

ENABLING &  
PROMOTING

A RESPONSIBLE  
LIQUOR INDUSTRY



**EASTERN CAPE**  
LIQUOR BOARD

# PROTECTION OF PERSONAL INFORMATION & PROMOTION OF ACCESS TO INFORMATION

## POLICY

# Policy Version Control

<b>Title</b>	PROTECTION OF PERSONAL INFORMATION & PROMOTION OF ACCESS TO INFORMATION POLICY			
<b>Created By</b>	OFFICE OF THE CEO			
<b>Version Number</b>	<b>Modified By</b>	<b>Modifications Made</b>	<b>Date Modified</b>	<b>Status</b>
2022	Legal Officer Office of the Chief Executive Officer	New	9 March 2022	Approved

## CONTENTS

1. INTRODUCTION.....	4
2. COLLECTION OF PERSONAL INFORMATION .....	4
3. COLLECTION OF EMPLOYEE INFORMATION .....	6
4. USE OF EMPLOYEE INFORMATION.....	6
5. COLLECTION OF SUPPLIER INFORMATION .....	7
6. USE OF SUPPLIER INFORMATION .....	7
7. COLLECTION OF STAKEHOLDERS INFORMATION .....	8
8. USE OF STAKEHOLDER INFORMATION .....	9
9. COLLECTION OF COMPLAINANT'S INFORMATION .....	9
10. USE OF COMPLAINANT'S INFORMATION .....	10
11. COLLECTION AND USE OF INFORMATION PERTAINING TO THE PROVISIONS OF THE EASTERN CAPE LIQUOR ACT AND ITS ASSOCIATED PROVISIONS.....	11
12. DISCLOSURE OF PERSONAL INFORMATION .....	11
13. SAFEGUARDING PERSONAL INFORMATION AND CONSENT.....	11
14. SECURITY BREACHES .....	11
15. ACCESS AND CORRECTION OF PERSONAL INFORMATION .....	13
16. RETENTION OF RECORDS.....	13
17. AMENDMENTS TO THIS POLICY.....	13
18. STANDARDS OF CONDUCT REQUIRED OF EMPLOYEES .....	13
19. POLICY APPROVAL .....	17

## **1. INTRODUCTION**

- 1.1 The Eastern Cape Liquor Board (ECLB) is obliged to comply with the Protection of Personal Information Act (No. 4 of 2013) ("POPI") as well as the Promotion of Access to Information Act (No. 2 of 2000) ("PAIA"), given that it processes liquor licence applications and associated processes in terms of its enabling statute, the Eastern Cape Liquor Act 10 of 2003 and it, it processes the personal information of its employees, suppliers, clients and other data subjects from time to time as well as that there may be requesters of information relating to the ECLB and its operations.
- 1.2 The ECLB guarantees its commitment to protecting data subject privacy as well as ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws. This is in line with the Constitutional provisions.
- 1.3 POPI requires the ECLB to inform its data subjects as to how their personal information is collected, processed, secured, disclosed and destroyed. This Policy sets out the manner in which the ECLB deals with such personal information as well as stipulates the general purpose for which such information is used. It also addresses the standards expected of employees of the ECLB in respect of their conduct in this regard.
- 1.4 Appropriate stakeholders should be made aware of the contents of this Policy when their consent is requested for the processing of their personal information or when there are interactions with data subjects.
- 1.5 The provisions of this Policy must be read along with the relevant practices and procedures that are used to operationalise the purpose hereof.
- 1.6 This Policy is supported by the ECLB's manual as required by section 14 of the Promotion of Access to Information Act 2 of 2000 as amended.

## **2. COLLECTION OF PERSONAL INFORMATION**

- 2.1 The ECLB collects stores and processes personal information pertaining to data subjects including its employees, suppliers, applicants, objectors, complainants and other stakeholders. The type of information collected and processed will depend on the purpose for which it is collected and will be processed for that scope of application only. Whenever appropriate, the ECLB will inform the data subject of the information required,

the purpose thereof, the rights of participation and the other relevant provisions contained at law.

2.2 The ECLB must indicate to the data subject the consequence of failing to provide such personal information. For example, the ECLB may not be able to employ an individual without certain personal information relating to that individual or the ECLB may not be in a position to render services to a client in the absence of certain information which is required.

2.3 Examples of the personal information the ECLB collects includes, but is not limited to information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person -

- 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 or opinions of another individual about the person; and
- 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.

i) the physical and residential address of the person.

### **3. COLLECTION OF EMPLOYEE INFORMATION**

3.1 For the purposes of this Policy, “employees” include potential, past and existing employees of ECLB.

3.2 The ECLB will, when appointing new employees, require information, including, but not limited to that listed above, from the prospective employee in order to process the employee’s information on the company’s system. Such information is reasonably necessary for the company’s record purposes as well as to ascertain if the prospective employee meets the requirements for the position to which he or she is being appointed and is suitable for such appointment.

3.3 The ECLB will use and process such employee information, as set out below, for purposes including, but not limited to, its employment records and to make lawful decisions in respect of that employee and its business.

### **4. USE OF EMPLOYEE INFORMATION**

4.1 Employees’ personal information will only be used for the purpose for which it was collected and intended. This would include, but is not limited to:

- 4.1.1 submissions to the Department of Labour
- 4.1.2 submissions to the Receiver of Revenue
- 4.1.3 for audit and recordkeeping purposes
- 4.1.4 in connection with legal proceedings
- 4.1.5 in connection with and to comply with legal and regulatory requirements
- 4.1.6 in connection with any administrative functions of the Company
- 4.1.7 disciplinary action or any other action to address the employee’s conduct or capacity
- 4.1.8 in respect of any employment benefits that the employee is entitled to
- 4.1.9 pre-and post employment checks and screening
- 4.1.10 any other relevant purpose to which the employee has been notified of
- 4.1.11 any compliance requirements at law.

4.2 Should information be processed for any other reason that is not in the legitimate interests of the employee, the ECLB will inform the employee accordingly.

4.3 The ECLB acknowledges that personal information may only be processed if certain conditions are met which, depending on the merits include -

- 4.3.1 The employee consents to the processing
- 4.3.2 The processing is necessary to attend to justifiable rights and obligations, for example contractual fulfilment
- 4.3.3 The processing complies with an obligation imposed by law on the company
- 4.3.4 Processing protects a legitimate interest of the employee
- 4.3.5 Processing is necessary for pursuing the legitimate interests of the ECLB or of a third party to whom information is supplied.

## **5. COLLECTION OF SUPPLIER INFORMATION**

5.1 For purposes of this Policy, suppliers include potential, past and existing suppliers.

5.2 The ECLB collects and processes its suppliers' personal information, such as that mentioned hereunder. The type of information will depend on the need for which it is collected and will be processed for that purpose only. Further examples of personal information collected from clients include, but is not limited to:

- 5.2.1 The supplier's identity number, name, surname, address, postal code
- 5.2.2 The suppliers residential and postal address
- 5.2.3 Contact information
- 5.2.4 Banking details
- 5.2.5 Company registration number
- 5.2.6 Full name of the legal entity
- 5.2.7 Tax and/or VAT number
- 5.2.8 Details of the contact person

## **6. USE OF SUPPLIER INFORMATION**

6.1 The supplier's personal information will only be used for the purpose for which it was collected and as agreed, if any such agreement is required at law. This may include, but not be limited to:

- 6.1.1 Quoting or tendering for services and/or products to the ECLB
- 6.1.2 Providing products and/ or services to the ECLB

- 6.1.3 In connection with sending accounts and communication in respect of services rendered and/or supplied products.
- 6.1.4 Referral to other service providers
- 6.1.5 Confirming, verifying and updating supplier details.
- 6.1.6 Contracts Management.
- 6.1.7 For audit and record keeping purposes
- 6.1.8 In connection with legal proceedings
- 6.1.9 In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

6.2 The ECLB acknowledges that personal information may only be processed if any of the conditions set out hereunder are met:

- 6.2.1 Supplier consents to the processing.
- 6.2.2 The processing is necessary to attend to rights and obligations that are justifiable, including fulfilling contractual provisions.
- 6.2.3 The processing complies with an obligation imposed by law.
- 6.2.4 Processing protects a legitimate interest of the party
- 6.2.5 Processing is necessary for pursuing the legitimate interests of the ECLB or of a third party to whom information is supplied.

## **7. COLLECTION OF STAKEHOLDER INFORMATION**

7.1 For purposes of this Policy, stakeholders include potential, past and existing persons, entities and members of the public which have partnered and/or are the target audience of the ECLB's social outreach programmes.

7.2 The ECLB collects and processes its stakeholder's personal information, such as that mentioned hereunder. The type of information will depend on the need for which it is collected and will be processed for that purpose only. Further examples of personal information collected from stakeholders include, but is not limited to:

- 7.2.1 The stakeholders name, surname.
- 7.2.2 The stakeholders residential and postal address
- 7.2.3 Contact information
- 7.2.4 Signatures
- 7.2.5 Gender classification
- 7.2.6 Race classification.



- 7.2.7 Full name of the legal entity
- 7.2.8 Tax and/or VAT number
- 7.2.9 Details of the contact person

## **8. USE OF STAKEHOLDER INFORMATION**

8.1 The stakeholder's personal information will only be used for the purpose for which it was collected and as agreed, if any such agreement is required at law. This may include, but not be limited to:

- 8.1.2 Provision of supporting evidence in respect of validation and/or audit of ECLB's achievement of targets.
- 8.1.3 To support compilation of statistics for reporting purposes.
- 8.1.4 Contracts Management.
- 8.1.5 For audit and record keeping purposes
- 8.1.6 In connection with legal proceedings
- 8.1.7 In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

8.2 The ECLB acknowledges that personal information may only be processed if any of the conditions set out hereunder are met:

- 8.2.1 Stakeholders consents to the processing.
- 8.2.2 The processing is necessary to attend to rights and obligations that are justifiable, including fulfilling contractual provisions.
- 8.2.3 The processing complies with an obligation imposed by law.
- 8.2.4 Processing protects a legitimate interest of the party.
- 8.2.5 Processing is necessary for pursuing the legitimate interests of the ECLB or of a third party to whom information is supplied.

## **9. COLLECTION OF COMPLAINANT INFORMATION**

9.1 For purposes of this Policy, Complainants include potential, past and existing Complainants who have lodged complaints against both licenced and unlicenced outlets. It is recorded that that Complainants are also enabled to lodge a complaint anonymously.

9.2 The ECLB collects and processes Complainants personal information, such as that mentioned hereunder. The type of information will depend on the need for which it is

collected and will be processed for that purpose only. Further examples of personal information collected from clients include, but is not limited to:

- 9.2.1 The Complainants, name, surname, residential and postal address, postal code
- 9.2.2 Contact information
- 9.2.3 Locality of the Complainant to the outlet

## **10. USE OF COMPLAINANT'S INFORMATION**

10.1 The Complainant's personal information will only be used for the purpose for which it was collected and as agreed, if any such agreement is required at law. This may include, but not be limited to:

- 10.1.1 In the processes of resolving the complaint which may include providing the licenced outlet the Complainant's details.
- 10.1.2 . Referral to South African Police Services, Municipal Enforcement Divisions or other related government intuitions.
- 10.1.3 For audit and record keeping purposes.
- 10.1.4 For any investigation if the complaint is related to fraud both internal or external.
- 10.1.5 In connection with legal proceedings
- 10.1.6 In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

10.2 The ECLB acknowledges that personal information may only be processed if any of the conditions set out hereunder are met:

- 10.2.1 Complainant consents to the processing
- 10.2.2 The processing is necessary to attend to rights and obligations that are justifiable, including fulfilling contractual provisions
- 10.2.3 The processing complies with an obligation imposed by law
- 10.2.4 Processing protects a legitimate interest of the party
- 10.2.5 Processing is necessary for pursuing the legitimate interests of the ECLB or of a third party to whom information is supplied.

## **11. COLLECTION AND USE OF INFORMATION PERTAINING TO THE PROVISIONS OF THE EASTERN CAPE LIQUOR ACT AND ITS ASSOCIATED PROVISIONS.**

11.1 It is recorded that the ECLB is empowered to collect and use personal information of an Applicant, interested parties such as Objectors and all other persons as enabled by means of the legislative provisions of its enabling Act 10 of 2003 and the associated Regulations.

## **12. DISCLOSURE OF PERSONAL INFORMATION**

12.1 Subject to legislative provisions providing the contrary, the ECLB may share data subject's personal information with third parties as well as obtain information from such third parties for reasons set out above.

12.2 The ECLB may also disclose data subject's information where there is a duty or a right to disclose in terms of applicable legislation, a contractual obligation, the law or where it may be necessary to protect the ECLB's rights.

## **13. SAFEGUARDING PERSONAL INFORMATION AND CONSENT**

13.1 It is a requirement of POPI to adequately protect the personal information the ECLB holds and to avoid unauthorised access and use of personal information.

13.2 The ECLB shall review its technical and operational security controls and processes on a regular basis to ensure that personal information is secure.

13.3 The ECLB shall appoint an Information and Deputy Information Officer who is responsible for the encouragement of compliance with the conditions of the lawful processing of personal information and other provisions of POPI.

## **14. SECURITY BREACHES**

14.1 Should the ECLB detect a security breach on any of its systems that contain personal information, the ECLB shall take the required steps to assess the nature and extent of the breach in order to ascertain if any information has been compromised.

14.2 The ECLB shall activate its Incident Response Plan which includes the notification of the affected parties and the Information Regulator should it have reason to believe that personal information has been compromised. Such notification shall only be made where the ECLB can identify the data subject to which the information relates. Where

it is not possible it may be necessary to consider website publication and whatever else the Information Regulator prescribes.

14.3 Notification will be provided in writing by means of either:

14.3.1 Email

14.3.2 registered mail

14.3.3 placed on the ECLB's website.

14.4 The notification shall provide the following information where possible:

14.1. description of possible consequences of the breach

14.2 measures taken to address the breach

14.3 recommendations to be taken by the data subject to mitigate adverse effects

14.4 the identity of the party responsible for the breach.

14.5 In addition to the above, the ECLB shall notify the Regulator of any breach and/or compromise to personal information in its possession and work closely with and comply with any recommendations issued by the Regulator.

The following provisions will apply in this regard as delegated by the Information Officer to the Deputy Information Officer: -

14.5.1 the Deputy Information Officer will be responsible for overseeing the investigation.

14.5.2 The Deputy Information Officer will be responsible for reporting to the Information Regulator within 2 working days of a breach/ compromise to personal information.

14.5.3 The Deputy Information Officer will be responsible for reporting to the Data Subject(s) within 2 working days of a breach/ compromise to personal information.

14.5.4 The timeframes above are guidelines and depending on the merits of the situation may require earlier or later reporting.

## **15. ACCESS AND CORRECTION OF PERSONAL INFORMATION**

15.1 Data subjects have the right to request access to any personal information that the ECLB holds about them.

15.2 Data subjects have the right to request the ECLB to update, correct or delete their personal information on reasonable grounds. Such requests must be made to the Information Officer.

15.3 Where an employee, stakeholder, complainant and/or supplier objects to the processing of their personal information, the ECLB may no longer process said personal information. The consequences of the failure to give consent to process the personal information must be set out before the employee or stakeholder, complainant and/or supplier confirms his/her objection.

15.4 The data subject must provide reasons for the objection to the processing of his/her personal information.

## **16. RETENTION OF RECORDS**

16.1 The ECLB shall ensure the safeguarding and protection of all personal information or data. The ECLB is required to retain certain information as prescribed by the respective laws and its retention policy.

## **17. AMENDMENTS TO THIS POLICY**

17.1 Amendments to this Policy will take place from time to time subject to the discretion of the ECLB and pursuant to any changes in the law. Such changes will be brought to the attention of employee's clients where it affects them.

## **18. STANDARDS OF CONDUCT REQUIRED OF EMPLOYEES**

18.1 In addition to the provisions contained within this POPI policy, the employment contract, the disciplinary code, the electronic communications and social media policy as well as any other document relating to employees, the following standards of conduct and practice and their accompanying underlying principles must be complied with at all times and a breach thereof may result in serious disciplinary action and even dismissal for a first offence.

### **18.1.1 Physical records and assets**

All physical records containing personal information as well as any hardware, devices or similar equipment must always be protected from unauthorised access and/ or damage and/ or loss and/ or other prejudice.

#### 18.1.2 Systems and platforms

Compliance with security requirements in respect of, for example, the following areas is crucial –

18.1.2.1 Changing, storage and sharing of usernames and passwords

18.1.2.2 Data back-ups and protection

18.1.2.3 Limitations on the use of personal devices such as external hard drives or similar storage options, mobile cellular phones and the like.

#### 18.1.3 Internal and external posting of personal information of ECLB data subjects

18.1.3.1 A prohibition on the sharing and/ or posting of personal information on any platforms outside of those that are ECLB approved under specific conditions as well as a total ban on posting and/ or transmitting personal information outside of the ECLB on social media and/ or any other similar platform.

#### 18.1.4 Conditions to be observed when collecting or processing personal information.

18.1.4.1 The following principles must be complied with when dealing with personal information and if there is any doubt, the written authority of the Deputy Information Officer must be obtained by the employee prior to the said processing –

##### **Accountability**

The employee must ensure that the conditions and all the measures that give effect to such conditions are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.

##### **Processing limitation**

Personal information must be processed

(a) lawfully; and

(b) in a reasonable manner that does not infringe the privacy of the data subject.

This includes considerations of minimality and adequacy given the purpose for which it is intended. In addition -

- The data subject or a competent person (data subject is a child) consents to the processing; or/ and
- The purpose is to carry out actions for the conclusion or performance of a contract; or/ and
- Processing complies with an obligation imposed by law on the responsible party; or/ and
- Processing protects a legitimate interest of the data subject; or/ and
- Processing is necessary for the proper performance of a public law duty by a public body; or/ and
- Processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied; or/ and
- Collection must be directly from the data subject, except as otherwise provided for unless the information is contained in or derived from a public record or has deliberately been made public by the data subject.

### **Purpose specification**

Personal information is collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.

### **Further processing limitation**

Further processing of personal information must be compatible with the purpose for which it was collected and consider -

(a) the consequences of the intended further processing for the data subject

(b) the manner in which the information has been collected; and

(c) any contractual rights and obligations between the parties.

### **Security Safeguards**

Employees must secure the integrity and confidentiality of personal information in their possession or under their 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.

Employees must take reasonable measures to—

(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under their 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.

Employees must have due regard to **generally accepted information security practices and procedures** which may apply to the situation generally or be required in terms of specific industry or professional rules and regulations.



## 19. POLICY APPROVAL


### Submitted by

  
.....  
Ms K. Oosthuysen

Legal Officer

Date: 9 March 2022


### Recommended by

  
.....  
Dr N. Makala

Chief Executive Officer

Date: 9 March 2022

### Approved by

  
.....  
Ms N. Tys

Chairperson: Board

Date: 09/03/2022