- English Version
- German Version

DATA PRIVACY INFORMATION WHISTLEBLOWING SYSTEM (TELL-GREINER.COM PLATFORM AND INTERNAL REPORTING CHANNELS) (PURSUANT TO ARTICLES 13 AND 14 GDPR)

Dear Whistleblower! Dear Website Visitor!

The protection and security of your personal data are important to us. In the following information sheet we provide you with an overview how we handle your data as part of our tell-greiner.com whistleblowing system or when you report locally to the Local Compliance Officer.

1. Who is responsible for data processing and who can I contact if I have questions?

Each business operation (company) is responsible for the data processing in whose sphere the registered violation is made. Each business operation remains responsible if it engages others (third parties such as Greiner AG) (**see Point 3**) for the performance of certain tasks.

If you have questions regarding the processing of your data, please contact the concerned business operation (contact data is available under subitem *locations* at https://www.greiner.com/en/index/) or at office.compliance@greiner.com .

2. Scope of processing

What is the source of the data ?

We process personal data of whistleblowers within the framework of the **whistleblowing system** to the extent we have received data from you. In the case of anonymous notifications, we process only the content of the notification.

We receive data on the person reported/accused from whistleblowers as well as third parties who are involved in the investigation (e.g. attorneys, advisors, witnesses, respondents).

In the course of a notification, there may also be processing of third party data (e.g. witnesses, respondents).

Which data categories are processed?

Included in personal data are, in particular,

- the identity data (e.g. name, title, etc. ...), contact details, function information (e.g. position) of the whistleblower as well as the content of the report.
- the identity data (e.g. name, title, etc.), contact details, function information (e.g. position) of the accused person;
- the identity data (e.g. name, title, etc.), contact details, function information (e.g. position) of the persons who receive or investigate the reports;
- as well as the content of the report, i.e. the facts reported;
- the evidence gathered in the course of the investigation;
- the report on the investigation and
- the outcome of the report.

In addition, we also store your personal data with regard to content and the course of the process as well as with regard to the measures taken.

For which purposes and on what legal basis are my data processed within the whistleblowing system (tell-greiner.com and local reporting channels)?

- Processing for the performance of a task carried out in the public interest (Art. 6 para. 1 lit. e and Art. 9 para. 2 lit. f and g GDPR; local whistleblower protection laws based on Union law,)
- Processing based on a legal obligation (Art. 6 para. 1 lit. c and Art. 9 para. 2 lit. f and g GDPR; local whistleblower protection laws based on Union law)
- Processing based on the legitimate interest of the Greiner company concerned (Art. 6 para. 1 lit. f and Art. 6 para. 1 lit. e and Art. 9 para. 2 lit. f and g GDPR)

All (personal) information which we process within the framework of the **whistleblowing system** serves the prevention and investigation of grievances, and ultimately compliance with the law.

Of particular importance are, *inter alia*, violations in the area of corruption and bribery, financial accounting regulations, tax evasion, illegal practices in association with banks such as money laundering and bank fraud, forgeries of financial documents or of financial statements.

Dealing with anonymous reports

Whistleblowers are free to submit reports anonymously or to disclose their identity. To minimize the risk of abuse, reports by name are preferred.

Objection to processing

If you do not wish the processing of personal data for legitimate reasons, you can file an objection to processing by contacting the contact point in **point 1**.

Is the provision of data required by law or contract or necessary for conclusion of a contract?

All Greiner operations as well as our employees are obliged to comply with all laws. Without the provision of certain personal data, we can/could not fulfil our duty of care to our employees or properly investigate grievances.

For purposes of completeness, we inform you that the trusted path to your supervisor, your competent Local Compliance Officer, your Division Compliance Officer or Group Compliance Officer of Greiner in Austria (compliance@greiner.com) is also open.

3. Transfer and foreign relations

Who receives my data?

The **central** tell-greiner.com **whistleblowing system** is operated by Greiner AG (Austria) on behalf of the Greiner Group companies. Reports are received here by the General Counsel and Compliance Officer as well as selected persons from the Internal Audit department.

With the **local reporting channel**, the submitted reports reach the Local Compliance Officer of the respective company or the external whistleblowing contact points directly.

In their responsibility as recipients and processors of reports, they are specially trained and expressly responsible for the confidentiality of the reported data. At the same time, they are obliged to make impartial decisions free from instructions.

In the event that the reported violation concerns employees with a management function or its significance extends across several regions, i.e. affects all or large parts of Greiner, the report may be forwarded to the responsible department of Greiner's parent company, **Greiner AG** in Austria, but only to the extent that this data is necessary for the fulfilment of its tasks.

In order to achieve the intended purposes, it may be necessary for us to transfer, disclose or grant access to your data to **other recipients** (internal departments involved in the investigation or external consultants;

authorities/public bodies, courts, lawyers, external consultants, insurance companies, ...) on a case-by-case basis.

Data subjects are generally not granted access to the personal data of other data subjects (e.g. whistleblower data) in order to protect their confidentiality.

IT infrastructure, maintenance and technical support for the **central** tell-greiner.com **whistleblowing system** are provided by an IT service provider (Austria). For the **local reporting channel**, our common cloud solutions for internal and external communication and collaboration as well as for video conferencing are used (Microsoft Corp.; data storage in the EU, privacy statement Microsoft).

We only work together with cooperation partners who offer adequate contractual guarantees that your data is also in safe hands with them.

Is data transmitted to a third country or to an international organisation?

Transmission of your personal data to countries outside the EEA occurs only, if the Greiner company has its registered office outside the EEA, in the event of court proceedings in a third country and exclusively to exercise legal rights.

How long are my data stored?

Your data, the disclosure/report and the information collected within the course of an investigation are stored in accordance with local legislation after termination of the investigation and deleted after the locally prescribed retention periods have expired. If the information is necessary for Greiner for the judicial assertion of rights or for defence against claims or for criminal prosecution of violations, we shall store them for the necessary (and thus for a longer) time period.

The following country-specific deletion periods are provided for:

Austria:	5 years after conclusion of the procedure/investigation, longer if necessary
Bulgaria:	5 years after conclusion of the procedure/investigation, longer if necessary
Czech Republic:	5 years after reporting/notification, (longer in the case of pending court or administrative proceedings)
Germany:	3 years after conclusion of proceedings/investigation
Italy:	5 years after conclusion of the procedure/investigation
Poland:	3 years after the end of the calendar year following the conclusion of the proceedings/investigation
Portugal:	5 years after reporting/notification, longer in the case of pending court or administrative proceedings)
Romania:	5 years after reporting/notification, (longer in the case of pending court or administrative proceedings)
Slovakia:	3 years after reporting/notification, (longer in the case of pending court or administrative proceedings)
Spain:	3 months after receipt if no investigation has been initiated, in the event of an investigation a maximum of 10 years
Sweden:	2 years after conclusion of the proceedings/investigation

In countries without statutory regulations, we retain the data for evidentiary purposes for those periods after the conclusion of proceedings/investigations during which claims arising from the employment relationship can be asserted in court in accordance with local legislation. In certain cases, longer retention periods may also be appropriate.

Belgium:	1 year after conclusion of the proceedings
Brazil:	5 years after conclusion of the proceedings
China:	3 years after conclusion of the proceedings
Estonia:	3 years after conclusion of the procedure

France: 5 years after conclusion of the procedure
Hungary: 3 years after completion of the procedure
India: 3 years after completion of the procedure
Indonesia: 10 years after completion of the procedure
Japan: 5 years after completion of the procedure
Mexico: 1 year after completion of the procedure
Netherlands: 2 years after conclusion of the procedure
Switzerland: 11 years after conclusion of the procedure
Serbia: 1 year after conclusion of the proceedings
Singapore: 6 years after conclusion of the proceedings
Thailand: 10 years after conclusion of the proceedings
Turkey: 10 years after completion of the procedure
United Kingdom: 6 years after completion of the procedure
Ukraine: 1 year after completion of the procedure
USA: 3 years after completion of the procedure
UAE /Dubai: 6 years after conclusion of the proceedings

4. Rights of affected parties (data subjects)

What data protection rights do I have?

We wish to inform you that at all times you have the right to:

- request information on which of your data is processed by us, but only if the confidentiality of the whistleblower is maintained (see Art. 15 GDPR),
- have your data rectified or erased if the legitimate interests of the concerned operation in the processing are not overriding (see Art. 16 GDPR),
- restrict the processing of your data (see Art. 18 GDPR),
- object to the data processing (see Art. 21 GDPR),
- assert data portability (see Art. 20 GDPR).

Is there a right to complain to a supervisory authority?

If contrary to expectations, there is a violation of your data protection rights, you have the right to file a complaint with the data protection authorities of your country, in particular at your domicile or place of work, or with another data protection supervisory authority in the EU. An overview can be found under data privacy authorities.

Is there automatic decision-making including profiling?

Neither automatic decision-making nor profiling occurs.

Is data processed for other purposes?

We wish to inform you that we process your data only for the above referenced purposes. In no event will further processing for other purposes occur.

We hope that this information sheet provides you with clarity as to the form and purposes for which we process your data. If you nevertheless have questions on the processing of your data, please contact the Contact Office in **Point 1**.

DATENSCHUTZINFORMATION WHISTLEBLOWING-SYSTEM (TELL-GREINER.COM PLATTFORM UND LOKALE MELDEWEGE) (NACH ART 13 und 14 DSGVO)

Sehr geehrter Hinweisgeber! Sehr geehrter Websitebesucher!

Der Schutz und die Sicherheit Ihrer persönlichen Daten sind uns ein wichtiges Anliegen. Im nachfolgenden Informationsblatt geben wir Ihnen einen Überblick, wie wir mit Ihren Daten im Rahmen unseres Whistleblowing-Systems tell-greiner.com bzw. bei lokaler Meldung an den Local Compliance Officer umgehen.

1. Wer ist verantwortlich für die Datenverarbeitung und an wen kann ich mich bei Fragen wenden?

Für die Datenverarbeitung verantwortlich ist jener Betrieb, in dessen Umfeld der gemeldete Verstoß erfolgte. Jener Betrieb bleibt auch dann Verantwortlicher, wenn er zur Erledigung bestimmter Aufgaben andere (Dritte wie die Greiner AG) (**vgl. Punkt 3**) beauftragt.

Sollten Sie Fragen zur Verarbeitung Ihrer Daten haben, wenden Sie sich bitte an den betroffenen Betrieb (Kontaktdaten sind abrufbar unter Unterpunkt *Standorte* auf https://www.greiner.com/index/) oder an office.compliance@greiner.com .

2. Verarbeitungsrahmen

Aus welcher Quelle stammen die Daten?

Von Hinweisgebern verarbeiten wir im Rahmen von Whistleblowing personenbezogene (kurz: „pb“) Daten, soweit wir diese von Ihnen erhalten haben. Bei anonymen Meldungen verarbeiten wir nur den Meldungsinhalt.

Daten über den Angezeigten/beschuldigte Person erhalten wir von Hinweisgebern sowie Dritten, die der Untersuchung beigezogen werden (z.B. Rechtsanwälte, Berater, Zeugen, Auskunftspersonen).

Im Zuge einer Meldung kann es auch zur Verarbeitung von Daten Dritter (z.B. Zeugen, Auskunftspersonen) kommen.

Welche Datenkategorien werden verarbeitet

Zu den pb Daten zählen insbesondere

- die Identitätsdaten (z.B. Name, Titel, etc.), Kontaktdaten, Funktionsinformationen (z.B. Position) des Hinweisgebers
- die Identitätsdaten (z.B. Name, Titel, etc.), Kontaktdaten, Funktionsinformationen (z.B. Position) der beschuldigten Person;
- die Identitätsdaten (z.B. Name, Titel, etc.), Kontaktdaten, Funktionsinformationen (z.B. Position) der Personen, die die Meldungen erhalten oder untersuchen;
- sowie der Inhalt der Meldung, also die gemeldeten Fakten;
- die im Laufe der Untersuchung gesammelten Beweise;
- den Bericht über die Untersuchung und
- das Ergebnis des Berichts.

Darüber hinaus speichern wir Ihre pb Daten auch zu Inhalt und Ablauf des Verfahrens sowie zu ergriffenen Maßnahmen.

Für welche Zwecke und auf welcher Rechtsgrundlage werden meine Daten im Rahmen von Whistleblowing (tell-greiner.com oder lokaler Meldeweg) verarbeitet?

- Verarbeitung zur Wahrnehmung einer Aufgabe im öffentlichen Interesse (Art. 6 Abs. 1 lit e und Art. 9 Abs. 2 lit f und g DSGVO; lokale Hinweisgeberschutzgesetze auf Grundlage Unionsrecht,)
- Verarbeitung basierend auf einer rechtlichen Verpflichtung (Art. 6 Abs. 1 lit c und und Art. 9 Abs. 2 lit f und g DSGVO; lokale Hinweisgeberschutzgesetze auf Grundlage Unionsrecht)
- Verarbeitung basierend auf berechtigtem Interesse des betroffenen Greiner Betriebs (Art 6 Abs 1 lit f und Art. 6 Abs. 1 lit e und Art. 9 Abs. 2 lit f und g DSGVO)

Sämtliche (pb) Informationen, die wir im Rahmen des **Hinweisgebersystems** verarbeiten, dienen der Prävention und Aufklärung von Missständen, schließlich zur Einhaltung der Gesetze.

Besonders gewichtig sind unter anderem Verstöße in den Bereichen Korruption und Bestechung, Buchführungsvorschriften, Steuerhinterziehung, illegale Praktiken im Zusammenhang mit Banken wie Geldwäsche und Bankbetrug, Fälschung von Finanzunterlagen oder Bilanzen.

Umgang mit anonymen Meldungen

Hinweisgebern steht es offen, Meldungen anonym zu erstatten oder Ihre Identität preiszugeben. Um das Missbrauchsrisiko zu minimieren, werden namentliche Hinweise bevorzugt.

Widerspruch gegen die Verarbeitung

Wenn Sie eine Verarbeitung pb Daten aus berücksichtigungswürdigen Gründen nicht wollen, können Sie gegen die Verarbeitung **Widerspruch** bei der Ansprechstelle in **Punkt 1** einlegen.

Ist die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich?

Alle Greiner Betriebe und auch unsere Mitarbeiter haben sich zur Einhaltung aller Gesetze verpflichtet. Ohne die Bereitstellung bestimmter pb Daten können/könnten wir unsere Fürsorgepflicht unseren Mitarbeitern gegenüber nicht erfüllen und Hinweisen zu Missständen nicht ordnungsgemäß nachgehen.

Der Vollständigkeit halber weisen wir darauf hin, dass selbstverständlich der vertraute Weg zu Ihrem Vorgesetzten, zu Ihrem zuständigen Local Compliance Officer, Ihrem Division Compliance Officer oder Group Compliance Officer von Greiner in Österreich (compliance@greiner.com) ebenso offensteht.

3. Weitergabe und Auslandsbezug

Wer erhält meine Daten?

Das **zentrale** tell-greiner.com **Whistleblowing-System** wird im Auftrag der Greiner Konzernbetriebe von der Greiner AG (Österreich) betrieben. Meldungen werden hier vom General Counsel und Compliance Officer sowie ausgewählten Personen der Abteilung Internal Audit empfangen.

Beim **lokalen Meldeweg** erreichen die eingereichten Meldungen direkt den Local Compliance Officer des jeweiligen Unternehmens bzw. die externen Whistleblowing Kontaktstellen.

In Ihrer Verantwortlichkeit als Empfänger und Bearbeiter von Hinweisen sind diese besonders geschult und ausdrücklich für die Vertraulichkeit der gemeldeten Daten verantwortlich. Gleichzeitig sind sie zur unparteiischen und weisungsfreien Entscheidung verpflichtet.

Für den Fall, dass der gemeldete Verstoß leitende Angestellte betrifft oder sich seine Bedeutung über mehrere Regionen erstreckt, also die gesamte oder große Teile von Greiner betrifft, kann die Meldung an

die zuständige Abteilung der Muttergesellschaft von Greiner, der **Greiner AG** in Österreich, weitergegeben werden, jedoch nur insoweit, als diese Daten zur Erfüllung ihrer Aufgaben erforderlich sind.

Um die angestrebten Zwecke zu erreichen, kann es fallweise notwendig sein, dass wir Ihre Daten **weiteren Empfängern** (an den Ermittlungen beteiligte interne Abteilungen oder externen Beratern; Behörden/öffentliche Stellen, Gerichten, Rechtsanwälten, Versicherungsunternehmen, ...) übermitteln, offenlegen oder Zugriff auf Ihre Daten gewähren.

Betroffene erhalten grundsätzlich keinen Zugriff auf personenbezogene Daten anderer Betroffener (z.B. Daten zum Hinweisgeber), um deren Vertraulichkeit zu wahren.

IT-Infrastruktur, Wartung sowie technischer Support für das **zentrale** tell-greiner.com **Whistleblowing-System** erfolgen durch einen IT-Dienstleister (Österreich). Beim **lokalen Meldeweg** kommen unsere gängigen Cloud-Lösungen zur internen und externen Kommunikation und Kollaboration sowie für Videokonferenzen zur Anwendung (Microsoft Corp.; Datenspeicherung in der EU, Datenschutzerklärung von Microsoft – Microsoft-Datenschutz).

Wir arbeiten nur mit Kooperationspartnern, die hinreichende vertragliche Garantien dafür bieten, dass Ihre Daten auch bei diesen in sicheren Händen sind.

Werden Daten an ein Drittland oder eine internationale Organisation übermittelt?

Eine Übermittlung Ihrer pb Daten an Länder außerhalb des EWR erfolgt nur, soweit das Greiner Unternehmen seinen Sitz außerhalb des EWR hat, und zwar anlässlich eines Gerichtsverfahrens in einem Drittland und ausschließlich zur Ausübung von Rechtsansprüchen.

Wie lange werden meine Daten gespeichert?

Ihre Daten, der Hinweis und die im Rahmen einer Untersuchung erhobenen Informationen werden entsprechend den lokalen Rechtsvorschriften nach Beendigung der Untersuchung aufbewahrt und nach Ablauf der lokal vorgeschriebenen Aufbewahrungsfristen gelöscht. Sofern die Informationen für die gerichtliche Geltendmachung von oder die Abwehr gegen Ansprüche oder für die strafrechtliche Verfolgung von Verstößen von Greiner erforderlich sind, werden sie aber für den dafür notwendigen (und somit für einen längeren) Zeitraum gespeichert.

Folgende länderabhängige Löschfristen sind vorgesehen:

Österreich:	5 Jahre nach Abschluss des Verfahrens/Ermittlungen, erforderlichenfalls länger
Bulgarien:	5 Jahre nach Abschluss des Verfahrens/Ermittlungen, erforderlichenfalls länger
Tschechische Republik:	5 Jahre nach Meldung (länger im Fall eines anhängigen Gerichts- oder Verwaltungsverfahrens)
Deutschland:	3 Jahre nach Abschluss des Verfahrens/Ermittlungen
Italien:	5 Jahre nach Abschluss des Verfahrens/Ermittlungen
Polen:	3 Jahre nach Ablauf des Kalenderjahres nach Abschluss des Verfahrens/Ermittlungen
Portugal:	5 Jahre nach Meldung, länger im Fall eines anhängigen Gerichts- oder Verwaltungsverfahrens
Rumänien:	5 Jahre nach Meldung, (länger im Fall eines anhängigen Gerichts- oder Verwaltungsverfahrens)
Slowakei:	3 Jahre nach Meldung, (länger im Fall eines anhängigen Gerichts- oder Verwaltungsverfahrens)
Spanien:	3 Monate nach Eingang, sofern keine Untersuchung eingeleitet wurde, im Falle einer Untersuchung maximal 10 Jahre
Schweden:	2 Jahre nach Abschluss des Verfahrens/Ermittlungen

In Ländern ohne gesetzliche Regelung bewahren wir die Daten zu Beweiszwecken für jene Zeiträume nach Abschluss der Verfahren/Ermittlungen auf, in denen nach lokaler Gesetzgebung Ansprüche aus dem Arbeitsverhältnis gerichtlich geltend gemacht werden können. In bestimmten Fällen können auch längere Aufbewahrungsfristen angemessen sein.

Belgien:	1 Jahr nach Abschluss des Verfahrens
Brasilien:	5 Jahre nach Abschluss des Verfahrens
China:	3 Jahre nach Abschluss des Verfahrens
Estland:	3 Jahre nach Abschluss des Verfahrens
Frankreich:	5 Jahre nach Abschluss des Verfahrens
Ungarn:	3 Jahre nach Abschluss des Verfahrens
Indien:	3 Jahre nach Abschluss des Verfahrens
Indonesien:	10 Jahre nach Abschluss des Verfahrens
Japan:	5 Jahre nach Abschluss des Verfahrens
Mexico:	1 Jahr nach Abschluss des Verfahrens
Niederlande:	2 Jahre nach Abschluss des Verfahrens
Schweiz:	11 Jahre nach Abschluss des Verfahrens
Serbien:	1 Jahr nach Abschluss des Verfahrens
Singapur:	6 Jahre nach Abschluss des Verfahrens
Thailand:	10 Jahre nach Abschluss des Verfahrens
Türkei:	10 Jahre nach Abschluss des Verfahrens
Vereinigtes Königreich:	6 Jahre nach Abschluss des Verfahrens
Ukraine:	1 Jahr nach Abschluss des Verfahrens
USA:	3 Jahre nach Abschluss des Verfahrens
VAE /Dubai:	6 Jahre nach Abschluss des Verfahrens

4. Betroffenenrechte

Welche Datenschutzrechte stehen mir zu?

Wir möchten Sie weiters darüber informieren, dass Sie jederzeit das Recht haben:

- Auskunft darüber zu verlangen, welche Daten von Ihnen bei uns verarbeitet werden (siehe Art 15 DSGVO), jedoch nur unter Wahrung der Vertraulichkeit des Hinweisgebers,
- Ihre Daten berichtigen oder löschen zu lassen, soweit nicht berechtigte Interessen des betroffenen Betriebs zur Verarbeitung überwiegen. (siehe Art 16 DSGVO),
- die Verarbeitung Ihrer Daten einzuschränken (siehe Art 18 DSGVO),
- der Datenverarbeitung zu widersprechen (siehe Art 21 DSGVO),
- auf Datenübertragbarkeit geltend machen können (siehe Art 20 DSGVO).

Besteht ein Beschwerderecht bei einer Aufsichtsbehörde?

Sollte es wider Erwarten zu einer Verletzung Ihrer Datenschutzrechte kommen, haben Sie das Recht, eine Beschwerde bei der Datenschutzbehörde Ihres Landes, insbesondere an Ihrem Aufenthalts- oder Arbeitsort, oder bei einer anderen Datenschutz-Aufsichtsbehörde in der EU zu erheben. Eine Übersicht finden Sie unter Datenschutzbehörden.

Besteht eine automatische Entscheidungsfindung einschließlich Profiling?

Es findet weder eine automatische Entscheidungsfindung noch Profiling statt.

Werden Daten zu anderen Zwecken weiterverarbeitet?

Schließlich möchten wir Sie auch darüber informieren, dass wir Ihre Daten nur zu den bereits oben aufgelisteten Zwecken verarbeiten. Eine (Weiter-)Verarbeitung zu anderen Zwecken wird keinesfalls vorgenommen.

Wir hoffen, Ihnen mit diesem Informationsblatt Klarheit darüber verschafft zu haben, in welcher Form und für welche Zwecke wir Ihre Daten verarbeiten. Sollten Sie dennoch Fragen zur Verarbeitung Ihrer Daten haben, wenden Sie sich bitte an die Ansprechstelle in **Punkt 1**.