 be entitled and have authorisation to initiate disciplinary proceedings against any *Personnel* who at any time breaches any technological and/or organisational and/or operational *Personal Information* protection standard, rule, custom, instruction, policy, practice and/or protocol (verbal, in writing or otherwise) ("rule") applicable in any department or area of the operations within the *Company*;

9.1.10 review and approve any contracts or agreements with third parties to the extent that they may handle or *Process Personal Information*;

9.1.11 attend to requests and queries from *Data Subjects* in respect of their respective *Data Subject* rights detailed under this Policy, including requests for access to their *Personal Information*; and

9.1.12 liaising with and/or co-operating with any regulators or investigators or officials who may be investigating a *Personal Information* privacy matter.

9.2 The IT Manager in the *Company* will be responsible for the following:

9.2.1 conducting cyber security risk assessments including base line risk assessments of all the *Company* information technology activities;

9.2.2 ensuring that adequate and effective IT operational and technological data protection procedures and standards are in place in order to address all IT security risks;

9.2.3 ensuring that all systems, services and equipment used for *Processing* and/or storing data or *Personal Information* adheres to internationally acceptable standards of security and data safeguarding, and is regularly updated to continue to comply with such standards;

9.2.4 issuing appropriate, clear, and regular rules and directives, whether for the *Company* as a whole or a particular part of it, department, person or level of person in relation to any aspect of the *Company*'s work, including password protocols, data access protocols, levels of persons who enjoy access to certain data sign-on and sign-off procedures, log-on and log-off procedures; the description of accessories, applications and equipment that will or may be used, and/or that may be used under any circumstances, and the like; and

9.2.5 evaluate any third-party services the *Company* is or may acquire to *Process* or store data, e.g. cloud computing services and ensuring that appropriate and effective operational and technological data protection procedures and standards are in place in order to address all IT security risks which may present themselves in respect of these external service providers.

10. GENERAL

10.1 The contents of this policy are updated on a regular basis and may therefore change without prior notice.

10.2 The *Company* has no control over the content once printed.

10.3 The *Company* or its *Personnel* is not criminally or civilly liable for anything done in good faith in the exercise or performance or purported exercise or performance of any power or duty in terms of this policy or applicable *Data Privacy and Security Laws* or other legislation.

ANNEXURE "A"

GLOSSARY

In this Policy, unless the context otherwise indicates:

1. "*8 Processing Conditions*" means the eight conditions for lawful *Processing* as contained in *POPIA*:

    1.1 accountability: the *Responsible Party* has an obligation to ensure that there is compliance with *POPIA* in respect of the *Processing* of *Personal Information* from the time the purpose for which it is *Processed* and the means of *Processing* are determined, as well as during the *Processing*;

    1.2 *Processing* limitation: *Personal Information* must be collected directly from a *Data Subject* to the extent necessary and must only be *Processed* with the consent of the *Data Subject* and must only be used for the purpose for which it was obtained;

    1.3 purpose specification: *Personal Information* must only be *Processed* for the specific purpose for which it was obtained and must not be retained for any longer than it is needed to achieve such purpose;

    1.4 further *Processing* limitation: further *Processing* of *Personal Information* must be compatible with the initial purpose for which the information was collected;

    1.5 information quality: the *Responsible Party* must ensure that *Personal Information* held is accurate and updated regularly and that the integrity of the information is maintained by appropriate security measures;

    1.6 openness: there must be transparency between the *Data Subject* and the *Responsible Party*;

    1.7 security safeguards: a *Responsible Party* must take reasonable steps to ensure that adequate safeguards are in place to ensure that *Personal Information* is being *Processed* responsibly and is not unlawfully accessed;

    1.8 *Data Subject* participation: the *Data Subject* must be made aware that their information is being *Processed* and must have provided their informed consent to such *Processing*;

2. "*Automated*" means any equipment capable of operating automatically in response to instructions given for the purpose of *Processing Personal Information*;

3. "*Bidvest Group*" means the Bidvest Group Ltd (registration number: 1946/021180/06) inclusive of its subsidiaries;

4. "*Company*" means Bidvest Services (Pty) Ltd t/a Bidvest Steiner (registration number: 2000/011155/07);

5. "*Data Privacy and Security Laws*" means all legislation concerning how *Personal Information* is collected, shared and used as well as the protection thereof from compromise, and includes but is not limited to *PAIA* and *POPIA*;

6. "*Data Subject*" means the person to whom the *Personal Information* relates and may be a natural or juristic person;

7. "*Information Officer*" means the person who fulfils the purpose referred to in section 51(1) of *PAIA* and section 55(1) of *POPIA*, encourages and oversees compliance with both *PAIA* and *POPIA* and performs such responsibilities as provided for in relevant *Data Privacy and Security Laws*, in conjunction with or as assisted by any Deputy *Information Officers* as designated by the *Information Officer*. The contact details are as follow:

Information Officer	
Physical address:	110 Loper Avenue, Aeroport, Spartan Extension 2, Kempton Park, 1619
Postal address:	P.O. Box 487, Isando, 1600
Telephone number (landline):	(011) 923-9490 / 0860 10 11 80
Electronic mail:	legal@steiner.co.za
Internet address (website):	www.steiner.co.za

8. "*Information Regulator*" means the Information Regulator established in terms of section 39 of *POPIA*:

Information Regulator	
Physical address:	JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001
Postal address:	P.O. Box 31533, Braamfontein, Johannesburg, 2017
Electronic mail (complaints):	complaints.IR@justice.gov.za
Electronic mail (general):	inforeg@justice.gov.za
Internet address (website):	www.justice.gov.za/inforeg

9. "*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 the *Responsible Party*;

10. "*PAIA*" means the Promotion of Access to Information Act No. 2 of 2000, as amended;

11. "*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:

    11.1 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 (including place of birth);

    11.2 information relating to the education or the medical, financial (e.g. bank details, tax number), criminal or employment history of the person;

    11.3 any identifying number (e.g. date of birth, identity or passport number of a natural person or the registration number of a juristic person), symbol, address (e.g. e-mail address or physical address), telephone number, location information, online identifier or other particular assigned to the person;

    11.4 the biometric information of the person including fingerprints or images by way of closed-circuit television;

    11.5 the personal opinions, views or preferences of the person e.g. union membership;

    11.6 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;

    11.7 the views or opinions of another individual about the person;

    11.8 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 e.g. founding documentation, authorised signatories or ultimate beneficial owner;

12. "*Personnel*" means an official of the *Company* or any person who works for or provides services to or on behalf of the *Company* and who receives or is entitled to receive remuneration or who assist in carrying out or conducting the business of the *Company* and includes directors and permanent, temporary and fixed-term contract employees;

13. "*POPIA*" means the Protection of Personal Information Act 4 of 2013;

14. "*Process*" or "*Processing*" or "*Processed*" means any operation or activity or any set of operations, whether or not by automatic means, concerning *Personal Information*, including:

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

14.2 dissemination by means of transmission, distribution or making available in any other form; or

14.3 merging, linking, as well as restriction, degradation, erasure, disposal, deletion or destruction of information;

15. "*Record*" means any recorded information:

15.1 regardless of form or medium, automated or non-automated, including any of the following:

(a) writing on any material;

(b) 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;

(c) label, marking or other writing that identifies or describes any thing of which it forms part, or to which it is attached by any means;

(d) book, map, plan, graph or drawing;

(e) 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;

15.2 in the possession or under the control of the *Company*;

15.3 whether or not it was created by the *Company*;

15.4 regardless of when it came into existence;

16. "*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* and for purpose of this manual it is the *Company*;

17. "*RSA*" means the Republic of South Africa.