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

Greiner intends to implement 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 Netherlands data protection law, Greiner guarantees the following:

1. Purposes and scope of the data processing:

The Greiner whistleblower system, with its objective of identification and investigation of infringements of the Greiner Code of Conduct, is limited to reports in the following areas:

- Fraud/misconduct accounting/invoice control
- Non-compliance with laws
- Human rights violation
- Breach of employment law regulations
- Discrimination
- Anticompetitive practices
- Bribery/corruption
- Breach of property rights
- Breach of environmental regulations
- Breach by the General Compliance Officer of Greiner in the above-mentioned areas

2. Treatment of the identity of the whistleblower:

Greiner allows but does not foster anonymous reports, however, it ensures to the reporters 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 mandatory guidelines.

3. 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 investigationThe report of the investigation; and
- The outcome of the report.

4. 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.

5. Data transfers outside the EU:

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

6. Data retention periods:

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

7. 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.

8. Information to be provided to potential whistleblowers:

Employees of the Greiner entity 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.

9. Information to be provided to the incriminated person:

In addition to the information as set out in point 8 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.

10. 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 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.

11. Information about data controller

The data controller is the employer in the Netherlands:

Greiner Bio-One B.V., Albert-Einstein-Weg 16, 2408 AR Alphen a/d Rijn, T: +31 172 420 900, F: +31 172 443 801, info@nl.gbo.com , www.gbo.com

Greiner Packaging B.V., Gildenveld 12a, 3892 DG Zeewolde, T: +31 36 5236160, F: +31 36 5236161, office.zeewolde@greiner-gpi.com , www.greiner-gpi.com