

# POLICY FOR REPORTING SERIOUS IRREGULARITIES

## 1 Purpose

Gruvaktiebolaget Viscaria (“**Viscaria**”) is committed to conducting its business in a responsible and transparent manner. The aim is to detect and prevent any misconduct within the business at an early stage.

Viscaria's internal reporting channel (the “**Reporting Channel**”) is an important part of this work. This policy (the “**Policy**”) provides information on how to report serious irregularities and the terms and conditions of the Reporting Channel, including, for example, who can report and what can be reported.

The Reporting Channel is not a whistleblowing channel under the Swedish Act on the Protection of Persons Reporting Irregularities (Sw. *lag (2021:890) om skydd för personer som rapporterar om missförhållanden*) (the “**Whistleblowing Act**”). The absence of a whistleblowing channel is due to the fact that Viscaria, with reference to the number of employees, is not subject to the obligation to have a whistleblowing channel under the Whistleblowing Act. This means that the possibilities for processing personal data are significantly more limited and that the Reporting Channel should only be used for the types of reports specified in Section 3 of the Policy.

If you wish to report information that is not covered by the Policy, please refer to Section 8 below.

## 2 Who can report?

The Reporting Channel is available to employees of Viscaria.

## 3 What can be reported?

The Reporting Channel should only be used to report serious irregularities. Serious irregularities refer to information that is necessary to investigate whether persons in key or leading positions within Viscaria are involved in acts relating to:

- > accounting or internal accounting control;
- > auditing;
- > corruption or bribery;
- > crime in the banking and financial sector; or
- > other serious irregularities relating to the organisation's vital interests or the life and health of individuals.

Issues that solely concern your own employment relationship – such as feedback on remuneration, leadership or similar issues – should therefore not be reported via the Reporting Channel. Such issues should instead be handled via your immediate manager or Viscaria's standard HR procedures.

## 4 How do you report?

The following are designated to receive reports in the Reporting Channel (the “Recipient”):

- > Lantero AB
- > Reporting to Viscaria's trusted group

Reports may be submitted in the following ways:

- > In writing via Lantero's reporting service, <https://wb.lantero.se/gruvaktiebolagetviscaria> (also available via QR code). The service is encrypted and login-protected. Lantero receives, registers, makes an initial assessment of, and forwards matters to the trusted group within Viscaria, or alternatively to an external investigator if needed.
- > For additional information about reporting, visit <https://lantero.se/whistleblowing/whistleblower>

## 5 **Can reports be made anonymously?**

Reports via Lantero can be made completely anonymously. However, to facilitate the investigation and handling of reports received, it is helpful if the Recipient can contact you to request further information. Viscaria therefore encourages you to provide your name and contact details when making a report. If the report is made anonymously, it is important that you follow up the case yourself in Lantero and check whether the Recipient has requested additional information.

## 6 **What happens to a report that has been submitted?**

Reports received will be investigated thoroughly and carefully. The Recipient may contact you for further information. If reporting is done via Lantero, it is therefore important that you save the ID and password protection you are assigned.

Reports received are treated confidentially and the information is only shared internally or externally to the extent necessary to conduct an investigation and remedy the deficiencies identified in the report.

If a report submitted to the Reporting Channel concerns an issue that is not covered by the Policy, Viscaria may delete the information and, if applicable, refer you to another function.

## 7 **External reports**

You have the right to report externally to authorities designated to receive and follow up on reports through established reporting channels. Reports should be submitted to the authority responsible for the relevant area. You can find the respective authority and its area of responsibility on the Swedish Work Environment Authority's website ([www.av.se](http://www.av.se)).

Reports can also be submitted directly to any of the EU institutions, bodies and agencies that have established external reporting channels and procedures for receiving reports of misconduct.

## 8 **Other channels**

Below is information about other available reporting channels within Viscaria and its affiliated companies, as well as references to where you can find information about the types of issues each channel is intended for.

- > **Viscaria Kiruna AB:** Viscaria Kiruna AB has established a whistleblowing channel in accordance with the Whistleblowing Act. Matters relating to Viscaria Kiruna AB and covered by the Whistleblowing Act must be reported via the whistleblowing channel for you to be covered by the protection provided by said act. Information about which matters qualify as whistleblowing matters, and should therefore be reported via Viscaria Kiruna AB's whistleblowing channel, is available on the Viscaria Group's website.

- > **Feedback channel:** Viscaria and its affiliated companies have established a feedback channel where anyone who comes into contact with the Viscaria Group's operations can submit observations, suggestions for improvement and other feedback. If a matter is not covered by the Policy or by Viscaria Kiruna AB's whistleblowing policy, you are welcome to use the feedback channel, which is available on the Viscaria Group's website.

If a matter submitted to the Reporting Channel concerns an issue that should be handled through one of the channels mentioned above, Viscaria may delete the information and instead refer you to the correct recipient.

## **Appendix 1 – Personal data processing**

Viscaria is the data controller for the processing of personal data in connection with the reporting and handling of cases under the Policy.

**Please note:** The processing of sensitive personal data (e.g. health data) and data relating to criminal offences (e.g. criminal charges) in a voluntary channel is severely restricted by law. The Reporting Channel is a voluntary channel, i.e. a channel that Viscaria is not obliged to establish under the Whistleblowing Act. In practice, this means that information about criminal offences often cannot be handled in the Reporting Channel, and that Viscaria may need to delete such information. As further explained in Section 8 of the Policy, Viscaria Kiruna AB has established a whistleblowing channel in accordance with the Whistleblowing Act. Cases relating to Viscaria Kiruna AB and which fall within the scope of the Whistleblowing Act are therefore referred to the aforementioned whistleblowing channel.

### **1.1 Personal data processed**

During the handling of cases under the Policy, the following categories of personal data may be processed:

- > identity and contact details of the reporting person (if provided) and information about employment or other working relationship;
- > information contained in the report, including information about the persons concerned or other third parties; and
- > other information revealed in the context of a case or in connection with subsequent measures.

Personal data is primarily collected from the reporting person, but may also originate from other persons involved in the matter, from internal investigations, or from authorities and other external sources.

### **1.2 Purpose and legal basis**

Personal data is mainly processed for the following purposes:

- > receiving, documenting, and following up on reports of misconduct;
- > if deemed appropriate, confirming receipt of the report and providing information on its status; and
- > if necessary, investigating the allegations made and taking the necessary measures.

Viscaria has a legitimate interest in maintaining a safe working environment and transparent operations. By receiving and handling reports of serious irregularities, Viscaria can identify risks, prevent irregularities and take necessary measures.

In exceptional cases, sensitive personal data may need to be processed, but only if necessary to fulfil Viscaria's obligations under employment law or to handle legal claims. The processing of data relating to criminal offences is strictly limited within the framework of the Reporting Channel and may only be carried out for persons in key or leading positions when necessary to investigate serious irregularities relating to accounting, internal accounting controls, auditing, bribery, crimes within the banking and financial sector, or other serious irregularities that may affect the vital interests of the organisation or the life and health of individuals.

### **1.3 Recipients of personal data**

Access to personal data is limited to specially designated persons or entities responsible for receiving and following up on reports in accordance with the Policy. Viscaria also uses an external supplier to administer the reporting channel on behalf of the company.

If necessary to investigate a report, certain information may be shared with others within Viscaria, such as HR or managers, but only to the extent that it is absolutely necessary. Once the case has been closed, information may be shared within Viscaria or with external recipients (e.g. legal representatives or authorities) if Viscaria is required to do so by law or if such sharing is necessary to handle legal claims. Where possible, the information is anonymised or restricted to protect the identity of the persons concerned.

### **1.4 Retention period**

Personal data is stored for as long as the case is active and for up to two years after the follow-up and necessary measures have been completed, unless a longer storage period is required to fulfil Viscaria's legal obligations or to handle legal claims.

### **1.5 Transfers outside the EU/EEA**

If personal data needs to be transferred to countries outside the EU/EEA (third countries), Viscaria ensures that the transfer is carried out in accordance with applicable data protection legislation. Protection may be based on the European Commission's adequacy decision or on other legal grounds, such as standard contractual clauses, supplemented by appropriate technical and organisational security measures.

### **1.6 Your rights**

Under applicable data protection legislation, you have the right to:

- > obtain confirmation as to whether Viscaria is processing personal data about you, and if so, to access it in the manner set out in applicable data protection legislation;
- > request that Viscaria correct inaccurate personal data about you;
- > request that Viscaria erase your personal data if there are no legal grounds for continuing the processing;
- > request that Viscaria restrict or cease the processing of your personal data, provided that there are no legal grounds for continuing the processing;
- > request to receive the personal data concerning you, which you have provided to Viscaria, in a structured, commonly used, machine-readable format (portability); and
- > withdraw your consent.

Please note that the above rights may be subject to certain restrictions. For example, a request for erasure may be refused if Viscaria is required by law to continue processing the personal data, or if we need to retain the data to handle legal claims. Access to personal data may also be restricted if it is deemed necessary to protect the identity of the reporting person or other individuals involved in a whistleblowing matter.

In order to confirm that the correct person is submitting a request for action as described above, Viscaria may perform an identity check.

You also have the right to submit a complaint to the Swedish Authority for Privacy Protection, [www.imy.se](http://www.imy.se), regarding Viscaria's personal data processing. On the authority's website, you can also find detailed information about your rights under applicable data protection legislation.

**1.7**

### **Contact details**

Questions about the processing of personal data in cases handled under the Policy or requests to exercise rights can be directed to:

Email: [info@viscaria.com](mailto:info@viscaria.com)