

Inhaltsverzeichnis / Table of content

Datenschutzerklärung für die Hinweisgeber des STI Group Hinweisgebersystems3

1. Wer ist für die Datenverarbeitung verantwortlich und an wen kann ich mich wenden?3
2. Welche personenbezogenen Daten verarbeiten wir?3
3. Wofür verarbeiten wir Ihre Daten (Zweck der Verarbeitung) und auf welcher Rechtsgrundlage?3
 - 3.1. Verarbeitungszwecke3
 - 3.2. Rechtgrundlage4
4. Wer bekommt meine Daten?5
5. Technische Umsetzung und Sicherheit Ihrer Daten5
6. Wie lange werden meine Daten gespeichert?5
7. Werden Daten in ein Drittland oder an eine internationale Organisation übermittelt?6
8. Welche weiteren Datenschutzrechte habe ich?6
9. Beschwerderecht bei einer Aufsichtsbehörde6

Data protection and privacy policy for the whistleblowers of the STI Group whistleblowing system7

1. Who is responsible for data processing and whom can I contact?7
2. What personal data do we process?7
3. What do we process your data for (purpose of processing) and on what legal basis?7
 - 3.1. Processing purposes7
 - 3.2. Legal basis8
4. Who gets my data?8
5. Technical implementation and security of your data9

6.	How long will my data be stored?	9
7.	Is data transferred to a third country or to an international organisation?.....	9
8.	What other data protection rights do I have?	9
9.	Right of appeal to a supervisory authority.....	10

Datenschutzerklärung für die Hinweisgeber des STI Group Hinweisgebersystems

Information zur Verarbeitung Ihrer personenbezogenen Daten gem. Artt. 13, 14 sowie 15-21 der Datenschutz-Grundverordnung (DSGVO)

Diese Datenschutzhinweise zur Nutzung des „STI Group Hinweisgebersystem“ gelten ausschließlich für die Datenverarbeitung im Zusammenhang mit dem Hinweisgebersystem. Mit diesen Datenschutzhinweisen informieren wir Sie gemäß der Europäischen Datenschutz-Grundverordnung (DS-GVO) und dem Bundesdatenschutzgesetz (BDSG) über die Verarbeitung Ihrer personenbezogenen Daten durch uns sowie über die Ihnen zustehenden Rechte bei der Abgabe von Hinweisen im „STI Group Hinweisgebersystem“. Diese Datenschutzhinweise werden, soweit erforderlich, aktualisiert und im Internet veröffentlicht. Wird im Folgenden „STI Group“ verwendet, so ist damit die STI – Gustav Stabernack GmbH oder eine der Gesellschaften der STI Group gemeint.

Die technische Umsetzung des Hinweisgebersystems erfolgt durch das Unternehmen product kitchen GmbH, Rehsteige 12, 73035 Göppingen in Deutschland, im Auftrag der STI Group.

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

Verantwortlicher im Sinne der DS-GVO für die Verarbeitung der Daten ist die

STI – Gustav Stabernack GmbH
Richard-Stabernack-Straße
36341 Lauterbach.

Die Kontaktdaten des Datenschutzbeauftragten lauten:

STI – Gustav Stabernack GmbH
- Datenschutzbeauftragter –
Richard-Stabernack-Straße
36341 Lauterbach
E-Mail: datenschutz@sti-group.com

2. Welche personenbezogenen Daten verarbeiten wir?

Grundsätzlich ist die Nutzung des Hinweisgebersystems ohne die Angabe personenbezogener Daten möglich. Aufgrund freier Textfelder im Meldeformular können jedoch personenbezogene Daten freiwillig von Ihnen bekanntgegeben werden. Der von Ihnen gegebene Hinweis kann darüber hinaus personenbezogene Daten Dritter enthalten.

Mit Ihrem Hinweis oder hinweisgebenden Ergänzungen haben Sie die Möglichkeit Anhänge zu senden. Bitte beachten Sie, dass auch Anhänge personenbezogene Daten enthalten können. Sollten Sie eine Meldung anonym abgeben wollen entfernen Sie bitte vor dem Versenden die personenbezogenen Daten im Anhang.

3. Wofür verarbeiten wir Ihre Daten (Zweck der Verarbeitung) und auf welcher Rechtsgrundlage?

3.1. Verarbeitungszwecke

Das Hinweisgebersystem ermöglicht Ihnen, mit uns in Verbindung zu treten und Hinweise zu Compliance- und

Rechtsverstößen zu melden. Wir verarbeiten Ihre personenbezogenen Daten, um die von Ihnen über das Hinweisgebersystem gemachte Meldung zu prüfen und die mutmaßlichen Compliance- und Rechtsverstöße zu untersuchen. Hierbei kann es vorkommen, dass wir Rückfragen an Sie haben. Dafür nutzen wir die Kommunikation über das Hinweisgebersystem.

Ihre Hinweise werden von den Mitgliedern der Compliance Arbeitsgruppe entgegengenommen und stets vertraulich behandelt. Alle zur Einsichtnahme autorisierten Personen sind ausdrücklich zur Vertraulichkeit verpflichtet.

3.2. Rechtgrundlage

Die Verarbeitung Ihrer Identifikationsdaten als Hinweisgeber erfolgt auf Basis Ihrer Einwilligung gem. Art. 6 Abs. 1 S.1 lit. a) DSGVO. Die Freiwilligkeit der Einwilligung ist dadurch gegeben, dass der Hinweis stets auch anonym erfolgen kann. Sofern Sie uns besondere Kategorien personenbezogener Daten bekanntgeben, verarbeiten wir diese auf der Grundlage Ihrer Einwilligung (Art. 9 Abs. 2 lit. a) DSGVO).

Die Einwilligung können Sie jederzeit ohne Angabe von Gründen widerrufen. Ein Widerruf der Einwilligung kann allerdings (in bestimmten Fällen) nur in einem befristeten Zeitrahmen seine volle Wirkung entfalten.

Das ergibt sich (in bestimmten Fällen) aus der Verpflichtung des Verantwortlichen gem. Art. 14 Abs. 3 lit. a) DSGVO, beschuldigte Personen über die gegen sie erhobenen Vorwürfe und durchgeführten Ermittlungen spätestens innerhalb eines Monats nach Erhalt der Meldung zu informieren, soweit dies dem Zweck der Erhebung nicht entgegensteht.

Die Information umfasst regelmäßig die Art der Daten, die Zweckbestimmung der Verarbeitung, die Speicherdauer, die Identität des datenschutzrechtlich Verantwortlichen und gegebenenfalls der hinweisgebenden Person. Ab einem fortgeschrittenen Bearbeitungsgrad / Ermittlungsstand ist eine Einstellung der Verarbeitung wie auch eine Löschung der Identifikationsdaten der hinweisgebenden Person i.d.R. nicht weiter möglich. Sobald Informationen inkl. Namen gegenüber zuständigen Behörden oder Gerichtsbarkeiten offengelegt wurden, befindet sich diese sowohl in unseren Unterlagen als auch bei den zuvor genannten Empfängern und können nicht ohne Weiteres gelöscht werden.

Des Weiteren verarbeiten wir Ihre personenbezogenen Daten, soweit dies zur Erfüllung rechtlicher Verpflichtungen notwendig ist. Darunter fallen insbesondere Meldungen von straf-, wettbewerbs- und arbeitsrechtlich relevanten Sachverhalten (Art. 6 Abs. 1 S.1 lit. c) DSGVO).

Schließlich erfolgt die Verarbeitung Ihrer personenbezogenen Daten, sofern dies zur Wahrung berechtigter Interessen der STI Group bzw. eines Dritten erforderlich ist (Art. 6 Abs. 1 S.1 lit. f) DSGVO). Wir haben ein berechtigtes Interesse insbesondere an der Verarbeitung der personenbezogenen Daten zur Prävention und Aufdeckung von Verstößen innerhalb des Unternehmens und zur Überprüfung der internen Prozesse auf ihre Rechtmäßigkeit.

In Einzelfällen erheben wir im Rahmen von Aufklärungsmaßnahmen auch besondere Kategorien personenbezogener Daten i.S.v. Art. 9 Abs. 1 DSGVO. Dies kann etwa der Fall sein, wenn ein von einem Hinweisgeber übermittelter Hinweis entsprechende Daten enthält. Zu den besonderen Kategorien personenbezogener Daten zählen insbesondere Gesundheitsdaten, Daten über eine mögliche Gewerkschaftszugehörigkeit oder Daten über politische oder religiöse Einstellungen. Sofern Sie uns besondere Kategorien personenbezogener Daten bekanntgeben, verarbeiten wir diese auf der Grundlage von Art. 9 Abs. 2 lit. b) und g) DSGVO.

Betrifft ein eingegangener Hinweis einen Beschäftigten der STI Group, dient die Verarbeitung zudem der Verhinderung von Straftaten oder sonstigen Rechtsverstößen, die im Zusammenhang mit dem Beschäftigtenverhältnis stehen. Dieses richtet sich nach Art. 88 Abs. 1 DSGVO i.V.m. § 26 Abs. 1 BDSG.

Wir weisen ausdrücklich darauf hin, dass Fälle denkbar sind, in denen die Verarbeitung auf mehrere, nebeneinander geltende Rechtsgrundlagen gestützt werden könnte. In einem solchen Fall behalten wir uns vor, die Verarbeitung auch im Falle des Widerrufs der Einwilligung auf eine andere, gesetzliche Rechtsgrundlage zu stützen. Darüber werden wir Sie im Falle des Widerrufs der Einwilligung entsprechend informieren.

Zudem verwenden wir Ihre personenbezogenen Daten in anonymisierter Form zu statistischen Zwecken.

4. Wer bekommt meine Daten?

Im Rahmen der Bearbeitung einer Meldung kann es notwendig sein, Hinweise innerhalb der STI Group weiterzugeben. Dies erfolgt insbesondere, wenn sich der Hinweis auf Vorgänge in den Tochtergesellschaften bezieht. Wir achten stets darauf, dass die einschlägigen datenschutzrechtlichen Bestimmungen bei der Weitergabe von Hinweisen eingehalten werden.

Zur Erfüllung des zuvor genannten Zwecks kann es zudem erforderlich sein, dass wir Ihre personenbezogenen Daten an externe Stellen wie Anwaltskanzleien, Straf- oder Wettbewerbsbehörden übermitteln.

In sämtlichen Fällen verbleibt die Verantwortung zur Datenverarbeitung bei der STI – Gustav Stabernack GmbH.

Auftragsverarbeitung

Für die Verarbeitung Ihrer personenbezogenen Daten setzen wir in gewissem Umfang spezialisierte Dienstleister ein, die Ihre Daten in unserem Auftrag verarbeiten. Unsere Dienstleister werden von uns sorgfältig ausgewählt und regelmäßig kontrolliert. Sie verarbeiten personenbezogene Daten nur in unserem Auftrag und nach unseren Weisungen auf der Grundlage entsprechender Vereinbarungen über eine Auftragsverarbeitung.

Übermittlung an Dritte

Wir teilen Ihre personenbezogenen Daten ggf. mit Behörden und sonstigen ermittelnden Stellen insbesondere zum Zweck der Sachverhaltsaufklärung und Bewertung der rechtlichen Folgen.

5. Technische Umsetzung und Sicherheit Ihrer Daten

Das Hinweisgebersystem enthält eine Möglichkeit zur anonymen Kommunikation über eine verschlüsselte (TLS) Verbindung (zwischen Client (Browser) und Server). Alle Daten der Datenbank werden zusätzlich zur clientseitigen Ende-zu-Ende Verschlüsselung der Hinweis-Daten vor dem Schreiben auf das Speichermedium nach aktuellem Stand der Technik verschlüsselt.

Die IP Adressen werden entsprechend der technischen Notwendigkeit von Netzwerkverbindungen im Internet nur temporär erfasst und anschließend gelöscht. Pseudonym/Benutzername und Passwort wird vom System automatisch nach Abgabe eines Hinweises dynamisch erzeugt. Die Zugangsdaten gelten nur für den Zugriff auf die Postbox dieses einen Falls, um beispielsweise Rückmeldungen der Verantwortlichen abzurufen oder Informationen nachzureichen. Zur Abgabe eines Hinweises sind keinerlei Zugangsdaten nötig - diese werden nach Abgabe des Hinweises generiert und dem Hinweisgeber angezeigt.

Zur sicheren und zuverlässigen Erbringung der Leistung des Hinweisgebersystems nutzt die product kitchen GmbH Auftragsverarbeiter mit Sitz in einem Mitgliedsstaat der Europäischen Union unter Beachtung der geltenden datenschutzrechtlichen Regelungen insbesondere der DSGVO. Die verschlüsselten Hinweis-Daten werden in europäischen und zertifizierten Datacenter verarbeitet. Aufgrund der Ende-zu-Ende Verschlüsselung der Hinweis-Daten zwischen Hinweisgeber und Fallbearbeitern ist ein anderweitiger Zugriff auf den Klartext der Meldung nicht gegeben.

Die Einhaltung der geltenden Datenschutzvorschriften wird durch entsprechende technische und organisatorische Maßnahmen sichergestellt.

6. Wie lange werden meine Daten gespeichert?

Ihre personenbezogenen Daten werden für einen Zeitraum gespeichert, der sich aus der Notwendigkeit zur Bearbeitung, Aufklärung und Dokumentation des (aus Ihrem Hinweis resultierenden) Sachverhaltes ergibt und anschließend nach Abschluss des Falles nach 24 Monaten gelöscht. Etwas anderes gilt, wenn geltende gesetzliche

Bestimmungen etwas anders verlangen (z.B. in Zusammenhang mit anhängigen Gerichtsverfahren), wobei entsprechende Verfahrensakten i.d.R. 10 Jahre aufbewahrt werden.

7. Werden Daten in ein Drittland oder an eine internationale Organisation übermittelt?

Wir übermitteln Ihre Daten grundsätzlich nicht in Staaten außerhalb des Europäischen Wirtschaftsraums - EWR (Drittländer).

8. Welche weiteren Datenschutzrechte habe ich?

Sie haben unter den jeweiligen gesetzlichen Voraussetzungen das Recht auf Auskunft (Art. 15 DS-GVO, § 34 BDSG, auf Berichtigung (Art. 16 DS-GVO), auf Löschung (Art. 17 DS-GVO, § 35 BDSG), auf Einschränkung der Verarbeitung (Art. 18 DS-GVO) sowie auf Datenübertragbarkeit (Art. 20 DS-GVO). Außerdem haben Sie ein Beschwerderecht bei einer Datenschutzaufsichtsbehörde (Art. 77 DS-GVO i.V.m. § 19 BDSG).

Sollten Sie von Ihren oben genannten Rechten Gebrauch machen, prüft der zuständige Bereich, ob die gesetzlichen Voraussetzungen hierfür erfüllt sind.

9. Beschwerderecht bei einer Aufsichtsbehörde

Jede betroffene Person hat das Recht auf Beschwerde bei einer Aufsichtsbehörde für den Datenschutz, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden Daten gegen datenschutzrechtliche Bestimmungen verstößt (Art. 77 der DSGVO). Die Beschwerde bei der Aufsichtsbehörde kann formlos erfolgen. Für die STI – Gustav Stabernack GmbH und der konzerngebundenen Gesellschaften ist folgende Aufsichtsbehörde für den Datenschutz zuständig:

HBDI - Der Hessische Beauftragte für Datenschutz und Informationsfreiheit
Gustav-Stresemann-Ring 1
65189 Wiesbaden

Telefon: 0611-1408 0

Website: <https://datenschutz.hessen.de/>

E-Mail: poststelle@datenschutz.hessen.de

Data protection and privacy policy for the whistleblowers of the STI Group whistleblowing system

Information on the processing of your personal data according to Art. 13, 14 and 15-21 of the General Data Protection Regulation (GDPR)

This data protection notice on the use of the "STI Group whistleblower system" applies exclusively to data processing in connection with the whistleblower system. With this data protection information, we inform you in accordance with the European Data Protection Regulation (GDPR) and the Federal Data Protection Act (BDSG) about the processing of your personal data by us and about the rights to which you are entitled when submitting information in the "STI Group whistleblower system". This data protection information will be updated as necessary and published on the Internet. Where "STI Group" is used in the following, this refers to STI - Gustav Stabernack GmbH or one of the companies of the STI Group.

The technical implementation of the whistleblower system is carried out by the company product kitchen GmbH, Rehsteige 12, 73035 Göppingen in Germany, on behalf of STI Group.

1. Who is responsible for data processing and whom can I contact?

The controller within the meaning of the GDPR for the processing of the data is the

STI - Gustav Stabernack GmbH
Richard-Stabernack-Straße
36341 Lauterbach.
Germany

The contact details of the Data Protection Officer are:

STI - Gustav Stabernack GmbH
- Data Protection Officer -
Richard-Stabernack-Straße
36341 Lauterbach
E-mail: datenschutz@sti-group.com

2. What personal data do we process?

In principle, it is possible to use the whistleblower system without providing personal data. However, due to free text fields in the reporting form, personal data may be disclosed by you voluntarily. The information you provide may also contain personal data of third parties.

You have the option of sending attachments with your note or note-providing additions. Please note that attachments may also contain personal data. If you wish to submit a report anonymously, please remove the personal data in the attachment before sending it.

3. What do we process your data for (purpose of processing) and on what legal basis?

3.1. Processing purposes

The whistleblower system allows you to contact us and report compliance and legal violations. We process your

personal data in order to check the report you have made via the whistleblower system and to investigate the alleged compliance and legal violations. In doing so, we may have queries for you. We use communication via the whistleblower system for this purpose.

Your comments will be received by the members of the Compliance Working Group and will always be treated confidentially. All persons authorised to inspect the information are expressly obliged to maintain confidentiality.

3.2. Legal basis

The processing of your identification data as a whistleblower is based on your consent pursuant to Art. 6 para. 1 sentence 1 lit. a) GDPR. The voluntary nature of the consent is given by the fact that the information can always be provided anonymously. If you provide us with special categories of personal data, we process these on the basis of your consent (Art. 9 para. 2 lit. a) GDPR).

You can revoke your consent at any time without giving reasons. However, a revocation of consent can (in certain cases) only have its full effect within a limited time frame.

This results (in certain cases) from the obligation of the controller under Art. 14(3)(a) of the GDPR to inform accused persons of the allegations made against them and investigations carried out within one month of receipt of the notification at the latest, provided this does not conflict with the purpose of the collection.

The information regularly includes the type of data, the purpose of the processing, the storage period, the identity of the data controller and, if applicable, the person providing the information. From an advanced stage of processing/investigation onwards, it is generally no longer possible to discontinue processing or to delete the identification data of the person providing the information. As soon as information including names has been disclosed to competent authorities or jurisdictions, it is stored in our records as well as with the aforementioned recipients and cannot be deleted without further ado.

Furthermore, we process your personal data insofar as this is necessary for the fulfilment of legal obligations. This includes, in particular, notifications of facts relevant under criminal, competition and labour law (Art. 6 para. 1 p.1 lit. c) GDPR).

Finally, your personal data is processed if this is necessary to protect the legitimate interests of the STI Group or a third party (Art. 6 para. 1 sentence 1 lit. f) GDPR). We have a legitimate interest in particular in the processing of personal data for the prevention and detection of violations within the company and to check the legality of internal processes.

In individual cases, we also collect special categories of personal data within the meaning of Article 9 (1) of the GDPR as part of educational measures. This may be the case, for example, if a tip transmitted by a whistleblower contains corresponding data. Special categories of personal data include, in particular, health data, data on possible trade union membership or data on political or religious attitudes. If you provide us with special categories of personal data, we process them on the basis of Art. 9 (2) (b) and (g) of the GDPR.

If a tip received relates to an employee of the STI Group, the processing also serves to prevent criminal offences or other legal violations in connection with the employee relationship. This is governed by Art. 88 Para. 1 GDPR in conjunction with § 26 Section 1 BDSG.

We expressly point out that cases are conceivable in which the processing could be based on several legal bases that apply alongside each other. In such a case, we reserve the right to base the processing on another, legal basis even in the event of revocation of consent. We will inform you of this accordingly in the event of withdrawal of consent.

We also use your personal data in anonymised form for statistical purposes.

4. Who gets my data?

When processing a report, it may be necessary to pass on information within the STI Group. This is particularly the case if the information relates to processes in the subsidiaries. We always ensure that the relevant data protection

regulations are complied with when passing on information.

In order to fulfil the aforementioned purpose, it may also be necessary for us to transfer your personal data to external bodies such as law firms, criminal or competition authorities.

In all cases, the responsibility for data processing remains with STI - Gustav Stabernack GmbH.

Job processing

To a certain extent, we use specialised service providers to process your personal data on our behalf. Our service providers are carefully selected and regularly monitored by us. They process personal data only on our behalf and according to our instructions on the basis of corresponding commissioned processing agreements.

Transmission to third parties

We may share your personal data with authorities and other investigating bodies, in particular for the purpose of clarifying the facts and assessing the legal consequences.

5. Technical implementation and security of your data

The whistleblower system includes a possibility for anonymous communication via an encrypted (TLS) connection (between client (browser) and server). All data in the database is encrypted in addition to the client-side end-to-end encryption of the tip data before writing it to the storage medium in accordance with the current state of the art.

In accordance with the technical necessity of network connections on the Internet, the IP addresses are only recorded temporarily and then deleted. Pseudonym/user name and password are automatically generated dynamically by the system after a notice has been submitted. The access data is only valid for accessing the mailbox of this one case, for example, to retrieve feedback from the responsible persons or to submit additional information. No access data is required to submit a report - it is generated after the report is submitted and displayed to the person submitting the report.

For the secure and reliable provision of the service of the whistleblower system, product kitchen GmbH uses order processors based in a member state of the European Union in compliance with the applicable data protection regulations, in particular the GDPR. The encrypted whistleblower data is processed in European and certified data centres. Due to the end-to-end encryption of the whistleblowing data between the whistleblower and the case handler, there is no other access to the plain text of the report.

Compliance with the applicable data protection regulations is ensured by appropriate technical and organisational measures.

6. How long will my data be stored?

Your personal data will be stored for a period of time resulting from the need to process, clarify and document the facts (resulting from your tip) and then deleted after 24 months following the conclusion of the case. Something else applies if applicable legal provisions require otherwise (e.g. in connection with pending court proceedings), in which case corresponding procedural files are generally retained for 10 years.

7. Is data transferred to a third country or to an international organisation?

As a matter of principle, we do not transfer your data to countries outside the European Economic Area - EEA (third countries).

8. What other data protection rights do I have?

You have the right to information (Art. 15 GDPR, § 34 BDSG), to correction (Art. 16 GDPR), to deletion (Art.

17 GDPR, § 35 BDSG), to restriction of processing (Art. 18 GDPR) and to data portability (Art. 20 GDPR) under the respective legal conditions. You also have the right to lodge a complaint with a data protection supervisory authority (Art. 77 GDPR in conjunction with § 19 BDSG).

Should you make use of your above-mentioned rights, the responsible department will check whether the legal requirements for this are met.

9. Right of appeal to a supervisory authority

Every data subject has the right to lodge a complaint with a data protection supervisory authority if he or she considers that the processing of data concerning him or her infringes data protection law (Art. 77 of the GDPR). The complaint to the supervisory authority can be made informally. The following supervisory authority for data protection is responsible for STI Group and the group companies:

HBDI - The Hessian Commissioner for Data Protection and Freedom of Information
Gustav-Stresemann-Ring 1
65189 Wiesbaden

Phone: 0611-1408 0

Website: <https://datenschutz.hessen.de/>

E-mail: poststelle@datenschutz.hessen.de