APPROVED
by the Chief Executive Officer of AB Akola Group
On 10/9/2024 by order No. V-24/25-005

AB AKOLA GROUP

PROCEDURE FOR THE PROVISION OF INFORMATION UNDER THE LAW ON THE PROTECTION OF WHISTLEBLOWERS OF THE REPUBLIC OF LITHUANIA

1. GENERAL PROVISIONS

1.1. **AB Akola Group**, legal entity's code 148030011, registered office at Subačiaus St. 5, Vilnius, the Republic of Lithuania ("**Company**"), Procedure for the Provision of Information under the Law on the Protection of Whistleblowers of the Republic of Lithuania ("**Procedure**") establishes procedures for the submission of information on breaches that are being allegedly arranged, have been committed or are being committed within the Company, for the receipt of information on breaches through the Company's internal channel for providing information on breaches, for the assessment of such information, and for the making of decisions.

1.2. Information received by the Company about breaches shall be received, registered, processed and the protection measures for persons providing information about a breach shall be ensured in accordance with the Law on the Protection of Whistleblowers of the Republic of Lithuania ("**Law**"), the Description of Procedures for the Establishment of the Internal Channels of Providing Information about Breaches and Ensuring their Functioning, approved by the Government of the Republic of Lithuania by the Resolution No. 1133 "On the Implementation of the Law on the Protection of Whistleblowers of the Republic of Lithuania" of 14 November 2018 ("**Description**"), other legislation, and the Procedure.

1.3. The definitions used in the Procedure shall have the meaning given to them in the Law and other legislation governing whistleblower protection requirements.

2. COMPETENT ENTITY

2.1. The Chief Executive Officer of the Company, by a separate order, designates a person(s) whose reputation and qualifications are beyond doubt as to their ability to properly implement the provisions of the Procedure and who shall administer the Company's internal channel for providing information on breaches ("**Competent Entity**").

2.2. The Competent Entity is not influenced or otherwise hindered in the performance of its functions under this Procedure, the Law or the Description.

2.3. The Competent Entity performs the following functions:

a) analyses and investigates information on breaches received through the internal channel for providing information on breaches;

b) ensures that a person who is or has been engaged in a recruitment or other pre-contractual, service, employment or contractual relationship with the Company (consultancy, contract, sub-contract, internship, apprenticeship, volunteering, etc.), as well as the self-employed person, shareholder or person belonging to the administrative, management or supervisory body of the Company (including non-executive members, as well as volunteers and paid or unpaid interns), or any natural person working under the supervision and direction of contractors, subcontractors and / or suppliers providing information about the breach ("**Person**") and the information provided by him / her will remain confidential, except for cases established by law;

c) cooperates with the Company's employees, administrative units, competent authorities by providing and / or obtaining necessary information;

d) collects and compiles depersonalized statistical data on the number of reports received and the outcome of their examination;

e) ensures that the information about the breach submitted through the Company's internal channel for providing information on breaches is collected and stored on a durable and, where necessary, retrievable medium where the relevant information relating to the breach can be found. The medium shall also store recorded conversations, if any, between the Person, who reported information about the breach, and the Competent Entity, minutes of conversations and other information related to the reported breach;

f) performs such other functions as may be prescribed by the Law and the Description.

2.4. The Competent Entity has the following rights in the exercise of its functions, including but not limited to:

a) obtain the necessary information and data from the Company's employees, departments and units not under its control;

b) when investigating information received through the internal channel for providing information on breaches, to take decisions related to the conduct of the investigation, which shall be binding on all employees and departments of the Company.

2.5. The Competent Entity ensures that the information about the breach received and the related data are stored securely and are accessible only to persons entitled to handle the information about the breach. The confidentiality of the person who provided the information shall be ensured during the procedures for the investigation of misconduct in public office or employment, insofar as this is objectively possible.

2.6. Employees of the Company who, by virtue of their functions, have access to the data provided by the Person who has provided information on the breach, or who are in a position to learn the data of the Person who has provided information on the breach, and who have been made aware of their liability for violation of the whistleblowers' protection requirements laid down in the Law and / or other legislation, shall be obliged to sign a Confidentiality Undertaking (ANNEX 1) and to undertake not to disclose to any third party the said information or data.

2.7. Confidentiality may be not secured when requested in writing by the Person who provided the information about the breach or where the information provided by the Person who provided the information about the breach is knowingly false.

3. PROVISION OF INFORMATION ON BREACHES

3.1. In accordance with the Law, information on breaches is provided in relation to the following factors:

a) a threat to public security or health, life or health of an individual;

b) environmental hazards;

c) impediment to or unlawful interference with investigations by law enforcement bodies or the administration of justice by courts;

d) financing of illegal activities;

e) illegal or non-transparent use of public funds or assets;

f) unlawfully acquired assets;

g) concealment of the effects of a committed breach, obstruction of quantification of the effects;

h) breaches referred to in the list approved by the Minister of Justice of the Republic of Lithuania, drawn up considering the scope of application of the European Union legal acts referred to in Directive (EU) 2019/1937;

i) damage to the financial interests of the European Union, as referred to in Article 325 of the Treaty on the Functioning of the European Union and further specified in the relevant European Union instruments;

j) breaches related to the internal market as referred to in Article 26(2) of the Treaty on the Functioning of the European Union, including breaches of the European Union's competition and State aid rules, as well as breaches related to the internal market as a result of acts in contravention of the rules on corporation tax or agreements aimed at obtaining a tax advantage to the detriment of the subject-matter or the purpose of the applicable corporation tax law;

k) other breaches.

3.2. A Person providing information through the Company's internal channel for providing information on breaches is not required to be fully does not have to be completely convinced of the truth of the facts being reported, nor is he / she under any obligation to make any assessment as to whether or not the violation of which he / she is reporting falls within the scope of a criminal offence or any other violation of the law, as defined by the legislation.

3.3. Information about a breach may be provided:

a) within the Company through its internal channel for providing information on breaches;

b) to the Prosecutor General's Office of the Republic of Lithuania by e-mail: *praneseju.apsauga@prokuraturos.lt*;

c) publicly.

3.4. If a Person chooses to submit information about the breach through the Company's internal channel for providing information on breaches, the Person may do so in one of the following ways:

a) by electronic means: by e-mail to *pranesk@akolagroup.lt*;

b) by completing the appropriate form;

c) by personally informing the Competent Entity.

3.5. A Person providing information about a breach has the right to provide the information by completing the breach notification form approved by the Description (ANNEX 2), or to report the breach by means of a free-form

notification, which shall contain the information specified in Section 3.6 of the Procedure and shall state that the information is provided in accordance with the Law.

3.6. A Person reporting a breach shall include in a notification:

a) specific factual circumstances of a breach;

b) the person who is arranging, is taking or has taken part in the commission of the breach;

c) whether the person has reported the breach and, if yes, who it has been reported to and whether a response has been received;

d) his / her name, surname, personal identification number or date of birth or, if he / she does not have a personal identification number – his / her contact details;

e) any other documents, data or information in their possession revealing indications of a possible breach.

4. RECEIVING, FORWARDING AND RECORDING INFORMATION ON BREACHES

4.1. The information received through the Company's internal channel for providing information on breaches in the manner set out in Section 3.4 of the Procedure shall be reviewed (listened to) by the Competent Entity at least once every 1 (one) business day during the Company's business hours.

4.2. The notification of a breach shall be received and recorded by the Competent Entity in a register designated for that purpose. This information on the breach shall be marked with a confidentiality flag.

4.3. Upon receipt of a notification, the Competent Entity shall notify the person who submitted the information about the breach of the receipt of the notification within 2 (two) business days from the receipt of the notification. The confidentiality of the Person making the notification shall be ensured from the moment of its receipt and the notification shall be promptly assessed.

4.4. Notices of breach received by the Company by means other than those referred to in paragraph 3.4 of the Procedure shall not be registered and shall be promptly transmitted by one of the means referred to in paragraph 3.4 of the Procedure. Upon receipt of confirmation of the delivery of the notification to the internal channel, the transmitted information on breach shall be deleted immediately.

4.5. Employees of the Company who, in the course of their duties, become aware of the personal data of a Person who has provided information about a breach, or the content of such information, shall be obliged to ensure the confidentiality of the said information and personal data, both during and after work.

5. ASSESING INFORMATION ON BREACHES, DECISION-MAKING

5.1. The Competent Entity takes one of the following decisions in respect of the breach information submitted through the internal channel for providing information on breaches:

a) to examine the information submitted concerning the breach;

b) if the information received about a breach gives reasonable grounds to believe that a criminal offence, an administrative offence or any other offence is being allegedly arranged, is being committed or has been committed, immediately, but no later than within two (2) business days from the date of receipt of the information, to forward the information received about the breach to an authority authorised to investigate such information, without the consent of the Person who has provided the information about the breach and to inform the Person;

c) to terminate the procedure for the examination of the information received concerning the breach if:

(i) the assessment reveals that the information provided about the breach does not meet with the provisions of the Law;

(ii) the information related to the breach is based on information that is manifestly untrue;

(iii) the information submitted in relation to the breach has already been investigated or is being investigated.

5.2. The Competent Entity informs the Person who submitted the information about the breach in writing of the decision taken on the examination of the information within no later than 10 (ten) business days from the receipt of the information about the breach. The decision not to examine the information on the breach must be reasoned.

5.3. The Competent Entity, after completing the examination of the information on the breach, shall inform the Person who submitted the information on the breach in writing within no later than two (2) business days of the decision it has taken, the outcome of the examination and the actions taken or planned to be taken, and shall indicate the procedure for appealing against the decision taken.

5.4. The Competent Entity shall advise the Person who submitted the information on the breach on the possible or actual adverse effects on the Person of the fact that the information on the breach has been provided, and on the means or remedies available to the Person, if the Person so requests.

5.5. Upon quantification of a breach, the Competent Entity shall inform the Person who provided the information about the breach of the liability imposed on the persons who committed the breach.

5.6. if the Person who has provided information about the breach has not received a response, or if the Company has not taken any action in response to the information provided, he / she shall have the right to directly address the competent authority - the Prosecutor General's Office of the Republic of Lithuania - in accordance with the provisions of Article 4(4)(4) of the Law and to submit a notification of breach to it.

6. CONSEQUENCES OF PROVIDING INFORMATION

6.1. Confidentiality will be applied to the person who has provided information about the breach.

6.2. The confidentiality requirement does not apply where:

a) requested in writing by the Person who submits or has submitted information about the breach;

b) the person provides information that is manifestly untrue.

6.3. The disclosure of the data and other information of a Person who has provided information about a breach to the competent authorities investigating pre-trial investigations or to other competent authorities investigating other breaches, without disclosing such data to the Company, is not to be considered a breach of confidentiality.

6.4. A Person shall not be subject to any contractual or non-contractual liability, including liability for defamation or slander, in respect of the provision of information about a breach, provided that he / she reasonably believed that he / she was providing true information when providing the information.

6.5. In the case of an anonymous whistleblower, protection, encouragement and assistance measures are applied in cases where the identity of the Person who has provided the information on breach has been disclosed and it is necessary to protect the Person from any adverse impact.

6.6. A Person shall only be liable for the damage caused by providing information on breach only if it is proved that the Person could not reasonably have believed that the information provided by the Person was true.

6.7. Provision of knowingly false information or information comprising a state secret or an official secret shall not offer a person guarantees under this Law. A person who has provided knowingly false information or disclosed a state secret or an official secret, or a professional secret shall be held liable under legal acts.

7. FINAL PROVISIONS

7.1. The Competent Entity shall be responsible for establishing an internal channel for providing information on breaches and securing its functioning. The Competent Entity shall notify employees, civil servants and officers regarding the internal channel for providing information on breaches in place at the institution and shall provide related information at the workplace in a manner accessible to all of them.

7.2. The Competent Entity 1 (one) time a year shall summarise the data on the receipt of information on breaches, the investigation of breaches and shall publish on the Company's website statistics on the number of cases where information on breaches has been submitted, the outcome of their assessment, the summary information on the breaches that have been disclosed on the basis of the information submitted by the Persons in accordance with the Procedure.

7.3. The Procedure shall enter into force on the date of the approval. The Procedure is approved by the Chief Executive Officer of the Company.

7.4. Each employee shall be made aware of the Procedure in the following manner:

a) immediately after the approval of the Procedure, the Procedure shall be sent to all employees by e-mail;

b) immediately following the approval of the Procedure, the Procedure shall be placed on the Company's server (or other location where all of the Company's internal memorandums, procedures and rules are stored) and shall be made available to employees there at all times;

c) each new employee shall be made aware of the Procedure on his / her first day of employment with the Company, either by being provided with the Procedure by e-mail or by being given access to the Procedure at the place referred to in Section 7.4.b).

7.5. A letter, notice or document sent by e-mail shall be deemed to have been served:

a) on the same business day if sent at least 1 (one) hour before the close of the Company's business hours;

b) on the next business day if sent more than 1 (one) hour before or after the close of the Company's business hours;

c) the next business day, if sent on a day of rest or public holiday;

d) the employee's next business day, if it was sent to the employee during the employee's annual leave or sick leave;

e) the employee's next business day after the secondment, if it was sent to the employee during the secondment and the secondment was not accompanied by an internet connection.

7.6. Immediately after the approval of the Procedure, the Procedure is posted on the website www.akolagroup.lt and is available at any time there.

7.7. The Procedure shall be binding on all employees of the Company, regardless of the term of their employment. Each employee shall be personally responsible for compliance with the Procedure.

7.8. An employee who violates this Procedure may be subject to the liability provided for in this Procedure, the Labour Code of the Republic of Lithuania and other legal acts.

7.9. The following Annexes are attached to the Procedure:

ANNEX 1 CONFIDENTIALITY UNDERTAKING FORM;

ANNEX 2 BREACH NOTIFICATION FORM.

ANNEX 1 CONFIDENTIALITY UNDERTAKING FORM

CONFIDENTIALITY UNDERTAKING

I, _____

(Name, surname)

_____

(Name of Company and structural unit, title)

confirm that:

1) I am familiar with the requirements of the Description of Procedures for the Establishment of the Internal Channels of Providing Information about Breaches and Ensuring their Functioning ("**Description**") and the Law on the Protection of Whistleblowers of the Republic of Lithuania ("**Law**") and other legal acts providing for the obligation not to disclose, not to pass on, in accordance with the functions performed by **AB Akola Group**, legal entity's code 148030011, registered office at Subačiaus St. 5, Vilnius, the Republic of Lithuania ("**Company**") received information about the breach, and I understand that I will have access to information about persons who are subject to confidentiality obligations under the provisions of the Law and other legal acts;
2) I have been warned that a breach of this undertaking may render me liable to prosecution for contravention of the requirements for the protection of individuals set out in the Law and / or other legislation; and

I undertake to:

3) ensure the confidentiality of the information on a breach received, not to disclose or communicate data and / or information on a breach entrusted to, or made known by, the person providing information on a breach to any third party not authorised to have access to such data and / or information, and not to use such data and / or information for his / her own personal interests or for the personal interests of third persons. Such information may be disclosed or communicated only to authorised persons or authorities in cases provided for by the laws of the Republic of Lithuania;
4) report to the supervisor any situation observed or of which I become aware which may threaten the security and confidentiality of such information;
5) fulfil the requirements of the Law, the Description and other legal acts of the Republic of Lithuania.

This undertaking shall remain in force for the duration of the employment relationship with the Company, as well as in the event of reassignment or termination of the employment relationship.

Signature: _____

Name, surname: _____

Title: _____

ANNEX 2 BREACH NOTIFICATION FORM

Government of the Republic of Lithuania
Resolution No. 1133 of 14 November 2018
Annex

(Breach Notification Form)

BREACH NOTIFICATION

20 ___ m. _____ ___ d.

_____
(place)

Details of the person reporting the breach	
Name, surname	
Personal identification number	
Workplace (service, employment or contractual relationship with the institution)	
Title	
Telephone number (contact notes)	
Personal e-mail or residential address	
Information about the breach	
1. What breach are you reporting? What is the nature of the breach?	
2. Who committed this breach? What could have been the person's motives in committing the breach?	
3. Place and time of the breach.	
Details of the person or persons who committed the breach	
Name, surname	
Workplace	
Title	
3. Are there any other persons who were or could have been involved in the breach? If yes, please specify who they are.	
4. Are there any other witnesses to the breach? If yes, please provide their contact details.	
Details of the witness or witnesses to the breach	
Name, surname	
Title	
Workplace	
Telephone number	
E-mail	
5. When the breach was committed and when you became aware of it or noticed it?	
6. What evidence could you provide to support an investigation into the breach? Please indicate any attached written or other data related to the breach.	
7. Have you already reported this breach to anyone? If you have, who was notified and did you receive a reply? If you have received a reply, please state the substance of the reply.	
8. Additional notes and comments.	

☐ I confirm that I am aware of the legal consequences for providing false information and that the information I provide is correct.

Date	Signature