

## **RULES ON REPORTING BREACHES AT OVOKO, UAB**

### **GENERAL PROVISIONS**

1. The aim of the Rules on Reporting Breaches (hereinafter referred to as the “Rules”) at Ovoko, UAB (hereinafter referred to as the “Company”) is to regulate the procedure for reporting information on breaches that have been committed, are being committed or are about to be committed at the Company through the internal channels (hereinafter referred to as the “Internal Channels”), receiving such reports, assessing and examining the information about the breach and informing the persons concerned.
2. These Rules set out the procedures for reporting the following types of breaches:
  - 2.1. Risks to public safety or health, or to the life or health of a person;
  - 2.2. Environmental risks;
  - 2.3. Obstructing or improperly influencing the investigations by law enforcement authorities or the administration of justice by the courts;
  - 2.4. Financing illegal activities;
  - 2.5. Illegal or non-transparent use of public funds or the Company’s assets;
  - 2.6. Illegally acquired property;
  - 2.7. Concealing the consequences of an infringement, or obstructing the identification of the extent of the consequences;
  - 2.8. The list of breaches set out in the list approved by Order No. 1R-53 of the Minister of Justice of the Republic of Lithuania of 15 February 2022;
  - 2.9. Damaging the financial interests of the European Union;
  - 2.10. Infringements of the competition and state aid rules;
  - 2.11. Other breaches.
3. Information received by the Company about a breach shall be received, registered and examined, and the protection measures for the persons providing information about the breach shall be ensured in accordance with these Rules, the Law on the Protection of Whistleblowers of the Republic of Lithuania (hereinafter referred to as the “Whistleblower Protection Law”) and Decree No. 1133 of the Government of the Republic of Lithuania “On the Implementation of the Law on the Protection of Whistleblowers of the Republic of Lithuania” dated 14 November 2018.
4. The definitions used in the Rules shall be understood as defined in the Whistleblower Protection Law and other legislation governing the whistleblower protection requirements.
5. Competent Entity – a person employed by the Company, appointed by order of the Company’s Chief Executive Officer, who shall administer the Internal Channels and perform the following functions:

- 5.1. Analyse and investigate the information on breaches received through the Internal Channels;
  - 5.2. Ensure the confidentiality of the person who provided the information about the breach through the Internal Channels;
  - 5.3. Cooperate with the employees and departments of the Company, as well as the competent authorities, by providing and/or obtaining the necessary information;
  - 5.4. Collect and compile personalised statistics on the number of notifications received and the outcome of their analyses;
  - 5.5. Ensure that the information provided by the Company through the Internal Channels regarding the breach is collected and stored in a durable and, where necessary, retrievable medium, where the relevant information relating to the breach can be found. Conversations, if any, recorded during meetings between the person providing information on the breach and the Competent Entity, minutes of the conversations and other information relating to the notified breach shall also be stored in the aforesaid medium;
  - 5.6. Perform the other functions set out in these Rules.
  - 5.7. And shall have the right to:
    - 5.7.1. Obtain the necessary information and data from the Company's employees and departments outside his/her control;
    - 5.7.2. Make decisions relating to the investigation, which shall be binding on all employees and departments of the Company, when investigating information received through the Internal Channels about a breach.
6. Whistleblower – a person who provides information about a breach through the Internal Channels. The person providing information about the breach shall have, or will have had, an employment relationship, contractual relationship (consultancy, contract, subcontract, internship, apprenticeship, volunteering, etc.) or other pre-contractual relationship with the Company, and may be a shareholder, member of a management or supervisory body, or a person working in a supervisory or management capacity with respect to the Company's contractors, sub-contractors and/or suppliers.

### **PROVIDING INFORMATION ON BREACHES**

7. The person submitting the information about the breach has the right to submit the information by filling in the notification form (Annex 1) established by the Government of the Republic of Lithuania, or to report the breach by means of a notification in a free form, which must include the following information:
  - 7.1. What kind of breach is being committed, has been committed or is about to be committed;
  - 7.2. When the breach is being committed, has been committed or is about to be committed;
  - 7.3. How the breach is being committed, has been committed or is about to be committed;
  - 7.4. Who is committing, has committed or is about to commit the breach;
  - 7.5. When and in what circumstances the breach came to their attention;
  - 7.6. Name, surname, personal identification number, workplace and other contact details of the person submitting the report;
  - 7.7. How and when is the best way to contact the whistleblower;

- 7.8. Any documents, data or information, if available, that may reveal the indications of a possible breach;
  - 7.9. Confirmation that the information about a possible breach is being provided in accordance with the Law on the Protection of Whistleblowers of the Republic of Lithuania.
8. The person providing information about the breach may submit it to the Company in one of the following ways:
- 8.1. By visiting the Competent Entity directly at Žirmūnų g. 70, Vilnius, Lithuania;
  - 8.2. By sending a notice to the address specified in the Annex to these Rules by post, indicating that the notice is addressed to the Competent Entity [Head of People Darius Dužinskas];
  - 8.3. By sending a notice in a free form, or by sending the notice in the Annex to these Rules, to the Company's email address at [inform@ovoko.com](mailto:inform@ovoko.com)

### **ACCEPTANCE AND REGISTRATION OF NOTIFICATIONS**

9. The information about a breach shall be accepted by the Competent Entity and recorded in a special register.
10. Information about a breach received by the Company at an email address other than the email address specified in the Rules shall not be registered, and shall be immediately forwarded to the email address specified in the Rules. Information received after being forwarded, in accordance with this paragraph, to an email address other than the one specified in the Rules shall be permanently destroyed without delay, but not later than within three working days.
11. The Competent Entity shall ensure that the resulting information on the breach and the related data are stored securely and are accessible only to persons entitled to process the information about the breach.
12. The person who provided the information about the breach is subject to the confidentiality requirement.
13. The confidentiality requirement does not apply if:
  - 13.1. The person who provided the information about the breach requests so in writing;
  - 13.2. The person provides information that he/she knows to be false.
14. The Competent Entity shall, upon the receipt of the information about the breach, if the person who has provided it so wishes, immediately inform that person in writing of the receipt of the information.
15. Employees of the Company working under employment contracts who, by the scope of their functions, have access to the data provided by the person providing information on the breach, or who may become aware of the details of the person who has provided such information, shall be made aware of their liability for a violation of the

whistleblowers' protection requirements laid down in the Whistleblower Protection Law and/or other legislation, shall be obliged to sign a confidentiality statement (Annex 2) and shall be obliged to refrain from disclosing such information or data to third parties.

16. Employees of the Company working under employment contracts who, by the scope of their duties, become aware of the personal data of the person who has provided information about the breach, or the content of such information, shall be obliged to ensure the confidentiality of the aforesaid information and personal data, both during and after their work.

#### **ASSESSMENT OF INFORMATION ON BREACHES AND DECISION MAKING**

17. Upon the receipt of information about the breach through the Internal Channels, the Competent Entity shall immediately assess that information and make one of the following decisions:

- 17.1. To analyse the information provided about the breach;

- 17.2. To terminate the procedure for dealing with the information received about the breach, if:

- 17.2.1. the assessment reveals that the information provided does not comply with the Whistleblower Protection Law;

- 17.2.2. the information about the breach is based on information that is clearly untrue;

- 17.2.3. the information about the breach has already been dealt with, or is currently being dealt with.

- 17.3. If the information received about the breach gives reasonable grounds to believe that a criminal offence, administrative offence or another infringement is about to be committed, is being committed or has been committed, the Competent Entity shall forward the information received about the possible breach to the authority authorised to investigate such information without the consent of the person who has provided the information about the breach, and shall inform the person concerned thereof within a period of two working days from the date of receipt of the information.

18. The Competent Entity shall, within ten working days from the receipt of information about the breach, inform the person who submitted the information on the breach in writing of the decision it has reached on the processing of that information. In cases where a decision is made not to investigate a breach, the reasons for that decision must be stated.

19. The Competent Entity shall, without delay, after completing the investigation of the information relating to the breach, inform the person who submitted the information relating to the breach in writing of the final decision he/she has reached, the outcome of the investigation and the actions taken or planned to be taken, and shall indicate the procedure for appealing against the decision that has been reached. If, in the course of the investigation of a breach, the fact of a breach has been established, the Competent

Entity shall inform the person who provided the information on the breach of the liability to be imposed on the persons who committed the breach.

20. If the person who has provided information about the breach has not received a response, or if the Company has not taken action in response to the information that was provided, he/she shall have the right, pursuant to Article 4(3)(4) of the Whistleblower Protection Law, to apply directly to the competent authority – the Prosecutor General of the Republic of Lithuania – and to submit a report on the breach.

## **21. FINAL PROVISIONS**

22. The Competent Entity shall provide advice to the Company's employees on the implementation of the Whistleblower Protection Law, as well as on the protection requirements, possible or actual adverse effects related to the fact of providing information about a breach, measures and remedies, shall assist in the implementation and functioning of the Internal Channels of the Company, and shall sign the confidentiality statement provided in the Annex to the present Rules.
23. The Competent Entity shall summarise the data on the receipt, investigation and processing of information on breaches on an annual basis, and shall provide to the Chief Executive Officer of the Company information on the number of cases where information on breaches has been submitted and the results of their assessment, and summarised information on the breaches that have been disclosed, on the basis of the information provided by persons in accordance with these Rules.
24. The Competent Entity shall be responsible for overseeing and monitoring the compliance with these Rules and for periodically reviewing the Rules at least once a year. The Competent Entity shall initiate amendments to the Rules, as necessary.

## Notification of a Breach

### NOTIFICATION OF A BREACH

\_\_\_\_\_, 20\_\_

Details of the person reporting the breach	
Name	
Personal identification code	
Workplace (existing or former employment or contractual relationship with the company)	
Position	
Telephone number (comments on the means of communication)	
Personal email or residential address	
Information about the breach	
1. What is the breach you are reporting? What kind of breach is it?	
1. Who has committed this breach? What could have been the person's motives behind committing the breach?	
2. Place and time of the breach.	
Details of the person or persons committing the breach	
Name	
Workplace	
Position	
3. Are there any other persons who were, or who 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	
Position	
Workplace	

Tel.	
E-mail	
5. When was the breach committed, and when did you become aware of it or notice it?	
6. What evidence could you provide to support an investigation of the breach? Please provide any accompanying written or other evidence of the breach.	
7. Have you already reported this breach to anyone? If you have reported it, who was notified and did you receive a reply? If you have received a reply, please state the essential elements.	
8. Additional notes and comments.	

I confirm that I am aware of the legal consequences of providing false information and that the information I hereby have provided herein is correct.

Date	Signature
------	-----------