# ANNEX TO THE TELL-GREINER.COM POLICY / POLICY FOR THE GREINER WHISTLEBLOWER SYSTEM IN SWEDEN

Greiner implements a whistleblower system, which is a voluntary, web-based reporting system of infringements of the Code of Conduct by Greiner employees.

In order to ensure adequate safeguards and compliance with European and Swedish data protection law, Greiner guarantees the following:

## 1. Purposes and scope of the data processing, limitations:

The Greiner whistleblower system, with its objective of identification and investigation of infringements of the Greiner Code of Conduct, is limited to key personnel and persons with leading positions within the company. So processing of personal data concerning legal offences may only refer to persons in key positions or leading positions within the company. As to persons who are neither key personnel or in leading positions, personal data concerning legal offences regarding them may not be processed by Greiner whistleblower system.

For clarification: internal information and reporting channels must be used unless it is objectively justified not to do so – in such cases, whistle blowing system can be used instead of the company's internal information and reporting channels in order to investigate whether the person in question has been involved in serious improprieties. This can for instance be the case if the reported person is part of the management and the suspected improprieties for that reason otherwise run the risk of not being properly handled. So the whistle blowing system shall constitute a complement to normal internal administration and is voluntary to use.

The Greiner whistleblower system, with its objective of identification and investigation of infringements of the Greiner Code of Conduct, is also limited to serious improprieties.

The serious improprieties must be concerning:

- accounting, internal accounting controls, auditing matters, fight against bribery, banking- and financial crime; or
- other serious improprieties concerning the company's or the group's vital interests or the life or health of individual persons, as for instance serious environmental crimes, major deficiencies as regards the security at the place of work and very serious forms of discrimination or harassments.

## 2. Deletion of personal data

As personal data should be deleted immediately when it is no longer necessary for the purpose for which it was collected, it is ensured that unnecessary personal data is not retained for as long as two months (unless of course it is indeed necessary, for instance in order to defend claim in court etc.).

The data subject has the right to request an excerpt of the register to check which information, if any, that is registered about him or her. In such cases, the identity of the person requesting information has to be ensured, so that data is not given to a person other than the data subject.

At the request of the data subject, personal data that is incorrect, incomplete or misleading has to be rectified.

The data subject reported receives certain information when their data is processed – however, not the identity of the whistle-blower. The giving of this information to the data subject can however be postponed until it does no longer impede the investigation.

A report that is found to be ungrounded shall be deleted immediately.

## 3. Information of data subjects

As there is the obligation to provide information to employees or other persons whose data may be processed, the data subject (reported employee) shall be informed if their personal data is processed (The information giving may however be postponed until it would no longer would impede the investigation.)

## 4. Information that the whistleblower should receive

In general, the whistle blower is not informed about what happens next after his/her report or the outcome as a result of his/her report. The whistle blower should not receive such information, as such information is personal data about the reported person and can contain very sensitive personal data such as allegations of misconduct or even legal offences.

If the whistle blower has an objective interest of receiving an update, for instance if the report regards an assault of the whistle blower committed by the reported person, then that could be an exception, justifying some information regarding the process relevant to the whistle blower being given.

## 5. Treatment of the identity of the whistleblower:

Greiner allows but does not foster anonymous reports, however, it ensures to the reporter full confidentiality concerning their identity, if it is disclosed.

Anonymous reports are only investigated if:

- the seriousness of the reported facts is established and factual elements are sufficiently detailed and
- the anonymous report is considered appropriate by the General Council and Compliance Officer within the framework of the Greiner Code of Conduct and this policy.

## 6. Categories of personal data recorded:

Only the following categories of data are processed through the intended whistleblower system:

- The identity, position and contact details of the whistleblower;
- The identity, position and contact details of the incriminated person;
- The identity, position and contact details of the persons receiving or investigating the reports;
- The facts reported;

- The evidence gathered in the course of the investigation;
- The report of the investigation;
- The outcome of the report.

## 7. Data transfer and recipients:

The Greiner whistleblower system is operated by Greiner AG in Austria. In this regard the Greiner entity has entered into an agreement with Greiner AG stipulating the handling of data reported via the whistleblower system prior to any transfer of personal data to the responsible department within the group. This written agreement obliges Greiner AG, as operator of the whistleblower system, to only transfer reports including accusations according to point 1. above to the responsible department within the group. Moreover, Greiner AG is obliged to delete the content of reports immediately after said reports were transmitted to the responsible department within the group.

The department handling the reports, the General Council and Compliance Officer, is strictly separated from any other group departments; all of its staff are particularly trained persons and explicitly responsible for the confidentiality of reported data.

The General Council and Compliance Officer in general processes all reports filed by whistleblowers on behalf of the Greiner entity and transfers reasonable reports to the responsible department at the Greiner entity.

In case, that the reported infringement concerns senior executives or its significance extends across several regions, thus, if it impacts the entire or large parts of Greiner, the report may be provided to the responsible department at mother company of Greiner, Greiner AG in Austria but only to the extent that these data are necessary for fulfilling their duties.

## 8. Data transfers outside the EU:

Greiner further guarantees that personal data processed through the Greiner whistleblower system is not transferred outside the EU.

## 9. Data retention periods:

Reported data will be deleted two months after termination of the investigation, at the latest.

## 10. Security measures:

The data controller has implemented appropriate security measures to protect the personal data against accidental, unlawful or unauthorized destruction, loss, alteration, access, disclosure or use, both (i) when the data are collected and (ii) when they are shared or stored. In particular the data can only be accessed via individual login and password, which are regularly modified or by any other authentication means. Details of access are further recorded and the regularity of such access is verified.

## 11. Information to be provided to potential whistleblowers:

Employees are notified about the following information by the "tell-greiner.com policy / policy for the Greiner whistleblower system":

- the identity of the data controller;
- the purposes of the Greiner whistleblower system and the matters which may be reported through it;
- the fact that the use of the Greiner whistleblower system is optional;
- the absence of consequences for employees if they do not use the scheme;
- the recipients of the reports;
- the existence for any person identified in the report of a right of access and rectification of his/her personal data and how he/she can exercise these rights; and
- the fact that whistleblowers may be subject to disciplinary and judicial action if they do not make a report in good faith but that they will not be disciplined or retaliated against in any way for making a report in good faith.

## 12. Information to be provided to the incriminated person:

In addition to the information as set out in point 12 above, the accused person will be informed of the following as soon as his/her data are recorded:

- the identity of the data controller;
- the allegations against that person;
- the recipients of the report;
- his/her rights of access and rectification of his/her personal data and how these rights can be exercised.

If necessary to take provisional measures, in particular to prevent the destruction of evidence, the above information may be provided to the incriminated person after such measures are adopted.

## 13. Respect for the rights of access and rectification:

The data controller has ensured that any persons identified in the reports can exercise their right of access, amend, cancel or oppose disclosure to their personal data and their right of rectification/erasure of their personal data by contacting the responsible department under data.protection@greiner.com.

Greiner also guarantees that the accused person will not obtain the identity of the whistleblower when exercising his /her right of access. In this regard, the identity of the whistleblower will not be disclosed to the incriminated person when exercising his/her right to access.

## 14. Information about data controller

The data controller is the employer, e.g., Vigmed Holding AB, Garnisonsgatan 10 / Kungsgatan 6, 254 66 Helsingborg, T: +46 42 280090, F: +46 42 6005333, info@vigmed.com , www.vigmed.com