FirstRand

FIRSTRAND GROUP DATA PROTECTION POLICY FOR SUPPLIERS AND BUSINESS PARTNERS

November 2022

TABLE OF CONTENTS

1 BACKGROUND AND PURPOSE 2
2 DEFINITIONS 2
3 APPLICABILITY 5
4 SCOPE OF APPLICATION 5
5 SUPPLIERS AND BUSINESS PARTNER OBLIGATIONS WHEN DEALING WITH PI AND RECORDS 6
6 AUDIT AND INSPECTION OF PI AND RECORDS 10
7 CROSS-BORDER TRANSFER 11
8 NOTIFICATIONS BY SUPPLIER OR BUSINESS PARTNER TO THE GROUP 11
9 THIRD-PARTY MANAGEMENT 11
10 TERMINATION EXPECTATIONS 12
11 GENERAL 12
12 OWNERSHIP AND REVIEW 12

1 BACKGROUND AND PURPOSE

FirstRand Limited and its subsidiary companies, including divisions, segments and business units (referred to as **FirstRand** or **the group**) recognise that personal information (**PI**) and records are important assets that must be protected. This document establishes a governance framework that sets out ethical and sound PI protection practices that are to be followed by all suppliers and business partners appointed by the group. This policy sets out the minimum PI protection requirements applicable to suppliers and business partners to preserve the integrity, confidentiality and availability of PI or records furnished to suppliers and business partners during the course and scope of their engagement with the group.

This policy will set out the rules of engagement in relation to how PI is handled by suppliers and business partners on behalf of FirstRand, as well as the minimum legal requirements that FirstRand requires suppliers and business partners to adhere to, including compliance with the requirements of the Protection of Personal Information Act 4 of 2013 (**POPIA**), the General Data Privacy Regulation (**GDPR**) and other legislation, where applicable from time to time, in their capacity as service providers or business partners to the group. This policy is applicable to all suppliers and applicable business partners who engage with the group and handle PI as defined in applicable law.

All group suppliers and business partners are expected to comply with all local legislative requirements within the jurisdiction in which they operate.

This policy serves as an additional measure which specifies the requirements that FirstRand has in relation to how suppliers and business partners are required to organise themselves and provide goods and/or services or collaborate in relation to agreements concluded with FirstRand and its affiliates.

FirstRand subscribes to the higher of the host-or-home principle when dealing with jurisdictions outside of South Africa. This means that where the supplier or business partner conducts business activities within a jurisdiction where the PI protection laws and regulations are of a higher standard than POPIA, then the provisions of those laws and regulations will take precedence over the provisions of POPIA, and vice versa.

2 DEFINITIONS

The following concepts will be used throughout this policy and are defined as follows:

Affiliate	Means (a) any subsidiary or a holding company or a subsidiary of the holding company of either party, or (b) any entity that controls, is controlled by or is under common control with either party. The terms "subsidiary" and "holding company" will have the meaning assigned thereto in Chapter 1 of the Companies Act, No. 71 of 2008 (the Companies Act). The term "control" means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of the entity through the ownership of voting securities representing 50% (fifty per cent) plus 1 (one) of the possible votes.
Agreement	Means the agreement entered into between the group and the supplier or business partner, as applicable.
Associate	Shall mean any entity or unincorporated joint venture in which FirstRand has the right to receive at least 20% (twenty per cent) of the profit share or similar benefit derived from such entity or unincorporated joint venture.

Business partner	A business partner, in the context of this policy, means a natural or juristic person (**person**) holding a business relationship with the group, where such relationship does not fall within the category of a supplier, employee or customer relationship, and which person processes PI for, on behalf of or together with FirstRand under the terms of the applicable agreement between the group and the person. (*For the avoidance of doubt, the term **business partner** is used for the sake of convenience and for descriptive purposes only and should not be construed to imply a partnership between the group and the business partner in a legal sense or as understood in law.)*
Child	A child is a natural person who is defined as a child by a country's legislation and who has not been recognised as an adult by the courts of a country.
Competent person	Means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.
Consent	Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of PI.
Customer	A customer is a natural or legal person who is a group customer or a person who provided their PI/SPI to the group in the context of a sale of acquiring goods or services.
Data subject	Means the person to whom PI relates. In reference to the group, this primarily but without limitation means customers, employees and operators/suppliers, other persons and third parties.
Employee	Means a person employed for wages or a salary, including permanent employees, non-permanent employees, contractors, secondees and contingent workers.
FirstRand or the group	Means FirstRand Limited and its subsidiary companies, including divisions, segments, and business units. Certain subsidiary companies may be excluded from the group description for the purposes of this policy (such as where the group is involved in private equity investments). Confirmation as to whether this policy applies to a specific company (a registered legal entity) associated with the group can be sought through the contact details provided in this policy. In this policy, any reference to "the group" or "FirstRand" includes any one or more (if they are acting jointly) group companies and all affiliates, associates, cessionaries, delegates, successors in title or third parties (authorised agents and contractors), when such parties are acting as responsible parties, joint responsible parties or operators in terms of applicable privacy laws, unless stated otherwise.
Generative artificial intelligence (GAI)	Generative artificial intelligence refers to a category of artificial intelligence technology that generates new outputs based on the data it has been trained on. Unlike traditional artificial intelligence systems that are designed to recognise patterns and make predictions, generative artificial intelligence creates new content in the form of images, text, audio, and more.
Juristic person	Means an existing company, corporation, trust, not-for-profit organisation or other legal entity recognised by law as having rights and duties.
Legislation	Means relevant and applicable data privacy and protection legislation, including but not limited to: • the Protection of Personal Information Act 4 of 2013 (POPIA); • the General Data Protection Regulation (GDPR); • the Data Protection (Bailiwick of Guernsey) Law, 2017; • the Data Protection (Jersey) Law 2018; and • the UK's Data Protection Act 2018.
Natural person	Means an identifiable, living human being.

Operator	Means a person who processes PI for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. This means any party that processes information on behalf of FirstRand.
PAIA	The Promotion of Access to Information Act 2 of 2000.
PCI standard	Means Payment Card Industry standard.
Personal information (PI)	Means information relating to an identifiable, living, natural person and where it is applicable an identifiable, existing juristic person, including, but not limited to: (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; (b) information relating to the education or the medical, financial, criminal or employment history of the person; (c) any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; (d) the biometric information of the person; (e) the personal opinions, views or preferences of the person; (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; (g) the views or opinions of another individual about the person; and (h) the name of the person if it appears with other PI relating to the person or if the disclosure of the name itself would reveal information about the person. In reference to this policy, PI must be seen primarily but without limitation as PI of group customers, employees and suppliers, and other persons and third parties.
PIN	Means "personal identification number", which is a secret numeric password known only to the user and a system to authenticate the user to the system.
POPIA	Protection of Personal Information Act 4 of 2013.
Processing	Means any operation or activity or any set of operations, whether or not by automatic means, concerning PI, including: (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; (b) dissemination by means of transmission, distribution or making available in any other form; or (c) merging, linking, as well as restriction, degradation, erasure or destruction of information.
Public record	Means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body.
Record	Means any recorded information: (a) regardless of form or medium, including any of the following: (i) writing on any type of material; (ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored; (iii) a label, marking or other writing that identifies or describes anything of which it forms a part, or to which it is attached by any means; (iv) a book, map, plan, graph or drawing;

	(v) a photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced; (b) being in the possession of or under the control of a responsible party; (c) whether or not it was created by a responsible party; and (d) regardless of when it came into existence.
Responsible party/ies	Means a public or private body or any other person which/who, alone or in conjunction with others, determines the purpose of and means for processing PI. In reference to this policy, the responsible parties are the FirstRand entities as defined above.
Sensitive cardholder PI	This information includes but is not limited to card validation codes/values, full track PI (from the magnetic strip or equivalent on a chip), PINs and PIN blocks. Authentication must be against cardholders and/or authorised payment card transactions in terms of PCI.
Special personal information (SPI)	Means any PI of a data subject, concerning: (a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health, sex life or biometric information of a data subject; or (b) the criminal behaviour of a data subject to the extent that such information relates to: (i) the alleged commission by a data subject of any offence; or (ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.
Supplier	Means a natural or juristic person who provides a product or renders services to the group.
DEFINITIONS FROM THE GDPR	
Controller	Means a juristic person in the group, registered in the United Kingdom, Guernsey or Jersey who, alone or jointly with others, determines the purposes and means for processing PI. Such purposes and means will be determined by the GDPR or privacy laws in the United Kingdom, Guernsey or Jersey.
Processor	Means a juristic person who processes PI on behalf of the controller.
Sub-processor	Means a juristic person defined in Annexures A1, A2 and A3 of this policy.

3 APPLICABILITY

This policy is applicable to all suppliers and business partners who collect and/or process PI and or/records for, on behalf of or together with the group. The group will at the time of the conclusion of any agreement, and regularly during the course and scope of its agreement with suppliers or business partners who collaborate with the group or provide goods and/or services which require the collection and/or processing of PI and/or records in accordance with this policy, provide them with a copy of this policy.

4 SCOPE OF APPLICATION

This policy is applicable to all PI, SPI and children's PI collected, retained, processed and disseminated by all suppliers and applicable business partners for, on behalf of, or together with the group in terms of an agreement between the group and the supplier or the business partner. This includes but is not limited to PI, SPI and/or children's PI of the employees of the group, group customers, employees of group customers, and third parties whose PI is in the possession of the group and subsequently processed on the group's behalf by the supplier or business partner.

This policy supports FirstRand's internal policies. Suppliers and business partners will be informed if they need to adhere to any other internal policy.

5 SUPPLIERS AND BUSINESS PARTNER OBLIGATIONS WHEN DEALING WITH PI AND RECORDS

5.1 Accountability

5.1.1 The supplier or business partner acknowledges and accepts that any PI and/or records received from the group and/or created by it for or on behalf of the group will not become the property of the supplier or business partner.

5.1.2 The supplier or business partner shall at all times be solely and fully responsible for all its employees, agents, subcontractors and other third parties who act on its behalf in the performance of their functions in terms of its relationship with the group.

5.1.3 The supplier or business partner may only make use of agents, subcontractors and third parties for the processing of the PI if:

- the group has been informed of the agent, subcontractor and third party used and such agent, subcontractor and third party has been approved by the group in writing;
- the supplier or business partner has conducted a privacy risk assessment of the agent, subcontractor and third party and the said agent, subcontractor and third party has passed the risk assessment and has the appropriate and necessary controls to mitigate any privacy risks; and
- the supplier or business partner concludes agreements with such agents, subcontractors and third parties on no less onerous terms than that which the supplier or business partner agreed on with the group.

5.1.4 By contracting with the group the supplier or business partner, in its performance of its mandate or the obligations under the applicable agreement, undertakes that its employees, agents, subcontractors and other third parties who act on its behalf in the performance of its functions in terms of its relationship with the group, and who shall have access to the group's PI and/or records, have signed the appropriate confidentiality undertakings; and that the supplier or business partner acknowledges and confirms that:

- it has appropriate internal policies dealing with privacy and security in place for purposes of compliance with privacy legislation;
- it has external privacy notices or policies which advise data subjects how it processes PI and which notices are aligned to the disclosure obligations of privacy legislation;
- its employees, agents, subcontractors and third parties have been provided with the appropriate training to ensure that they understand the provisions of privacy legislation and PI privacy principles in general, as well as their roles and responsibilities in relation to the provision of service to the group as a responsible party;
- it will at all times adhere to the provisions, updates and amendments of privacy legislation;
- when processing PI of children or SPI, it will at all times act in accordance with any special provisions provided for in privacy legislation and the provisions of the agreement with the group; and
- it will share PI with its agents, employees' subcontractors and other third parties only as strictly necessary, and to the extent necessary to process the PI in accordance with the agreement with the group.

5.1.5 During the course and scope of its agreement with the group, the supplier and/or business partner will not utilise group PI, SPI and/or records, including proprietary information, on GAI technologies in the provision of their services to the group. If the supplier and/or business partner is dependent on these technologies to provide a service to the group, the supplier and/or business partner must obtain prior written authorisation from FirstRand to do so. Where the supplier and/or business partner obtains approval to utilise GAI platforms, it shall be prohibited from utilising GAI in a manner that is inappropriate and contrary to the group's policies and standards. The supplier and/or business partner shall also refrain from the following activities (the below list is not exhaustive):

- utilising group PI, SPI and/or records, including proprietary information, in natural language processing or predictive analytics on an open-source GAI platform;
- utilising GAI that exploits the vulnerabilities of a specific group of persons due to age or any SPI categories which will lead to detrimental or unfavourable treatment of data subjects; and
- utilising GAI in a manner that contravenes data privacy and protection laws and copyright infringement laws.

The following policy statements relate only to the GDPR, the UK Data Protection Act 2018 and the UK GDPR, where in scope:

5.1.6 Where the supplier or business partner is confirmed as a processor by the group, and where, as a result of providing the service to a controller and such a service requires the collection and/or processing of PI belonging to the controller, the controller and the supplier will conclude a PI transfer agreement on the terms outlined in Annexures A1, A2 and A3 (which are not negotiable).

5.1.7 Where the supplier or business partner is confirmed as a sub-processor by the group, as a result of providing the service to the group, who is a processor, and such a service requires the collection and/or processing of PI belonging to a controller, the supplier or business partner will conclude a data transfer agreement with the group on the terms set out in Annexures A1, A2 and A3 of this policy (which is not negotiable).

The following policy statement relates only to the provision of cloud services, where in scope:

5.1.8 Where the supplier is a cloud service provider, the group will provide to the supplier its cloud services-specific terms and conditions, which will be incorporated into the agreement with the supplier.

5.2 Processing limitation

5.2.1 The supplier or business partner will, as far as possible, collect PI directly from the data subject to whom the PI relates unless: the information is contained in or derived from a public record; or deliberately made public by the data subject; or the data subject has consented thereto; or it is in the legitimate interest of the data subject or the group; or collection from another source is legally required; or needed for court proceedings or national security; or otherwise directed in writing by the group; or such PI and/or record is provided by the group.

5.2.2 The supplier or business partner will process PI of data subjects lawfully and in a reasonable manner so that it does not unreasonably intrude on the data subject's right to privacy. The supplier or business partner will ensure that, where legally necessary for a particular processing action, consent is collected from the data subject as per the instructions provided by the group, and that such consent will be retained as per records management best practice principles.

5.2. Purpose specification

5.2.3 The supplier or business partner shall collect PI and/or records only as far as such PI is necessary for the supplier or business partner to comply with the agreement, or for the exercise of the supplier's rights or instructions in terms of the agreement with the group.

5.2.4 The group requires the supplier or business partner to maintain all PI and/or records for the period required by the applicable legislation and to keep an up-to-date retention schedule as required by records management principles. The supplier or business partner will be required to maintain the records and apply records management best practice principles to all PI, in accordance with the applicable legislation, irrespective of the form. All retention periods, disposal methods and/or processes must be documented and the evidence of the destruction of all records must be maintained. A copy or applicable extract of the group's records retention and destruction policies will be made available where necessary or required.

5.3 Further processing limitation

5.3.1 The supplier or business partner shall only collect and/or process PI and/or records for the purpose for which it was originally collected and to fulfil all its obligations to the group in terms of its agreement with the group.

5.3.2 If there is a requirement for any further processing of PI and/or records, authorisation from the group will be requested in writing by the supplier or business partner. No reliance may be placed by the supplier or business partner on the exceptions contained in section 15 of POPIA.

5.4 Information quality

5.4.1 The supplier or business partner shall ensure that, where PI is processed in fulfilment of its obligations under any agreement with the group, that such PI is complete, accurate, not misleading and updated where necessary. Should the supplier or business partner become aware of any PI changes, the supplier or business partner must as soon as practically possible inform the group of such changes; and whether a data subject's PI is incomplete, inaccurate or misleading so that the necessary updates are made.

5.5 Openness

5.5.1 If the supplier or business partner collects PI, SPI or children's PI on behalf of the group, the supplier or business partner must notify the data subject from whom the information is being collected, to the extent required by applicable privacy laws, of the following:

- that the supplier or business partner is acting on behalf of the group;
- what information is being collected;
- the purpose of the collection of that information;
- any legal requirements for collection;
- whether the supply of the information is voluntary or mandatory;
- the consequences for failure to supply such information;
- the name and address of the responsible party;
- where applicable, whether the responsible party intends to transfer the information across a border or borders, to another country and the level of protection afforded the information by that country;
- the right of the data subject to access and correct the PI; and

- any further information as required by the group (such as the recipients of the information, existence of the right to access/rectify the information, existence of the right to object to the processing of the information, and the right to lodge a complaint to the Information Regulator and its contact details).

5.5.2 All employees, agents and subcontractors of the supplier or business partner shall take reasonable steps to identify themselves to a data subject who has been contacted. Further to that, the data subject must be informed that the said supplier or business partner is acting on behalf of the group.

5.6 Security safeguards

5.6.1 The supplier or business partner shall secure the integrity and confidentiality of all PI and/or records in its possession by putting appropriate, reasonable, technical and organisational measures in place to prevent loss or unauthorised destruction of PI, as well as to prevent unlawful access to or processing of PI in the supplier's or business partner's possession.

5.6.2 The supplier or business partner must complete the group PI third-party privacy assessment prior to the conclusion of the agreement. The control environment must be agreed upon with the group prior to the commencement of the engagement.

5.6.3 The supplier and business partner are prohibited from disclosing or transferring PI and/or records to any external third party, except for the purposes of fulfilling their obligations in terms of the relationship with the group; or unless otherwise directed to do so by the group in writing; or unless otherwise required by law.

5.6.4 Where the supplier or business partner is requested to disclose PI and/or records for a purpose not authorised under the agreement with the group, or if disclosure is required by law, then the supplier or business partner will immediately notify the group regarding the request or demand disclosure in writing, and must not disclose the PI unless directed to do so in writing by the group, or unless otherwise required by law. Where disclosure is required by law, the supplier or business partner will, where possible, provide the group with reasonable written notice of such requirement in order to provide the group with an opportunity to exercise its rights, and will only disclose such PI and/or records as it is strictly required to disclose by law.

5.6.5 The supplier or business partner shall identify all reasonably foreseeable internal and external risks to PI in the fulfilment of its obligations in terms of the agreement with the group. Appropriate safeguards must be established and maintained against the identified risks. Regular verification of the effective implementation of such safeguards and continual review and updates of safeguards in response to new risks must be undertaken by the supplier and business partner. Records of the reviews must be retained.

5.6.6 The group may, at any time and upon reasonable notice to the supplier or business partner, enter the premises of the supplier or business partner to inspect or audit, or request a third party to audit the supplier's or business partner's compliance with this policy. This includes but is not limited to security and information management requirements under the provisions of privacy legislation and/or the terms and conditions of the agreement as concluded between the supplier or business partner and the group. The supplier or business partner is required to cooperate with any such audit or inspection.

5.6.7 The supplier or business partner must notify the responsible party (the group) immediately where there are reasonable grounds to believe that the PI that it processes on behalf of the group has been accessed or acquired by any unauthorised person or entity.

5.6.8 The group will nominate a contact person to receive such privacy incidents, which will also be specified in the agreement.

5.6.9 At the time of the privacy incident, the supplier or business partner must report the privacy incident information to the group as per Annexure B.

5.6.10 The group will put in place internal processes and procedures with clearly defined roles and responsibilities. This will ensure that the discovery or identification, recording and management of security compromises as they arise, are in line with its internal privacy incident management plan.

5.6.11 In the event that the supplier or business partner handles or processes payment card information on behalf of the group, they must at all times fully comply with the relevant and current standard as outlined in the Payment Card Industry Data Security Standard (PCI DSS) (www.pcisecuritystandards.org) to ensure continuous protection of sensitive cardholder data. The supplier or business partner will at all times be responsible for security when processing and transmitting card information and PI. The group may, as and when required, request proof of compliance to PCI DSS.

5.7 Data subject participation

5.7.1 A data subject has the right to, after providing adequate proof of identity and after payment of any fee required by law (if applicable):

- enquire if PI about them has been collected by the supplier or business partner on behalf of the group;
- enquire how the PI is being used by the supplier or business partner whilst acting on behalf of the group;
- enquire whom the information has been disclosed to by the supplier or business partner whilst acting on behalf of the group;
- challenge the accuracy and completeness of PI in the possession of the supplier or business partner who is acting on behalf of the group;
- object to the processing of such PI by the supplier or business partner who is processing on behalf of the group; and
- withdraw their consent to the processing of their PI by the supplier or business partner who is processing on behalf of the group.

5.7.2 The supplier or business partner must immediately direct any requests by a data subject to access and/or amend any PI, or requests to withdraw consent to the processing of their PI that the supplier or business partner holds on behalf of the group, to the group to be handled in terms of the group's PAIA manual and process.

6 AUDIT AND INSPECTION OF PI AND RECORDS

6.1 Prior to the conclusion of any agreement with any supplier or business partner that will process PI and/or records on behalf of the group, the group may conduct a third-party privacy assessment when required.

6.2 The group reserves the right to audit, upon providing the supplier with reasonable notice of the said audit, the controls implemented by the supplier and business partner throughout the duration of the agreement, as a measure of continued due diligence or privacy risk mitigation on the part of the group.

6.3 The group reserves the right to audit:

- the supplier's or business partner's adherence to privacy principles, as well as security, information and records management practices, but most importantly the supplier's or business partner's compliance with the policy requirements set out herein; and
- the PI and/or records that the supplier or business partner holds on behalf of the group in performance of its obligations towards the group.

7 CROSS-BORDER TRANSFER

7.1 In cases where the supplier or business partner (or any of its subcontractors) is domiciled outside the Republic of South Africa, or transfers PI and/or records outside the Republic of South Africa whilst collaborating with or providing the group with goods and/or services, such information may only be transferred in terms of the agreement with FirstRand.

7.2 Where the processing of PI occurs in a country which has legislation more stringent than POPIA, then the more stringent legislation's provisions will be applicable to the processing of such personal information.

7.3 The supplier and business partner may not transfer PI that is being processed on behalf of the group outside the borders of the Republic of South Africa unless:

- the supplier, business partner or third party who is receiving the information is subject to a PI protection law, binding corporate rules or binding agreement rules that effectively uphold the principles of reasonable processing and contain provisions that have substantively similar provisions to POPIA regarding transfer of PI to foreign jurisdictions;
- the data subject has provided consent for the transfer;
- the transfer of such PI is required for the performance of a contract between the data subject and the group;
- the transfer of such PI is necessary for the performance of a contract concluded between the group and a third party, in the interest of the data subject;
- the transfer of such PI is for the benefit of the data subject and it is not practical to obtain consent and the data subject would have provided such consent had the data subject been able to; or
- with the prior written approval of the group.

8 NOTIFICATIONS BY SUPPLIER OR BUSINESS PARTNER TO THE GROUP

8.1 All notifications to the group relating to access to PI and/or records in the possession of a supplier or business partner that contain PI but belong to the group, shall be addressed to the group in writing.

8.2 These notifications include notifications to comply with requests from the Information Regulator in terms of POPIA compliance; requests for access to PI; requests to address complaints from the Information Regulator; and requests to access information, in terms of PAIA, that is the property of the group.

9 THIRD-PARTY MANAGEMENT

9.1 The supplier or business partner must inform the group in writing, prior to engaging the services of a third party or subcontractor, to assist in providing services in terms of the main agreement with the group. The group may approve or decline the use of such third party or subcontractor.

9.2 Where the group approves the appointment of such third party or subcontractor, the supplier or business partner shall provide the group with written confirmation of such appointment, which includes the identity and location of such third party or subcontractor.

9.3 The supplier or business partner may only disclose PI and/or records to third parties under the following circumstances:

- in the case that the supplier or business partner has contracted with a third party to provide goods and/or services on behalf of the supplier or business partner in order for the supplier or business partner to perform its obligations under the agreement with the group;
- has the consent of the data subject;
- to protect the legitimate interest of the data subject;
- to pursue the legitimate interest of the group;
- to pursue the legitimate interest of a third party; or
- in cases where the supplier or business partner is under a legal duty to share PI and/or records, to comply with a legal obligation.

9.4 In sharing this information, the supplier or business partner shall ensure that the third party provides the same level of protection to the PI as required by this policy, the agreement with the group and applicable PI protection laws. The contract between the third party and/or supplier or business partner must adhere to the requirements contained in this policy. For the purposes of this section, "third party" means any person or entity other than the supplier and/or operator, the group or other persons authorised by the group to process PI for the responsible party, this being the group.

10 TERMINATION EXPECTATIONS

10.1 At termination of the agreement, the supplier or business partner will, at the direction of the group:

- return to the group all PI and/or records that contain PI that belong to the group that were created throughout the duration of the agreement, including PI and/or records that were provided to the supplier and business partner at the inception of the engagement with the group, irrespective of when they were created or provided; or
- provide the group with the destruction certificate indicating that all PI and/or records that contain PI that were the possession of the supplier or business partner have been destroyed; and
- ensure that all PI and/or records in the possession of a third party (as defined in paragraph 9.4) or subcontractor are returned to the group.

11 GENERAL

The group reserves its right to enforce its rights as stated in the agreement between the group and the supplier or business partner if the supplier or business partner fails to comply with the provisions of this policy or the applicable legislation provisions. Failure to comply with the provisions of this policy may, without limitation, result in legal action and/or termination of the master agreement with the group.

12 OWNERSHIP AND REVIEW

This policy is owned by FirstRand Group Compliance and must be reviewed at least every two years. This policy will also be reviewed when any applicable code of conduct under POPIA is published or there is any amendment to any overarching legislation.

-END-

ANNEXURE B

Reporting of privacy incidents by suppliers and business partners

(a) Reporter information

Name, surname, employee number, email address, cell number of person reporting the privacy incident.

(b) Description of the privacy incident circumstances

1. Root cause information relating to the privacy incident. The root cause should be further classified according to: external causal factors (e.g. phishing attacks, denial of services); people causal factors (e.g. unauthorised activity by internal or external staff in relation to the PI); governance causal factors (e.g. no proper escalation processes and lack of proper oversight in relation to PI processing activities); process causal factors (e.g. inefficient/ineffective process design or inadequate or ineffective procedures in relation to the exchange of PI with third parties); and technology, infrastructure, facilities causal factors (e.g. inadequate data/system security including access/protection/configuration).
2. Does the privacy incident involve identifiable PI or is the PI anonymised?
3. Date of the privacy incident.
4. Who was the privacy incident reported to?
5. Systems involved?
6. How many (volume of) records affected?
7. How many customers/data subjects affected?
8. Does the privacy incident include special personal information or sensitive information of a data subject?
9. Group operating business/customer segments/business unit(s) affected.
10. Confirmation of the number of FirstRand customers impacted, emanating from the FirstRand data which has been compromised.
11. Provide a list of the affected data fields, emanating from the FirstRand data which has been compromised.
12. Provide a proposed remediation plan for the data breach.
13. Provide a brief description of the potential service disruptions anticipated from the Supplier and/or Business Partner as a result of the data breach, including interim plans to manage the disruption.

(c) Remediation actions

1. Information relating to the remedial actions undertaken by the supplier or business partner. Such actions should be described in detail.
2. The Supplier and/or Business Partner must provide assurance that when a privacy incident occurs, the incident will be reported to FirstRand in terms of the agreed timelines, set out in the agreement.
3. The Supplier and/or Business Partner must provide assurance that, where the Supplier and/or Business Partner is an Operator of FirstRand, they will cooperate and assist FirstRand with the requisite information to enable FirstRand to fulfill its regulatory obligations. The Supplier and/or Business Partner will not be permitted to release any communications or notifications without FirstRand's approval and consent.
4. The Supplier and/or Business Partner must provide assurance that, where the Supplier and/or Business Partner is a joint responsible party or joint Data Controller with FirstRand, the Supplier and/or Business Partner will collaborate and cooperate with FirstRand and agree on the communications and remedial actions disclosed to regulators and the public.

(d) Non-compliance to privacy law and/or other legislation

Specify which sections in the applicable privacy legislation has been breached.