



**EXPORT CREDIT INSURANCE CORPORATION  
OF SOUTH AFRICA SOC LIMITED (ECIC)**

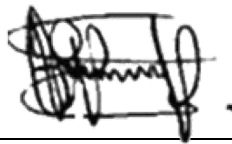
**DATA PROTECTION AND PRIVACY POLICY**

## Foreword

This Data Protection and Privacy Policy is applicable to the Export Credit Insurance Corporation of South Africa SOC Ltd for the sole use of ECIC Staff, Management and the Board. It shall be updated once every three years or from time to time considering changes in the marketplace and / or government legislation that impacts on the way ECIC conducts business.

## Revision History

Revised Series	Version. Revision	ECIC Approval Date	Next Review Dated



Chief Executive Officer

05 - 11-2020

Date



Chairperson of Risk Committee

05/11/2020

Date



Chairperson of the Board

05/11/2020

Date

# Table of Contents

Foreword .....	2
Revision History .....	2
1. DEFINITIONS.....	4
2. INTRODUCTION .....	9
4. PURPOSE .....	10
5. APPLICATION.....	10
6. CONDITIONS FOR LAWFUL PROCESSING OF PESONAL INFORMATION .....	10
7. STORAGE OF PERSONAL INFORMATION .....	27
8. PERSONAL INFORMATION FOR DIRECT MARKETING PURPOSES .....	28
9. FAILURE TO PROVIDE PERSONAL INFORMATION.....	28
10. PROVISION OF PERSONAL INFORMATION TO THIRD PARTIES .....	28
11. PERSONAL INFORMATION FOR EMPLOYMENT RELATIONSHIP .....	29
13. TELECOMMUNICATION AND INTERNET .....	30
14. USER DATA AND INTERNET .....	30
15. REPORTING OF BREACHES OF PERSONAL INFORMATION .....	31
16. RESPONSIBILITIES FOR COMPLIANCE WITH THIS POLICY.....	31
17. TRAINING AND AWARENESS .....	36
18. REVIEW OF THE POLICY .....	36
19. NON – COMPLIANCE.....	37
20. LINKS TO OTHER POLICIES.....	37

## 1. DEFINITIONS

In this Policy (as defined below), unless the context requires otherwise, the following terms shall have the meanings given to them –

- 1.1 “**biometrics**” means a technique of personal information that is based on physical, physiological or behavior characterization including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition;
- 1.2 “**Board**” means the board of ECIC directors;
- 1.3 “**child**” means any natural person under the age of 18 (eighteen) years; who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning himself or herself;
- 1.4 “**code of conduct**” means a code of conduct issued in terms of chapter 7 of the Protection of Personal Information Act (Act No.4 of 2013);
- 1.5 “**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;
- 1.6 “**consent**” means any voluntary, specific and informed expression of will in terms of which permission is given for processing personal information;
- 1.7 “**Constitution**” means the Constitution of the Republic of South Africa, 1996;
- 1.8 “**data subject**” means the ECIC clients or suppliers who may be natural or juristic persons or any other person(s) or employees in respect of whom the ECIC Processes Personal Information;
- 1.9 “**de-identify**” in relation to personal information of a data subject, means to delete any information that –
  - (a) identifies the data subject;
  - (b) can be used or manipulated by a reasonably foreseeable method to identify the data subject;
  - (c) can be linked by a reasonably foreseeable method to other information that identifies the data subject; and “**de-identified**” has the same meaning;
- 1.10 “**direct marketing**” means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of—

- (a) promoting or offering to supply, in the ordinary course of buy any goods or services to the data subject; or
- (b) requesting the data subject to make a donation of any kind for any reason;

1.11 **“electronic communication”** means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient’s terminal equipment until it is collected by the recipient;

1.13 **“employee”** means ECIC employee

1.14 **“enforcement notice”** means a notice issued in terms of section 95 of POPIA;

1.15 **“EXCO”** Executive Management of ECIC;

1.16 **“filing system”** - means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria;

1.17 **“information matching programme”** - means the comparison, whether manually or by means of any electronic or other device, of any document that contains personal information about ten or more data subjects with one or more documents that contains personal information of ten or more data subjects, for the purpose of production or verifying information that may be used for the purpose of taking any action regarding an identifiable data subject

1.18 **“information officer”** of, or in relation to, a –

- (a) public body means an information officer or deputy information officers as contemplated in terms of section 1 or 17 of PAIA; or
- (b) the person who is responsible for ensuring the organisation's compliance with POPIA and duly appointed by the Board;

1.19 **“ICT”** means Information and Communications Technology;

1.20 **“operator”** means a person or entity who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that responsible party;

1.21 **“PAIA”** means Promotion of Access to Information Act (No 2 of 2000)

1.22 **“person”** means a natural person or a juristic person;

1.23 **“personal information”** means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to -

1.23.1 information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

1.23.2 information relating to the education or the medical, financial, criminal or employment history of the person;

1.23.3 any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

1.23.4 the biometric information of the person;

1.23.5 the personal opinions, views or preferences of the person;

1.23.6 correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

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

1.23.8 the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;

1.23.9 including special personal information;

1.24 **“Policy”** means this Data Protection and Privacy Policy;

1.25 **“POPIA”** or **“Act”** means the Protection of Personal Information Act, No 4 of 2013;

1.26 **“prescribed”** means prescribed by regulation or by a code of conduct;

1.27 **“private body”** means

(a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity;

(b) a partnership which carries or has carried on any trade, business or

profession; or

(c) any former or existing juristic person, but excludes a public body;

1.28 “**processing**” means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including -

1.28.1 the collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use, of personal information;

1.28.2 dissemination of personal information by means of transmission, distribution or making available in any other form by electronic communications or other means; or

1.28.3 merging, linking, blocking, degradation, erasure or destruction of personal information. For the purposes of this definition, “**process**” or “**processes**” has a corresponding meaning;

1.29 “**pseudonymization**” Processing of personal data in such a manner that the personal information can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable person;

1.30 “**public body**” means:

(a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or

(b) any other functionary or institution when—

(i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or

(ii) exercising a public power or performing a public function in terms of any legislation;

1.31 “**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;

1.32 “**record**” means any recorded information,

- (a) regardless of form or medium, including any of the following:
  - (i) writing on any material;
  - (ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
  - (iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
  - (iv) book, map, plan, graph or drawing;
  - (v) photograph, film, negative, tape or another device in which one or more visual images are embodied to be capable, with or without the aid of some other equipment, of being reproduced;
- (b) in the possession or under the control of a responsible party;
- (c) whether or not it was created by a responsible party; and
- (d) regardless of when it came into existence;

1.33 “**Regulator**” means the information regulator established in terms of the Act;

1.34 “**re-identify**”, in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that—

- (a) identifies the data subject;
- (b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
- (c) can be linked by a reasonably foreseeable method to other information that identifies the data subject and “**re-identified**” has a corresponding meaning;

1.35 “**Republic**” means the Republic of South Africa;

1.36 “**restriction**” means to withhold from circulation, use or publication of any personal information that forms part of a filing system, but not to delete or destroy such information;

- 1.37 **“responsible party”** means the person who determines the purpose of and means for processing personal information and in the context of this Policy means ECIC;
- 1.38 **“special personal information”** means personal information concerning a data subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, health, sexual life, biometric information or criminal behavior and personal information of children;
- 1.39 **“third-party/ies”** means any independent contractor, supplier, vendor, agent, client, consultant, sub-contractor or another representative of the ECIC; and
- 1.40 **“this Act”** includes any regulation or code of conduct made under this POPIA.

## **2. INTRODUCTION**

- 2.1 This Policy regulates the use and protection of personal information that the ECIC processes, including a third party to whom the information is supplied by ECIC.
- 2.2 The ECIC acknowledges the need to ensure that personal information is handled with care and is committed to ensuring that it and any operator or third party acting on its behalf complies with the requirements of the Act for the processing of personal information.

## **3. REGULATORY AND GUIDANCE FRAMEWORK**

The following legislation and frameworks were considered for guidance in formulating this Policy:

- 3.1 Promotion of Access to Information Act 2 of 2000;
- 3.2 Protection of Personal Information Act 4 of 2013;
- 3.3 Electronic Communication and Transaction Act 25 of 2000;
- 3.5 Archives and Records service of South Africa Act 43 of 1996;
- 3.6 Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002(RICA);
- 3.7 Public Finance Management Act 1 of 1999 (as amended by Act 29 of 1999)

3.8 Constitution of the Republic of South Africa (Act No.106 of 1996).

#### **4. PURPOSE**

4.1 POPIA imposes obligations on both public and private bodies for the processing of personal information.

4.2 The purpose of this Policy is to inform data subjects about how the ECIC processes their personal information by, inter alia, collecting or collating, receiving, recording, storing, updating, distributing, erasing or destroying, disclosing and/or generally using the data subject's personal information.

4.3 The Policy also set standard for the ECIC stakeholders such as employees, clients, directors, vendors or suppliers and any other third parties on how to legally treat or process personal information.

#### **5. APPLICATION**

5.1 ECIC, in its capacity as responsible party, shall strive to observe, and comply with, its obligations under the POPIA as well as internationally accepted information protection principles, practices and guidelines when it processes personal information from or in respect of a data subject.

5.2 This policy applies to personal information records collected by the ECIC in connection with its business activities. This includes information collected offline through mail or physical delivery, and online through websites, email, branded pages on third-party platforms and applications accessed or used through such websites or third-party platforms which are operated by or on behalf of the ECIC.

5.3 This Policy does not apply to the information practices of third-party companies, (including, without limitation, their websites, platforms and/or applications) which we do not own or control; or individuals that the ECIC does not manage or employ, unless such third party is acting as an operator acting on behalf ECIC. These third-party sites may have their own privacy policies and terms and conditions and should be read before using those third-party sites.

#### **6. CONDITIONS FOR LAWFUL PROCESSING OF PESONAL INFORMATION**

##### **6.1 Accountability**

The ECIC will ensure that the conditions and all measures that give effect to such conditions in this item 6 are complied with at the time of determining the

purpose and means of the processing of personal information during the processing itself.

## **6.2 Processing Limitation**

### **6.2.1 Lawfulness in Processing**

ECIC will only be processing personal information lawfully, fairly and in a transparent and reasonable manner that does not infringe the privacy of a data subject.

### **6.2.2 Minimality**

ECIC may only collect personal information to the extent absolutely necessary to fulfill the defined purpose. Processing will be adequate, relevant, and limited to what is necessary in relation to the purposes for which the data is processed.

### **6.2.3 Consent, Justification and Objection**

6.2.3.1 ECIC may only process personal information if –

- (a) the data Subject or a competent person where the data subject is a child consents to the processing;
- b) processing is necessary for the performance of contracts with the data subject (e.g. the storage and use of necessary personal data in the context of an employment- or service contract);
- (c) processing is necessary for compliance with legal obligations imposed on ECIC, e.g. insurance laws;
- (d) processing protects a legitimate interest of the data subject;
- (e) processing is necessary for the proper performance of a public duty by a public body; and
- (f) processing is necessary for pursuing the legitimate interest of ECIC or a third party to whom the information is supplied.

6.2.3.2 ECIC bears the burden of proof for the data subject or competent person's consent referred to in paragraph 6.2.3.1(a).

- 6.2.3.3 Furthermore, ECIC recognises that a data subject may withdraw his, her or its consent referred to in paragraph 6.2.3.1(a) at any time, provided that the lawfulness of the Processing of personal information in terms of paragraphs 6.2.3.1(b) to (f) will not be affected.
- 6.2.3.4 If a data subject, at any time, objects to the processing of his or her or its personal information, in terms of paragraphs 6.2.3.1 (d) to (f), on reasonable grounds relating to his or her or its particular situation, unless legislation provides for such processing or for purpose of direct marketing other than direct marketing by means of unsolicited electronic communication, ECIC may no longer process the personal information.

#### **6.2.4 Collection directly from data subject**

- 6.2.4.1 ECIC will only collect personal information directly from the data subject. If this is not the case, the data subject will be notified, particularly about the types of personal data that are being collected, processed, and/or used and for which specific purposes this occurs.
- 6.2.4.2 ECIC recognizes the following exceptions to collecting personal information directly from the data subject:
- (a) the personal information is contained in or derived from a public record or has deliberately been made public by the data subject;
  - (b) the data subject or a competent person where the data subject is a child has consented to the collection of the personal information from another source;
  - (c) collection of the personal information from another source would not prejudice a legitimate interest of the data subject;
  - (d) collection of the personal information from another source is necessary -
    - (i) to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
    - (ii) to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Services Act, 1997(Act No.34 of 1997);

- (iii) for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;
- (iv) in the interests of national security or
- (v) to maintain the legitimate interests of ECIC or a third party to whom the information is supplied;
- (e) compliance would prejudice a lawful collection; or
- (f) compliance is not reasonably practicable in the circumstances of the particular case.

## **6.3 Purpose Specification**

### **6.3.1 Collection for Specific Purpose**

- 6.3.1.1 ECIC may only collect personal information for specific, explicit purposes and it may not be processed in a manner that is incompatible with those purposes.
- 6.3.1.2 The specific purpose will be defined before data collection. ECIC will process personal information for a purpose other than that for which the data have been collected only in exceptional cases, where the Act or other applicable law permits processing for another purpose or if it is based on the data subject's consent.
- 6.3.1.3 To ascertain whether the other purposes are compatible with the original purposes, the reasonable expectations of the data subject towards ECIC regarding such further processing, the type of data used, the possible consequences of the intended further processing for the data subject, and measures of encryption or pseudonymization will be considered.
- 6.3.1.4 The ECIC may use personal information for the following purposes –
  - (a) providing any legal or advisory services to the data subject from time to time;
  - (b) receiving services or products provided by the data subject to the ECIC from time to time;
  - (c) conducting its insurance and related business activities with data subjects;

- (d) responding to any correspondence that the data subject may send to the ECIC, including via email or by telephone;
- (e) contacting the data subject from time to time, where specific consent has been given to follow-up with a data subject by the ECIC or for the data subject to be put on the ECIC mailing list;
- (f) for such other purposes to which the data subject may consent from time to time; and
- (g) for such other purposes authorised in terms of applicable law.

## **6.3.2 Retention and Restriction of Records**

6.3.2.1 ECIC will not retain records of personal information any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, provided:

- (a) retention of the record is required or authorized by law;
- (b) ECIC reasonably requires the record for lawful purposes related to its functions or activities;
- (c) retention of the record is required by a contract between the parties thereto; and
- (d) the data subject or a competent person if the data subject is a child has consented to the retention of the record.

6.3.2.2 Personal information that is no longer needed after the expiration of legal or business process-related periods must be deleted or destroyed. There may be an indication of interests that merit protection or historical, statistical, or research significance of this information in individual cases. If so, the information will remain on file until the interests that merit protection have been clarified legally, or ECIC has evaluated the information to determine whether it must be retained for historical, statistical or research purposes.

6.3.2.3 The destruction or deletion of a record of personal information will be done in a manner that prevents its

reconstruction, identification or re-identification, in an intelligible form

- 6.3.2.4 ECIC will restrict the processing of personal information if –
- (a) its accuracy is contested by the data subject, for a period enabling the ECIC to verify the accuracy of the information;
  - (b) ECIC no longer needs the personal information for achieving the purpose for which the information was collected or subsequently collected or processed, but it must be maintained for purposes of proof;
  - (c) the processing is unlawful, and the data subject opposes its destruction or deletion and requests the restriction of its use instead; or
  - (d) the data subject requests to transmit the personal Information into another automated processing system.
- 6.3.2.5 Personal information referred to in paragraph 6.3.2.4 above, except for storage, will only be processed for purposes of proof, or with the consent of a competent person in respect of a child, or for the protection of the rights of another natural or legal person or if such processing is in the public interest.
- 6.3.2.6 In circumstances where processing of personal information is restricted pursuant to paragraph 6.3.2.4 above, ECIC will inform the data subject before lifting the restriction on processing.

## **6.4 Further Processing Limitation**

### **6.4.1 Further processing to be compatible with the purpose of collection**

- 6.4.1.1 ECIC may further process personal information in accordance or compatible with the purpose for which it was collected in terms of paragraph 6.3.
- 6.4.1.2 To assess whether further processing is compatible with the purpose of collection, ECIC will take account of—

- (a) the relationship between the purpose of the intended further processing and the purpose for which the information has been collected;
- (b) the nature of the information concerned;
- (c) the consequences of the intended further processing for the data subject;
- (d) the way the information has been collected; and
- (e) any contractual rights and obligations between the parties.

6.4.1.3 ECIC recognizes that further processing of personal information is not incompatible with the purpose of collection if—

- (a) the data subject or a competent person where the data subject is a child has consented to the further processing of the information;
- (b) the information is available in or derived from a public record or has deliberately been made public by the data subject;
- (c) further processing is necessary—
  - (i) to avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution and punishment of offences;
  - (ii) to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);
  - (iii) for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or
  - iv) in the interests of national security;
- (d) the further processing of the information is necessary to prevent or mitigate a serious and imminent threat to—
  - (i) public health or public safety; or

- (ii) the life or health of the data subject or another individual;
- (e) the information is used for historical, statistical or research purposes and the responsible party ensures that the further processing is carried out solely for such purposes and will not be published in an identifiable form; or
- (f) the further processing of the information is in accordance with an exemption granted under section 37 of the Act (by the Regulator, if it is in the public interest).

## **6.5 Quality of Information**

6.5.1 ECIC will take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary, considering the purpose for which the personal information is collected or further processed.

6.5.2 ECIC will take suitable steps to ensure that inaccurate or incomplete data are deleted, corrected, supplemented or updated.

## **6.6 Openness**

### **6.6.1 Documentation**

ECIC will maintain the documentation of all processing operations under its responsibility as referred to in paragraph 6.3.2 above and in accordance with section 51 of PAIA.

### **6.6.2 Notification to data subject when collecting personal information**

6.6.2.1 In collecting personal information, ECIC will take reasonably practicable steps to ensure that the data subject is aware of—

- (a) the information being collected and where the information is not collected from the data subject, the source from which it is collected;
- (b) the name and address of the responsible party;

- (c) the purpose for which the information is being collected;
- (d) whether or not the supply of the information by that data subject is voluntary or mandatory;
- (e) the consequences of failure to provide the information;
- (f) any particular law authorising or requiring the collection of the information;
- (g) the fact that, where applicable, ECIC intends to transfer the information to another country or international organisation and the level of protection afforded to the information by that other country or international organisation;
- (h) any further information such as the—
  - (i) recipient or category of recipients of the information;
  - (ii) nature or category of the information;
  - (iii) existence of the right of access to and the right to rectify the information collected;
  - (iv) existence of the right to object to the processing of personal information as referred to in paragraph 6.2.3.4; and
  - (v) right to lodge a complaint with the Information Regulator and the contact details of the Information Regulator.

6.6.2.2 The steps referred to in paragraph 6.6.2.1 above will be taken by ECIC —

- (a) if the personal information is collected directly from the data subject, before the information is collected, unless the data subject is already aware of the information referred to in that subsection; or
- (b) in any other case, before the information is collected or as soon as reasonably practicable after it has been collected.

6.6.2.3 If ECIC has previously taken the steps referred to in paragraph 6.6.2.1 above, ECIC therefore complies with paragraph 6.6.2.1, in relation to the subsequent collection from the data subject of the same information for the purpose.

6.6.2.4 ECIC will not necessarily comply with paragraph 6.6.2.1 if—

- (a) the data subject or a competent person where the data subject is a child has provided consent for the non-compliance;
- (b) non-compliance would not prejudice the legitimate interests of the data subject as set out in terms of this Act;
- (c) non-compliance is necessary—
  - (i) to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
  - (ii) to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);
  - (iii) for the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated; or
  - (iv) in the interests of national security;
- (d) compliance would prejudice a lawful purpose of the collection;
- (e) compliance is not reasonably practicable in the circumstances of the particular case; or
- (f) the information will—
  - (i) not be used in a form in which the data subject may be identified; or
  - (ii) be used for historical, statistical or research purposes.

## **6.7 Security Safeguards**

### **6.7.1 Security Measures for the Integrity and Confidentiality of Personal Information**

6.7.1.1 ECIC will secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent—

- (a) loss of, damage to or unauthorised destruction of personal information; and
- (b) unlawful access to or processing of personal information.

6.7.1.2 In order to give effect to paragraph 6.7.1.1 above, ECIC will take reasonable measures to—

- (a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
- (b) establish and maintain appropriate safeguards against the risks identified;
- (c) regularly verify that the safeguards are effectively implemented; and
- (d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

6.7.1.3 ECIC will have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

## **6.7.2 Information processed by an operator or person acting under authority**

6.7.2.1 An operator or anyone processing personal information in accordance with the requirements of the Act, on behalf of ECIC, will be required by ECIC to—

- (a) process such information only with the knowledge or authorisation from ECIC; and
- (b) treat personal information which comes to their knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of their duties.

### **6.7.3 Security measures regarding information processed by an operator or person acting under authority**

6.7.3.1 ECIC will, in terms of a written contract between the responsible party and the operator, ensure that the operator which processes personal information for the responsible party establishes and maintains the security measures referred to in paragraph 6.7.1.1 above.

6.7.3.2 The operator will be required by ECIC to notify ECIC immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

### **6.7.4 Notification of security compromises**

6.7.4.1 Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, ECIC will notify—

- (a) the Regulator; and
- (b) subject to paragraph 6.7.4.3, the data subject, unless the identity of such data subject cannot be established.

6.7.4.2 The notification referred to in paragraph 6.7.4.1 will be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

6.7.4.3 ECIC may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.

6.7.4.4 The notification to a data subject referred to in paragraph 6.7.4.1 above will be in writing and communicated to the data subject in at least one of the following ways:

- (a) Mailed to the data subject's last known physical or postal address;
- (b) sent by e-mail to the data subject's last known e-mail address;
- (c) placed in a prominent position on the website of the responsible party;
- (d) published in the news media; or
- (e) as may be directed by the Regulator.

6.7.4.5 The notification referred to in paragraph 6.7.4.1 will provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including—

- (a) a description of the possible consequences of the security compromise;
- (b) a description of the measures that the responsible party intends to take or has taken to address the security compromise;
- (c) a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and
- (d) if known to the ECIC, the identity of the unauthorised person who may have accessed or acquired the personal information.

6.7.4.6 The Regulator may direct ECIC to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

## **6.8 Data Subject Participation**

### **6.8.1 Access to Personal Information**

6.8.1.1 ECIC recognizes that a data subject, having provided adequate proof of identity, has the right to—

- (a) request ECIC to confirm, free of charge, whether or not the ECIC holds personal information about the data subject; and
- (b) request from ECIC the record or a description of the personal information about the data subject held by the responsible party, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information—
  - (i) within a reasonable time;
  - (ii) at a prescribed fee, if any;
  - (iii) in a reasonable manner and format; and
  - (iv) in a form that is generally understandable.

6.8.1.2 If, in response to a request in terms of paragraph 6.8.1.1 above, personal information is communicated to a data subject, the data subject will be advised of the right in terms of paragraph 6.8.2 below, to request the correction of information.

6.8.1.3 If a data subject is required by ECIC to pay a fee for services provided to the data subject in terms of paragraph 6.8.1.1.(b) above, to enable the ECIC to respond to a request, ECIC —

- (a) will give the applicant a written estimate of the fee before providing the services; and
- (b) may require the applicant to pay a deposit for all or part of the fee.

6.8.1.4 ECIC may refuse to disclose any information requested in terms of paragraph 6.8.1.1 above, based on the grounds for refusal of access to records set- out in the applicable sections of Chapter 4 of PAIA. In addition, the provisions of sections 30 and 61 of PAIA are applicable in respect of access to health or other records.

6.8.1.5 If a request for access to personal information is made to ECIC and part of that information may be refused by ECIC in terms of paragraph 6.8.1.4 above, every other part must be disclosed.

## 6.8.2 Correction of Personal Information

- 6.8.2.1 A data subject may, in the prescribed manner, request ECIC to—
- (a) correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or
  - (b) destroy or delete a record of personal information about the data subject that the ECIC responsible party is no longer authorised to retain in terms of paragraph 6.3.2 above.
- 6.8.2.2 On receipt of a request in terms of paragraph 6.8.2.1 above, ECIC must, as soon as reasonably practicable—
- (a) correct the information;
  - (b) destroy or delete the information;
  - (c) provide the data subject, to his or her satisfaction, with credible evidence in support of the information; or
  - (d) where agreement cannot be reached between the responsible party and the data subject, and if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made.
- 6.8.2.3 If ECIC has taken steps under paragraph 6.8.2.2 above, that result in a change to the information and the changed information has an impact on decisions that have been or will be taken in respect of the data subject in question, the responsible party must, if reasonably practicable, inform each person or body or responsible party to whom the personal information has been disclosed of those steps.
- 6.8.2.4 ECIC will notify a data subject, who has made a request in terms of paragraph 6.8.2.1 above, of the action taken as a result of the request.

### **6.8.3 Manner of access**

ECIC will provide the data subject with any such personal information to the extent required in terms of sections 18 and 53 of PAIA and in terms of any of the ECIC's policies and procedures which apply in terms of the PAIA.

## **6.9 Processing of Special Personal Information**

### **6.9.1 Prohibition on Processing of Special Personal Information**

6.9.1.1 ECIC may, subject to paragraph 6.9.2 below, not process personal information concerning—

- (a) 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
- (b) the criminal behavior 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.

### **6.9.2 General authorisation concerning special personal information**

6.9.2.1 The prohibition on processing personal information, as referred to in paragraph 6.9.1, will not apply to ECIC if the —

- (a) processing is carried out with the consent of a data subject referred to in paragraph 6.9.1;
- (b) processing is necessary for the establishment, exercise or defence of a right or obligation in law;
- (c) processing is necessary to comply with an obligation of international public law;

- (d) processing is 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 data subject to a disproportionate extent;
- (e) information has deliberately been made public by the data subject.

6.9.2.2 The Regulator may, subject to paragraph 6.9.2.3 below, upon application by ECIC and by notice in the Government Gazette, authorise ECIC 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.

6.9.2.3 The Regulator may impose reasonable conditions in respect of any authorisation granted under paragraph 6.9.2.2 above.

## **6.10 Processing of personal information of children**

### **6.10.1 Prohibition on processing personal information of children**

ECIC may, subject to paragraph 6.10.2 below, not process personal information concerning a child.

### **6.10.2 General authorisation concerning personal information of children**

6.10.2.1 The prohibition on processing personal information of children, as referred to in paragraph 6.10.1 above, will not apply to ECIC if the processing is

- (a) carried out with the prior consent of a competent person;
- (b) necessary for the establishment, exercise or defence of a right or obligation in law;
- (c) necessary to comply with an obligation of international public law;
- (d) 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; or
- (e) of personal information which has deliberately been made public by the child with the consent of a competent person.

## **7. STORAGE OF PERSONAL INFORMATION**

- 7.1 The ECIC will keep the personal information that it processes on behalf of data subjects either at its business premises or secured on its ICT network servers or cloud backups with contracted third parties, in South Africa or another country. Where ECIC and service providers maintain servers and facilities, ECIC will take steps, including by way of contracts, to ensure that it and the data continue to be protected regardless of its location in a manner consistent with the standards of protection required under applicable law. Furthermore, ECIC will require such third parties to store data in a de-identified manner and only ECIC has the means to re-identify such data.
- 7.2 The ECIC's third-party service providers, including data storage and processing providers, may, from time to time, also have access to a data subject's personal information in connection with purposes for which the personal information was initially collected to be processed.
- 7.3 The ECIC will ensure that such third-party service providers will process the personal information in accordance with the provisions of this Policy, all other relevant internal policies and procedures and the Act.

## **8. PERSONAL INFORMATION FOR DIRECT MARKETING PURPOSES**

- 8.1 The ECIC acknowledges that it may only use personal information to contact the data subject for purposes of direct marketing from time to time where it is permissible to do so, via sms or e-mails or social media.
- 8.2 ECIC may use personal information to contact any data subject and/or market the ECIC's services directly to the data subject(s) if the data subject is one of the ECIC's existing clients who has consented to receive such marketing data, or the data subject has requested to receive marketing material from the ECIC or the ECIC has the data subject's consent to market its services directly to the data subject.
- 8.3 If the data subject is an existing client and has provided the required consent, the ECIC will only use his/her/its personal information if it had obtained the personal information through the provision of a service to the data subject and only in relation to similar services to the ones the ECIC previously provided to the data subject.
- 8.4 The ECIC will ensure that a reasonable opportunity is given to the data subjects to object to the use of their personal information for the ECIC's marketing purposes when collecting the personal information and on each communication to the data subject for purposes of direct marketing.
- 8.5 The ECIC will not use data subject's personal information to send the data subject marketing materials if the data subject has requested not to receive them.

## **9. FAILURE TO PROVIDE PERSONAL INFORMATION**

- 9.1 Should ECIC need to collect personal information by law, such as in-relation to anti-money laundering or under the terms of a contract that the ECIC may have with a data subject and the data subject fails to provide the personal data when requested, ECIC may be unable to perform the contract it has with the data subject or is attempting to enter into with the data subject.
- 9.2 In such a case, the ECIC may have to decline to provide or receive the relevant services, and the data subject will be notified where this is the case.

## **10 PROVISION OF PERSONAL INFORMATION TO THIRD PARTIES**

- 10.1 ECIC may disclose personal information to third-party service providers and will enter into written agreements with such third-party service providers to ensure that they process any Personal Information in accordance with the provisions of this Policy and the Act.

- 10.2 The ECIC notes that such third parties may assist the ECIC with the purposes listed in paragraph 6.3.1.4 above, for example, service providers may be used, inter alia, to provide telephone support, assist in the provision of ICT or marketing products or services, notify the data subjects of any pertinent information concerning the ECIC, and/or for data storage.
- 10.3 The ECIC will disclose personal information with the consent of the data subject or if the ECIC is permitted to do so without such consent in accordance with the applicable laws or the Act.
- 10.4 It should be noted that the processing of personal information in a foreign jurisdiction may be subject to the laws of the country in which the personal information is held, and may be subject to disclosure to the governments, courts of law, enforcement or regulatory agencies of such other country, pursuant to the laws of such country, without the consent of a data subject.

## **11. PERSONAL INFORMATION FOR EMPLOYMENT RELATIONSHIP**

- 11.1 In employment relationships, personal information can be processed if needed to initiate, carry out and terminate the employment agreement with ECIC.
- 11.2 When initiating an employment relationship with ECIC, the applicants' personal information can be processed. If the candidate is rejected, his/her data must be deleted in observance of the required retention period, unless the applicant has agreed to remain on file for a future selection process.
- 11.3 Consent is also needed to use the personal information for further application processes.
- 11.4 In the existing employment relationship, personal information processing must always relate to the purpose of the employment agreement if none of the circumstances for authorized data processing apply.
- 11.5 If it should be necessary during the application procedure to collect information on an applicant from a third party, the requirements of the confidentiality must be observed. In cases of doubt, consent must be obtained from the data subject.
- 11.6 Employee's personal information can be processed upon consent of the person concerned. Declarations of consent must be submitted voluntarily. Involuntary consent is void. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In certain circumstances, consent may be given verbally, in which case it must be properly documented.

## **11.7 Automated Decisions**

- 11.7.1 If personal information is processed automatically as part of the employment relationship, and specific personal details are evaluated (e.g. as part of personnel selection or the evaluation of skills profiles), this automatic processing cannot be the sole basis for decisions that would have negative consequences or significant problems for the affected employee.
- 11.7.2 To avoid erroneous decisions, the automated process must ensure that a natural person evaluates the content of the situation, and that this evaluation is the basis for the decision. The data subject must also be informed of the facts and results of automated individual decisions and the possibility to respond.

## **12. PERSONAL INFORMATION FOR CUSTOMERS, SERVICE PROVIDERS AND PARTNERS**

- 12.1 Personal information of the relevant data subjects such as customers, service providers and partners can be processed in order to establish, execute and terminate a contract. This also includes advisory services for the partner under the contract if this is related to the contractual purpose.
- 12.2 Prior to a contract or during the contract initiation phase, personal information can be processed to prepare bids or purchase orders or to fulfill other requests of data subjects that relate to contract conclusion. Data subjects can be contacted during the contract preparation process using the information that they have provided. Subject to section 6.8, any restrictions requested by the data subjects must be complied with.

## **13 TELECOMMUNICATION AND INTERNET**

ECIC provides employees with telephone equipment, computer hardware, e-mail platform, intranet and internet and other company resources should be primarily used for work-related assignments. They can be used within the applicable legal regulations and in compliance with the ECIC User Acceptance and Electronic Communications Policy.

## **14 USER DATA AND INTERNET**

- 14.1 If ECIC collects personal information, processes and uses it on websites or in apps, the data subject will be informed of this in a privacy statement and,

if applicable, information about cookies. The privacy statement and any cookie information reflected on the ECIC's website, so that it is easy to identify, directly accessible and consistently available for the data subjects.

- 14.2 If user profiles (tracking) are created to evaluate the use of websites and apps, the data subject will always be informed accordingly in the privacy statement. Personal tracking may only be effected if it is permitted upon consent of the data subject. If tracking uses a pseudonym, the data subject will be given the chance to opt out in the privacy statement.
- 14.3 If websites or apps can access personal information in an area restricted to registered users, the identification and authentication of the data subject will offer adequate protection during access.

## **15. REPORTING OF BREACHES OF PERSONAL INFORMATION**

- 15.1 All employees must inform their supervisors/line managers, immediately about cases of violations against this Policy or incidences of breach of protection of personal information or loss thereof.
- 15.2 The manager responsible for the function or the unit is required to inform the Information Officer immediately about data protection incidents.
- 15.3 In cases of;
- improper transmission of personal data to third parties,
  - improper access by third parties to personal data, or
  - loss of personal data;

a report must be compiled by the Information Officer about the data breach incidents and how it is being managed and submitted to the Information Regulator as required under POPIA.

- 15.4 Any breach of data protection or incidences should be dealt with and managed in terms of the Data Breach Response Plan Manual.

## **16. RESPONSIBILITIES FOR COMPLIANCE WITH THIS POLICY**

### **16.1 Board of Directors of ECIC and Risk Committee**

- 16.1.1 The Board and Risk Committee are responsible for ensuring that ECIC complies with this Policy
- 16.1.2 The Board must appoint the Information Officer and Deputy Information Officer. The names of the appointed individuals

must be submitted to the Regulator to approve such appointment.

16.1.3 The internal handling of personal information will be an agenda item on the EXCO meetings, Board and Committees meetings, on a quarterly basis and shall include a report of any privacy complaints and breaches against the ECIC and detailed reports analysing any data breaches experienced during this time period.

16.1.4 Such a report must be compiled by the Information Officer and tabled at EXCO, Risk Committee and Board meetings.

## **16.2 Executive Management of ECIC**

16.2.1 The responsibility for compliance with data protection requirements rests with the executive management of ECIC that processes the personal information for its business purposes.

16.2.2 Executive management may delegate the task to fulfill this responsibility to managers at different levels within the organizational framework and the associated business processes.

16.2.3 Accordingly, line managers have a mandate to implement the Policy requirements within their respective lines of business. With the assistance and guidance of the Compliance Officer, Information Officer and Chief Risk Officer, line managers must formulate processes and procedures to guide their subordinates on how to process personal information in compliance with this Policy.

16.2.4 Executive Management must ensure that-

(a) the Information Officer/Deputy Information Officer is equipped with the time and budget they need to perform their duties, including the participation in necessary education and training activities.

(b) the processes are in compliance with this Policy and applicable law; and

- (c) in coordination with the Information Officer/Deputy Information Officer that all necessary communications are sent to the Regulator.

### **16.3 Information Officer and Deputy Information Officer**

- 16.3.1 The Information Officer/Deputy Information Officer is responsible for;
- (a) ensuring the consistent implementation of this Policy, the Data Breach Manual, the Act and applicable regulations;
  - (b) defining personal information protection and privacy strategy in harmony with ECIC's corporate strategic objectives;
  - (c) advise line managers and employees in general on how to process personal information in compliance with this Policy, including requiring the relevant consent and confidentiality undertakings from data subjects;
  - (d) conduct training and awareness campaigns on the Policy and the Act;
  - (e) attend to complaints and queries from data subjects and other stakeholders
  - (f) serving as a liaison person between the ECIC and the Regulator and other stakeholders; and
  - (e) reporting data breaches to the Regulator.
- 16.3.2 If a data subject wishes to file a complaint with regard to the processing of his or her or its personal information, he or she or it can do so by directing an e-mail to the Information Officer: [information\\_officer@ecic.co.za](mailto:information_officer@ecic.co.za)
- 16.3.3 The data subject will be notified about all measures taken based on the complaint within one (1) month at the latest and in accordance with requirements of section 6.7.4.

## **16.4 The Chief Risk Officer**

- 16.4.1 The Chief Risk Officer must regularly evaluate the safeguard measures that are in place to ensure they are adequate for the protection of personal information in ECIC's possession and third parties contracted by ECIC.
- 16.4.2 To the extent that such safeguard measures are not adequate, the Chief Risk Officer must recommend adequate measures and monitor compliance with such measures.
- 16.4.3 The Chief Risk Officer must report or highlight any risk, perceived or real, relating to processing of personal information to EXCO, Risk Committee and Board.

## **16.5 General Counsel**

- 16.5.1 The General Counsel must ensure that all contractual relationships involving the processing of personal information adequately address the protection of such personal information and relevant contractual undertakings must be included in each contract with customers, employees, suppliers or service providers, including requiring the relevant consent and confidentiality undertakings from data subjects.

## **16.6 Human Capital Head /Manager**

- 16.6.1 All ECIC employees and all other individuals working on behalf of ECIC must acknowledge, before they start their activities for ECIC, to keep personal information confidential and to not collect, process, or use such information without authorization when access to personal data cannot be excluded. This must include the information of the consequences of breaches of these obligations.
- 16.6.2 All ECIC employees must be made aware of this Policy and other internal company guidelines that regulate the use of personal information. This instruction must be documented in written or electronic form.
- 16.6.3 The responsibility for obtaining the confidentiality commitments, in respect of employees lies with ECIC Human Capital Unit.

## **16.7 Employees**

- 16.7.1 All ECIC employees are required to handle all personal information that they can access in the course of performing

their duties for ECIC with strict confidentiality and in accordance with this Policy and may not collect, process, or use such data without authorization.

- 16.7.2 ECIC employees may only process personal information within the scope necessary to fulfill their duties as defined by their employment contracts.
- 16.7.3 Any unauthorized collection, processing, or use of such personal information by employees is prohibited.
- 16.7.4 Employees are forbidden to use personal data for private or commercial purposes, to disclose it to unauthorized persons, or to make it available in any other way.
- 16.7.5 When in doubt on how to process or deal with personal information employees may turn to their superiors or line managers, Information Officer or Deputy Information Officer for guidance.

## **16.8 ICT Head /Manager**

- 16.8.1 The ICT Manager must ensure that adequate technical measures are in place to secure the ECIC's ICT infrastructure to prevent any data breaches in respect of personal information stored on servers and generally in compliance with the ICT Security Policy, this Policy and/or Act.
- 16.8.2 In the circumstances where a service provider is hired to process personal information or ECIC's personal information is stored on service providers' servers or on cloud environment, the ICT Manager must ensure that an agreement must be concluded with service provider and such agreement must contain provisions limiting or prohibiting the processing of personal information and related security measures that are required from the service provider to prevent any data breach. ECIC retains full responsibility for correct performance of personal information processing. The service provider can process personal data only as per the instructions from the ECIC.
- 16.8.4 In identifying the service provider, the ICT Manager must ensure that the following requirements are met:

- (a) The service provider must be chosen based on its ability to cover the required technical and organisational protective measures.
- (b) A service provider can document its compliance with personal information security requirements by presenting suitable certification. Depending on the risk of data processing, the reviews must be repeated on a regular basis during the term of the contract.

#### **16.9 Facilities/Records Management Head/Manager:**

- 16.9.1 Ensure that any records of personal information in ECIC's possession are stored safely in accordance with the Records Management Policy and this Policy.
- 16.9.2 Any records of personal information which are required to be disposed of or deleted, are deleted or disposed of in accordance with the Records Management Policy.

#### **16.10 Head: Marketing and Communication**

The Head of Marketing and Communications shall be responsible for drafting and release of any communications or statement to be made by the Information Officer to the media or press, following any breach of personal information as contemplated in the Data Breach Response Manual Plan.

### **17 TRAINING AND AWARENESS**

- 17.1 Mandatory training will be provided to all ECIC staff on compliance with POPIA and this Policy by the Information Officer
- 17.2 Training will be provided by the Information Officer to all new ECIC employees, including temporary and contracted staff during the first month of employment at ECIC.
- 17.3 All ECIC employees will also be required to undertake refresher training on a regular basis.

### **18 REVIEW OF THE POLICY**

- 18.1 This Policy shall be reviewed once every three years and on a regular basis, if there are legislative changes or changes to the Policy

18.2 Any changes to this Policy must be approved by the Risk Committee and Board

## **19 NON – COMPLIANCE**

Any non-compliance with the terms of this Policy could have serious legal and reputational repercussions for the ECIC and may cause significant damage to the ECIC. Therefore, any non-compliance could lead to disciplinary action being taken against the relevant employees.

## **20. LINKS TO OTHER POLICIES**

The Policy should be read together with the following policies and plans:

20.1 Data Breach Response Plan Manual;

20.2 ECIC Business Continuity Management Policy;

20.3 ICT Disaster Recovery Plan;

20.4 ICT Security Policy;

20.5 ICT User Acceptance and Electronic Communications Policy

20.6 Records Management Policy;

20.7 Communications Policy;

20.8 Complaints Policy; and

20.9 PAIA Manual.