



# DATA PROCESSING POLICY (SOUTH AFRICA)\_EXTERNAL

**This Policy prescribes the principles and standards which Experian South Africa requires its third parties to adhere to when it processes Personal Information sent to, or obtained from, Experian whether directly or indirectly.**

All third parties submitting Personal Information to Experian, processing personal information on behalf of Experian, processing Personal Information when accessing Experian's systems or who receives Personal Information from Experian, must comply with the Protection of Personal Information Act, 2013 ("POPIA").

This Policy prescribes the principles and standards by which Experian will require above-mentioned third parties to process Personal Information in order to comply with POPIA and ensure that a Data Subject's right to privacy is not infringed.

## WHAT EVERY EMPLOYEE NEEDS TO KNOW ABOUT THIS POLICY

<b>WHO</b>	This Policy applies to all third parties who (i) access Personal Information from Experian, whether directly or indirectly (i.e. through a re-seller partner); (ii) who provides Personal Information to Experian (whether directly or indirectly); who (iii) process Personal information on Experian's behalf or who (iv) process Personal Information when they access Experian's systems (" <b>Third Parties</b> ").
<b>WHAT</b>	This Policy describes the principles that Third Parties must apply when providing Personal Information to Experian, or accessing Personal Information from Experian. The Policy requires all Third Parties to comply with POPIA, the NCA and other laws and regulations including industry or association rules and standards.
<b>WHY</b>	This Policy is important because it establish the standards required to Process Personal Information when providing it to, or accessing it from, Experian.

**KEY POLICY  
POINTS**

- Third Parties must ensure that they comply with POPIA and the NCA when requesting data or services (directly or indirectly) from Experian and should ensure that their requests are lawful.
- Third Parties must ensure that they meet the obligations of POPIA and the NCA (where applicable) when they provide Personal Information to Experian. For the avoidance of doubt, this Policy outlines the need to comply with POPIA when Processing the Personal Information of both natural and juristic entities.
- Third Parties must ensure that they keep data secure and confidential.
- Third Parties must ensure that where there is confirmed or suspected unauthorised access to Personal Information obtained from Experian, they notify Experian of such access immediately.



# 1. Introduction and Background

Experian South Africa (Pty) Ltd ("**Experian**") Processes Personal Information of both natural and juristic entities in accordance with POPIA and Experian is committed to complying with POPIA and the conditions for the lawful Processing of Personal Information. Experian is a registered consumer credit bureau with the National Credit Regulator (with registration number: NCRCB16). Experian furthermore operates as a commercial bureau, a full data hosting bureau, and is a member of the Credit Bureau Association ("**CBA**"), the South African Credit Risk Reporting Association ("**SACRRA**") and the Direct Marketing Association of South Africa ("**DMASA**").

Depending on the circumstances, Experian could act as a Responsible Party or as an Operator for purposes of POPIA.

As a registered consumer credit bureau, Experian plays a key role in South Africa's financial ecosystem and as a result, we are heavily regulated by various acts of legislation, the core of which is the National Credit Act and its Regulations ("**NCA**"), as well as POPIA.

The process in terms of which Experian manages the consumer credit data is complex and there are various stakeholders in the industry that play a role in this data management process. These stakeholders include the data providers, the industry associations (including SACRRA), as well as all the credit bureaus in South Africa. In the circumstances where Experian acts as the Responsible Party, it means that Experian has certain responsibilities under POPIA to ensure that the Personal Information is used fairly and lawfully and that it remains protected at all times. In other circumstances, Experian acts as the Operator for its clients (when they request Personal Information from Experian) as well as for data providers (when they submit Personal Information to Experian). Due to this complex environment and because of the sensitive data that Experian Processes (both as a Responsible Party and an Operator) it is critical that all entities who do business with Experian, subscribe to specific standards when either submitting data to Experian or when requesting data from Experian or Processing data on Experian's behalf.

## 2. Objective & Scope

### 2.1. Objective

The key Policy objectives is to ensure that when Personal Information is shared with, or obtained from Third Parties, that the Personal Information is processed in accordance with the requirements of POPIA and any other applicable Data Protection Legislation, is kept safe and secured at all times and that the personal integrity of the Personal Information is respected. Experian is committed to ensuring the protection of the Personal Information entrusted to it by its stakeholders, its clients and its business partners. The Purpose of this document is to set out the rules and standards that all Third Parties who request Personal Information from Experian, submit Personal Information to Experian, or who processes Personal Information on behalf of Experian, should subscribe to and follow.

## 2.2. Policy Scope

The Policy applies to all Third Parties and the terms of this Policy shall be deemed to form part of the Third Party's agreement with Experian ("the **Agreement**").

## 3. Terms and Definitions

Term	Definition
"consent"	the Data Subject agrees by a statement or positive action to the Processing of his or her Personal Information by a clear affirmative act that is freely given, specific, informed, and unambiguous.
"Consumer Credit Information"	<p>means information concerning—</p> <ul style="list-style-type: none"> <li>(a) a person's credit history, including applications for credit, credit agreements to which the person is or has been a party, pattern of payment or default under any such credit agreements, debt re-arrangement in terms of the National Credit Act, incidence of enforcement actions with respect to any such credit agreement, the circumstances of termination of any such credit agreement, and related matters;</li> <li>(b) a person's financial history, including the person's past and current income, assets and debts, and other matters within the scope of that person's financial means, prospects, and obligations, as defined in section 78(3) of the National Credit Act and related matters;</li> <li>(c) a person's education, employment, career, professional or business history, including the circumstances of termination of any employment, career, professional or business relationship, and related matters; or</li> <li>(d) a person's identity, including the person's name, date of birth, identity number, marital status and family relationships, past and current addresses and other contact details, and related matters.</li> </ul>
"Data Protection Legislation"	means any data protection or data privacy laws applicable in the Republic of South Africa from time to time, including but not limited to the Protection of Personal Information Act 4 of 2013, the Promotion of Access to Information Act, 2 of 2000, the Electronic Communications and Transactions Act 25 of 2002, the Consumer Protection Act 68 of 2008 and the National Credit Act 34 of 2005, together with the Regulations thereto.
"Data Subject"	the person to whom Personal Information relates.
"Experian"	Experian South Africa (Pty) Limited
"Experian Data"	means any data, including Personal Information, supplied to the Third Party or its personnel by or on behalf of Experian or an affiliate of Experian, or Processed by or on behalf of Experian or an Affiliate of Experian or its personnel where Experian is the Responsible Party in relation to that data.

“NCA”	the National Credit Act 34 of 2005 together with the Regulations thereto.
“person”	a natural person or a juristic person.
“Personal Information”	any other information which may be treated or defined as "personal information" in terms of any applicable laws, including Data Protection Legislation.
“Personal Information Breach”	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Information transmitted, stored or otherwise processed.
“Processing”	means to collect, receive, record, organise, collate, store, develop, retrieve, consult, use, disseminate or perform any other act or action, including any other act or action which may be treated or defined as " <b>process</b> " or " <b>processing</b> " in terms of any applicable laws (including Data Protection Legislation). The word " <b>processed</b> " shall have a corresponding meaning.
“Responsible Party”	also known as a “controller”, determines the purposes and the means for Processing Personal Information i.e. determines how to collect, store, and use the Personal Information.
“Special Personal Information”	means categories of particularly sensitive Personal Information, such as information regarding a person’s health or sex life, racial or ethnic origin, religious or philosophical beliefs, sexual orientation, criminal behaviour or trade union membership and biometric information. Special Personal Information require higher levels of protection. Experian will only Process Special Personal Information when it has a clear legal justification for processing this type of Personal Information. Experian has implemented appropriate policies and safeguards to ensure it applies the strictest privacy standards when it Processes Special Personal Information.
“Third Party”	Means a third party who provides Personal Information to Experian, submits Personal Information to Experian, who processes Personal Information on behalf of Experian, or who accesses Experian systems and can then obtain access to Personal Information, whether directly or indirectly. This includes clients, vendors, service providers, re-sellers and end-users of re-sellers (including the Third Parties of re-sellers).
“Third Party Data”	Means, collectively, all Personal Information provided to Experian by the Third Party or otherwise pertaining or relating to the Third Party.



## 4. Policy Requirements

### 4.1. PERSONAL INFORMATION AND DATA PROTECTION

4.1.1. The Third Party will ensure that –

- 4.1.1.1. where it has or will provide information and/or data, or access to information or data, including Personal Information, to Experian or where it requests data or information or services from Experian, that it meets the requirements of Data Protection Legislation and specifically that it meets the lawful conditions of Processing as set out in section 11 of POPIA and that, where required, it has obtained the required permissions and consents to the extent necessary and in compliance with the provisions of the Data Protection Legislation and/or any other relevant legislation relating to consumer protection to enable it to lawfully provide and/or access such information or data, including Personal Information, to and/or from Experian;
- 4.1.1.2. if required, that in respect of all Third Party Data, it has obtained all the required consents from and or provided the necessary notifications to the person or entity to whom such Personal Information relates, as well as any regulators or other third parties (as applicable), that is necessary to ensure compliance by the Third Party and Experian with Data Protection Legislation, including in relation to (i) the transmission of the Third Party Data by the Third Party to Experian in accordance with the Agreement or otherwise permitted by applicable law, including Data Protection Legislation; (ii) the transmission by the Third Party or Experian of the Third Party Data to other third parties in accordance with the Agreement or as otherwise permitted by Data Protection Legislation; (iii) the Processing of the Third Party Data by Experian, in any country in which the Third Party Data is Processed by Experian; and (iv) the sharing of the Personal Information by Experian with the Third Party;
- 4.1.1.3. it will not request Experian to process Special Personal Information, specifically the information of Children (as defined in POPIA);
- 4.1.1.4. the Third Party will process Personal Information only in accordance with the Agreement and in terms of a lawful purpose.
- 4.1.1.5. the Third Party's Personnel will only access and use Personal Information received from Experian in accordance with the Agreement and shall maintain the confidentiality of such Personal Information.
- 4.1.1.6. the Third Party shall not transfer any Personal Information outside the Republic of South Africa, unless with Experian's prior written consent and upon meeting the requirements of POPIA for cross-border transfer of Personal Information;
- 4.1.1.7. the Third Party will comply with all applicable industry codes of conduct to the extent that they regulate or relate to the Processing of Personal Information;

- 4.1.1.8. it shall use and apply appropriate measures, procedures and controls in relation to Personal Information, in accordance with best industry practice;
- 4.1.1.9. it shall not do anything, or omit to do anything, which will cause Experian to contravene any applicable laws, including any Data Protection Legislation;
- 4.1.1.10. it shall keep Experian Data confidential; and
- 4.1.1.11. it shall at all times strictly comply with Experian policies and procedures pertaining to the protection, privacy, processing and destruction of Personal Information (that has been shared with the Third Party) that apply to Experian and to which Experian is subject.

4.1.2. The Third Party may only process Experian Data:

- 4.1.2.1. for the specific purposes for which it was disclosed to the Third Party, and as defined in any agreement concluded between Experian and the Third Party; and/or
- 4.1.2.2. as required or permitted by applicable law, including any Data Protection Legislation; and/or
- 4.1.2.3. with the express prior written consent of Experian.

## 4.2. SECURITY MEASURES

The Third Party shall implement reasonable and appropriate technical and organisational measures and precautions necessary to ensure the integrity and confidentiality of all Personal Information and to prevent any (i) loss of, damage to, or unauthorised destruction of the Personal Information; or (ii) unauthorised or unlawful access to or processing of the Personal Information and (iii) accidental loss or destruction of, or damage to, that Personal Information in accordance with the requirements in section 19 of POPIA. The Third Party will ensure a level of data security relating to the Personal Information that is appropriate to the risk presented by the processing and maintain the following safeguards:

### 4.2.1 Policies and Governance

- 4.2.1.1 The Third Party shall have in effect and apply an information security program to protect Personal Information. Such information security program will be consistent with industry standards and will be sufficient to:
  - 4.2.1.1.1 protect the security and confidentiality of the Personal Information received from Experian;
  - 4.2.1.1.2 protect against any anticipated threats or hazards to the security or integrity of the Personal Information received from Experian; and
  - 4.2.1.1.3 protect against unauthorised access to or use of the Personal Information received from Experian that could result in substantial harm or inconvenience to Experian or the Data Subject.
- 4.2.1.2 The Third Party agrees to comply with and shall ensure that all its employees, Authorised Users and sub-contractors abide by Experian's information security policies and requirements, including this Policy, (as communicated to the Third Party from time to time in writing) and the Data Protection Legislation. The

Third Party shall ensure that Personal Information received from Experian is processed in accordance with Experian's information security policies and procedures relating to information security and data protection as notified to the Third Party from time to time in writing and that it is Processed and distributed in a manner that ensures that the Personal Information and/or Consumer Credit Information remains confidential and secure.

#### **4.2.2 Network Security and Encryption**

4.2.2.1 The Third Party will safeguard the confidentiality and integrity of all Personal Information received from Experian and maintain strong, industry-standard encryption techniques. The Third Party shall ensure that, meeting industry standards, all Personal Information is encrypted at rest and while in transit, that employees, agents and sub-contractors cannot access Personal Information on their personal devices and that all hardware (including computers and laptops) are encrypted.

4.2.2.2 The Third Party's internet connections will be protected with dedicated, industry-recognised firewalls that are configured and managed consistent with industry standards.

4.2.2.3 The Third Party shall ensure that it has a security program in place which will be consistent with industry standards and which will be sufficient to protect the Personal Information against unauthorised access, unlawful destruction, loss and threats, and which will ensure the confidentiality and protection of the Personal Information against unauthorised disclosure and that the Third Party shall have an incident response plan in place.

4.2.2.4 The Third Party will apply a data retention and destruction/expungement policy and procedures in line with industry standards, will ensure that malware and detection services will be used to protect Personal Information from viruses, that Personal Information usage by Authorised Users will be monitored and that appropriate access control measures will be employed. The Third Party shall furthermore provide Experian within 5 (five) business days with assurance or a certificate confirming that Personal Information has been deleted and expunged upon request from Experian.

4.2.2.5 The Third Party will apply regular fraud detection, prevention, reporting and escalation procedures and ensure that a sufficient business continuity processes is in place.

#### **4.2.3 Isolation of Personal Information**

4.2.3.1 The Third Party will keep all Personal Information received from Experian separate from other information so that it can be identified as Personal Information.

4.2.3.2 The Third Party will ensure that the Personal Information received from Experian is securely stored when in storage. Any cloud storage outside of South Africa should be done meeting the requirements of Data Protection Legislation and requires Experian prior written consent.

#### **4.2.4 Authorisation of users**



4.2.4.1 The Third Party will ensure that only its Authorised Users will have access to Personal Information received from Experian and such Authorised Users' log-in details and passwords remain confidential and are removed upon termination of the Authorised User's employment with the Third Party .

4.2.4.2 The Third Party will ensure that passwords will meet the necessary complexity requirements and should expire within a reasonable time.

4.2.4.3 The Third Party will regularly provide training and awareness to its personnel on data security and confidentiality.

#### 4.2.5 **Virus and Malware Protection**

4.2.5.1 The Third Party shall implement malware detection/scanning services and procedures to protect all Personal Information received from Experian against viruses and malware and will keep its anti-virus programs up to date.

#### 4.2.6 **Physical Security**

4.2.6.1 The Third Party shall limit physical access to its premises where any Personal Information received from Experian can be accessed by Authorised Users only.

#### 4.2.7 **Security Compromises**

4.2.7.1 The Third Party shall establish processes and procedures for identifying and responding to any IT incidents/cyber incidents/data incidents or other security compromises or Personal Information Breach (each an "**Incident**").

4.2.7.2 If the Third Party reasonably suspects or becomes aware of any actual or suspected Incident it will:

4.2.7.2.1 immediately, but no later than twenty-four (24) hours of reasonable suspecting or becoming aware of an Incident, notify Experian of the Incident by e-mail to: [informationofficerafrica@experian.com](mailto:informationofficerafrica@experian.com); and

4.2.7.2.2 investigate the Incident and provide Experian with detailed information about the Incident; and

4.2.7.2.3 at its own cost, take all necessary steps to mitigate the extent of the loss or compromise of the Personal Information and restore the integrity of the affected information systems as quickly as possible, and will provide Experian with any and all necessary information that Experian may request pursuant to the Incident and to assist Experian to meet any regulatory requirements and obligations in respect of the Personal Information or Services; and

4.2.7.2.4 assist Experian (in any reasonable format as will be required by Experian from time to time) to comply with any requests for access to Data from Data Subjects.

### 4.3. **AUDITS AND CERTIFICATIONS**

#### **Right to Audit**

- 4.3.1 Experian may conduct audits and security risk assessments to assess the Third Party's information security program during normal business hours and upon 3 (three) month's prior written notice of such audit or assessment (which 3 month period may be reduced in the event of an audit by an external Regulator, in which event Experian will provide the Third Party with notice as soon as Experian becomes aware of the need for the audit) which notice will include the scope of the audit in the form of an audit engagement letter.
- 4.3.2 During such audits, Experian shall at all times comply with Data Protection Legislation and those of the Third Party's reasonable security procedures and confidentiality requirements provided to Experian in writing in advance of any such audit.
- 4.3.3 All third party external audit costs will be borne by Experian, unless the audit contains adverse findings, in which event the costs will be borne by the Third Party.

#### **Certification**

- 4.3.4 Alternatively to the audit above, and if requested in writing, the Third Party may provide an industry-standard security certification, or third party assessment report (e.g. SOC 2 Type II or ISO27001) to evidence the existence and implementation of security measures as set forth in clause 4.2 above.

#### **Remediation**

- 4.3.5 The Third Party will remediate any errors or deficiencies identified in an audit that could reasonably be expected to have a material adverse impact on the Personal Information received from Experian.

#### **Assistance**

- 4.3.6 Experian may require the Third Party to provide audit assistance to Experian in the event of Experian having to undergo a regulatory and/or data security and confidentiality audits (whether internal or external), which audits will be subject to the entering into of confidentiality undertakings.

Please direct all comments and questions related to this Policy to the DPO mailbox [informationofficerafrica@experian.com](mailto:informationofficerafrica@experian.com).



## 13. Appendices

### Appendix A – Document Management and Version History

<b>Document ID Number:</b>	20210630.02
<b>Policy Type:</b>	South Africa
<b>Parent Policy:</b>	Data Processing Policy (EMEA), Data Processing Policy (SA), Privacy Notice_External
<b>Target Audience:</b>	Experian South Africa and all third parties
<b>Executive Policy Owner:</b>	Chief Legal Officer
<b>Governance Head:</b>	Data Privacy Office Africa Head
<b>Committee Endorsement:</b>	Africa Executive Leadership Team
<b>Approval Frequency:</b>	12 months
<b>Effective Date:</b>	01 <sup>st</sup> July 2021
<b>Last Date Approved:</b>	30 June 2021

<b>Version</b>	<b>Effective Date</b>	<b>Approval Date</b>	<b>Author</b>	<b>Approved by</b>	<b>Revision</b>
1.0	01 June 2021	30 June 2021	Annelene Dippenaar	Janine West	1