GRÄNGES

Whistleblower function

Information and rules

Version: 1.1

Datum: December 12, 2018

TABLE OF CONTENTS

INTRODUCTION

For us it is essential that information about irregularities comes to light. We have therefore implemented a Whistleblower function as a complement to our open corporate climate in order to detect irregularities that may seriously harm our business or our employees.

The purpose of the system is to provide a channel where events or circumstances can be reported without the whistleblower having to fear retaliation. It is our hope that any irregularities can quickly be uncovered and remedied before the underlying causes grow and become unmanageable.

This document describes how Gränges' Whistleblower function works in practice.

AIM

Gränges' Whistleblower function aims to ensure:

- That employees and other stakeholders inform Gränges of serious improprieties within the group.
- That information submitted is handled correctly in line with applicable legislation and regulation.
- That each person who informs Gränges in good faith is protected from retaliation.

WHAT CAN BE REPORTED?

In practice, the Whistleblower function can be used to report all types of irregularities. However, we recommend that you as an employee at Gränges report concerns about individuals who are not in senior management positions directly to local management, a relevant functional group in your region or at Gränges HQ, such as Legal, HR or Finance, or the General Counsel, in line with the reporting channels described in Gränges' Code of Conduct. It is important to emphasize that the Whistleblower function can always be used by Gränges' employees.

The Swedish Data Protection Authority and General Data Protection Regulation (GDPR) regulate which people and what type of information can be **stored and processed** via a system such as this. Sometimes the information that is provided via the system can contain sensitive personal data, including when the person who is suspected of an irregularity is mentioned by name. Personal data may therefore only be stored when very strong reasons exist.

In line with the recommendation from the Data Protection Authority, Gränges is only allowed to **store and process** serious irregularities that concern people in senior management positions, e.g.:

- Executives (all levels)
- Management group
- Board members

- Other key personnel

Only information which is objectively justifiable is stored and processed, i.e. when its purpose is to investigate whether the person in question has been involved in serious irregularities. Examples of serious irregularities include:

- Financial crimes such as passive and active bribery, theft, fraud and forgery, accounting fraud and other violations of accounting and tax law.
- A conflict of interest between an employee and Gränges.
- Other serious irregularities that affect the company's vital interests or the lives and health of individuals, include serious environmental crimes, major safety deficiencies at the workplace and very serious forms of discrimination or harassment.

The above-mentioned are just some examples of irregularities. If you are unsure about whether to report a problem, we recommend that you report it. If your matter cannot be processed within the system you will – provided you have given your contact details – receive information about this and advice about whom to contact.

WHO CAN REPORT?

Anyone who suspects circumstances that conflict with the law, regulations, policies or guidelines and which seriously concern the company or its employees can make a report.

The reporting routine can be used by employees (irrespective of employment form) at all Gränges' companies. Customers, suppliers, partners and other stakeholders can also use the system.

HOW DO I MAKE A REPORT?

1. Report anonymously through the reporting tool via URL wb.2secure.se and fill in the company code **lcr629**.
2. Write a letter and send to 2Secure, P.O Box 140, SE-221 00 Lund, Sweden.
3. Call +46 771 779 977 or 800 4455223 for US employees at any time (24/7-availability).

HOW DO I REPORT OTHER CONCERNS?

If you are an employee and want to report other concerns or irregularities, you can reach out to your manager or your manager's manager, a relevant functional group such as Legal, HR or Finance in your region or at Gränges HQ, or the General Counsel. Such concerns or irregularities could be (but are not limited to):

- Disputes, errors, complaints
- Dissatisfaction with pay
- Less serious examples of harassment
- Minor theft
- Suspected crimes committed by people in non-executive positions.

THE REPORTING SYSTEM

To ensure the whistleblower's anonymity, we provide a reporting tool from an external and independent company. The reporting channel is encrypted and password protected. You never have to reveal your identity if you do not wish to. Using the system is also completely voluntary.

- You do not need evidence for your suspicions, but no accusations may be made with malicious intent or with the knowledge that the accusation is false.
- It is important that you describe all the facts of the matter, including the circumstances that you think may not be important.
- Please explain the reasons for your report as clearly as possible and attach all materials that may be relevant.

To make your report, copy this address wb.2secure.se and fill in the company code: **lcr629** to log on at the whistleblowing page.

WHO RECEIVES YOUR REPORT?

In whistleblower matters, Gränges cooperates with 2Secure which is an external and independent company. All reports are received and handled by 2Secure. They have long experience of investigations and global capacity if it is needed.

2Secure works in consultation with *Gränges Ethics Committee*. No details on the whistleblower will be disclosed unless you as the whistleblower have provided your consent. You can choose either to be totally anonymous to 2Secure's investigators or tell them who you are. Regardless, all reports are investigated and processed.

FEEDBACK

Within two weeks after making your report you can log on again with your login and password to see any follow-up questions/comments from the investigators that have received your report. You can monitor your matter via wb.2secure.se if you have noted the code that you receive when you register your report. You should log on regularly as the investigators may need to ask you supplementary questions, and in certain cases, to act as quickly as possible.

HOW YOUR PERSONAL DATA IS HANDLED (SWEDISH DATA PROTECTION ACT AND GENERAL DATA PROTECTION REGULATION)

You can be totally anonymous when using the Whistleblower function. Gränges takes great consideration of the protection of personal privacy. Below we have listed some key points about the Data Protection Act and the GDPR that can be useful for you to know.

Personal data

In all cases, Gränges is obligated to comply with the law regarding the processing of personal data. It is essential that anyone who provides information via the Whistleblower function feels secure about doing so.

Anonymity

As whistleblower you choose either to provide your contact details or remain anonymous. All reports are taken seriously and investigated regardless. It facilitates for the continued work of our external investigators if we can contact you to obtain supplementary information. Your contact details will therefore be requested. But providing these details is completely voluntary.

No IP addresses are registered and the system does not use cookies. If you are using a computer that is connected to Gränges, however, it may be stated on the Internet log that you have visited the website when you made your report. If you do not wish this information to be visible, you should use a computer which is not connected to Gränges' network.

All data communication and storage of personal data is encrypted to prevent it being distorted or becoming known to unauthorised persons.

Personal data control

Gränges AB and its respective subsidiaries where the person who is reported for an irregularity is employed is responsible for processing personal data in accordance with the law. Gränges is thereby the data controller for all personal data processed in the Whistleblower service.

The purpose of registering personal data

Personal data will only be used for investigation within the Whistleblower function. In the section WHAT CAN BE REPORTED (page 3) you can read about under which circumstances reports and information can be stored and processed through the system. As an employee you do not have to assess and judge whether the Whistleblower function should be used. It is up to the Whistleblower function and the Ethics Committee to judge which employees and/or representatives can be reported via this system. You can also read about which types of irregularities can be stored and processed.

If you report someone who does not belong to the appropriate category or if the irregularity is not serious enough to be handled within the Whistleblower function, the matter will be closed and all personal data will be erased. If you, in this context, have chosen to reveal your identity, you will receive a message when this assessment has been made, including information about where you can turn instead.

Who has access to the personal data?

Personal data will only be used by *Gränges Ethics Committee* and by the independent external company that has assigned to handle the report. The data is only accessible to the

people who work on the investigation in question. In certain cases, an independent IT consultant can be engaged for forensic investigations. The investigation may be handed over to the police or other authority such as the Swedish Economic Crime Authority.

What personal data is registered?

Initially, the data that you provide as whistleblower is registered. If there is an investigation, the information that is needed to investigate suspected irregularities will be registered, which primarily includes name, position, suspected irregularity and the circumstances on which the report is based. Information will then be obtained from sources that are deemed necessary for investigating the irregularity.

For how long may personal data be kept?

Personal data is erased automatically three weeks after the matter regarding the reported irregularity was closed.

Information to the reported party

A person who is reported in the Whistleblower function will receive special information. If there is a risk that this may jeopardise the continued investigation, the information will not be provided until it is no longer deemed to be a risk. In addition, no extracts from registers are provided during this period.

Extracts from registers

As a whistleblower you have the right to receive, free of charge, information about the personal data on you that is registered in the Whistleblower service. Such a request for an extract from a register shall be made in writing and be signed. Please send it to 2Secure, Dataskyddsombud, Box 34037, SE-100 26 Stockholm, Sweden.

If any of the details are incorrect, incomplete or misleading you have the right to request that they be corrected. An extract from a register sent to a reported person who is in a key personnel/senior position will not contain any information identifying you as the whistleblower. The information may therefore be provided in summarized form.