

salvagnini

**DATENSCHUTZINFORMATIONEN
GEMÄSS ART. 13-14 DSGVO**





Dieses Dokument enthält die gemäß Artikel 13 und 14 der EU-Verordnung 679/2016 (DSGVO) erforderlichen Informationen in Bezug auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die aus verschiedenen Gründen an der Meldung erheblicher Verstöße gemäß dem Whistleblower-Verfahren beteiligt sind die Salvagnini-Gruppe.

Inhaber der Verarbeitung personenbezogener Daten

Der für die Datenverarbeitung Verantwortliche ist:

- SALVAGNINI ITALIA SPA, mit Sitz in Via Ingegnere Guido Salvagnini, 51, 36040 Sarego (VI) – ITALIEN
- SALVAGNINI MACHINENBAU SPA, mit Sitz in Dr. Guido Salvagnini-Straße 1, 4482 Ennsdorf, LG. St. Pölten – ÖSTERREICH (insbesondere ist jedes Unternehmen der Datenverantwortliche für die Daten im Zusammenhang mit Berichten über seine Organisation).

Miteigentum

Die eingegangenen Berichte werden über einen zentralen Dienst im SaaS-Modus verwaltet und von SALVAGNINI ITALIA bereitgestellt, auch im Namen der anderen Tochtergesellschaften der Salvagnini-Gruppe. Dieser Dienst umfasst die Verarbeitung von Daten, die zwischen den Tochtergesellschaften und der SALVAGNINI ITALIA SPA geteilt werden, unter Anwendung einer gemeinsamen Verantwortlichkeitsregelung zwischen ihnen gemäß Art. 26 DSGVO. Weitere Einzelheiten zu den Bedingungen der Miteigentumsvereinbarung finden Sie im Whistleblowing-Verfahren der Gruppe, das auf der Website www.salvagninigroup.com im Abschnitt Whistleblowing eingesehen werden kann.



Persönliche Daten und freiwilliger Beitrag

Grundsätzlich kann das Whistleblowing-System **ohne Angabe** eigener oder fremder **personenbezogener Daten** genutzt werden. Im Rahmen des Meldeverfahrens können Sie jedoch **freiwillig** personenbezogene Daten preisgeben, insbesondere Angaben zu Ihrer Identität, Ihrem Vor- und Nachnamen, Ihrem Wohnsitzland, Ihrer Telefonnummer oder E-Mail-Adresse.

In der Regel **erfragen oder verarbeiten wir keine besonderen Kategorien personenbezogener Daten, z. B.** über die rassische und/oder ethnische Herkunft, religiöse und/oder philosophische Überzeugungen, die Mitgliedschaft in einer Gewerkschaft oder die sexuelle Orientierung oder das Leben. Aufgrund von Freitextfeldern im Anmeldeformular können solche besonderen Kategorien personenbezogener Daten jedoch von Ihnen freiwillig angegeben werden, wenn Sie dies für erforderlich halten.

Der Bericht kann auch **personenbezogene Daten von Dritten** enthalten.

Die Personen, auf die sich die verarbeiteten personenbezogenen Daten beziehen, sind

1. Personen, die Kenntnis von dem gemeldeten Sachverhalt haben oder die in jedem Fall nach einer Meldung um Auskunft gebeten werden
2. „beteiligte Personen“ (d. h. diejenigen, die für den Verstoß, den Gegenstand der Meldung sind, verantwortlich gemacht werden)
3. „geschützte Personen“ (d. h. diejenigen, die den obligatorischen Schutz genießen, der in der Whistleblower-Gesetzgebung in Bezug auf eine Meldung vorgesehen ist),
4. natürliche Fallmanager-Personen
5. andere Personen, die aus verschiedenen Gründen auf die Existenz aufmerksam gemacht werden und ihnen folgen können -Up-Up des Berichts

Zu den verarbeiteten Daten können gerichtlich oder verwaltungsbehördlich strafbare Daten und Unterlassungen gehören, insbesondere auch bei Verdacht auf die Begehung einer Straftat, bei strafrechtlicher Verurteilung oder bei vorbeugenden Maßnahmen gemäß Art. 10 DSGVO. Diese Daten gemäß Art. 10 DSGVO dürfen nur bei zwingender Notwendigkeit verarbeitet werden, werden schriftlich dokumentiert und nur im unbedingt erforderlichen Umfang aufbewahrt, nachdem die Entscheidung über die Straftat in einem Verfahren, in dem sie verarbeitet wurden, rechtskräftig geworden ist; Die Lagerung erfolgt möglichst ohne Wiederaufbereitung.

Die Angabe Ihrer persönlichen Daten ist **fakultativ**, so dass die Nichtbereitstellung dieser Daten Ihr Recht auf Rückmeldung nach der Übermittlung Ihres Berichts und, falls Sie Ihre Identität offengelegt haben, auf den gesetzlich vorgesehenen Schutz nicht beeinträchtigt.



Melder, die personenbezogene Daten ihres Wissens über das für die Weiterverfolgung der Meldung erforderliche Maß hinaus verarbeiten, übernehmen die Rolle des Datenverantwortlichen im Sinne von Art. 4 Nr. 7 DSGVO.

Weitergabe von personenbezogenen Daten

Der für die Verarbeitung Verantwortliche kann die Daten unter Wahrung der **Vertraulichkeit der** Identität des Meldenden und unter Beachtung des Grundsatzes der strikten Notwendigkeit, der Verhältnismäßigkeit und der Minimierung an folgende Stellen **weitergeben**

- 1** **Andere interne Funktionen des Inhabers, deren** Einbeziehung in die Untersuchung einer Meldung die Fallmanager des Inhabers für angemessen halten.
- 2** **Case Manager**, d. h. die von dem empfangenden Unternehmen benannten internen oder externen Stellen, die die Meldung aufnehmen und/oder in der Sache prüfen und/oder Folgemaßnahmen ergreifen, einschließlich der Rückmeldung an den Meldenden.
- 3** **Dritte, die ausdrücklich als externe** Datenverarbeiter für die Zwecke des Hostings, der Wartung oder der technischen Verwaltung des Rechenzentrums und der Online-Plattform, die von Ihnen zur Durchführung der Berichterstattung verwendet wird, sowie der zugehörigen Datenbank **benannt werden**.
- 4** **Zuständige externe Behörden gemäß den** geltenden Vorschriften (z. B. Justizbehörden, Polizeibehörden, Finanzpolizei, ANAC - Nationale Anti-Korruptionsbehörde usw.).
- 5** **Anwaltskanzleien und/oder Rechtsberater, Corporate-Compliance-Berater und/oder andere Personen, die an der Bewertung der Meldung beteiligt sind** (z. B. Sachverständige, technische Berater, andere Unternehmen unserer Gruppe, bei denen die Untersuchung und Entscheidungsfindung bei Meldungen zentralisiert ist oder die in irgendeiner Weise an einem gemeldeten Verstoß beteiligt sind).



Technische Umsetzung und Sicherheit Ihrer Daten

Der Online-Meldekanal enthält eine Option für die anonyme Kommunikation über eine verschlüsselte Verbindung. Bei der Nutzung des Deliktmeldesystems werden die IP-Adresse und die Geolokalisierung des von Ihnen verwendeten Geräts (PC, Tablet, Smartphone) zu keinem Zeitpunkt gespeichert. Wir empfehlen Ihnen, sich nach Möglichkeit **nicht von einem Firmengerät aus mit dem Meldesystem zu verbinden**. Bei der Übermittlung Ihrer Meldung müssen Sie ein Passwort für den Zugang zu einem sicheren Posteingang erstellen, damit Sie anschließend auf geschützte Weise mit uns kommunizieren können. **Es ist Ihre Pflicht, die Vertraulichkeit sowohl des Identifikationscodes Ihrer Meldung (der Ihnen von unserem System mitgeteilt wird) als auch des Passworts für den Zugang zum sicheren Posteingang angemessen zu schützen**. Wir treffen geeignete technische und organisatorische Maßnahmen, um den Datenschutz und die Vertraulichkeit zu gewährleisten. Der verwendete Internet-Kommunikationskanal ist mit fortschrittlichen Protokollen verschlüsselt. Die Daten werden in einem ISO 27001-zertifiziertem Rechenzentrum in Deutschland oder der Schweiz in verschlüsseltem Format gespeichert.

Personenbezogene Daten, die für die Bearbeitung einer Meldung nicht erforderlich sind, werden nicht erfasst bzw. bei unbeabsichtigter Erhebung unverzüglich gelöscht.

Die Verarbeitung personenbezogener Daten ist rechtmäßig, soweit sie einem öffentlichen Interesse zum Zwecke der Verhinderung oder Ahndung von Rechtsverstößen und in diesem Zusammenhang der Auskunftserteilung und Überprüfung der Rechtslage entspricht.

Zu den oben beschriebenen Zwecken können die Hinweisgeber eine Verarbeitung personenbezogener Daten vornehmen, soweit die für ihre Meldung erforderlichen Daten erforderlich sind.

Extra-EWR-Datenübermittlung

Jegliche Datenübermittlung in Länder außerhalb des EWR-Raums beschränkt sich auf die Nutzung eines individuellen Produktivitäts-Cloud-Dienstes, der auf Rechenzentren in den USA basiert (z. B. Microsoft Office 365), und wird durch i) die Vereinbarung von Standardvertragsklauseln zwischen unserem Unternehmen und dem Drittanbieter gemäß dem von der EU-Kommission genehmigten Modell und/oder ii) die Bestimmungen des zwischen der EU und den USA abgeschlossenen bilateralen Abkommens namens "Trans-Atlantic Data Protection" gewährleistet. unser Unternehmen und der Drittanbieter Standardvertragsklauseln nach dem von der EU-Kommission genehmigten Muster und/oder ii) die Bestimmungen des zwischen der EU und den USA geschlossenen bilateralen Abkommens mit der Bezeichnung "Trans-Atlantic Data Protection Framework" und/oder einen Angemessenheitsbeschluss



der EU-Kommission über die Datenschutzgesetzgebung der USA (ab dessen Inkrafttreten). Im Falle einer Datenübermittlung in die Schweiz ist die Garantie für die Übermittlung der Angemessenheitsbeschluss der EU-Kommission über die Schweizer Datenschutzgesetze.

Die Daten können an die Tochtergesellschaften, die die Datenverantwortlichen sind (oder an andere von ihnen autorisierte Personen) mit Sitz in den USA, in Brasilien und in Mexiko, durch das Unternehmen SALVAGNINI ITALIA SPA als Leiter der Datenverarbeitung übermittelt werden im Namen der Datenverantwortlichen selbst auf der Grundlage eines Vertrags zur Beauftragung zentraler Verwaltungsdienste für den Lebenszyklus von Meldungen über Verstöße im Zusammenhang mit diesen Datenverantwortlichen, indem der Zugriff auf dieselben Daten bereitgestellt wird. über den Saas Integrity Line-Dienst. In diesem Fall beschränkt sich die Übermittlung von Zeit zu Zeit auf die Daten zu den Berichten, die sich auf die einzelne Tochtergesellschaft beziehen, und wird durch die Garantie unterstützt, die darin besteht, dass zwischen den Parteien Standardvertragsklauseln vereinbart werden, die dem von genehmigten Muster entsprechen der EU-Kommission.

Die Daten werden **nicht weitergegeben**, es sei denn, das nationale Recht oder das Recht der Europäischen Union sieht dies ausdrücklich vor.

Zweck und Rechtsgrundlage

Die Daten werden zu folgenden Zwecken verarbeitet:

1. Beurteilung der Zulässigkeit und Begründetheit der von Ihnen übermittelten Meldung
2. Durchführung von Maßnahmen zum Schutz und zur Unterstützung der durch die Whistleblowing-Gesetzgebung geschützten Personen
3. Verfolgen Sie den Bericht weiter und ergreifen Sie, wenn möglich, Maßnahmen, um auf die Ergebnisse eines Berichts zu reagieren
4. Durchführung von Disziplinarmaßnahmen gegen den Hinweisgeber, der den Verstoß vorsätzlich oder grob fahrlässig gemeldet hat, oder gegen beteiligte Personen, die für den gemeldeten Verstoß verantwortlich sind
5. Die Ergebnisse von Berichten als Beweismittel in Gerichtsverfahren verwenden



Weitere Einzelheiten zu den Rechtsgrundlagen

Im Einzelfall ist die vorherige Zustimmung des Hinweisgebers erforderlich, insbesondere:

- Für den Fall, dass die Weiterverfolgung der Meldung seitens des Verantwortlichen die Einleitung eines Disziplinarverfahrens erfordert und die Streitigkeit ganz oder teilweise auf der erhaltenen Meldung beruht und die Kenntnis der Identität der meldenden Person für die Verteidigung des Angeklagten unerlässlich ist, kann diese Meldung für die Zwecke des Disziplinarverfahrens nur dann verwendet werden, wenn die ausdrückliche Einwilligung der meldenden Person zur Offenlegung ihrer Identität vorliegt;
- wenn die Meldung über eine registrierte Telefonleitung oder ein anderes registriertes Sprachnachrichtensystem erfolgt, um dem beauftragten Personal die entsprechende Dokumentation durch Aufzeichnung auf einem zum Speichern und Abhören geeigneten Gerät oder mittels einer vollständigen Transkription zu ermöglichen. Im Falle einer Niederschrift kann der Hinweisgeber durch seine Unterschrift den Inhalt der Niederschrift überprüfen, berichtigen oder bestätigen;
- wenn die Meldung auf Wunsch des Hinweisgebers mündlich im Rahmen einer Besprechung mit dem verantwortlichen Personal erfolgt, wobei die Meldung mit vorheriger Zustimmung des Hinweisgebers vom verantwortlichen Personal durch Aufzeichnung auf einem zum Speichern und Abhören geeigneten Gerät oder durch einen Bericht dokumentiert wird. Bei Protokollen kann der Hinweisgeber das Sitzungsprotokoll durch seine Unterschrift prüfen, korrigieren und bestätigen.

In Bezug auf disziplinarische Zwecke ist die Rechtsgrundlage das berechtigte Interesse des für die Verarbeitung Verantwortlichen an der Verfolgung von Verstößen gegen das Whistleblowing-Verfahren des für die Verarbeitung Verantwortlichen und/oder allgemeiner gegen die Rechtsvorschriften über Whistleblowing in Disziplinarverfahren.

Haltbarkeitsdauer

Personenbezogene Daten, die der für die Verarbeitung Verantwortlichen erhalten hat, die aber für die Bewertung des Berichts nicht unbedingt erforderlich sind, werden unverzüglich gelöscht.

Die Meldedaten und die zugehörigen Unterlagen werden so lange aufbewahrt, wie es für die Bearbeitung des Berichts erforderlich ist, spätestens jedoch 5 (fünf) Jahre (in Italien), or 2 (zwei) Jahre (in Österreich), ab dem Datum der Mitteilung des endgültigen Ergebnisses des Meldeverfahrens, vorbehaltlich der Verpflichtung zur Vertraulichkeit der Informationen sowie der Begrenzung der Aufbewahrung, wie in den geltenden Vorschriften vorgesehen, und darüber hinaus so lange, wie es für den Abschluss eines bereits eingeleiteten Verwaltungs- oder Gerichtsverfahrens oder eines Ermittlungsverfahrens nach der Strafprozessordnung erforderlich ist.



Rechte

Die meldende Person kann sich jederzeit ohne jegliche Formalitäten an den für die Verarbeitung Verantwortlichen wenden, um die folgenden Rechte auszuüben: a) Zugang zu den Daten, b) Berichtigung der Daten, wenn sie unrichtig sind, c) Aktualisierung der Daten, wenn sie veraltet sind, d) Antrag auf Löschung der Daten, e) Antrag auf Einschränkung der Datenverarbeitung, f) jederzeit Widerspruch gegen die Verarbeitung der Daten aus Gründen, die sich aus ihrer besonderen Situation ergeben, g) Benachrichtigung über eine Datenschutzverletzung zu erhalten, wenn diese ein hohes Risiko für die Grundrechte oder Grundfreiheiten der betroffenen Parteien darstellt, h) (hat der Hinweisgeber seine Identität preisgegeben oder ist dies im Falle einer anonymen Meldung auch ohne Offenlegung seiner Identität möglich) den Text einer Meldung, die anschließend vom Datenverantwortlichen transkribiert wurde, prüft, korrigiert und genehmigt in einer Form eingehen, die nicht der Verwendung einer Schriftform bedarf (z. B. durch persönliches Treffen, Telefongespräch oder andere nicht aufgezeichnete mündliche Form, gewöhnlicher Brief). Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der bis zum Widerruf erfolgten Verarbeitung und Kommunikation nicht berührt.

Nachdem wir einen Nachweis Ihrer Identität angefordert haben (es sei denn, Sie haben beschlossen, anonym zu bleiben), werden wir Ihren Antrag auf Ausübung Ihrer Rechte innerhalb von 30 Tagen nach Eingang der Meldung bestätigen, es sei denn, eine besondere Untersuchung ist erforderlich; in diesem Fall werden wir Ihnen eine Mitteilung zukommen lassen.

Solange und soweit es erforderlich ist, um die Identität eines Hinweisgebers, eines anderen geschützten Subjekts im Sinne der geltenden Gesetzgebung oder von Personen, die an einer Folgemaßnahme interessiert sind (z. B. Fallmanager, Personen, die über den gemeldeten Sachverhalt informiert sind, zu schützen).) und zur Erreichung der Zwecke der Verhinderung und Ahndung von Verstößen, insbesondere zur Verhinderung von Versuchen zur Verhinderung, Beeinträchtigung oder Verzögerung der Informationen oder Folgehandlungen auf der Grundlage der Informationen, insbesondere für die Dauer eines behördlichen oder gerichtlichen Verfahrens oder eines Vorverfahrens gemäß Nach der Strafprozessordnung gelten folgende Rechte einer natürlichen Person nicht:

- Recht auf Auskunft, Recht auf Berichtigung, Recht auf Löschung, Recht auf Einschränkung der Verarbeitung, Recht auf Widerspruch, Recht auf Meldung einer Verletzung des Schutzes personenbezogener Daten.

Daher wird der Datenverantwortliche bei Eintritt der oben genannten Bedingungen davon absehen, Informationen an eine von einer Meldung betroffene Person weiterzugeben.

Wenn der Meldende der Ansicht ist, dass die oben genannten Rechte verletzt wurden, kann er jederzeit eine Beschwerde bei der zuständigen Aufsichtsbehörde einreichen.

In Italien ist die Aufsichtsbehörde die Garante per la protezione dei dati personali mit Sitz in Piazza Venezia, 11 - 00187 Roma (Italien), PEC: protocollo@pec.gpdp.it.

