- English Version
- Spanish Version

ANEXO A LA POLÍTICA DE TELL-GREINER.COM/POLÍTICA PARA EL SISTEMA DE DENUNCIAS DEL GRUPO GREINER EN ESPAÑA

El Grupo Greiner aplica un sistema de denuncias, que es un sistema basado en la web y voluntario de infracciones del Código de Conducta por parte de los empleados del Grupo Greiner.

Para garantizar las salvaguardias adecuadas y el cumplimiento de la ley de protección de datos española y europea, el Grupo Greiner garantiza:

1. Propósitos y ámbito del procesamiento de datos, limitaciones:

De acuerdo con la normativa española vigente, el sistema de denuncias del Grupo Greiner, con el objetivo de identificar e investigar las infracciones del Código de Conducta, no permite denuncias anónimas. De modo que las infracciones no se deben notificar de un modo anónimo por lo que las denuncias anónimas no se aceptan.

2. Supresión de los datos personales

Un dato personal debe suprimirse inmediatamente cuando ya no sea necesario para el objetivo para el que fue recopilado. Así se garantiza que los datos personales innecesarios no se conserven durante más de tres meses (a no ser que sea necesario, por ejemplo para defender una reclamación ante un tribunal, etc.).

El interesado/la interesada tiene el derecho de solicitar un extracto del registro para comprobar qué información de él/ella, si la hubiera, está registrada. En dichos casos, tiene que asegurarse la identidad de la persona que solicita la información, de modo que los datos no se proporcionen a otra persona diferente al interesado/a la interesada.

A petición del interesado/de la interesada, los datos personales que sean incorrectos, incompletos o engañosos tienen que rectificarse.

El interesado/la interesada investigado/-a recibe cierta información cuando sus datos se procesan, sin embargo, no recibe la identidad del/de la denunciante. Puede posponerse la presentación de esta información al interesado/a la interesada hasta que no obstaculice la investigación. Los informes infundados se eliminarán inmediatamente

3. Información de los interesados

Como existe la obligación de proporcionar información a los empleados o a otras personas

cuyos datos se vayan a procesar, el interesado/la interesada (empleado/-a investigado/-a) será informado si se procesan sus datos personales. (Puede posponerse la presentación de esta información al interesado/a la interesada hasta que no obstaculice la investigación).

El individuo investigado debe ser informado expresamente por el controlador/la controladora

de datos, tres (3) meses desde la fecha en la que se registraron, acerca del contenido del procesamiento, el origen de los datos, la existencia de un archivo de datos personales o que los datos se vayan a procesar, los propósitos del mismo y los receptores de la información, la existencia de derechos de acceso, la rectificación, la eliminación y la objeción y la identidad y dirección del controlador/de la controladora o, cuando proceda, su representante.

4. Información que debe recibir el/la denunciante

En general, el/la denunciante no recibe información acerca de lo que ocurre a continuación

después de presentar su denuncia o del resultado como consecuencia de la misma. El/la denunciante no debe recibir dicha información, ya que se trata de datos personales de la persona investigada y pueden ser muy confidenciales como denuncias por falta de conducta o incluso delitos legales.

Si el/la denunciante está interesado/-a en recibir una actualización, por ejemplo, si la denuncia trata una agresión del/de la denunciante cometida por la persona investigada, esta podría ser una excepción, justificando alguna información que trata el proceso correspondiente al/a la denunciante.

5. Categorías de datos personales registrados:

Solamente se procesan las siguientes categorías de datos en el sistema de denuncias previsto:

- La identidad, el puesto y los datos de contacto del/de la denunciante.
- La identidad, el puesto y los datos de contacto de la persona incriminada.
- La identidad, el puesto y los datos de contacto de las personas que reciban o investiguen los informes.
- Los hechos expuestos.
- Las pruebas recopiladas durante el curso de la investigación.
- El informe de la investigación.
- El resultado de la denuncia.

6. Transferencia de datos y destinatarios:

El sistema de denuncias del Grupo Greiner es operado por Greiner Holding AG en Austria.

A este respecto, la entidad Greiner ha firmado un contrato con Greiner Holding AG en el que se establece el tratamiento de datos investigados mediante el sistema de denuncias antes de realizar cualquier transferencia de datos al departamento competente del grupo. Este contrato escrito obliga a Greiner Holding AG, como operador del sistema de denuncias, a no solo transferir denuncias sino también documentos de acuerdo con el punto 1 anterior al departamento competente del grupo. Además, Greiner Holding AG está obligado a eliminar el contenido de las denuncias inmediatamente después de que dichos documentos se hayan transmitido al departamento competente del grupo.

El departamento que gestiona las denuncias, el Consejo General y el responsable del cumplimiento, están estrictamente separados de otros departamentos del grupo. Todo el personal está formado especialmente y son responsables explícitamente de la confidencialidad de los datos investigados.

El Consejo General y el responsable de cumplimiento en procesos generales realizan las denuncias mediante los denunciantes en nombre de la entidad Greiner y transfieren los documentos pertinentes al departamento competente de la entidad Greiner.

En el caso de que la infracción investigada implique a los altos ejecutivos o sus representantes en varias regiones, si afecta a todo el Grupo Greiner o una parte importante, la denuncia se presentará en el departamento competente de la compañía matriz del Grupo Greiner, Greiner Holding AG en Austria, pero solamente en la medida en que esos datos sean necesarios para el cumplimiento de sus obligaciones.

7. Transferencias de datos fuera de la UE:

El Grupo Greiner garantiza que los datos personales procesados mediante el sistema de denuncias de Greiner no se transfieren fuera de la UE.

8. Períodos de conservación de datos:

Los datos investigados se eliminarán tres meses después de la finalización de la investigación, a más tardar.

9. Medidas de seguridad:

El controlador/la controladora de datos ha aplicado las medidas de seguridad adecuadas para proteger los datos personales contra la destrucción, la pérdida, la alteración, el acceso, la divulgación o el uso accidental, ilegal o no autorizado (i) cuando se recopilen los datos y (ii) cuando se compartan o almacenen. En concreto, solo se puede acceder a los datos a través de un inicio de sesión y una contraseña individuales que se modifican con regularidad o mediante otros medios de autenticación. Los datos de acceso se registran posteriormente y se verifican con regularidad dichos accesos.

10. Información que se debe proporcionar a los posibles denunciantes:

Los empleados recibirán una notificación con la siguiente información mediante la "política tell-greiner.com / política para el sistema de denuncias del Grupo Greiner":

- La identidad del controlador/de la controladora de datos.
- Los objetivos del sistema de denuncias del Grupo Greiner y los asuntos que se investigarán
- con él.
- El hecho de que el uso del sistema de denuncias del Grupo Greiner es optativo.
- La ausencia de consecuencias para los empleados si no utilizan este sistema.
- Los destinatarios de las denuncias.
- La existencia de una persona identificada en la denuncia con derecho de acceso y rectificación
- de sus datos personales y cómo puede ejercer esos derechos.
- El hecho de que los denunciantes estarán sujetos a acciones disciplinarias y judiciales si no realizan una denuncian de buena fe pero que no serán castigados ni se tomarán represalias contra ellos de ningún modo por presentar una denuncia de buena fe.

11. Información que se debe proporcionar a la persona incriminada:

Además de la información establecida en el punto 12 anterior, la persona acusada recibirá la siguiente información tan pronto como se registren sus datos:

- La identidad del controlador/de la controladora de datos.
- Las denuncias contra esa persona.
- Los destinatarios de la denuncia.
- Los derechos de acceso y rectificación de sus datos personales y cómo se pueden ejercer dichos derechos.

Si es necesario tomar medidas provisionales, especialmente para evitar la destrucción de pruebas, la información anterior se proporcionará a la persona incriminada después de adoptar dichas medidas.

12. Respeto de los derechos de acceso y rectificación:

El controlador/la controladora de datos ha garantizado que las personas identificadas en las denuncias puedan ejercer sus derechos de acceso, enmienda, cancelación u oposición a la cancelación de sus datos personales y su derecho de rectificación/eliminación poniéndose en contacto con el departamento competente en data.protection@greiner.at

El Grupo Greiner también garantiza que la persona acusada no obtendrá la identidad del/de la denunciante cuando ejerza su derecho de acceso. A este respecto, la identidad del/de la denunciante no se revelará a la persona incriminada cuando ejerza su derecho de acceso.

13. Información acerca del controlador/de la controladora de datos

El controlador/la controladora de datos es el empleador/la empleadora:

Es decir, Vacuette España, S.A., Avenida Somosierra, 22 - 2a planta Nave G, 28703 San Sebastián de los Reyes, T: +34 91 652 77 07, F: +34 91 652 33 35, info@vacuette.es, www.vacuette.es

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

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 Spanish data protection law, Greiner guarantees the following:

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

Pursuant to the current Spanish legislation, the Greiner whistleblower system, with its objective of identification and investigation of infringements of the Greiner Code of Conduct does not allow anonymous complaints. So, infringements must not be notified anonymously / anonymous reports are not accepted.

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 three 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.)

The reported individual must be expressly informed by the data controller, within three (3) months from the date the data were recorded, about the processing content, the origin of the data, the existence of a personal data file or that the data will be processed, the purposes thereof and the recipients of the information, the existence of rights of access, rectification, erasure and objection, and the identity and address of the controller or, as appropriate, its representative.

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. 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; and
- The outcome of the report.

6. 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.

7. Data transfers outside the EU:

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

8. Data retention periods:

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

9. 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.

10. 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.

11. 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.

12. 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.

13. Information about data controller

The data controller is the employer: e.g. Vacuette España, S.A., Avenida Somosierra, 22 - 2a planta Nave G, 28703 San Sebastián de los Reyes, T: +34 91 652 77 07, F: +34 91 652 33 35, info@vacuette.es, www.vacuette.es