# BIDVEST DATA PROTECTION POLICY

## Statement from the Bidvest 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 of both legal and natural persons.
This Data Protection Policy establishes uniform data protection standards within the Group.

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.

CONTENTS

## BACKGROUND TO PERSONAL INFORMATION PROTECTION

The protection of individuals and legal entities personal information is a fundamental constitutional and human right.

**Personal Information processing laws**

In many territories around the world, including in the European Union (EU), the United Kingdom (UK), Singapore, Canada, New Zealand (NZ), California and in South Africa (SA), legislators have defined under various data protection laws, certain data processing principles and related standards, for the protection of personal data, some laws which apply to natural persons only, and some, such as the South African law known as the Protection of Personal Information Act, 14 of 2013 ("**POPIA**"), which applies to both natural and legal persons, including the requirement that such personal information may only be transferred to other countries if the local law applicable at the place of destination provides for similar levels or standards of data protection, as that afforded by the territory or country from where the personal information is transferred.

**Areas where the Group companies process personal data**

The Group is a business-to-business services, trading and distribution entity operating in the areas of consumer, pharmaceutical and industrial products, financial services, freight management, office and print solutions, outsourced hard and soft services, travel services and automotive retailing. Despite being rooted in Southern Africa, the Group companies operate both locally and internationally.

Inherent in the provision of these goods and services, the companies in the Group continually have access to and need to process personal information and information relating to individuals and legal entities, which processing takes place in Southern Africa, the United Kingdom, Ireland, Spain, Germany, Hong Kong, the Isle of Man and Mauritius.

Failure to comply with the data protection laws, may have severe consequences for the Group, including criminal sanctions, civil claims and damages and potential administrative fines of up to R10 million in South Africa, and up to €20 million or 4% of the Group's total worldwide annual turnover, whichever is higher, in the EU.

This Policy sets out how the various Group companies process personal information in order to meet the data protection standards of the Group and in order to comply with the legal standards which apply in the territories where such processing takes place.

| GLOSSARY**: A comprehensive Glossary of terms used throughout this Policy can be found under Schedule 1.** |
| --- |
| For the purposes of this Policy unless otherwise noted, all references to the "Group" or the "Company" includes a reference to all The Bidvest Group Limited companies and subsidiaries. To view a comprehensive list of the aforementioned entities, click the following link: https://www.bidvest-reports.co.za/integrated-reports/2020/annexure-a-interest-in-subsidiaries-and-associates.php<br>The term **"data privacy"** is used in this policy as an umbrella term to encompass concepts of autonomy, privacy, protection of personal information or data protection, security and responsible personal information or data management.<br>The term **"personal data"** and "**personal information"** is used interchangeably in this Policy to describe any information relating to an identified or identifiable natural person ("data subject"), consistent with Article 4(1) of the European Union's General Data Protection Regulation ("**GDPR**") and to an identified or identifiable natural person and any identified or identifiable legal entity ("data subject"), consistent with the provisions of **POPIA** in relation to personal information. |

## PURPOSE OF THIS POLICY

This Policy seeks to ensure that the Group:

- Complies with international legal standards and best practices for the receipt, importing, processing, handling, storing, sharing and disposal of personal information belonging to individuals and legal entities ("data subjects"), which data subjects include without detracting from the generality thereof, employees, service providers, clients, and third parties;
- Protects the privacy rights of all data subjects with whom it engages, including inter - company within the Group;
- Is transparent in relation to the processing of personal data, especially in relation to what personal information it collects, the reasons for such collection and how it collects, handles, shares, stores and destroys such personal data; and
- Is aware of the risks in relation to the personal information including data breaches, unlawful access to personal data protection controls in order to manage data risks.

Importantly this Policy establishes uniform and suitable data protection procedures and standards within the Group for the processing of personal data.

In line with the above this Policy sets out:

- The Group's responsibilities under the data protection laws which apply in the areas where the Group operates, and how it will comply with these laws;
- How the Group processes personal data which is owned, applies to and/or relates to identifiable or identified individuals and legal entities, including employees, service providers, and other third parties, known as data subjects; and
- The instruction for directors, employees and other Group representatives when handling personal data.

## 1 APPLICATION AND SCOPE OF THIS POLICY

1.1. This Policy applies to the following persons:

- all Group employees, who for the purposes of this Policy will include permanent, fixed term and temporary employees, directors, interns, third party representatives, agents, sponsors and representatives who are carrying out work for or on behalf of the Group (hereinafter referred to as “employees”); and
- all operators, service providers, contractors and agents acting for or on behalf of the Group, provided they have been made aware of this Policy.

1.2. The rules and standards set out in this Policy applies to all personal data processed by the companies in the Group 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.

1.3. All employees who process personal information on behalf of the companies in the Group are expected to comply with the company’s legal obligations in so far as they relate to the handling and 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 data, investigators, administrative penalties, criminal charges and fines, civil claims and damages, as well as reputational risk.

1.4. All employees who process personal information on behalf of the Group must 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, practices, protocols and training to ensure such compliance.

1.5. Compliance with this Policy and related company policies and procedures is mandatory.

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

## 2 DATA PROTECTION PRINCIPLES

The data processing laws are based on a set of core principles that the Group must observe and comply with at all times from the moment that personal information is collected by the particular Group Company, until the moment that the personal information is archived, deleted or destroyed. These principles are detailed below:

### 2.1 Accountability

2.1.1 The Company is responsible for and must be able to demonstrate compliance with the data protection principles and the Company’s other obligations under the applicable data processing laws. This is known as the ‘accountability principle’.

2.1.2 The Company must ensure that it has adequate resources, systems and processes in place to demonstrate compliance with its data processing obligations, including:

- appointing a suitably qualified and experienced Information Officer under POPIA and a Data Protection Officer (DPO) under the GDPR and providing them with adequate support and resources;
- ensuring that at the time of deciding how the Company will process personal data, and throughout its processing, implementing appropriate technical and organisational measures that are designed to ensure compliance with the data protection principles (known as 'Data Protection by Design');
- 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 data, the period of storage and the accessibility of the personal information (known as 'Data Protection by Default');
- ensuring that where any intended processing presents a high risk to the rights and freedoms of data subjects, the Company has carried out an assessment of those risks and is taking steps to mitigate those risks, by undertaking a 'Data Protection Impact Assessment';
- integrating data protection into the Company's internal procedures and documents, by way of privacy policies and processing notices;
- regularly training the Company's directors, employees and those who process personal information on behalf of the Company on the GDPR, POPIA, this Policy and the Company's related policies and procedures, and maintaining a record of all such training; and
- regularly testing the measures implemented by the Group and or 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.

**2.2 Lawfulness, fairness and transparency**

The Company must only process personal information in a lawful, fair and in a transparent manner.

**2.3 Purpose limitation**

The Company must only collect and process personal information for a specified, explicit and legitimate purpose.

**2.4 Data minimisation**

The Company must ensure that personal information which is processed by it is adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed.

**2.5 Accuracy**

The Company must ensure that personal information which is processed by it is accurate and where necessary kept up to date.

**2.6 Storage limitation**

The Company must ensure that personal information which is processed by it is not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed.

### 2.7 Security, integrity and confidentiality

The Company must ensure that personal information which is processed by it is done in a manner that ensures its security using appropriate technical and organisational measures to protect the data against unauthorised or unlawful processing and against accidental loss, destruction or damage.

### 2.8 Transfers of personal information outside the Processing territories

The Company must ensure that personal information which is processed by it is not transferred outside the borders of South Africa, the UK, or the EEA (which includes the use of any website or application that is hosted on servers located outside the borders of South Africa, the UK or the EEA) to another country without appropriate safeguards being in place.

### 2.9 Data subject rights and requests

The Company must allow data subjects to exercise their rights in relation to their personal data.

## 3 PROCESSES IMPLEMENTED BY THE COMPANY IN ORDER TO ENSURE THAT THE DATA PROTECTION PRINCIPLES ARE GIVEN EFFECT TO

### 3.1 Lawfulness and consent to process under certain circumstances

3.1.1 In order to collect and process personal information for any specific purpose, the Company must always have a lawful basis and purpose for doing so.

3.1.2 Consent to process a data subject's personal information will not always be required. The Company in terms of the data processing laws will be allowed to lawfully process a data subject's personal information without the data subject's consent under the following circumstances:

- The processing is **necessary for conclusion of the performance of a contract** to which the data subject is a party (for instance a contract of employment or registration with the Company as a vendor);
- The processing is necessary in order for the Company to **comply with certain legal obligations** (for instance, to comply with the labour laws);
- The processing is in order to **protect the legitimate or vital interests** of the data subject, or of the Company or another person (this will equate to a situation where the processing is necessary to protect the individual's life); or
- 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.

3.1.3 Where the processing of a data subject's personal information is required for purposes which are not detailed under section 3.1.2 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 where the processing is taking place in South Africa, then the consent can be implied – i.e. consent can be done by way of a gesture or simple indication of agreement, whereas, where the personal information is processed in the UK or the EU, then such consent has to be express, i.e. it has to be given expressly by way of ticking a box or signing a document.

3.1.4 Furthermore, where consent is required from the data subject, then such consent must be freely and genuinely given (there must not be any imbalance in the relationship between the Company and the data subject and consent must not be a condition for the provision of any product or service).

3.1.5 Where, in terms of the data processing laws, consent to process a data subjects' personal information is required, such consent may at any time be withdrawn by the data subject. If consent is withdrawn, then the Company will no longer be allowed to continue processing such 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.

3.1.6 Where a third party provides the Company with another's personal information (for example, CV's housing a job applicant's personal information provided by a recruitment agent or credit bureau records housing personal data about a creditor which is provided by a credit bureau in relation to a data subject's credit worthiness or where personal information pertaining to a service provider's employee is provided by a service provider) the Company must obtain confirmation that it was collected by the third party in accordance with the data privacy law requirements and 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 owner thereof.

3.1.7 The data processing laws distinguish between personal information and "special personal information" which is also known as "sensitive personal data". Special personal data concerns the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics, health, sex life or sexual orientation.

3.1.8 Under the **GDPR**, in order to process **special personal information** at least one of the following conditions must be met:

- the data subject must consent to the processing of such data for one or more specified purposes;
- the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the Company or of the data subject in the field of employment, social security, and social protection law;
- the processing is necessary to protect the legitimate interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- the Company is an entity with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that entity or to persons who have regular contact with it in connection with its purposes and that the personal information is not disclosed outside the entity without the consent of the data subjects;
- the processing relates to personal information which is clearly made public by the data subject;
- the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
- the processing is necessary for substantial public interest reasons, on the basis of law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
- the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment or the management of health or social care systems or services on the basis of law or pursuant to a contract with a health professional, subject to the Company providing for suitable and specific measures to safeguard the fundamental rights and interests of the data subject; and

- the processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy).

3.1.9 Under **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:

- the processing is carried out with the consent of a data subject;
- the processing is necessary for the establishment, exercise or defence of a right or obligation in law;
- the processing is necessary to comply with an obligation of international public law;
- 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; 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 data subject to a disproportionate extent;
- the information has deliberately been made public by the data subject;
- 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;
- 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;
- 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;
- 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;
- where the processing concerns one's health or sex life, and such processing is carried out by (a) 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; (b) insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations, if such processing is necessary for – (i) assessing the risk to be insured by the insurance company or covered by the medical scheme and that data subject has not objected to the processing; (ii) the performance of an insurance or medical scheme agreement; or (iii) the enforcement of any contractual rights and obligations; (c) schools, if such processing is necessary to provide special support for pupils or making special arrangements in connection with their health or sex life; (d) any public or private body managing the care of a child if such processing is necessary for the performance of their lawful duties; (e) any public body, if such processing is necessary in connection with the implementation of prison sentences or detention measures; or (f) administrative bodies, pension funds, employers or institutions working for them, if such processing is necessary for – (i) the implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health or sex life of the data subject; or (ii) the

reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity, and provided that such information is kept confidential;

- where the processing concerns a person'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 employees such processing is done in accordance with the rules established in compliance with labour legislation;
- where the processing concerns a person under the age of 18, such processing is carried out with the prior consent of a competent person; or is necessary for the establishment, exercise or defence of a right or obligation in law; or is necessary to comply with an obligation of international public law; or for historical, statistical or research purposes to the extent that – (i) the purpose serves a public interest and the processing is necessary for the purpose concerned; or (ii) 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; and
- where the processing concerns special personal information which has deliberately been made public by the child with the consent of a competent person.

3.1.10 Directors, employees and others processing personal information on behalf of the Company must only process **special personal information** if it is able to justify such processing as described above. Processing **special personal information** without the data subjects' consent, or where such processing cannot be justified, may result in disciplinary action and in certain circumstances, may constitute a criminal offence, give rise to civil liability or administrative penalties.

### 3.2 Purpose specific

3.2.1 The Company, including directors, employees and others processing personal information on behalf of the Company must only collect and process personal information for specified, explicit and legitimate purposes that have been communicated to data subjects **before** the personal information is collected.

3.2.2 When collecting and using a data subject's personal data, the Company, including its directors, employees and others 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 affected data subjects. No data subject should be surprised to learn that their personal information has been collected, consulted, used or otherwise processed by the Company. In other words any use or processing of a data subject's personal information must be purpose specific, and the data subject must be told about such processing and how such data will be used, before the intended use of the data. This accords with the universal data protection principles referred to under section 2 above, which states that the processing of a data subject's personal information will only be lawful if the data subject has been provided with an explanation for the processing, including the purpose, which has to be:

- specific (not given in respect of multiple unrelated purposes);
- informed (explained in plain and accessible language);
- unambiguous and given by a clear affirmative action (meaning opt-in; silence, inactivity or pre-ticked boxes will not be sufficient); and
- separate and unbundled from any other terms and conditions provided to the data subject.

3.2.3 The Company, it's directors, employees and other 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 directors, employees and others processing personal information on behalf of the Company want to process additional personal information for a new 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 data has to be processed, and where necessary, if required, obtain the data subject's consent to such processing.

**3.3 Data minimisation**

3.3.1 The personal information that the Company or its directors, employees and others processing personal information on behalf of the Company collect and process must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed.

3.3.2 Directors, employees and others 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.

**3.4 Accuracy**

3.4.1 The personal information that the Company it's directors, employees and others 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 directors, employees and others processing personal information on behalf of the Company discover, or are notified, that the data is inaccurate.

3.4.2 Directors, employees and others 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.

**3.5 Security, integrity and confidentiality**

3.5.1 The personal information that the Company, its directors, employees and others processing personal information on behalf of the Company collect and process must be secured by appropriate technical and organisational measures which guard against accidental loss, destruction or damage, and against unauthorised or unlawful processing.

3.5.2 The Company has developed, implemented and maintains 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.

3.5.3 Directors, employees and others processing personal information on behalf of the Company must ensure that they:

- observe and comply with all the Company's information security policies, especially those pertaining to personal information security at all times;

- 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;
- ensure that the confidentiality and security of personal information is maintained at all times;
- 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 IT Manager and where transferred or uploaded to cloud computing services from computers, devices and applications, that these services have been approved by their IT Manager;
- ensure that prescribed security measures and controls are implemented, or where instructed, followed to prevent all and any unauthorised access to personal information, the accidental deletion of personal information or the exposure of personal information to malicious hacking attempts;
- 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;
- ensure that all hard copies of personal data, 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 departmental head and when so removed, that such data is encrypted if it is on a removable media device.
- 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 their IT Manager;
- 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 department head 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 data is encrypted;
- ensure that where personal information is stored on paper, that it is not left in places where persons can view the data, 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;
- 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 data, please refer to the relevant Company's data retention and destruction policy.
- ensure that all device screens, when not in use, are always locked especially when left unattended;
- ensure that all personal information transferred within the Group's network and infrastructure is only transmitted over secure networks, including wireless and wired networks
- 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 data, 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;
- ensure that personal information is not transferred or sent to any entity not authorised directly to receive it;
- 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);

- ensure that where personal information is to be sent by facsimile transmission, ensure that the recipient has been informed in advance of the transmission and that he or she is waiting by the fax machine to receive the data;
- 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”;
- 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 employees; and
- 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 IT department, which software must at all times be kept up-to-date.

**3.6 Retention of personal information**

3.6.1 Storing personal information for longer than necessary may increase the severity of a data 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.

3.6.2 Where appropriate, directors, employees and others 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.

**3.7 Sharing personal data**

3.7.1 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.

3.7.2 Directors, employees and other processing personal information on behalf of the Company are not permitted to share personal information with third parties, unless:

- there is a legitimate company need to share the personal data;
- 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
- 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 under a data transfer agreement, or where acting as an operator or a processor, (i.e. such person will be processing the personal information on behalf of the Company), has concluded an Operator Agreement (identified under Schedule “2”) with the Company, before receipt of the personal data.

### 3.8 Transfers outside of the European Economic Area (EEA) or South Africa

3.8.1 The data processing laws prohibit the transfer of the personal information outside of South Africa, the UK and/or territories within the EEA, including transmitting, sending, viewing or accessing personal information in or to a different country, unless:

- the data subject consents to such processing; or
- 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 processing laws applicable in South Africa, the UK and/or territories within the EEA.

3.8.2 Following the above, directors, employees and others processing personal information on behalf of the Company are not permitted to transfer personal information to areas outside South Africa, the UK and/or territories within the EEA, unless one of the following controls and safeguards are in place, (which can be obtained from the Information Officer on request):

- the European Commission or the South African Data Privacy 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 data remains protected as it was in the country or territory from where it came;
- the third party receiving the data in the foreign country has an approved set of standard binding corporate rules which apply to personal information which is transferred as between its own companies which make up its group, which companies are located in a territory or country which falls outside South Africa, the UK and/or territories within the EEA, which rules set out how the personal information will be protected as it was in the country or territory from where it came;
- the Company has a standard data transfer contract or Operator 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 houses the rules which will have to be followed by the third party in order to ensure that such data remains protected as it was in the country or territory from where it came;
- the recipient party has an approved code of conduct in place which has been approved by the Information Regulators or Information Commissioners Office (**ICO**) under the GDPR as applicable, which allows such transfers;
- the data subject has given its express and explicit consent to the proposed transfer, having been fully informed of any potential risks;
- 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 vital interests of the data subject in circumstances where the data subject is incapable of giving consent; or
- the transfer is necessary, in limited circumstances to protect the parties' legitimate interests.

3.8.3 Whenever a director, employee and or any other representative needs to transfer personal information to areas outside South Africa, the UK and/or territories within the EEA, it has a duty to ensure that one of the controls and safeguards detailed above are in place.

### 3.9 Transparency and processing notices

3.9.1 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 privacy notices or processing notices **before** it collects and processes their personal data.

3.9.2 The data privacy laws set out a detailed list of information that must be contained in all privacy notices and processing notices, including the types of personal information collected; the purposes for which they will be processed; the lawful basis relied upon for such processing; the period for which the personal information will be retained; who the Company may share the personal information with; and, if the Company intends to transfer personal information to countries outside South Africa or outside the EEA, the mechanism relied upon for such transfer as well as the respective rights of the data subjects.

3.9.3 Whenever a director, employee and or any other representative processes personal information on behalf of the Company, such person must ensure that the data subject is made aware of the information set out below:

- the types of personal information collected and the purpose or reason for the collection;
- the lawful basis relied upon for such processing or whether consent is required for the processing;
- the period for which the personal information will be retained;
- who the Company will be sharing the personal information with, including external transfers and the mechanism relied upon for such transfer;
- the security measures which are in place to protect the data; and
- the respective rights of the data subjects.

3.9.4 In order to streamline the above requirements, the Company has developed and implemented a series of "processing notices" which have to be presented to the various data subjects with whom the Company engages with and which notices are located on The Bidvest Group website:

- Internal Processing Notice - for employees; directors; job applicants; learnership applicants
- External Processing Notice - for users of website/sites; interactors; applicants for funding or CSI/bursary; Customers and Clients; Contractors/Vendors/Service Providers; Regulators and Public Bodies; Business Partners,Tenants.
- Visitors Processing Notice - for all visitors/people coming onto company premises/offices

3.9.5 Directors, employees and/or any other representatives who processes personal information on behalf of the Company, in order to give effect to the obligations set out under section 3.9.3 above, must ensure that all documents and/or records where personal information is recorded and/or housed or which calls for or sets out that personal information is required, must house a data 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:

- the provisions of the data processing laws;
- the Company's processing notices; and

- where applicable, the Company's standard binding corporate rules, its standard data transfer contract and/or Operator Agreement.

3.9.6 The data processing clause referred to above is recommended to read as follows:

*COMPLIANCE WITH PERSONAL INFORMATION PROCESSING LAWS*

*"In terms of a variety of data privacy laws applicable around the world, including the Protection of Personal Information Act 4 of 2013, ("**POPIA")**, where a person processes another's personal information, then in such event, the person processing the personal information may only do so if such processing is lawful, legitimate and responsible and is done in accordance with the provisions of the data privacy laws, including **POPIA**. The Company, in order to perform its company objectives, will have to process certain personal information which is owned or held by data subjects from time to time.*

*In order to comply with the provisions of these data privacy laws, including **POPIA**, the Company must:*

*i) provide the data subject with a number of details pertaining to the processing of the data subject's personal information, before such information is processed, which details are housed under the Company's Processing Notice, located on its website, which the data subject is requested to read; and*

*ii) obtain consent from the data subject to process its personal information, unless such processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; is required in order to comply with an obligation imposed by law; is necessary to protect or pursue the legitimate interest(s) of the data subject, the Company or a third party to whom the personal information is provided to; or is necessary for the proper performance of a public law duty by a public body.*

*The data subject hereby agrees to read the Processing Notice and in this regard consents to the Company processing its personal information, save where such consent is not required as per the provisions of clause ii) above, the data subject accepting that the Company is lawfully able to process such personal information without its consent.*

** Where appliable the following: Where the Company provides personal information to another, who is tasked with processing the personal information on behalf of the Company in its capacity as a "Data Processor" or an "Operator" as defined under the EU General Data Protection Regulation (**GDPR**) and **POPIA**, then in such case, the provisions set out under **Schedule 2**, headed "Data Processing and/or Operator Agreement" will apply to such Processing, which terms will be incorporated into, and read together with this document."*

**3.10 Data subject rights and requests**

- The data processing laws provide data subjects with a number of rights in relation to their personal data, including the right to access its data, and to change it.
- The Company has developed, implemented and will maintain certain processes which give effect to these data subject rights, as described below, which processes will be directed to and handled directly by the relevant Company's Data Processing Officer, Information Officer or his or her deputy, and no other.
- All directors, employees and persons processing personal information on behalf of the Company must take note of and give effect to these processes as described below.

3.10.1 The right to withdraw consent

- Where a data subject has had to give its consent to the processing of its personal data, the data subject in such case will have the right to withdraw such consent at any time, which withdrawal will apply from the date of withdrawal only and which will not affect the legality of the processing of its personal information to which the consent applies prior to the withdrawal.

- In order to give notice of the withdrawal of consent, the data subject must complete the standard Company "withdrawal of consent notice" form (Form 3), available on the Group website, which form must be emailed to the applicable Company's Information Officer or the Group Information Officer for further attention. Should the Information Officer give effect to such withdrawal, a stop processing notice will be sent to the affected director, employee or person processing such personal information on behalf of the Company together with the consequences of such decision, who will then be required to stop the processing of the affected personal data.

3.10.2 The right to be informed

- A data subject has the right to be told why 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 or held, and how the personal information will be safeguarded.
- In order to give effect to this right, the Company has developed a series of processing or privacy notices which are described under section 3.9 above.
- Directors, employees and/or any other representatives who processes personal information on behalf of the Company, in order to give effect to a data subject's right to be informed, must ensure that all documents and/or records where personal information is recorded and/or housed or which calls for or sets out that personal information or information is required, house a data processing clause which records or states in such document or record, that personal information will be processed and that such processing is subject to the Company's standard processing or privacy notices.

3.10.3 The data subject's right to have access to its personal data

- All data subjects have the right at any time to ask any person or entity who holds its personal data, including the Company, for access to their personal data, including finding out more about the personal information which the Company holds about them, what it is doing with that personal data, and why it is processing the personal data.
- In South Africa, in terms of **POPIA**, this has to be exercised using the "request for access to information" procedure which is described under a law known as the Promotion of Access to Information Act, 2000 (PAIA) and which request procedure is more fully set out under the Groups' PAIA Manual or if applicable, the particular Group Company's own PAIA Manual.
- All request for information held by the Company, including personal information has to be made using the standard request procedure referred to above, which request will be submitted directly to, and which will be handled directly by, the relevant Group Company Information Officer or his or her deputy or when relevant the Group Information Officer, in accordance with the provisions of PAIA.
- If any director, employee and/or any other representatives who processes personal information on behalf of the Company is asked for any information which pertains to a data subject or to the Company, such person making the request must be referred firstly to the relevant Group Company Information Officer or his/her Deputy or if necessary, the Group Information Officer for further assistance.

3.10.4 Rectification of personal data

- All data subjects have the right to request that their personal information is updated or rectified where it is inaccurate, incomplete or out of date. The standard Company “rectification” form (Form 2) for requests is available on the Group website.
- The relevant company Data Protection Officer or the Information Officer on receipt of the request, provided it is submitted on the prescribed form, will where able, rectify so far as possible, the personal information in question, and inform the data subject of the rectification. Furthermore, in the event that any affected personal information has been disclosed to third parties, those parties will also be informed of any such rectification and the reasons therefor.

3.10.5 The right to object and/or restrict processing

- Data subjects have the right to object to the Company processing their personal information based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company has legitimate grounds for such processing which override the data subject’s interests, rights, and freedoms, or that the processing is necessary for the performance of a legal or statutory duty or the conduct of legal claims.
- Where a data subjects objects to the Company processing its personal information for direct marketing purposes, the Company must immediately stop any further direct marketing.
- A data subject furthermore has the right to object to the processing of its personal information coupled with the right to ask the Company to restrict processing the personal information where the data subject:
    - believes that the personal information is inaccurate;
    - believes that the processing was unlawful and the data subject prefers restriction of processing over erasure;
    - believes that the personal information is no longer necessary in relation to the purposes for which it was collected but one is required to establish, exercise or defend a legal claim and needs to retain the data; or
    - has objected to the processing pending a determination whether the Company’s legitimate interest’s grounds for processing the personal information override those of the data subject.
- In accordance with the above, the data subject may object to, and ask the Company to place a restriction on the processing of the personal information which the Company holds, which request has to be made using the standard Company “objection” form (Form 1), available on the Group website. Such form will be sent to the relevant Company Data Protection Officer or Information Officer or his or her deputies or the Group Information Officer for determination and action.
- If the relevant Data Protection Officer or Information Officer, as applicable in the circumstances is in agreement with and succumbs to the request of the data subject, then the Company shall pend any further processing of the personal information in question and retain only the amount of personal information concerning that data subject (if any) that is necessary to ensure that the personal information in question is not processed further.
- In the event that any affected personal information has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

3.10.6 The right to data portability

- This is the right of the data subject to receive or ask the Company to transfer to a third party, a copy of the data subject's personal information in a structured, commonly used machine readable format.
- To facilitate the right of data portability, the data subject must complete the standard Company "data portability" form (Form 4) which form is on the Group website. The data subject must submit same to the relevant Group Company Data Processing Officer or Information Officer or his deputy or the Group Information Officer, who will attend to and where possible facilitate the request if technically feasible. All requests for copies of personal information shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

3.10.7 The right to object to direct marketing

- A data subject who has opted into any form of direct marketing has the right to opt out from any subsequent direct marketing, i.e. it has the right to ask the Company not to process its personal information for any further direct marketing purposes.
- A data subject can either submit its request using the prescribed objection notice (see notice referred to under the second point of section 3.10.5 above or alternatively simply use the opt out request which the Company is obliged to include in all its electronic direct marketing communications.

3.10.8 The right to object to decisions based solely on automated processing including Profiling

- 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 which request must be made by completing and submitting the standard Company "objection" form which is available on the Group website.

3.10.9 The right to erasure (right to be forgotten)

- A data subject has the right to request that the Company erases the personal information which the Company holds about it in the following circumstances:
    - it is no longer necessary for the Company to hold that personal information with respect to the purpose(s) for which it was originally collected or processed;
    - the data subject wishes to withdraw its consent;
    - the data subject objects to the Company holding and processing its personal information (and there is no overriding legitimate interest to allow the Company to continue doing so);
    - the personal information has been processed unlawfully; or
    - personal information needs to be erased in order for the Company to comply with a particular legal obligation.
- The request for erasure must be submitted using the standard Company erasure form, which request will be handled and subsequent decision made, by the relevant Group Company Data Processing Officer or Information Officer and/or his or her deputies, as applicable.

- Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject must be informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the employee data subject shall be informed.
- In the event that any personal information that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

3.10.10 The right to be notified of a personal information breach

- A data subject must be notified of a personal information breach which involves its personal data, which notice will be prepared by and conveyed to affected data subjects by the relevant Group Company Data Processing Officer or Information Officer.

3.10.11 The right to complain

- A data subject has the right to lodge a complaint or objection with regards to the processing of its personal data, which complaint or objection must set out and concern a non-compliance by the Company with the data processing principles or concern a non-compliance with the data processing laws.
- The data subject is encouraged to make use of the standard Company "objection" form (Form 1) available on the Group website. Such form must be submitted to the relevant Group Company's Data Processing Officer or Information Officer and or the Group Information Officer who will direct it to the relevant Group Company.
- On receipt of the complaint or objection, the relevant Company Data Processing Officer or Information Officer will attempt to hear and resolve the matter and failing resolution will provide the data subject with a non-resolution notice.
- If the Data Processing Officer or the Information Officer and data subject are able to resolve the matter, a record setting out the solution will be complied, and signed by the parties and any other affected persons provided with details of the resolution.
- Where the parties are unable to resolve the matter, the data subject on receipt of the abovementioned notice will have the right to refer the complaint onwards, in the case of an alleged **POPIA** breach or infringement to the Information Regulator, or in the case of an alleged **GDPR** breach or infringement to the Information Commissions Officer or another appropriate supervisory authority.
- In order to give effect to the above, all directors, employees and/or any other representatives who processes personal information on behalf of the Company, must familiarise themselves with these rights and the related processes, and ensure that all data subjects are informed of these rights and the procedure which has to be followed when a data subject wishes to make use of these rights.

### 3.11 Data Protection Impact Assessments

3.11.1 A Data Protection Impact Assessment (DPIA), also known as a Privacy Impact Assessment, is a process to help identify and minimise the data protection risks involved in projects, processes and activities involving the processing of personal data.

3.11.2 In order to assess the impact of the data privacy 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 Information Officer and his or her deputies and which will form the basis of the Company's data privacy framework.

3.11.3 Further DPIA's must 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.

3.11.4 A DPIA must:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to the individual; and
- identify any additional measures to mitigate those risks.

3.11.5 Without exception all DPIA's must be assessed and signed off by the Company Data Processing Officer or Information Officer and, where relevant, IT Services.

3.11.6 In order to give effect to the above, all directors, employees and/or any other representatives 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.

**3.12 Direct marketing**

3.12.1 The Company and its directors, employees and/or other representatives who processes personal information on behalf of the Company must 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.

3.12.2 The Company and its directors, employees and/or other representatives who process personal information on behalf of the Company must ensure that before they send direct marketing to non-customers that they receive appropriate opt in consents in the prescribed manner and form as per the provisions of **POPIA**.

3.12.3 The Company and its directors, employees and/or any other representatives 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.

3.12.4 The Company has developed a direct marketing policy and guideline and all directors, employees or persons who process personal information on behalf of a particular Company must 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.

### 3.13 Operators

3.13.1 An operator (as defined under **POPIA**) or a processor (as defined under the **GDPR**) is an entity who processes personal information on behalf of the Company without coming under its direct control.

3.13.2 All operators and processors have to conclude the Company's standard data transfer contract or Operator Agreement prior to them receiving and or processing personal information on behalf of the particular Company, which agreement houses the rules which will have to be followed by the operator or processor in order to ensure that such data is processed and protected in accordance with the processing laws and the particular Group Company's security procedures and standards.

3.13.3 Directors, employees or persons who process personal information on behalf of the Company must ensure that when they appoint an operator (as defined under **POPIA**) or a processor (as defined under the **GDPR**) that the relevant standard data transfer contract or Operator Agreement is concluded with such operator or processor prior to them receiving and or processing personal information on behalf of the Company.

### 3.14 Profiling

3.14.1 The Companies from time to time, use personal information for profiling purposes which is done via "cookies" on their particular company websites.

3.14.2 Directors, employees or persons who process personal information on behalf of the Company, must ensure that when personal information is used for profiling purposes, that the following takes place:

- 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;
- Appropriate mathematical or statistical procedures are used;
- 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
- All personal information processed for profiling purposes shall be secured to prevent discriminatory effects arising out of profiling.

### 3.15 Training

3.15.1 The Company will conduct regular training sessions covering the contents of the data privacy laws and the Company's related personal information processing policies and procedures, which will be available to all directors, employees and/or persons who process personal information on behalf of the Company.

3.15.2 All directors, employees and/or persons who process personal information on behalf of the Company, must ensure that they have undertaken the necessary training, that they understand the privacy 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 processing laws, the training, the related policies and procedures and/or any guidelines issued by the Company from time to time.

### 3.16 Record-keeping

3.16.1 The Company must keep full and accurate records of all its processing activities in accordance with the data processing laws and related requirements including:

- the name and details of the particular Group Companies Data Protection Officer appointed by the particular Group Company in the UK or the EEU or the particular Group Companies Information Officer and any deputies as appointed by the particular Group Company in South Africa;
- all processors and/or operators who process personal information on behalf of the particular Group Company;
- the purposes for which the Company collects, holds and processes personal data;
- details of the categories of personal information collected, held and processed by the Company;
- details of any transfers of personal information to non-South African, UK or non-EEA operations situated in countries outside the EEU, the UK and South Africa, including all mechanisms and security safeguards
- details of all retention periods in respect of personal information as per the particular Group Companies data retention and destruction policy; and
- detailed descriptions of all technical and organisational measures taken by the particular Company to ensure the security of personal data.

### 3.17 Archiving and destruction of data

3.17.1 The Company to facilitate the correct creation, use, storage, archive, retrieval and ultimate destruction of records has developed a records management and retention policy and records retention schedule.

3.17.2 Directors, employees and others processing personal information on behalf of the Company must ensure that when they process personal data, that such data is processed in strict compliance with the Company's records management and retention policy and records retention schedule.

3.17.3 Directors, employees and others processing personal information on behalf of the Company must 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 the particular Company's retention Policy and records retention schedule.

### 3.18 Reporting personal information breaches

3.18.1 In the event of a personal information breach, the Company has a duty to give notice of such breach to the ICO in the case of a breach in the EU and to the Information Regulator in the case of a breach in South Africa, and to the affected data subjects.

3.18.2 The Company has put in place appropriate procedures to deal with any personal information breach and will notify the ICO / Information Regulator and/or the data subjects when it is legally required to do so.

3.18.3 All cyber and or data breaches, including ones which involve personal information are strictly private and confidential.

3.18.4 All personal information breaches must be reported immediately to the Company's Information Officer in South Africa, or where applicable, if the breach has occurred in the EEU or the UK, the Company's Data Protection Officer, which report must include the following details:

- Categories and approximate number of data subjects concerned;
- Categories and approximate number of personal information records concerned;
- The likely cause of the consequences of the breach; and
- Details of the measures taken, or proposed to be taken, to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

3.18.5 Only the applicable Company's Information Officer with the approval of the particular Company's Board has the right to report any personal information or security breach to the ICO / Information Regulator and/or the affected data subjects, as the case may be.

3.18.6 Directors, employees and/or any other representatives 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 relevant Companies Information Officer, or Data Protection Officer, as the case may be, any known or suspected data breach and to take all appropriate steps to preserve evidence relating to the breach.

## 4 GOVERNANCE

### 4.1 Information Officers, Data Protection Officers and Deputies

4.1.1 The Group has appointed in South Africa, in respect of all personal information processed in South Africa, Adv C. Krige who will act instead of the Group CEO, as the Group's duly appointed Information Officer or Data Protection Officer.

4.1.2 The Information Officer / Data Protection Officer have the right to appoint and to delegate certain activities to Deputy Information Officers or Data Protection Officers. Each separate Group Company in turn will appoint its own Information Officer or Data Protection Officer for their particular Company. Any communications applicable to personal information or personal data processed by a particular Company in the Group and addressed to the Group Information Officer or Data Protection Officer, will be in turn be directed to the applicable appointed Group Company Information Officer to deal with accordingly.

4.1.3 The Companies **Information Officer and or the Data Protection Officer** will be responsible for the following:

- developing, constructing and once prepared, implementing and overseeing a Company-wide personal information processing framework and related roadmap;
- developing, constructing and once prepared, implementing and overseeing the various personal information processing policies and procedures, including this Policy;

- monitoring compliance with this Policy, the various personal information processing policies and the data processing laws;
- arranging and implementing data protection training to all directors, employees and other persons who process personal information on behalf of the Company;
- providing ongoing guidance and advice on personal information processing;
- conducting DPIA's when required, including base line risk assessments of all the Companies personal information processing activities;
- ensuring that all operational and technological data protection standards are in place and are complied with;
- 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;
- receiving and considering reports from IT about compliance with all technological and operational data protection standards and protocols;
- be entitled and have authorisation to initiate disciplinary proceedings against any employee who at any time breaches any technological and/or organisational and/or operational data 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;
- review and approve any contracts or agreements with third parties to the extent that they may handle or process data subject information;
- attend to requests and queries from data subjects in respect of their respective data subject rights detailed under section 3.10 of this Policy, including requests for access to their personal data or information; and
- liaising with and/or co-operating with any regulators or investigators or officials who may be investigating a data privacy matter.

**4.2 IT Manager**

4.2.1 Each Company shall appoint an IT Manager. The respective IT Manager in each Company shall have the right to appoint and to delegate certain activities to deputy IT Personnel.

4.2.2 The IT Manager in each Company will be responsible for the following:

- conducting cyber security risk assessments including base line risk assessments of all the Company information technology activities;
- 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;
- ensuring that all systems, services and equipment used for processing and/or storing data adheres to internationally acceptable standards of security and data safeguarding, and is regularly updated to continue to comply with such standards;
- 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

- evaluate any third-party services the Company is considering 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.

## 5 RELATED POLICIES AND PROCEDURES

This Policy forms part of a broader Information Governance Framework with other policies, guidance and procedures listed below. Compliance with these is mandatory. Any breach of the requirements contained in these documents may result in disciplinary action.

- Bidvest Code of Ethics
- Information Technology Policies applicable in the Group
- Privacy Policy

Further information on data protection policy, procedures and issues, including specific practical guidance on issues of particular relevance to the Company staff, can be found on the Group Intranet.

## 6 NON COMPLIANCE

Any transgression of this Policy will be investigated and may lead to disciplinary action being taken against the offender.

## 7 VERSION AND AMENDMENTS

| Version | Author / Primary reviewer | Details of changes | Date | Approved by | Approved date |
|---|---|---|---|---|---|
| **1.1** | **C Krige** | **Initial draft – new policy** | **9.03.2021** | **I.Roux** | **15/03/2021** |

This Policy is effective as of 1 April 2021

**Schedule 1 – Glossary**

| | |
|---|---|
| **automated processing** | any form of processing (including profiling) that is undertaken by automated means to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning their performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements |
| **consent** | any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal information about them |
| **Controller (GDPR) or Responsible Party (POPIA)** | the person or organisation that determines the purposes and means of processing personal data |
| **criminal convictions and offences** | personal information relating to criminal convictions, the commission or alleged commission of an offence, proceedings for the commission or alleged commission of an offence and sentencing |
| **Data privacy laws / data protection laws** | In the UK and the EU, the European Union's General Data Protection Regulation ("GDPR") and in South Africa, the Protection of Personal Information Act, 14 of 2013 (POPIA) |
| **Data Protection Impact Assessment (DPIA)** | a tool used to identify and reduce the risks of a processing activity and which must be undertaken in certain circumstances specified in the **GDPR**, also known as 'Privacy Impact Assessments |
| **Data Protection Officer (DPO) (GDPR)** | GDPR- a person required to be appointed in specific circumstances under the GDPR and who must have expert knowledge of data protection law and practice, being the Company's main representative on data protection matters<br>(note: each company in the Group constitutes a separate entity requiring a DPO) |
| **data subject** | an individual or legal entity (**POPIA**) to whom personal information relates and who can be identified or is identifiable from personal data<br>an individual (**GDPR**) to whom personal information relates and who can be identified or is identifiable from personal data |
| **DPA 2018** | the UK Data Protection Act 2018 |
| **EEA** | the 28 countries in the European Union and Iceland, Lichtenstein and Norway |
| **explicit consent** | a higher standard of consent that requires a very clear and specific statement rather than an action which is suggestive of consent |
| **GDPR** | the General Data Protection Regulation (Regulation (EU) 2016/679) |
| **ICO**<br><br>**Information Regulator** | Information Commissioners Office (ICO) under the GDPR<br><br>in South Africa the equivalent being the Information Regulator<br>(in terms of POPIA) |

| | |
|---|---|
| **Information Officer (IO) (POPIA)** | **POPIA**- a person required to be appointed under **POPIA** and who must have expert knowledge of data protection law and practice, being the Company's main representative on data protection matters<br>(note: each company in the Group constitutes a separate entity requiring an IO) |
| **personal data /personal information** | **any information identifying a data subject or information relating to a data subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal information includes criminal convictions and offences data, special categories of personal information and pseudonymised personal information but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal information can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour** |
| **personal information breach** | **a breach of security lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information transmitted, stored or otherwise processed and which compromises the confidentiality, integrity, availability and/or security of the personal data** |
| **privacy notices** | **see processing notices below** |
| **Processing Areas** | **the European Union, the UK and South Africa** |
| **processing notices** | a notice setting out information that must be provided to data subjects before collecting personal information from them, including notices aimed at a specific group of individuals or notices that are presented to a data subject on a 'just- in-time' basis (also known as 'privacy notice' or 'data protection notice') |
| **process, processes, processing** | any activity or set of activities which involves personal information including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or making available, alignment or combination, restriction, erasure or destruction |
| **pseudonymised, pseudonymisation** | replacing information that directly or indirectly identifies an individual with one or more artificial identifiers (for example, a numerical identifier or other code) or pseudonyms so that the data subject cannot be identified without combining the identifier or pseudonym with other information which has been kept separately and securely. Personal information that has been pseudonymised is still treated as personal information (unlike personal information which has been anonymised) |
| **related procedures** | the related procedures referred to in section 5 above |
| **special categories of personal data or special personal information** | means information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and, for the purposes of this policy personal information relating to criminal offences and convictions. |

**Schedule 2 – Operator Agreement Template**