- English Version
- French Version

ANNEXE AUX DIRECTIVES OBLIGATOIRES DU SYSTÈME D'ALERTE PROFESSIONNELLE DU GREINER GROUP LE SYSTÈME D'ALERTE PROFESSIONNELLE GREINER

Le Greiner Group souhaite mettre en œuvre un système d'alerte professionnelle - un système de déclaration Web sur une base volontaire des infractions au Code de conduite (joint) par les employés du Greiner Group.

Afin d'assurer les protections adéquates et la conformité avec les législations européenne et française en matière de protection des données, le Greiner Group garantit, conformément à l'« autorisation unique N° AU-004 » de la Commission Nationale de l'Informatique et des Libertés du 8 décembre 2005, telle qu'amendée en janvier 2014, les points suivants :

1. Objets et portée du traitement des données :

Le système d'alerte professionnelle du Greiner Group, afin d'identifier et d'enquêter sur les infractions au Code de conduite du Greiner Group, est limité aux déclarations dans les domaines suivants :

- Fraude /faute en comptabilité /contrôle de facture
- Défaut de conformité avec la législation
- Violation des droits de l'Homme
- Infraction au droit du travail
- Discrimination
- Pratiques anticoncurrentielles
- Pots-de-vin /corruption
- Infraction aux droits de propriété
- Infraction à la réglementation environnementale
- Infraction du Directeur général pour la conformité du Greiner Group dans les domaines susmentionnés

2. Traitement de l'identité du lanceur d'alerte :

Le Greiner Group accepte, sans les recommander, les déclarations anonymes. Toutefois, le groupe assure aux déclarants la confidentialité totale de leur identité s'ils la divulguent.

Les déclarations anonymes font l'objet d'une enquête uniquement dans les cas suivants :

- la gravité des faits déclarés est établie et les éléments factuels sont suffisamment détaillés ; et
- la déclaration anonyme est considérée appropriée par le Directeur juridique et le Directeur pour la conformité selon le cadre de travail du Code de conduite de Greiner et ces directives obligatoires.

3. Catégories de données personnelles consignées :

Seules les catégories suivantes de données sont traitées via le système d'alerte professionnelle prévu :

- Identité, poste et coordonnées du lanceur d'alerte

- Identité, poste et coordonnées de la personne incriminée ;
- Identité, poste et coordonnées des personnes recevant ou enquêtant sur les déclarations ;
- Faits déclarés ;
- Preuves recueillies dans le cadre de l'enquête ;Rapport d'enquête ; et
- Résultat de la déclaration.

3. Transfert de données et destinataires :

Le système d'alerte professionnelle du Greiner Group est confié à Greiner AG en Autriche. À cet égard, l'entité Greiner a conclu un accord avec Greiner AG stipulant le traitement des données déclarées via le système d'alerte professionnelle avant tout transfert de données personnelles au service responsable au sein du groupe. Cet accord écrit oblige Greiner AG, exploitant du système d'alerte professionnelle, à transférer uniquement des déclarations incluant des accusations conformes au point 1 précédent au service responsable au sein du groupe. De plus, Greiner AG est tenu d'effacer le contenu des déclarations immédiatement après leur transmission au service responsable au sein du groupe.

Le service gérant les déclarations, le Directeur juridique et le Directeur pour la conformité sont strictement séparés de tout autre service du groupe. L'ensemble de leur personnel est constitué de personnes spécifiquement formées et est explicitement responsable de la confidentialité des données déclarées.

En règle générale, le Directeur juridique et le Directeur pour la conformité traite toutes les déclarations renseignées par les lanceurs d'alerte au nom de l'entité Greiner et transfèrent les déclarations raisonnables au service responsable de l'entité Greiner.

Si l'infraction déclarée concerne des dirigeants ou si sa portée couvre plusieurs régions et affecte donc l'intégralité, ou une grande part, du Greiner Group, la déclaration peut être communiquée au service responsable à la société-mère du Greiner Group, Greiner AG en Autriche, mais uniquement dans la mesure où ces données sont nécessaires pour l'accomplissement de ses devoirs.

4. Transferts de données hors de l'UE :

Le Greiner Group garantit en outre que les données personnelles traitées via le système d'alerte professionnelle de Greiner ne seront pas transférées hors de l'UE.

5. Périodes de conservation des données :

Les données déclarées sont effacées deux mois après la finalisation de l'enquête, au plus tard.

6. Mesures de sécurité :

Le contrôleur des données a mis en œuvre des mesures de sécurité appropriées afin de protéger les données personnelles contre toute destruction, perte, altération, accès, divulgation ou usage accidentel, illégal ou dépourvu d'autorisation aussi bien (i) lorsque les données sont recueillies que (ii) lorsqu'elles sont partagées ou stockées. En particulier, les données sont uniquement accessibles grâce à un identifiant et un mot de passe individuels, régulièrement modifiés, ou par tout autre moyen d'authentification. Les détails des accès sont en outre consignés et la régularité de ces accès est vérifiée

7. Informations à fournir aux lanceurs d'alerte potentiels :

Via « tell-greiner.com policy / Politique pour le système d'alerte professionnelle du Greiner Group », les employés de l'entité Greiner sont notifiés des informations suivantes :

- identité du contrôleur des données ;
- objets du système d'alerte professionnelle du Greiner Group et aspects qu'il permet de déclarer ;
- caractère optionnel de l'usage du système d'alerte professionnelle du Greiner Group ;
- absence de conséquences pour les employés s'ils n'emploient pas le système ;
- destinataires des déclarations ;
- existence pour toute personne identifiée dans la déclaration de droits d'accès et de rectification de ses données personnelles et mode d'exercice de ces droits ; et
- possibilité pour les lanceurs d'alerte d'être les sujets d'actions disciplinaires et de poursuites légales en cas de déclaration de mauvaise foi mais absence d'action disciplinaire et de représailles à leur encontre, de quelque manière que ce soit, en cas de déclaration de bonne foi.

8. Informations à fournir à la personne incriminée :

Outre les informations énoncées au point 8 précédent, la personne accusée est informée des éléments suivants dès que ses données sont consignées :

- identité du contrôleur des données ;
- allégations à l'encontre de cette personne ;
- destinataires de la déclaration ;
- son droit d'accès et de rectification de ses données personnelles et mode d'exercice de ces droits

Si des mesures conservatoires s'imposent, en particulier pour empêcher la destruction de preuves, les informations précédentes peuvent n'être fournies à la personne incriminée qu'après l'adoption de ces mesures.

9. Respect des droits d'accès et de rectification :

Le contrôleur des données s'est assuré que quiconque identifié dans les déclarations peut exercer son droit d'accès à ses données personnelles et son droit de rectification /suppression de ses données personnelles en contactant le responsable du service à data.protection@greiner.com. Le Greiner Group garantit également que la personne accusée n'obtiendra pas l'identité du lanceur d'alerte en exerçant son droit d'accès.

11. Informations sur le contrôleur de date

Le responsable du traitement est l'employeur en France:

Greiner Bio-One France S.A.S., 3-7 Avenue du Cap Horn, Les Ulis - BP 31, 91941 Courtaboeuf,
T: +33 1 6986 2525, F: +33 1 6986 2535, office@fr.gbo.com , www.gbo.com

Greiner Extrusion S.A.S., 206 Chemin des Artisans, 74550 Perrignier, T: +33 450724791, F: +33 450724912
office(at)greinerextrusion.fr, www.greiner-extrusion-group.com

Greiner Packaging Distribution SARL, 3 Allée de l'économie, 67370 Wiwersheim, T: +33 3 88 51 49 78, office.wiwersheim@greiner-gpi.com, www.greiner-gpi.com

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

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 French data protection law, Greiner guarantees in accordance with the Commission Nationale de l'Informatique et des Libertes's "Single Authorization No. AU-004" of December 8, 2005, as amended in January 2014, 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 report

- The evidence gathered in the course of the investigation;
- The 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 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 Greiner entity and transfers reasonable reports to the responsible department at 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 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 date controller

The data controller is the employer in France:

Greiner Bio-One France S.A.S., 3-7 Avenue du Cap Horn, Les Ulis - BP 31, 91941 Courtaboeuf,
T: +33 1 6986 2525, F: +33 1 6986 2535, office@fr.gbo.com , www.gbo.com

Greiner Extrusion S.A.S., 206 Chemin des Artisans, 74550 Perrignier, T: +33 450724791, F: +33 450724912
office@greinerextrusion.fr , www.greiner-extrusion-group.com

Greiner Packaging Distribution SARL, 3 Allée de l'économie, 67370 Wiwersheim, T: +33 3 88 51 49 78, office.wiwersheim@greiner-gpi.com , www.greiner-gpi.com