ECSA

ENGINEERING COUNCIL OF SOUTH AFRICA

An Effective Regulator Assuring Engineering Excellence

PRIVACY PROCEDURE

ENGINEERING COUNCIL OF SOUTH AFRICA
Tel: 011 6079500 | Fax: 011 6229295
Email: engineer@ecsa.co.za | Website: www.ecsa.co.za

Table of Contents

TERMS, ABRREVIATIONS AND DEFINITONS

TERM AND ABBREVIATION	DEFINITION
The Act	Protection of Personal Information Act, 2013 (Act No. 4 of 2013), as amended
Data Subject	the person to whom Personal Information relates, including ECSA governing council, members, registered persons, applicants for registration, employees, prospective employees and members of the public who lodge complaints or request information;
Data Destruction	the manner which ECSA regulates the effective destruction of the *Personal Information* in its possession or control in accordance with the Act
Deputy Information Officer	Legal Practitioner or any person(s) who may be designated by the Information Officer to perform certain delegated duties and responsibilities of the Information Officer
Information Officer	Chief Executive Officer, the acting Chief Executive Officer or an equivalent officer or any person duly authorized by that officer
Operator	a person who processes Personal Information for ECSA in terms of a contract or mandate, without coming under the direct authority of ECSA
Personal Information	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, e-mail 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 of opinions of another individual about the person; h. 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;

Processing	any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information, including: a. the collection, receipt, recording, organization, 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;
"Process" and **"Processed"**	will have the same meaning
Regulator	the Information Regulator established in terms of section 39 of the Act
Responsible Party	a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing Personal Information

1. INTRODUCTION

1.2 A Privacy Policy was developed in compliance with the provisions of the Act and its Regulations in order to give effect to the Constitutional right to privacy.

1.3 The Privacy Procedure provides guidelines on procedural or practical aspects of the Privacy Policy.

2. APPLICABILITY

2.1 The Privacy Procedure applies to all Personal Information processed by ECSA in the exercise of its functions and obligations as a statutory body established by the Engineering Profession Act, 2000 (Act No. 46 of 2000); including the Personal Information of ECSA's governing council, members, registered persons, applicants for registration, employees, prospective employees and service providers or suppliers.

3. LAWFUL PROCESSING OF PERSONAL INFORMATION

3.1 ECSA is required, in the normal exercise of its functions and obligations as a statutory body, to process the Personal Information of Data Subjects from time to time in accordance with the eight conditions for lawful processing as set out in the Privacy Policy and Act.

3.2 All employees, members and any other person who processes Personal Information on behalf of ECSA, must be familiar with, understand and comply with all the conditions for lawful processing of Personal Information as set out in the Privacy Policy. All queries must be directed to the Information officer and/or any other person designated by ECSA.

4. PRIOR CONSENT

4.1 Prior to processing any Personal Information whether from its employees, prospective employees, members, nominee members, registered persons or applicants for registration, all employees must obtain the written consent of such Data Subjects.

4.2 The consent forms to be signed by each respective category of Data Subject are marked as Annexures **A1 to A3.**

4.3 Employees must ensure that all the information contained in the consent forms is clearly explained to the Data Subjects when they sign the consent forms and that the purpose for processing their Personal Information is identified and understood.

5. PROCESSING PERSONAL INFORMATION

5.1 Employees must take reasonable practical steps to ensure that the Personal Information is complete, accurate, not misleading and updated where necessary, having regard to the purpose for which the Personal Information of Data Subjects is being collected or further processed.

5.2 All employees including any other person processing Personal Information on behalf of ECSA must treat such information as confidential and take steps to adhere to the security requirements or measures as set out in the Data Security Policy.

6. FURTHER PROCESSING OF PERSONAL INFORMATION

6.1 If after the initial consent has been obtained from Data Subjects it becomes apparent that further Processing is required which is not compatible with the initial purpose of the Processing as recorded in the original consent form, Employees or any other persons authorized on behalf of ECSA must request the Data Subject to sign another Consent Form (Annexure A) recording such further purpose.

7. OBJECTION OR WITHDRAWAL OF CONSENT BY DATA SUBJECT

7.1 A Data Subject may object to the Processing of Personal Information at any time, should such information not be utilized for the purposes it was intended for, and should such withdrawal of consent not be in contravention of any legislative requirements and shall not interfere with the ability of ECSA to continue to manage the employment relationship or its ability to exercise and manage its statutory duties.

7.2 Upon receipt of such a request Employees should ask the Data Subject to complete the relevant form marked Annexure **B** and acknowledge receipt thereof once received. Thereafter the Employee must bring the request to the attention of the Information Office or Deputy Information officer or any other delegated person.

7.3 ECSA employees may no longer process Personal Information once it has been withdrawn.

8. DATA SUBJECT PARTICIPATION

8.1 The Data Subject may, after providing adequate proof of their identity, request access to relevant Personal Information, which must then be provided to the Data Subject.

8.2 The Data Subject may request that their Personal Information be corrected or deleted or that a record containing Personal Information of the Data Subject be destroyed or deleted if the Data Subject believes that the Personal Information or record of the Personal Information is: -

8.2.1 inaccurate;

8.2.2 irrelevant;

8.2.3 excessive;

8.2.4 out of date;

8.2.5 incomplete;

8.2.6 misleading; or

8.2.7 has been obtained unlawfully.

8.3 Employees receiving such a request must ensure that the Data Subject completes and submits the required form marked Annexure **C**.

8.4 Upon receipt of the completed form the Employee must as soon as reasonably practicable, and in compliance with the Act: -

8.4.1 correct the Personal Information;

8.4.2 destroy or delete the Personal Information;

8.4.3 provide the Data Subject, to his or her satisfaction, with credible evidence in support of the Personal Information; or

8.4.4 where agreement cannot be reached between ECSA 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, an indication that a correction of the information has been requested but has not been made.

9. DESTRUCTION OF PERSONAL INFORMATION

9.1 In order to implement effective destruction of the Personal Information in ECSA's possession or control, delegated Employees from each Division including, IT, Legal, Compliance and Finance must prepare, on an annual basis, an inventory of Personal Information that needs to be destroyed as stipulated in the Privacy Policy.

9.2 The inventory should be approved by the Head of each Division and final approval thereof rests with the Information Officer or Deputy Information Officer as may be delegated.

10. MANNER OF DESTRUCTION

10.1 ECSA may use internal or external resources and systems to destroy Personal Information.

10.2 If external contractors are utilized, the Information Officer or delegated authority must ensure that an appropriate contract has been signed with the operator. The Contractor must immediately notify ECSA where there are reasonable grounds to believe that Personal Information has been accessed or acquired by any unauthorised person.

10.3 Hard copies of Personal Information may be destroyed using any of the following methods: shredding, incinerating, pulverizing or any other method providing that the Personal Information must be unreadable, indecipherable and may not be reconstructed in any intelligible form.

10.4 ECSA will delete and/or de-identify all electronic or soft copies of Personal Information, including information stored on video or voice recordings, in a manner that prevents its reconstruction in an intelligible form. “De-identify” means to delete any information that

10.4.1 identifies the Data Subject;

10.4.2 can be used or manipulated by a reasonably foreseeable method to identify the Data Subject; or

10.4.3 can be linked by a reasonably foreseeable method to other information that identifies the Data Subject.

10.5 Subject to clause 10.4, electronic or soft copies of Personal Information can be destroyed or de-identified using any method such as: data erasure software, degaussing, physical destruction.

10.6 All hardware such as desktops, laptops, electronic media, mobile phones, hard drives, flash memory devices, CDs, DVDs, Blu-Rays, and other storage drives which have become obsolete to ECSA and which may be retired, sold or otherwise disposed of will be decommissioned to ensure that all Personal Information on those devices is

deleted or de- identified as set out in clause 10.4 above.

10.7 The Quality Business Unit responsible for carrying out or performing the destruction of all Personal Information will issue certification forms containing detailed information about the destruction of Personal Information and the date of destruction.

11. DATA BREACH PROCEDURE

Responsibility and Definition

11.1 The Information Officer has overall responsibility in relation to any breach of Personal Information notifications at ECSA.

11.2 A Personal Information breach is a breach of security leading to the accidental or unlawful Processing of a Data Subject's Personal Information.

11.3 Examples of potential breaches include the following: -

11.3.1 Loss or theft of Personal Information or equipment where such information is stored (e.g. loss or theft of a laptop);

11.3.2 Inappropriate access controls to Personal Information;

11.3.3 Sending an e-mail or SMS to the wrong recipient; or

11.3.4 Hacking, phishing and other IT related attacks.

11.4 Employees are encouraged to report any concerns in relation to potential Personal Information breaches even if the concern in the mind of the employee is not of a serious nature or does not meet the criteria for a breach to the Information Officer, Deputy Information Officer or delegated person

Procedure for Reporting

11.5 Where an Employee knows or suspects that there has been a potential unlawful

processing of Personal Information of a Data Subject at ECSA, the Employee must within 72 hours of becoming aware of the breach submit a breach report form to the Information Officer, a Deputy Information Officer or any other person who has been appointed by the Information Officer. A standard breach report form is attached hereto marked as Annexure **D**

11.6 The Employee should not take any further action in relation to the alleged breach. In particular, the Employee or their manager must not notify any affected persons of the alleged breach while ECSA is dealing with the breach in accordance with the obligations set out herein.

11.7 The Deputy Information Officer will acknowledge receipt of the breach report form and will be responsible for dealing with the report in collaboration with the Information Officer.

Managing and Recording the Breach

11.8 Upon being notified of an alleged Personal Information breach, the Information Officer, the Deputy Information Officer and any delegated person will collectively take steps to investigate whether any breach has in fact occurred.

11.9 If such a breach has occurred, ECSA will as soon as reasonably possible [but at least within 72 hours thereafter] taking into account the needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of ECSA's information system, do the following: -

11.9.1 Attempt to contain the breach, where possible;

11.9.2 Attempt to recover, rectify or delete the Personal Information which has been lost, damaged or disclosed;

11.9.3 Assess and record the breach in a breach register of ECSA;

11.9.4 Notify the Regulator in writing;

11.9.5 Notify the Data Subject(s) affected by the breach in writing unless the identity of the Data Subject(s) cannot be established;

11.9.6 Notify other appropriate parties of the breach such as insurers, third parties who may have been affected or the South Africa Police Services where the breach involves theft; and

11.9.7 Take steps to prevent similar future breaches.

Notification to a Data subject

11.10 As indicated, the Data Subject affected by the breach must be notified in writing as soon as reasonably possible by the Information Officer, the Deputy Information Officer or any delegated person.

11.11 The notification may be communicated to the Data Subject in at least one of the following ways: -

11.11.1 Sent via normal mail delivery to the Data Subject's last known physical or postal address;

11.11.2 E-mailed to the Data Subject's last known e-mail address;

11.11.3 Placed in a prominent position on the website of ECSA;

11.11.4 Published in the news media; or

11.11.5 as may be directed by the Regulator.

11.12 The notification must provide sufficient information to allow the Data Subject to take protective measures against potential consequences of the compromise. The information contained in the notification must include: -

11.12.1 A description of the possible consequences of a security compromise;

11.12.2 A description of the measures that ECSA intends to take or has taken to

address the security compromise;

11.12.3 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

11.12.4 If known to ECSA, the identity of the unauthorised person who may have accessed or acquired the personal information of the Data Subject.

11.13 The notification to a Data Subject may only be delayed if a public body responsible for the investigation of offences or the Regulator determines that the notification will impede criminal investigation.

Complaints to the Regulator

11.14 Employees must exhaust all internal procedures of ECSA before lodging a complaint with the Regulator alleging interference with the protection of their Personal Information.

11.15 Any other person may submit a complaint in writing to the Regulator alleging interference with the protection of the Personal Information of a Data Subject.

12. REVIEW

12.1 Changes to the Act and its Regulations will be monitored by ECSA and further amendments may be required to this Procedure in order for ECSA to remain compliant with its legal obligations.

12.2 ECSA will however monitor the effectiveness of this Procedure over a period and will be entitled to conduct a full review of the Procedures set out herein if necessary.

13. ANNEXURES:

A1 , A2 AND A3- CONSENT FORMS

B- OBJECTION TO PROCESSING

C- CORRECTION OR DELETION OR PERSONAL INFORMATION

D- BREACH REPORT

14. APPROVAL AND EFFECTIVE DATE

The Procedure is subject to the approval of the ECSA Governing Council and shall take effect on the day after the approval date.

15. The Policy was approved by the ECSA Governing Council on _____

_____ _____

Signed: **Date**

Revision Number	Revision Date	Revision Details	Approved By

ANNEXURE "A1"

EMPLOYEE CONSENT FORM

1. INTRODUCTION

1.1. The purpose of the Protection of Personal Information Act 4 of 2013 ("**POPIA**") is, *inter alia*, to give effect to the right to privacy and regulate the way in which personal information is processed.

1.2. In view of the requirements of POPIA ECSA requires the written consent of its employees to process their personal information.

1.3. Personal information includes but is not limited to an employee's identity number, contact details, medical, banking account, financial, prior criminal convictions, education information and employment history, images such as still pictures, video, voice and other similar data. The processing of personal information is thus essential in facilitating an employee's employment with ECSA.

1.4. In accordance with the provisions of POPI, ECSA will implement appropriate and reasonable security safeguards in order to ensure the integrity and confidentiality of personal information in its possession and/or under its control.

1.5. ECSA has implemented POPIA policies such as the Privacy Policy, Data Retention Policy, the Data Security Policy and the Employee shall acquaint themselves with and

be bound by all the policies and practices of ECSA, as implemented or amended by ECSA from time to time.

1.6. Should the Employee be in any doubt about the interpretation or application of any policy or practices of ECSA they shall seek guidance from the Information Officer or Deputy Information officer before taking any step

2. COLLECTION & PROCESSING OF PERSONAL INFORMATION

2.1. ECSA will collect and process personal information and special personal information of its employees for *inter alia* the following purposes: -

2.1.1. granting employee's access to ECSA's premises (including by way of biometric access control facilities);

2.1.2. remunerating employees;

2.1.3. conducting criminal, credit, reference, and other related reference checks on employees;

2.1.4. complying with the laws authorising or requiring such processing including but not limited to the Basic Conditions of Employment Act. 1997(Act No. 75 of 1997), the Labour Relations Act, 1995 (Act No. 66 of 1995), the Employment Equity Act, 1998 (Act No. 55 of 1998), the Compensation for Occupational Injuries and Diseases Act , 1997 (Act No. 61 of 1997), the Occupational Health and Safety Act, 2, 1993 (Act No, 85 of 1993), the Income Tax Act, 1962 (Act No. 58 of 1962); and

2.1.5. otherwise securing and facilitating employees' employment with ECSA, including rendering employee value added services, employee administration, training, performance reviews, talent management and other reasons related to the management of staff.

3. CONSENT

3.1. In view of the employment relationship between the parties, the Employee hereby expressly consents to: -

3.1.1. the processing of their personal information and special personal information as defined in POPIA by ECSA, any affiliate party and/or any third parties including ECSA's agents/contractors authorised by ECSA to process such personal information; and

3.1.2. the transfer of their personal information and special personal information to any of ECSA's agents, contractors, affiliated parties outside of the Republic of South Africa for the specific purposes for which it was collected as set out above. In this regard ECSA will only transfer personal information outside of the Republic of South Africa or permit transborder information flow in accordance with the provisions of POPIA.

3.2. The personal information will be stored by ECSA: -

3.2.1. for no longer than is necessary to achieve the purpose for which it was collected, unless further retention is: -

3.2.1.1. required by law or contractual obligation;

3.2.1.2. otherwise reasonably required by ECSA; or

3.2.1.3. retained further with the employee's consent.

3.2.2. after which point the personal information will be de-identified: -

3.2.2.1. in hard copy and/or electronic copy; and

3.2.2.2. subject to security safeguards that are adequate to ensure the integrity and confidentiality of the personal information.

3.3. The Employee acknowledges that the personal information provided to ECSA is accurate and correct and undertakes to advise ECSA of any changes in the personal information.

4. **EMPLOYEE OBLIGATIONS**

4.1. The Employee understands and agrees that they may, in the performance of their duties, operate as a "*processor*" and/or "*operator*" of personal information, as defined in POPIA.

4.2. Accordingly, the Employee warrants that they shall adhere to all applicable duties and obligations of a "processor" and/or "operator" as defined and required under POPIA and ECSA's Privacy Policy.

4.3. The Employee is also aware that ECSA is not necessarily the "Responsible Party", as defined by POPI, when processing the personal data of data subjects. As such, the Employee may be required to engage with third parties to ensure that the Employee's duties under POPIA are satisfied.

4.4. ECSA has appointed an Information Officer and Deputy Information Officers who manage all data-related queries at ECSA. Where the Employee is unsure whether any proposed action/situation may constitute a breach of their obligations under POPI, they are required to discuss it with the line manager before taking any step.

SIGNED AT_____ON THIS THE_____DAY OF _____202.

_____

THE EMPLOYEE

ANNEXURE "A2"

JOB APPLICANT'S CONSENT FORM

1. INTRODUCTION

1.1 The purpose of the Protection of Personal Information Act 4 of 2013 ("**POPIA**") is, *inter alia*, to give effect to the right to privacy and regulate the way in which personal information is processed.

1.2 In view of the requirements of POPIA ECSA requires the written consent of job applicants to process their personal information.

1.3 Personal information includes but is not limited to a job applicant's name, identity number, contact details, medical, banking account, financial, prior criminal convictions, education information and employment history, images such as still pictures, video, voice and other similar data and any other such information which would be required to conduct interviews and, if successful, to conclude an employment contract.

1.4 In accordance with the provisions of POPI, ECSA will implement appropriate and reasonable security safeguards in order to ensure the integrity and confidentiality of personal information in its possession and/or under its control.

1.5 ECSA has implemented POPIA policies such as the Privacy Policy, Data Retention Policy, the Data Security Policy and the job applicant may request these documents in order to acquaint themselves with their contents.

2 COLLECTION & PROCESSING OF PERSONAL INFORMATION

2.1 ECSA will collect and process personal information and special personal information of a job applicant for *inter alia* the following purposes: -

2.1.1 where applicable, for granting the job applicant access to ECSA's premises (including by way of biometric access control facilities);

2.1.2 collecting and capturing the job applicant's personal or special personal information;

2.1.3 storing the job applicant's information to establish their suitability for any current or future employment opportunities at ECSA;

2.1.4 for verifying and confirming the job applicant's identity and their suitability for the advertised role;

2.1.5 for the conducting of recruitment interviews;

2.1.6 for onboarding successful applicants;

2.1.7 to conduct appropriate checks on educational/ skills qualifications, employment history, registrations, licenses, criminal record and credit history where required and permitted in terms of the National Credit Act;

2.1.8 to conduct social media background screening on all social media platforms;

2.1.9 to conclude employment agreements with successful job applicants;

2.1.10 complying with any laws that may be relevant to the relationship.

3 CONSENT

3.1 In view of aforementioned, the job applicant hereby expressly consents to: -

3.1.1 the processing of their personal information and special personal information as defined in POPIA by ECSA, any affiliate party and/or any third parties including ECSA's agents/contractors authorised by ECSA to process such personal information; and

3.1.2 the transfer of their personal information and special personal information to any of ECSA's agents, contractors, affiliated parties outside of the Republic of South Africa for the specific purposes for which it was collected as set out above. In this regard ECSA will only transfer personal information outside of the Republic of South Africa or permit transborder information flow in accordance with the provisions of POPIA.

3.2 The personal information will be stored by ECSA: -

3.2.1 for no longer than is necessary to achieve the purpose for which it was collected, unless further retention is: -

3.2.1.1 required by law or contractual obligation;

3.2.1.2 otherwise reasonably required by ECSA; or

3.2.1.3 retained further with the employee's consent.

3.2.2 after which point the personal information will be de-identified: -

3.2.2.1 in hard copy and/or electronic copy; and

3.2.2.2 subject to security safeguards that are adequate to ensure the integrity and confidentiality of the personal information.

3.3 The job applicant acknowledges that the personal information provided to ECSA is accurate and correct and undertakes to advise ECSA of any changes in the personal information.

SIGNED AT_____ON THIS THE_____DAY OF _____2025.

_____

THE JOB APPLICANT

ANNEXURE "A3"

COUNCIL MEMBERS AND NOMINEES FOR MEMBERSHIP CONSENT FORM

1. INTRODUCTION

1.1. The purpose of the Protection of Personal Information Act 4 of 2013 ("**POPIA**") is, *inter alia*, to give effect to the right to privacy and regulate the way in which personal information is processed.

1.2. In view of the requirements of POPIA ECSA requires the written consent of Council members and nominees for membership to the Counsel to process their personal information.

1.3. Personal information includes but is not limited to a member or nominee's name, identity number, contact details, medical, banking account, financial, prior criminal convictions, education information and employment history, images such as still pictures, video, voice and other similar data and any other similar information which would be required to administer and regulate ECSA's relationship with its Council members or nominees for membership.

1.4. In accordance with the provisions of POPI, ECSA will implement appropriate and reasonable security safeguards in order to ensure the integrity and confidentiality of personal information in its possession and/or under its control.

1.5. ECSA has implemented POPIA policies such as the Privacy Policy, Data Retention Policy, the Data Security Policy and members or nominees for membership may request these documents in order to acquaint themselves with their contents.

2. COLLECTION & PROCESSING OF PERSONAL INFORMATION

2.1. ECSA will collect and process personal information and special personal information of a member or nominee for membership for *inter alia* the following purposes: -

2.1.1. where applicable, for granting such member or nominee for membership access to ECSA's premises (including by way of biometric access control facilities);

2.1.2. collecting and capturing their personal or special personal information in order for ECSA to fulfil its statutory obligations;

2.1.3. storing their information to establish their eligibility or suitability for membership to the Council in accordance with the provisions of the Engineering Profession Act, 46 of 2000;

2.1.4. verifying and confirming the member or nominee's identity;

2.1.5. the conducting of interviews;

2.1.6. onboarding nominees who are successfully appointed;

2.1.7. conducting appropriate checks on educational/ skills qualifications, employment or professional history, registrations, licenses, criminal record and credit history where required and permitted in terms of the National Credit Act;

2.1.8. conducting social media background screening on all social media platforms;

2.1.9. concluding agreements with successful nominees and members governing their relationship with ECSA;

2.1.10. complying with any laws that may be relevant to the relationship.

3. CONSENT

3.1. In view of the aforementioned, the member or nominee for membership hereby expressly consents to: -

3.1.1. the processing of their personal information and special personal information as defined in POPIA by ECSA, any affiliate party and/or any third parties including ECSA's agents/contractors authorised by ECSA to process such personal information; and

3.1.2. the transfer of their personal information and special personal information to any of ECSA's agents, contractors, affiliated parties outside of the Republic of South Africa for the specific purposes for which it was collected as set out above. In this regard ECSA will only transfer personal information outside of the Republic of South Africa or permit transborder information flow in accordance with the provisions of POPIA.

3.2. The personal information will be stored by ECSA: -

3.2.1. for no longer than is necessary to achieve the purpose for which it was collected, unless further retention is: -

3.2.1.1. required by law or contractual obligation;

3.2.1.2. otherwise reasonably required by ECSA; or

3.2.1.3. required subject to the member or nominee's consent.

3.2.2. after which point the personal information will be de-identified: -

3.2.2.1. in hard copy and/or electronic copy; and

3.2.2.2. subject to security safeguards that are adequate to ensure the integrity and confidentiality of the personal information.

3.3. The member or nominee for membership acknowledges that the personal information provided to ECSA is accurate and correct and undertakes to advise ECSA of any changes in the personal information.

SIGNED AT_____ON THIS THE_____DAY OF _____202. .

_____

MEMBER OR NOMINEE FOR MEMBERSHIP

ANNEXURE "B"

FORM 1
OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE ACT

Note:

1. Affidavits or other documentary evidence in support of the objection must be attached.
2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.

Reference Number ……

A: DETAILS OF DATA SUBJECT	
Name and surname of Data Subject:	
Residential, postal or business address:	**Code ( )**
Contact number(s):	
Fax number:	
E-mail address:	
B: DETAILS OF RESPONSIBLE PARTY	
Name and surname of responsible party (if the responsible party is a natural person):	
Residential, postal or business address:	**Code ( )**
Contact number(s):	
Fax number:	
E-mail address:	
Name of public or private body (if the responsible party is not a natural person):	
Residential, postal or business address:	**Code ( )**

Contact number(s):	
Fax number:	
E-mail address:	
C: REASONS FOR OBJECTION (Please provide detailed reasons for the objection)	

Signed at …… this …….. day of ……20….

……..
Signature of Data Subject (applicant)

ANNEXURE "C"

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTRUCTION OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE ACT

Note:

1. Affidavits or other documentary evidence in support of the objection must be attached.
2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.

Reference Number ……

Mark the appropriate box with an 'x".
Request for:

☐ Correction or deletion of the Personal Information about the Data Subject which is in possession or under the control of the responsible party.

☐ Destroying or deletion of a record of Personal Information about the Data Subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

A: DETAILS OF DATA SUBJECT	
Name and surname of Data Subject:	
Residential, postal or business address:	**Code ( )**
Contact number(s):	
Fax number:	
E-mail address:	
B: DETAILS OF RESPONSIBLE PARTY	
Name and surname of responsible party (if the responsible party is a natural person):	
Residential, postal or business address:	**Code ( )**
Contact number(s):	
Fax number:	
E-mail address:	

Name of public or private body (if the responsible party is not a natural person):	
Residential, postal or business address:	**Code ( )**
Contact number(s):	
Fax number:	
E-mail address:	
C: REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT / *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY (Please provide details for the request)	

***Delete whichever is not applicable**

Signed at …….. this …….. day of …… 20…….

……..
Signature of Data Subject

ANNEXURE "D"

PERSONAL INFORMATION BREACH REPORT FORM

Date and Time of Notification of Breach	
Details of person who you notified of breach - **Name and Surname** - **Position** - **Contract Details**	
Details of Breach (attach separate page, if necessary)	
Nature and Content of Personal Information Involved	
Number of person(s) Affected (If Known)	
Details of Persons(s) Affected (if Known) - **Name and Surname**	

- **Position** - **Contract Details**	
Details of person(s) unlawfully Processing the Personal Information (if known) - **Name and Surname** - **Position** - **Contract Details**	