- English Version
- Portugese Version

ANEXO PARA A POLÍTICA TELL-GREINER.COM / POLÍTICA PARA O SISTEMA DE DENÚNCIAS DO GRUPO GREINER EM PORTUGAL

O Grupo Greiner implementa um sistema de denúncias, que é um sistema voluntário, baseado na web, de denúncias de infrações do Código de Conduta por funcionários do Grupo Greiner.

Para garantir proteções adequadas e o cumprimento da legislação europeia e portuguesa em matéria de proteção de dados, o Grupo Greiner garante o seguinte:

1. Finalidades e âmbito do processamento de dados, limitações:

Nos termos da atual legislação portuguesa, o sistema de denúncias do Grupo Greiner, com o objetivo de identificar e investigar infracções ao Código de Conduta do Grupo Greiner, não permite reclamações anónimas. Assim, as infrações não devem ser notificadas de forma anónima/relatórios anónimos não são aceites.

Apenas os funcionários devem poder reportar através do sistema de denúncias do Grupo Greiner. Assim, o sistema de denúncias do Grupo Greiner não deve ser disponibilizado para parceiros de negócios e clientes. Quaisquer relatórios dos mesmos devem ser feitos ao Diretor Jurídico e ao Diretor de Conformidade do Grupo Greiner na Áustria (maximilian.wellner@greiner.at), ao Diretor de Conformidade Local competente ou, se o assunto se referir ao Diretor de Conformidade do Grupo, à Direção (management@greiner.at).

Somente pessoas que executam atos de contabilidade, controlos contabilísticos internos, auditorias, bem como ações relacionadas com a corrupção, crimes bancários e financeiros podem ser denunciadas.

O âmbito dos assuntos que podem ser denunciados é restrito a: contabilidade, controlos contabilísticos internos, auditorias, corrupção, bem como crimes bancários e financeiros. Assim, apenas os assuntos referidos no Código de Conduta no número 4 (Proibição de qualquer Suborno ou Corrupção) ou qualquer outro que sejam práticas financeiras irregulares.

Quaisquer denúncias relativas à suspeita de violação de outra natureza (ou seja, que não esteja relacionada à contabilidade, controlos contabilísticos internos, auditorias, corrupção, bem como crimes bancários e financeiros), incluindo violações do Código de Conduta, devem ser relatadas pelos meios padronizados. (diferente da plataforma tell-greinerAssim, fazendo um relatório através do sistema de

denúncias, na categoria de incidentes apenas estes três deverão ser selecionados: (i) Suborno/corrupção (ii) Fraude/má conduta contabilística/controlo de faturas e (iii) violação do GCO do Grupo Greiner

2. Eliminação de dados pessoais

Dado que os dados pessoais devem ser imediatamente eliminados quando já não são necessários para o propósito para o qual foram recolhidos, é assegurado que os dados pessoais desnecessários não são conservados por mais de seis meses (a menos que isso seja realmente necessário, como para defender um pedido em tribunal, etc.).

O titular dos dados tem o direito de solicitar um extrato do registo para verificar que informações, se houver, estão registadas sobre ele. Nestes casos, a identidade da pessoa que solicita a informação deve ser assegurada, para que os dados não sejam dados a uma pessoa que não seja o titular dos dados.

A pedido do titular dos dados, os dados pessoais incorretos, incompletos ou enganosos devem ser retificados.

O titular dos dados denunciado recebe certas informações quando os seus dados são processados - no entanto, não a identidade do denunciante (exceto em caso de difamação de má fé pela pessoa denunciante). A divulgação destas informações ao titular dos dados pode, no entanto, ser adiada até que já não impeça a investigação.

Um relatório que se descobrir não ser fundamentado deve ser eliminado imediatamente.

3. Informação dos titulares de dados

Como existe a obrigação de fornecer informações aos funcionários ou outras pessoas cujos dados possam ser processados, o titular dos dados (funcionário denunciado) deve ser informado se os seus dados pessoais forem processados (A informação pode, no entanto, ser adiada até deixar de impedir a investigação.)

4. Informação que a pessoa denunciante deve receber

Em geral, a pessoa denunciante não é informado sobre o que vai acontecer após a sua denúncia ou a conclusão como resultado do seu relatório. A pessoa denunciante não deve receber estas informações, pois as mesmas são dados pessoais sobre a pessoa denunciada e podem conter dados pessoais muito sensíveis, como denúncias de má conduta ou mesmo ofensas legais.

Se a pessoa denunciante tiver um interesse objetivo em receber uma atualização, por exemplo, se a denúncia disser respeito a um assalto à pessoa denunciante cometido pela pessoa denunciada, isso poderia ser uma exceção, justificando dar algumas informações sobre o processo relevante à pessoa denunciante.

5. Categorias registadas de dados pessoais:

Apenas as seguintes categorias de dados são processadas através do sistema de denúncia pretendido:

- A identidade e posição de trabalho da pessoa denunciante;
- A identidade e posição de trabalho da pessoa incriminada (denunciada);

- A identidade e os deveres dos funcionários que recolhem e processam os dados
- Os factos denunciados podem ser considerados suspeitos;
- Os factos reunidos no decorrer da investigação;
- Destino da denúncia

A denúncia só se pode referir a factos relacionados com a contabilidade, controlos contabilísticos internos, auditorias, corrupção e crimes bancários e financeiros.

5. Transferência de dados e destinatários:

O sistema de denúncias do Grupo Greiner é operado pela Greiner AG na Áustria. A este respeito, a entidade Greiner celebrou um acordo com a Greiner AG, estipulando o tratamento dos dados comunicados através do sistema de denúncias antes de qualquer transferência de dados pessoais para o departamento responsável dentro do grupo. Este acordo por escrito obriga a Greiner AG, como operadora do sistema de denúncias, a transferir para o departamento responsável dentro do grupo apenas denúncias incluindo acusações de acordo com o ponto 1 acima. Além disso, a Greiner AG é obrigada a eliminar o conteúdo das denúncias imediatamente após os referidos relatórios terem sido transmitidos ao departamento responsável dentro do grupo.

O departamento encarregado das denúncias, o Conselho Geral e o Departamento de Conformidade, são estritamente separados de quaisquer outros departamentos do grupo; todos os funcionários são pessoas especialmente treinadas e explicitamente responsáveis pela confidencialidade dos dados denunciados.

O Conselho Geral e o Departamento de Conformidade em geral processam todos as denúncias apresentadas pelas pessoas denunciantes em nome da entidade Greiner e transferem relatórios razoáveis para o departamento responsável da entidade Greiner.

No caso da infração reportada se referir a executivos seniores ou a sua significância se estender por várias regiões, assim, se afetar a totalidade ou grande parte do Grupo Greiner, a denúncia pode ser fornecido ao departamento responsável da empresa-mãe do Grupo Greiner, Greiner AG na Áustria, mas apenas na medida em que esses dados sejam necessários para o cumprimento das suas obrigações.

6. Transferência de dados fora de UE:

O Greiner Group garante ainda que os dados pessoais tratados através do sistema de denúncias da Greiner não são transferidos para fora da UE.

7. Períodos de retenção dos dados:

Os dados denunciados serão eliminados seis meses após a conclusão da investigação, o mais tardar.

8. Medidas de segurança:

O controlador de dados implementou medidas de segurança apropriadas para proteger os dados pessoais contra a destruição, perda, alteração, acesso, divulgação ou uso acidental, ilegal ou não autorizado, (i) quando os dados são recolhidos e (ii) quando são partilhados ou armazenados. Particularmente, os dados só podem ser acedidos através de inicio de sessão e palavra-passe individuais, que são alterados regularmente ou por qualquer outro meio de autenticação. Os detalhes de acesso são guardados e a regularidade desse mesmo acesso é verificada.

9. Informações a fornecer às possíveis pessoas denunciantes:

Os funcionários são notificados sobre as seguintes informações pela "política tell-greiner.com/política do sistema de denúncias do Grupo Greiner":

- a identidade do controlador de dados;
- os propósitos do sistema de denúncias do Grupo Greiner e os assuntos que podem ser relatados através do mesmo;
- o facto da utilização do sistema de denúncias do Grupo Greiner ser opcional;
- a ausência de consequências para os funcionários se estes não usarem o esquema;
- os destinatários das denúncias;
- a existência, para qualquer pessoa identificada na denúncia, de um direito de acesso e retificação dos seus dados pessoais e como ele/ela pode exercer esses direitos; e
- o facto das pessoas denunciantes poderem estar sujeitos a ações disciplinares e judiciais, se não apresentarem uma denúncia em boa fé, mas que não serão disciplinados ou sofrer retaliação de qualquer forma por terem feito um relatório em boa fé. Não existe consequência por não denunciar.

10. Informações a serem fornecidas à pessoa incriminada:

Para além das informações indicadas no ponto 12, a pessoa acusada será informada do seguinte, assim que os seus dados sejam registados:

- a identidade do controlador de dados;
- os propósitos do sistema de denúncias do Grupo Greiner e os assuntos que podem ser relatados através do mesmo;
- Os dados denunciados
- as alegações contra essa pessoa;
- os destinatários da denúncia;

- os seus direitos de acesso e retificação dos seus dados pessoais e como estes direitos podem ser exercidos.

Se necessário, para tomar medidas provisórias, em especial para impedir a destruição de provas, as informações acima mencionadas podem ser fornecidas à pessoa incriminada após a adoção dessas mesmas medidas.

11. Respeito pelos direitos de acesso e retificação:

O controlador de dados garantiu que qualquer pessoa identificada nas denúncias possa exercer o seu direito de acesso, alteração, cancelamento ou de se opor à divulgação dos seus dados pessoais e o seu direito de retificação/eliminação dos seus dados pessoais, entrando em contacto com o departamento responsável sob data.protection@greiner.com.

O Grupo Greiner também garante que o acusado não obterá a identidade da pessoa denunciante ao exercer o seu direito de acesso. A este respeito, a identidade da pessoa denunciante não será divulgada à pessoa incriminada no exercício do seu direito de acesso.

12. Informação sobre o controlador de dados

O controlador de dados é o empregador:

por exemplo, Vacuette Portugal Importação e Exportação de Material Hospitalar S.A., Avenida José Ramos Maia, n.º 220 C, Touguinhó, 4480-575 Vila do Conde, T: +351 252 647 721, F: +351 252 647 722, info@vacuette.pt, www.vacuette.pt

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

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 Portuguese data protection law, Greiner guarantees the following:

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

Pursuant to the current Portuguese 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.

Only employees should be able to report trough the Greiner whistleblower system. Thus the Greiner whistleblower system should not be made available to business partners and customers. Any reports from them should be made to the General Counsel and Group Compliance Officer of Greiner in Austria (maximilian.wellner@greiner.com) , to the competent Local Compliance Officer or, if the matter concerns the Group Compliance Officer, to the Board (management@greiner.com).

Only persons that perform acts of management-related areas of accounting, internal accounting controls, auditing, as well as actions related with corruption, banking and finance crimes may be reported.

The scope of subject matters that may be reported is restricted to: accounting, internal accounting controls, auditing, corruption as well as banking and finance crimes. Thus, only matters referred in the Code of Conduct in number 4 (Prohibition of any Bribery or Corruption) or any other that are irregular financial practices.

Any reports regarding the suspicion of a breach of other nature (i.e., that is not related to accounting, internal accounting controls, auditing, corruption as well as banking and finance crimes), including breaches of the Code of Conduct should be reported by standard means (other than the tell-greiner platform).
So, doing a report through the whistleblowing system, in the incident category only these three shall be selected: (i) Bribery/corruption (ii) Fraud/misconduct accounting/invoice control and (iii) breach of GCO of Greiner.

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 (except in case of bad faith defamation by the whistleblower). 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. Categories of personal data recorded:

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

- The identity and job position of the whistleblower;
- The identity and job position of the incriminated (reported) person;
- The identity and duties of the staff that collect and process the data
- The facts reported that could be deemed suspicious;
- The facts gathered in the course of the investigation;
- Destination of the report

The report may only concern facts related to accounting, internal accounting controls, auditing, corruption and banking and finance crimes.

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 two months after termination of the investigation, at the latest.
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.

9. 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. There is no consequence for not reporting

10. 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 purposes of the Greiner whistleblower system and the matters which may be reported through it;
- the reported data

- 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.

11. 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.

12. Information about data controller

The data controller is the employer in Portugal, e.g., Vacuette Portugal Importação e Exportação de Material Hospitalar S.A., Avenida José Ramos Maia, n.º 220 C, Touguinhó, 4480-575 Vila do Conde, T: +351 252 647 721, F: +351 252 647 722, info@vacuette.pt , www.vacuette.pt