Whistleblowing-System / Make It Right Global Hotline

This document provides information on the OSI Group Whistleblowing System, the *Make It Right Global Hotline,* the processing of reports of potential grievances in the OSI Group and its associated supply chains under the OSI Group Whistleblowing System in accordance with Directive (EU) 2019/1937 on the protection of persons reporting breaches of Union law and on compliance with Member State law implementing the Directive and in accordance with the German Supply Chain Due Diligence Act. The information contained herein is available in all Member State languages. Please refer to the published information and your Data Subject Rights (GDPR) in your local language below.

Document Owner: Heiko Maniero.

Version: 1.00
Classification: Public
Approved by: Heiko Maniero, Anne-Sophie Konrad, Christian Franz, Robert Bridge.
Information Contained: Business Data
Date: 2023-12-15

Table of Contents

GERMAN: Hinweisgebersystem (interne Meldestelle)

Unsere Werte bilden das Fundament für unsere Geschäftspraktiken und reflektieren unser Engagement für Integrität, Transparenz und eine positive Unternehmenskultur. Unser Hinweisgebersystem ist ein essenzielles Instrument zur Förderung von Verantwortungsbewusstsein und zur Gewährleistung eines ethischen Geschäftsbetriebs. Diese Verfahrensordnung dient dazu, den Ablauf und die Prinzipien unserer Untersuchungsprozesse transparent zu gestalten und sicherzustellen, dass alle Hinweise, die über unser System eingehen, angemessen und professionell behandelt werden.

OSI setzt sich für einen offenen Dialog ein und erkennt die Bedeutung von Hinweisgebern als wichtige Partner in unserem Bestreben an, höchste Standards in allen Bereichen unseres Unternehmens zu wahren.

I. Verfahrensordnung für das Hinweisgebersystem von OSI

I. Zweck und Geltungsbereich:

1. Zweck: Diese Verfahrensordnung regelt die Handhabung und Untersuchung von Hinweisen, die über das Hinweisgebersystem Make It Right Global Hotline eingehen. Ziel ist es, sicherzustellen, dass alle erhaltenen Hinweise transparent, effizient und gemäß den ethischen Standards der OSI bearbeitet werden.

2. Geltungsbereich: Diese Verfahrensordnung gilt für alle Mitarbeitenden, Geschäftspartner, Lieferanten und sonstigen Stakeholder in der gesamten Wertschöpfungskette, die das Hinweisgebersystem nutzen, um konkrete Anhaltspunkte zu einem möglichen Fehlverhalten, Bedenken oder Hinweise zu teilen. Das Hinweisgebersystem ist nicht zur Bearbeitung von Produkt- und dienstleistungsbezogenen Anliegen vorgesehen. Derartige Fragen oder Themen können direkt über das Kontaktformular auf der Unternehmenswebseite adressiert werden.

II. Einreichung von Hinweisen:

1. Anonymität und Vertraulichkeit:

Das Hinweisgebersystem ermöglicht unter anderem die anonyme Übermittlung von Hinweisen, soweit dies die nationalen Gesetze zulassen.

Alle Informationen, die im Rahmen des Hinweisgebersystems behandelt werden, unterliegen strenger Vertraulichkeit.

2. Hinweisarten:

Das System ermöglicht die Abgabe von Hinweisen, soweit konkrete Anhaltspunkte zu einem möglichen Fehlverhalten, Bedenken oder Hinweise dazu bestehen. Dies betrifft Verstöße von Mitarbeitern oder Geschäftspartnern gegen geltende Gesetze, Verordnungen etc. (insbesondere die in § 2 des Hinweisgeberschutzgesetzes oder der EU-Richtlinie 2019/1937 genannten) oder unternehmensinterne Regelungen (insbesondere Verstöße gegen den Code of Conduct) oder menschenrechtliche und ökologische Risiken, die auf direkte oder indirekte Lieferanten zurückzuführen sind, sowie Verstöße gegen menschenrechtliche und ökologische Verpflichtungen nach dem Lieferketten-Sorgfaltspflichtgesetz (LkSG). Darunter fallen unter anderem Verstöße gegen den OSI Supplier Code of Conduct, Kartellrecht, Korruption, Diebstahl, Diskriminierung, Missachtung von Sicherheit und Gesundheitsschutz am Arbeitsplatz, Kinderarbeit, Boden-, Wasser- oder Luftverschmutzung, schädliche Lärmemissionen, inakzeptabler Wasserverbrauch, Herstellung oder Verwendung bestimmter langlebiger organischer Schadstoffe sowie die unerlaubte Ein- und Ausfuhr von Abfällen.

3. Zugang zum System:

Hinweisgebende haben in verschiedenen Sprachen Zugang zum extern betreuten Meldesystem unter:

EthicsPoint - OSI Group, LLC

- in Textform über ein Formular im Onlineportal oder
- telefonisch (aus verschiedenen Ländern gebührenfrei erreichbar)

III. Bearbeitung von Hinweisen:

1. Eingang und Erstbewertung:

Nach Eingang einer Mitteilung über die vom Hinweisgebersystem betreuten externen Meldekanäle wird diese zunächst dokumentiert und mit einem individuellen Aktenzeichen versehen. Die OSI Compliance Abteilung nimmt alle Hinweise entgegen und führt eine Erstbewertung durch, um die Plausibilität und Stichhaltigkeit zu bestimmen.

2. Untersuchung:

Bei relevanten Hinweisen wird eine gründliche, objektive und vertrauliche Untersuchung eingeleitet. Sofern dies für die Bearbeitung von Meldungen oder für das Ergreifen von Maßnahmen notwendig ist, werden andere Abteilungen hinzugezogen oder diese um Unterstützung gebeten. Außerdem können zusätzliche Informationen von der hinweisgebenden Person angefordert werden.

Die Dauer einer Untersuchung bis zu ihrem Abschluss hängt von der Komplexität des Falles, den erforderlichen Untersuchungsmaßnahmen und der Verfügbarkeit von Informationen oder betroffenen

Parteien im Einzelfall ab. Es werden alle Anstrengungen unternommen, um die Untersuchung so effizient und zügig wie möglich abzuschließen.

3. Rückmeldung an den Hinweisgeber:

Der Hinweisgeber erhält innerhalb von 7 Tagen, soweit möglich und ohne die Anonymität zu gefährden, eine Rückmeldung über den Eingang seines Hinweises.

Wenn die hinweisgebende Person den Hinweis online oder telefonisch eingereicht hat, erhält sie Anmeldeinformationen, die es ihr ermöglichen, die Meldung weiterzuverfolgen und anonymes Feedback zu erhalten (wenn sie dies wünscht). Insbesondere kann das Stellen von Verständnisfragen und die Einholung weiterer Informationen notwendig sein.

Im weiteren Verlauf (spätestens 3 Monate nach Erhalt der Eingangsbestätigung) wird zum Stand der Untersuchung über geplante bzw. bereits eingeleitete Maßnahmen oder ggf. mangels hinreichenden Verdachtes über eine Einstellung informiert.

IV. Schutz von Hinweisgebern:

1. Non-Retaliation:

OSI unternimmt alle zumutbaren Anstrengungen, dass Hinweisgeber vor jeglicher Form der Vergeltung, Benachteiligung oder sonstigen Repressalien geschützt werden.

Disziplinarmaßnahmen aufgrund der Abgabe von Hinweisen gegen Personen, die nach bestem Wissen und Gewissen an Untersuchungen mitwirken, sind untersagt und werden nicht geduldet.

2. Vertraulichkeit wahren:

Personen, die an der Untersuchung beteiligt sind, sind zur strengen Vertraulichkeit verpflichtet.

V. Dokumentation und Aufbewahrung:

1. Dokumentation:

Alle Schritte der Untersuchung werden sorgfältig dokumentiert.

Die Dokumentation dient der Transparenz und Nachvollziehbarkeit des Verfahrens.

2. Aufbewahrungsfrist:

Die Unterlagen werden gemäß den gesetzlichen Vorgaben und internen Richtlinien aufbewahrt.

VI. Überprüfung und Anpassung:

Diese Verfahrensordnung wird regelmäßig überprüft und bei Bedarf angepasst, um sicherzustellen, dass sie den aktuellen gesetzlichen Anforderungen und den Unternehmenszielen entspricht.

II. Aufklärung gemäß Art. 13 DS-GVO (für hinweisgebende Personen):

Name und Kontaktdaten des Verantwortlichen: Siehe Impressum auf der Webseite. Kontaktdaten des Datenschutzbeauftragten und gegebenenfalls des Vertreters: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 München. Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung: Einhaltung des Hinweisgeberschutzgesetzes (HinSchG) und des Lieferkettensorgfaltspflichtengesetzes (LkSG), Rechtsgrundlage ist Art. 6 (1) (c) DS-GVO i.V.m. §§ 8, 9 LkSG und § 10 HinSchG, soweit dies zur Erfüllung der in §§ 13 und 24 HinSchG bezeichneten Aufgaben erforderlich ist, sowie die Einhaltung der Richtlinie (EU) 2019/1937 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden und das daraus resultierende nationale Recht der Mitgliedsstaaten sowie die Einhaltung von geltenden Rechtsvorschriften aus anderen Ländern. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten: Strafverfolgungsbehörden, Bußgeldstellen und sonstige Behörden sowie Rechtsanwälte, Gruppenunternehmen oder Arbeitgeber. Geplante Übermittlung an Drittländer: Eingabe in das Online-System von Navex sowie Weiterübermittlung an Stellen innerhalb der Unternehmensgruppe, Arbeitgeber oder Rechtsanwälte. Ein EU-Standardvertrag und das UK-Addendum zum EU-Standardvertrag wurden mit Navex abgeschlossen. Ferner ist Navex Mitglied im EU-U.S. Data Privacy Framework, im Swiss-U.S. Data Privacy Framework und in der UK Extension to the EU-U.S. Data Privacy Framework. Für andere Übermittlungen kann es an einem Angemessenheitsbeschluss fehlen. Für solche Datenübermittlungen werden die EU Standardvertragsklauseln abgeschlossen. Kriterien für die Festlegung der Speicherdauer: Die Dokumentation wird drei Jahre nach Abschluss des Verfahrens gelöscht. Die Dokumentation kann länger aufbewahrt werden, um die Anforderungen der geltenden Rechtsvorschriften zu erfüllen, solange dies erforderlich und verhältnismäßig ist.

Nach der Datenschutzgrundverordnung besteht ein Recht auf Auskunft über die Sie betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder ein Widerspruchsrecht gegen die Verarbeitung sowie das Recht auf Datenübertragbarkeit. Sie haben das Recht sich bei der zuständigen Datenschutz-Aufsichtsbehörde mit Bezug auf die Verarbeitung zu beschweren. Die Bereitstellung von personenbezogenen Daten ist weder gesetzlich noch vertraglich vorgeschrieben und auch nicht für einen Vertragsabschluss erforderlich, weshalb Sie nicht verpflichtet sind, der Meldestelle personenbezogene Daten bereitzustellen. Mögliche Folgen der Nichtbereitstellung sind, dass die Meldung nicht oder verzögert bearbeitet wird, oder dass

sie verworfen wird, und dass Ihnen keine Informationen oder Auskünfte in Bezug auf die Meldung erteilt werden können. Es besteht keine automatisierte Entscheidungsfindung.

III. Aufklärung gemäß Art. 14 DS-GVO (für andere betroffene Personen):

Name und Kontaktdaten des Verantwortlichen: Siehe Impressum auf der Webseite. Kontaktdaten des Datenschutzbeauftragten und gegebenenfalls des Vertreters: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 München. Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung: Einhaltung des Hinweisgeberschutzgesetzes (HinSchG) und des Lieferkettensorgfaltspflichtengesetzes (LkSG), Rechtsgrundlage ist Art. 6 (1) (c) DS-GVO i.V.m. §§ 8, 9 LkSG und § 10 HinSchG, soweit dies zur Erfüllung der in §§ 13 und 24 HinSchG bezeichneten Aufgaben erforderlich ist, sowie die Einhaltung der Richtlinie (EU) 2019/1937 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden und das daraus resultierende nationale Recht der Mitgliedsstaaten sowie die Einhaltung von geltenden Rechtsvorschriften aus anderen Ländern. Kategorien personenbezogener Daten, die verarbeitet werden: Hinweisdaten. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten: Strafverfolgungsbehörden, Bußgeldstellen und sonstige Behörden sowie Rechtsanwälte, Gruppenunternehmen oder Arbeitgeber. Geplante Übermittlung an Drittländer: Eingabe in das Online-System von Navex sowie Weiterübermittlung an Stellen innerhalb der Unternehmensgruppe, Arbeitgeber oder Rechtsanwälte. Ein EU-Standardvertrag und das UK-Addendum zum EU-Standardvertrag wurden mit Navex abgeschlossen. Ferner ist Navex Mitglied im EU-U.S. Data Privacy Framework, im Swiss-U.S. Data Privacy Framework und in der UK Extension to the EU-U.S. Data Privacy Framework. Für andere Übermittlungen kann es an einem Angemessenheitsbeschluss fehlen. Für solche Datenübermittlungen werden die EU Standardvertragsklauseln abgeschlossen. Kriterien für die Festlegung der Speicherdauer: Die Dokumentation wird drei Jahre nach Abschluss des Verfahrens gelöscht. Die Dokumentation kann länger aufbewahrt werden, um die Anforderungen der geltenden Rechtsvorschriften zu erfüllen, solange dies erforderlich und verhältnismäßig ist. Die Quelle der personenbezogenen Daten ist die hinweisgebende Person und/oder das betroffene Unternehmen.

Nach der Datenschutzgrundverordnung besteht gegebenenfalls ein Recht auf Auskunft über die Sie betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder ein Widerspruchsrecht gegen die Verarbeitung sowie das Recht auf Datenübertragbarkeit. Sie haben das Recht sich bei der zuständigen Datenschutz-Aufsichtsbehörde mit Bezug auf die Verarbeitung zu beschweren. Es besteht keine automatisierte Entscheidungsfindung. Die Erteilung weiterer Informationen erweist sich als unmöglich.

ENGLISH: Whistleblower system (internal reporting channels)

Our values form the foundation for our business practices and reflect our commitment to integrity, transparency, and a positive corporate culture. Our whistleblowing system is an essential tool for promoting accountability and ensuring ethical business operations. These rules of procedure serve to make the process and principles of our investigation processes transparent and ensure that all reports received through our system are handled appropriately and professionally.

OSI is committed to open dialogue and recognizes the importance of whistleblowers as key partners in our efforts to maintain the highest standards in all areas of our business.

I. Rules of Procedure for the OSI Whistleblower System

I. Purpose and scope:

1. Purpose: These Rules of Procedure govern the handling and investigation of reports received through the Make It Right Global Hotline whistleblowing system. The aim is to ensure that all reports received are handled transparently, efficiently and in accordance with OSI's ethical standards.

2. Scope of application: These rules of procedure apply to all employees, business partners, suppliers and other stakeholders throughout the value chain who use the whistleblower system to share specific indications of possible misconduct, concerns, or tips. The whistleblower system is not intended for processing product and service-related concerns. Such questions or issues can be addressed directly via the contact form on the company website.

II. Submission of information:

1. Anonymity and Confidentiality:

The whistleblower system allows, among other things, for the anonymous submission of whistleblowing reports, to the extent permitted by national laws.

All information handled within the framework of the whistleblower system is subject to strict confidentiality.

2. Types of reports:

The system enables whistleblowers to submit reports where there are concrete indications of possible misconduct, concerns, or indications of such. This concerns violations by employees or business partners of applicable laws, regulations etc. (in particular those mentioned in Section 2 of the Whistleblower Protection Act or EU Directive 2019/1937) or internal company regulations (in particular violations of the Code of Conduct) or human rights and environmental risks attributable to direct or indirect suppliers as well as violations of human rights and environmental obligations under the Supply

Chain Due Diligence Act (LkSG). These include violations of the OSI Code of Conduct, antitrust law, corruption, theft, discrimination, disregard for occupational health and safety, child labor, soil, water or air pollution, harmful noise emissions, unacceptable water consumption, the production or use of certain persistent organic pollutants and the unauthorized import and export of waste.

3. Access to the system:

Whistleblowers have access to the externally managed reporting system in different languages at:

EthicsPoint - OSI Group, LLC

- in text form via a form in the online portal or
- by telephone (toll-free from various countries)

III. Processing of reports:

1. Receipt and Initial Assessment:

Once a report is received via the external reporting channels managed by the whistleblower system, it is first documented and assigned an individual file number. OSI Compliance receives all reports and carries out an initial assessment to determine their plausibility and validity.

2. Investigation:

A thorough, objective, and confidential investigation will be initiated for relevant tips. If necessary to receive reports or take action, other departments will be consulted or asked for assistance. Additional information may also be requested from the whistleblower.

The duration of an investigation until its conclusion depends on the complexity of the case, the investigative measures required, and the availability of information or parties involved in the individual case. Every effort will be made to complete the investigation as efficiently and expeditiously as possible.

3. Feedback to the Whistleblower:

The whistleblower will receive feedback on the receipt of their tip within 7 days, where possible and without jeopardizing anonymity.

If the whistleblower has submitted the report online or by telephone, they will receive login information that enables them to follow up on the report and receive anonymous feedback (if they wish). In particular, it may be necessary to ask comprehension questions and obtain further information.

In the further course of the investigation (no later than 3 months after receipt of the confirmation of receipt), information will be provided on the status of the investigation regarding planned or already initiated measures or, if there is insufficient suspicion, on the discontinuation of the investigation.

IV. Protection of Whistleblowers:

1. Non-Retaliation:

OSI undertakes all reasonable efforts to ensure that whistleblowers will be protected from any form of retaliation, disadvantage, or other reprisals.

Disciplinary action based on whistleblowing against individuals who cooperate in good faith with investigations is prohibited and will not be tolerated.

2. Confidentiality:

Persons involved in the investigation are bound to strict confidentiality.

V. Documentation and storage:

1. Documentation:

All steps of the investigation are carefully documented.

The documentation serves the transparency and traceability of the procedure.

2. Retention period:

Documentation is retained in accordance with legal requirements and internal guidelines.

VI. Review and adjustment:

These procedural rules are regularly reviewed and adapted as necessary to ensure that they comply with current legal requirements and corporate objectives.

II. Information pursuant to Art. 13 GDPR (for persons providing information):

Name and contact details of the controller: See imprint on the website. Contact details of the data protection officer and, if applicable, the representative: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Munich, Germany. Purposes for which the personal data are to be processed and the legal basis for the processing: Compliance with the Whistleblower Protection Act (HinSchG) and the Supply Chain Due Diligence Act (LkSG), legal basis is Art. 6 (1) (c) GDPR in conjunction with Sections 8, 9 LkSG and Section 10 HinSchG, insofar as this is necessary to fulfill the tasks specified in Sections 13 and 24 HinSchG, as well as compliance with Directive (EU) 2019/1937 on the protection of persons reporting breaches of Union law and the resulting national law of the Member States and compliance with applicable legislation from other countries. Recipients or categories of recipients of the personal data: Law enforcement authorities, fining authorities, and other

authorities as well as lawyers, group companies or employers. Planned transfer to third countries: Entry into the Navex online system and onward transfer to entities within the group, employers, or lawyers. The EU Standard Contractual Clauses and the UK Addendum to the EU Standard Contractual Clauses have been concluded with Navex. Navex is also a member of the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework, and the UK Extension to the EU-U.S. Data Privacy Framework. For other transfers, there may be no adequacy decision. The EU Standard Contractual Clauses and the UK Addendum to the EU Standard Contractual Clauses are used for such transfers. Criteria for determining the storage period: The documentation is deleted three years after the end of the procedure. The documentation may be kept for longer to meet the requirements of the applicable legislation if this is necessary and proportionate.

Under the General Data Protection Regulation, you have the right of access to personal data concerning you and the right to rectification or erasure or restriction of processing or the right to object to processing and the right to data portability. You have the right to lodge a complaint with the competent data protection supervisory authority regarding the processing. The provision of personal data is not required by law or contract and is not necessary for the conclusion of a contract, which is why you are not obliged to provide personal data to the whistleblowing hotline. Possible consequences of non-provision are that the report will not be processed or will be processed with a delay, or that it will be rejected, and that no information or information relating to the report can be provided to you. There is no automated decision-making.

III. Information pursuant to Art. 14 of the GDPR (for other data subjects):

Name and contact details of the controller: See imprint on the website. Contact details of the data protection officer and, if applicable, the representative: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Munich, Germany. Purposes for which the personal data are to be processed and the legal basis for the processing: Compliance with the Whistleblower Protection Act (HinSchG) and the Supply Chain Due Diligence Act (LkSG), legal basis is Art. 6 (1) (c) GDPR in conjunction with Sections 8, 9 LkSG and Section 10 HinSchG, insofar as this is necessary to fulfill the tasks specified in Sections 13 and 24 HinSchG, as well as compliance with Directive (EU) 2019/1937 on the protection of persons reporting breaches of Union law and the resulting national law of the Member States and compliance with applicable legislation from other countries. Categories of personal data processed: Whistleblowing data. Recipients or categories of recipients of the personal data: Law enforcement authorities, fining authorities, and other authorities as well as lawyers, group companies or employers. Planned transfer to third countries: Entry into the Navex online system and onward transfer to entities within the group, employers, or lawyers. The EU Standard Contractual Clauses and the UK Addendum to the EU Standard Contractual Clauses have been concluded with Navex. Navex is also a member of the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework, and the UK Extension to the EU-U.S. Data Privacy Framework. For other transfers, there may be no adequacy decision. The EU Standard Contractual Clauses and the UK Addendum to the EU Standard

Contractual Clauses are used for such transfers. Criteria for determining the storage period: The documentation is deleted three years after the end of the procedure. The documentation may be kept for longer to meet the requirements of applicable legislation if this is necessary and proportionate. The source of the personal data is the whistleblower and/or the company concerned.

Under the General Data Protection Regulation, you may have the right of access to personal data concerning you and the right to rectification or erasure or restriction of processing or the right to object to processing and the right to data portability. You have the right to lodge a complaint with the competent data protection supervisory authority with regard to the processing. There is no automated decision-making. The provision of further information proves to be impossible.

POLISH: System zgłaszania nieprawidłowości (wewnętrzne kanały zgłaszania)

Nasze wartości stanowią podstawę naszych praktyk biznesowych i odzwierciedlają nasze zaangażowanie w uczciwość, przejrzystość i pozytywną kulturę korporacyjną. Nasz system zgłaszania nieprawidłowości jest podstawowym narzędziem promowania odpowiedzialności i zapewniania etycznych działań biznesowych. Niniejszy regulamin ma na celu zapewnienie przejrzystości procesu i zasad naszych procesów dochodzeniowych oraz zagwarantowanie, że wszystkie zgłoszenia otrzymane za pośrednictwem naszego systemu są obsługiwane w sposób właściwy i profesjonalny.

OSI angażuje się w otwarty dialog i uznaje znaczenie sygnalistów jako kluczowych partnerów w naszych wysiłkach na rzecz utrzymania najwyższych standardów we wszystkich obszarach naszej działalności.

I. Regulamin Systemu Zgłaszania Nieprawidłowości OSI

I. Cel i zakres:

1. Cel: Niniejszy regulamin reguluje obsługę i badanie zgłoszeń otrzymanych za pośrednictwem globalnego systemu zgłaszania nieprawidłowości Make It Right Global Hotline. Celem jest zapewnienie, że wszystkie otrzymane zgłoszenia są rozpatrywane w sposób przejrzysty, skuteczny i zgodny ze standardami etycznymi OSI.

2. Zakres zastosowania: Niniejszy regulamin ma zastosowanie do wszystkich pracowników, partnerów biznesowych, dostawców i innych interesariuszy w całym łańcuchu wartości, którzy korzystają z systemu zgłaszania nieprawidłowości w celu podzielenia się konkretnymi wskazówkami dotyczącymi możliwego niewłaściwego postępowania, obawami lub wskazówkami. System zgłaszania nieprawidłowości nie jest przeznaczony do rozpatrywania wątpliwości związanych z produktami i usługami. Takie pytania lub kwestie można kierować bezpośrednio za pośrednictwem formularza kontaktowego na stronie internetowej firmy.

II. Przekazywanie informacji:

1. anonimowość i poufność:

System zgłaszania nieprawidłowości umożliwia między innymi anonimowe składanie zgłoszeń w zakresie dozwolonym przez prawo krajowe.

Wszystkie informacje przetwarzane w ramach systemu zgłaszania nieprawidłowości podlegają ścisłej poufności.

2. Rodzaje raportów:

System umożliwia sygnalistom składanie zgłoszeń, gdy istnieją konkretne przesłanki wskazujące na możliwe niewłaściwe postępowanie, obawy lub takie przesłanki. Dotyczy to naruszeń przez pracowników lub partnerów biznesowych obowiązujących przepisów ustawowych, wykonawczych itp. (w szczególności wymienionych w sekcji 2 ustawy o ochronie sygnalistów lub dyrektywy UE 2019/1937) lub wewnętrznych regulacji firmy (w szczególności naruszeń kodeksu postępowania) lub praw człowieka i zagrożeń dla środowiska, które można przypisać bezpośrednim lub pośrednim dostawcom, a także naruszeń praw człowieka i obowiązków środowiskowych wynikających z ustawy o należytej staranności w łańcuchu dostaw (LkSG). Obejmują one naruszenia Kodeksu postępowania OSI, prawa antymonopolowego, korupcji, kradzieży, dyskryminacji, lekceważenia bezpieczeństwa i higieny pracy, pracy dzieci, zanieczyszczenia gleby, wody lub powietrza, szkodliwych emisji hałasu, niedopuszczalnego zużycia wody, produkcji lub stosowania niektórych trwałych zanieczyszczeń organicznych oraz nieautoryzowanego importu i eksportu odpadów.

3. dostęp do systemu:

Sygnaliści mają dostęp do zewnętrznie zarządzanego systemu zgłoszeń w różnych językach pod adresem:

EthicsPoint - OSI Group, LLC

- w formie tekstowej za pośrednictwem formularza w portalu internetowym lub
- telefonicznie (bezpłatnie z różnych krajów)

III. Przetwarzanie raportów:

1. Odbiór i wstępna ocena:

Po otrzymaniu zgłoszenia za pośrednictwem zewnętrznych kanałów raportowania zarządzanych przez system whistleblower, jest ono najpierw dokumentowane i przypisywany jest mu indywidualny numer akt. OSI Compliance otrzymuje wszystkie zgłoszenia i przeprowadza wstępną ocenę w celu określenia ich wiarygodności i ważności.

2. Dochodzenie:

W przypadku istotnych wskazówek zostanie wszczęte dokładne, obiektywne i poufne dochodzenie. Jeśli będzie to konieczne w celu otrzymania zgłoszenia lub podjęcia działań, skonsultujemy się z innymi działami lub poprosimy je o pomoc. Sygnalista może również zostać poproszony o dodatkowe informacje.

Czas trwania dochodzenia do jego zakończenia zależy od złożoności sprawy, wymaganych środków dochodzeniowych oraz dostępności informacji lub stron zaangażowanych w daną sprawę. Dołożymy wszelkich starań, aby zakończyć dochodzenie tak skutecznie i szybko, jak to możliwe.

3. Informacje zwrotne dla Sygnalisty:

Sygnalista otrzyma informację zwrotną o otrzymaniu zgłoszenia w ciągu 7 dni, o ile to możliwe i bez narażania anonimowości.

Jeśli sygnalista dokonał zgłoszenia online lub telefonicznie, otrzyma dane logowania, które umożliwią mu śledzenie zgłoszenia i otrzymywanie anonimowych informacji zwrotnych (jeśli sobie tego życzy). W szczególności konieczne może być zadawanie zrozumiałych pytań i uzyskiwanie dalszych informacji.

W dalszym toku dochodzenia (nie później niż 3 miesiące po otrzymaniu potwierdzenia odbioru) zostaną przekazane informacje o statusie dochodzenia w odniesieniu do planowanych lub już wszczętych środków lub, jeśli nie ma wystarczających podejrzeń, o umorzeniu dochodzenia.

IV. Ochrona sygnalistów:

1. Brak działań odwetowych:

OSI podejmuje wszelkie uzasadnione starania, aby zapewnić, że osoby zgłaszające nieprawidłowości będą chronione przed wszelkimi formami odwetu, niekorzystnymi warunkami lub innymi represjami.

Działania dyscyplinarne oparte na informowaniu o nieprawidłowościach wobec osób, które w dobrej wierze współpracują przy dochodzeniach, są zabronione i nie będą tolerowane.

2. Poufność:

Osoby zaangażowane w dochodzenie są zobowiązane do zachowania ścisłej poufności.

V. Dokumentacja i przechowywanie:

1. Dokumentacja:

Wszystkie etapy dochodzenia są starannie dokumentowane.

Dokumentacja służy przejrzystości i identyfikowalności procedury.

2. Okres przechowywania:

Dokumentacja jest przechowywana zgodnie z wymogami prawnymi i wewnętrznymi wytycznymi.

VI. Przegląd i dostosowanie:

Te zasady proceduralne są regularnie przeglądane i dostosowywane w razie potrzeby, aby zapewnić ich zgodność z aktualnymi wymogami prawnymi i celami korporacyjnymi.

II. Informacje zgodnie z art. 13 RODO (dla osób udzielających informacji):

Nazwa i dane kontaktowe administratora: Patrz nadruk na stronie internetowej. Dane kontaktowe inspektora ochrony danych i, w stosownych przypadkach, przedstawiciela: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Monachium, Niemcy. Cele przetwarzania danych osobowych i podstawa prawna przetwarzania: Zgodność z ustawą o ochronie sygnalistów (HinSchG) i ustawą o należytej staranności w łańcuchu dostaw (LkSG), podstawą prawną jest Art. 6 ust. 1 lit. c) RODO w związku z art. 8, 9 LkSG i art. 10 HinSchG, o ile jest to konieczne do realizacji zadań określonych w art. 13 i 24 HinSchG, a także zgodność z dyrektywą (UE) 2019/1937 w sprawie ochrony osób zgłaszających naruszenia prawa Unii i wynikającym z niej prawem krajowym państw członkowskich oraz zgodność z obowiązującymi przepisami innych krajów. Odbiorcy lub kategorie odbiorców danych osobowych: Organy ścigania, organy nakładające grzywny i inne organy, a także prawnicy, spółki należące do grupy lub pracodawcy. Planowane przekazywanie danych do krajów trzecich: Wprowadzenie do systemu online Navex i dalsze przekazanie podmiotom w ramach grupy, pracodawcom lub prawnikom. Standardowe klauzule umowne UE i brytyjskie uzupełnienie do standardowych klauzul umownych UE zostały zawarte z Navex. Navex jest również członkiem Ram Prywatności Danych UE-USA, Ram Prywatności Danych Szwajcaria-USA oraz brytyjskiego rozszerzenia Ram Prywatności Danych UE-USA. W przypadku innych transferów może nie być decyzji stwierdzającej odpowiedni poziom ochrony. Do takich transferów stosuje się standardowe klauzule umowne UE i brytyjskie uzupełnienie standardowych klauzul umownych UE. Kryteria określania okresu przechowywania: Dokumentacja jest usuwana trzy lata po zakończeniu procedury. Dokumentacja może być przechowywana dłużej w celu spełnienia wymogów obowiązujących przepisów, jeśli jest to konieczne i proporcjonalne.

Zgodnie z ogólnym rozporządzeniem o ochronie danych użytkownik ma prawo dostępu do dotyczących go danych osobowych oraz prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania lub prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych. Użytkownik ma prawo do wniesienia skargi dotyczącej przetwarzania danych do właściwego organu nadzorczego ds. ochrony danych. Podanie danych osobowych nie jest wymagane przepisami prawa ani umową i nie jest konieczne do zawarcia umowy, dlatego nie jesteś zobowiązany do podania danych osobowych na infolinii whistleblowingowej. Możliwe konsekwencje nieprzekazania danych to brak przetwarzania zgłoszenia lub jego opóźnione przetwarzanie, odrzucenie zgłoszenia oraz brak możliwości przekazania użytkownikowi informacji związanych ze zgłoszeniem. Nie ma zautomatyzowanego podejmowania decyzji.

III. Informacje zgodnie z art. 14 RODO (dla innych osób, których dane dotyczą):

Nazwa i dane kontaktowe administratora: Patrz nadruk na stronie internetowej. Dane kontaktowe inspektora ochrony danych i, w stosownych przypadkach, przedstawiciela: Prof. Dr. h.c. Heiko Jonny

Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Monachium, Niemcy. Cele przetwarzania danych osobowych i podstawa prawna przetwarzania: Zgodność z ustawą o ochronie sygnalistów (HinSchG) i ustawą o należytej staranności w łańcuchu dostaw (LkSG), podstawą prawną jest Art. 6 ust. 1 lit. c) RODO w związku z art. 8, 9 LkSG i art. 10 HinSchG, o ile jest to konieczne do realizacji zadań określonych w art. 13 i 24 HinSchG, a także zgodność z dyrektywą (UE) 2019/1937 w sprawie ochrony osób zgłaszających naruszenia prawa Unii i wynikającym z niej prawem krajowym państw członkowskich oraz zgodność z obowiązującymi przepisami innych krajów. Kategorie przetwarzanych danych osobowych: Dane dotyczące whistleblowingu. Odbiorcy lub kategorie odbiorców danych osobowych: Organy ścigania, organy nakładające grzywny i inne organy, a także prawnicy, spółki należące do grupy lub pracodawcy. Planowane przekazywanie danych do krajów trzecich: Wprowadzenie do systemu online Navex i dalsze przekazanie podmiotom w ramach grupy, pracodawcom lub prawnikom. Standardowe klauzule umowne UE i brytyjskie uzupełnienie do standardowych klauzul umownych UE zostały zawarte z Navex. Navex jest również członkiem Ram Prywatności Danych UE-USA, Ram Prywatności Danych Szwajcaria-USA oraz brytyjskiego rozszerzenia Ram Prywatności Danych UE-USA. W przypadku innych transferów może nie być decyzji stwierdzającej odpowiedni poziom ochrony. Do takich transferów stosuje się standardowe klauzule umowne UE i brytyjskie uzupełnienie standardowych klauzul umownych UE. Kryteria określania okresu przechowywania: Dokumentacja jest usuwana trzy lata po zakończeniu procedury. Dokumentacja może być przechowywana dłużej w celu spełnienia wymogów obowiązujących przepisów, jeśli jest to konieczne i proporcjonalne. Źródłem danych osobowych jest zgłaszający i/lub spółka, której dotyczy zgłoszenie.

Zgodnie z ogólnym rozporządzeniem o ochronie danych osobowych użytkownik może mieć prawo dostępu do dotyczących go danych osobowych oraz prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania lub prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych. Użytkownik ma prawo do wniesienia skargi do właściwego organu nadzorczego ds. ochrony danych w odniesieniu do przetwarzania. Nie ma zautomatyzowanego podejmowania decyzji. Udzielenie dalszych informacji okazuje się niemożliwe.

SPANISH: Sistema de denuncia de irregularidades (canales de denuncia internos)

Nuestros valores constituyen la base de nuestras prácticas empresariales y reflejan nuestro compromiso con la integridad, la transparencia y una cultura corporativa positiva. Nuestro sistema de denuncia de irregularidades es una herramienta esencial para promover la responsabilidad y garantizar unas operaciones empresariales éticas. Estas normas de procedimiento sirven para que el proceso y los principios de nuestros procesos de investigación sean transparentes y garanticen que todas las denuncias recibidas a través de nuestro sistema se traten de forma adecuada y profesional.

OSI está comprometida con el diálogo abierto y reconoce la importancia de los denunciantes como socios clave en nuestros esfuerzos por mantener los más altos estándares en todas las áreas de nuestro negocio.

I. Reglamento interno del sistema de denuncia de irregularidades de las IIS

I. Objeto y ámbito de aplicación:

1. Finalidad: El presente Reglamento regula la tramitación e investigación de las denuncias recibidas a través del sistema de denuncia de irregularidades de la Línea Directa Mundial de Make It Right. El objetivo es garantizar que todas las denuncias recibidas se gestionen de forma transparente, eficiente y de acuerdo con las normas éticas de OSI.

2. Ámbito de aplicación: Estas normas de procedimiento se aplican a todos los empleados, socios comerciales, proveedores y otras partes interesadas a lo largo de la cadena de valor que utilicen el sistema de denuncia de irregularidades para compartir indicios específicos de posibles conductas indebidas, preocupaciones o pistas. El sistema de denuncia de irregularidades no está pensado para procesar preocupaciones relacionadas con productos y servicios. Tales cuestiones o problemas pueden abordarse directamente a través del formulario de contacto del sitio web de la empresa.

II. Presentación de información:

1. Anonimato y confidencialidad:

El sistema de denuncia de irregularidades permite, entre otras cosas, la presentación anónima de denuncias, en la medida en que lo permita la legislación nacional.

Toda la información tratada en el marco del sistema de denuncia de irregularidades está sujeta a una estricta confidencialidad.

2. Tipos de informes:

El sistema permite a los denunciantes presentar informes cuando existan indicios concretos de posibles conductas indebidas, preocupaciones o indicios de las mismas. Se trata de infracciones por parte de empleados o socios comerciales de las leyes, reglamentos, etc. aplicables (en particular los mencionados en el artículo 2 de la Ley de Protección de los Denunciantes o la Directiva 2019/1937 de la UE) o los reglamentos internos de la empresa (en particular las infracciones del Código de Conducta) o los derechos humanos y los riesgos medioambientales atribuibles a proveedores directos o indirectos, así como las infracciones de las obligaciones en materia de derechos humanos y medio ambiente en virtud de la Ley de Diligencia Debida en la Cadena de Suministro (LkSG). Entre ellas se incluyen las infracciones del Código de Conducta de las IIS, la legislación antimonopolio, la corrupción, el robo, la discriminación, la falta de respeto por la salud y la seguridad en el trabajo, el trabajo infantil, la contaminación del suelo, el agua o el aire, las emisiones sonoras nocivas, el consumo inaceptable de agua, la producción o el uso de determinados contaminantes orgánicos persistentes y la importación y exportación no autorizadas de residuos.

3. Acceso al sistema:

Los denunciantes tienen acceso al sistema de denuncia gestionado externamente en diferentes idiomas en:

EthicsPoint - OSI Group, LLC

- en forma de texto a través de un formulario del portal en línea o
- por teléfono (gratuito desde varios países)

III. Tramitación de informes:

1. Recepción y evaluación inicial:

Una vez que se recibe una denuncia a través de los canales de denuncia externos gestionados por el sistema de denuncia de irregularidades, primero se documenta y se le asigna un número de expediente individual. OSI Compliance recibe todas las denuncias y realiza una evaluación inicial para determinar su plausibilidad y validez.

2. Investigación:

Se iniciará una investigación exhaustiva, objetiva y confidencial de las pistas pertinentes. Si es necesario para recibir las denuncias o tomar medidas, se consultará a otros departamentos o se les pedirá ayuda. También se podrá solicitar información adicional al denunciante.

La duración de una investigación hasta su conclusión depende de la complejidad del caso, de las medidas de investigación necesarias y de la disponibilidad de información o de las partes implicadas en el caso concreto. Se hará todo lo posible para completar la investigación de la manera más eficiente y rápida posible.

3. Información al denunciante:

El denunciante recibirá información sobre la recepción de su denuncia en un plazo de 7 días, siempre que sea posible y sin poner en peligro su anonimato.

Si el denunciante ha presentado la denuncia en línea o por teléfono, recibirá información de acceso que le permitirá hacer un seguimiento de la denuncia y recibir comentarios anónimos (si lo desea). En particular, puede ser necesario hacer preguntas de comprensión y obtener más información.

En el curso ulterior de la investigación (a más tardar 3 meses después de la recepción del acuse de recibo), se facilitará información sobre el estado de la investigación en relación con las medidas previstas o ya iniciadas o, si no hay suficientes sospechas, sobre la interrupción de la investigación.

IV. Protección de los denunciantes:

1. No represalias:

OSI realiza todos los esfuerzos razonables para garantizar que los denunciantes estén protegidos de cualquier forma de represalia, desventaja u otras represalias.

Las medidas disciplinarias basadas en la denuncia de irregularidades contra personas que cooperan de buena fe con las investigaciones están prohibidas y no se tolerarán.

2. Confidencialidad:

Las personas implicadas en la investigación están obligadas a mantener una estricta confidencialidad.

V. Documentación y almacenamiento:

1. Documentación:

Todos los pasos de la investigación se documentan cuidadosamente.

La documentación está al servicio de la transparencia y la trazabilidad del procedimiento.

2. Periodo de conservación:

La documentación se conserva de acuerdo con los requisitos legales y las directrices internas.

VI. Revisión y ajuste:

Estas normas de procedimiento se revisan periódicamente y se adaptan en caso necesario para garantizar que cumplen los requisitos legales vigentes y los objetivos de la empresa.

II. Información con arreglo al art. 13 GDPR (para las personas que facilitan información):

Nombre y datos de contacto del responsable del tratamiento: Véase el pie de imprenta en el sitio web. Datos de contacto del responsable de la protección de datos y, en su caso, del representante: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Munich, Alemania. Fines para los que se tratarán los datos personales y fundamento jurídico del tratamiento: Cumplimiento de la Ley de Protección de Denunciantes (HinSchG) y de la Ley de Diligencia Debida en la Cadena de Suministro (LkSG), la base jurídica es el art. 6 (1) (c) GDPR en relación con las Secciones 8, 9 LkSG y la Sección 10 HinSchG, en la medida en que esto sea necesario para cumplir con las tareas especificadas en las Secciones 13 y 24 HinSchG, así como el cumplimiento de la Directiva (UE) 2019/1937 sobre la protección de las personas que denuncian infracciones del derecho de la Unión y la legislación nacional resultante de los Estados miembros y el cumplimiento de la legislación aplicable de otros países. Destinatarios o categorías de destinatarios de los datos personales: Autoridades policiales, autoridades sancionadoras y otras autoridades, así como abogados, empresas del grupo o empleadores. Transferencias previstas a terceros países: Entrada en el sistema en línea Navex y posterior transferencia a entidades del grupo, empleadores o abogados. Las cláusulas contractuales tipo de la UE y el apéndice del Reino Unido a las cláusulas contractuales tipo de la UE se han suscrito con Navex. Navex también es miembro del Marco de Privacidad de Datos UE-EE.UU., del Marco de Privacidad de Datos Suiza-EE.UU. y de la Extensión del Reino Unido al Marco de Privacidad de Datos UE-EE.UU.. Para otras transferencias, puede no haber decisión de adecuación. Para estas transferencias se utilizan las Cláusulas Contractuales Tipo de la UE y el Anexo del Reino Unido a las Cláusulas Contractuales Tipo de la UE. Criterios para determinar el periodo de conservación: La documentación se elimina tres años después de la finalización del procedimiento. La documentación puede conservarse durante más tiempo para cumplir los requisitos de la legislación aplicable si resulta necesario y proporcionado.

En virtud del Reglamento General de Protección de Datos, usted tiene derecho a acceder a los datos personales que le conciernen y derecho de rectificación o supresión o limitación del tratamiento o derecho de oposición al tratamiento y derecho a la portabilidad de los datos. Tiene derecho a presentar una reclamación ante la autoridad de control competente en materia de protección de datos en relación con el tratamiento. El suministro de datos personales no es obligatorio por ley o por contrato y no es necesario para la celebración de un contrato, por lo que no está obligado a proporcionar datos personales a la línea directa de denuncia de irregularidades. Las posibles consecuencias de la no facilitación son que la denuncia no se tramitará o se tramitará con retraso, o que será rechazada, y que no se le podrá facilitar información o datos relativos a la denuncia. No hay toma de decisiones automatizada.

III. Información con arreglo al art. 14 del RGPD (para otros interesados):

Nombre y datos de contacto del responsable del tratamiento: Véase el pie de imprenta en el sitio web. Datos de contacto del responsable de la protección de datos y, en su caso, del representante: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Munich, Alemania. Fines para los que se tratarán los datos personales y fundamento jurídico del tratamiento: Cumplimiento de la Ley de Protección de Denunciantes (HinSchG) y de la Ley de Diligencia Debida en la Cadena de Suministro (LkSG), la base jurídica es el art. 6 (1) (c) GDPR en relación con las Secciones 8, 9 LkSG y la Sección 10 HinSchG, en la medida en que esto sea necesario para cumplir con las tareas especificadas en las Secciones 13 y 24 HinSchG, así como el cumplimiento de la Directiva (UE) 2019/1937 sobre la protección de las personas que denuncian infracciones del derecho de la Unión y la legislación nacional resultante de los Estados miembros y el cumplimiento de la legislación aplicable de otros países. Categorías de datos personales tratados: Datos de denuncia. Destinatarios o categorías de destinatarios de los datos personales: Autoridades policiales, autoridades sancionadoras y otras autoridades, así como abogados, empresas del grupo o empleadores. Transferencia prevista a terceros países: Entrada en el sistema en línea Navex y posterior transferencia a entidades del grupo, empleadores o abogados. Las cláusulas contractuales tipo de la UE y el apéndice del Reino Unido a las cláusulas contractuales tipo de la UE se han suscrito con Navex. Navex también es miembro del Marco de Privacidad de Datos UE-EE.UU., del Marco de Privacidad de Datos Suiza-EE.UU. y de la Extensión del Reino Unido al Marco de Privacidad de Datos UE-EE.UU.. Para otras transferencias, puede no haber decisión de adecuación. Para estas transferencias se utilizan las Cláusulas Contractuales Tipo de la UE y el Anexo del Reino Unido a las Cláusulas Contractuales Tipo de la UE. Criterios para determinar el periodo de conservación: La documentación se elimina tres años después de la finalización del procedimiento. La documentación puede conservarse durante más tiempo para cumplir los requisitos de la legislación aplicable si resulta necesario y proporcionado. La fuente de los datos personales es el denunciante y/o la empresa afectada.

En virtud del Reglamento General de Protección de Datos, usted puede tener derecho de acceso a los datos personales que le conciernen y derecho de rectificación o supresión o limitación del tratamiento, o derecho de oposición al tratamiento y derecho a la portabilidad de los datos. Tiene derecho a presentar una reclamación ante la autoridad de control competente en materia de protección de datos en relación con el tratamiento. No hay toma de decisiones automatizada. Resulta imposible facilitar más información.

FRENCH: Système d'alerte (canaux de signalement internes)

Nos valeurs constituent le fondement de nos pratiques commerciales et reflètent notre engagement en faveur de l'intégrité, de la transparence et d'une culture d'entreprise positive. Notre système de dénonciation est un outil essentiel pour promouvoir la responsabilité et garantir des opérations commerciales éthiques. Ces règles de procédure servent à rendre transparents le processus et les principes de nos procédures d'enquête et à garantir que tous les rapports reçus par l'intermédiaire de notre système sont traités de manière appropriée et professionnelle.

OSI s'engage à dialoguer ouvertement et reconnaît l'importance des dénonciateurs en tant que partenaires clés dans nos efforts pour maintenir les normes les plus élevées dans tous les domaines de notre activité.

I. Règles de procédure pour le système d'alerte de l'OSI

I. Objet et champ d'application:

1. objectif: ces règles de procédure régissent le traitement et l'investigation des rapports reçus par le biais du système de dénonciation de Make It Right Global Hotline. L'objectif est de garantir que tous les rapports reçus sont traités de manière transparente, efficace et conformément aux normes éthiques de l'OSI.

2. champ d'application: Les présentes règles de procédure s'appliquent à tous les employés, partenaires commerciaux, fournisseurs et autres parties prenantes de la chaîne de valeur qui utilisent le système d'alerte pour partager des indications spécifiques sur d'éventuelles fautes professionnelles, des préoccupations ou des conseils. Le système d'alerte n'est pas destiné à traiter les problèmes liés aux produits et aux services. Ces questions ou problèmes peuvent être adressés directement via le formulaire de contact sur le site web de l'entreprise.

II. Soumission d'informations:

1. l' anonymat et la confidentialité:

Le système de dénonciation permet, entre autres, la soumission anonyme de rapports de dénonciation, dans la mesure où les lois nationales l'autorisent.

Toutes les informations traitées dans le cadre du système de dénonciation sont soumises à une stricte confidentialité.

2. les types de rapports:

Le système permet aux lanceurs d'alerte de soumettre des rapports lorsqu'il existe des indications concrètes d'une éventuelle mauvaise conduite, de préoccupations ou d'indications en ce sens. Cela

concerne les violations par des employés ou des partenaires commerciaux des lois, règlements, etc. applicables (en particulier ceux mentionnés à l'article 2 de la loi sur la protection des lanceurs d'alerte ou de la directive 2019/1937 de l'UE) ou des règlements internes de l'entreprise (en particulier les violations du code de conduite) ou les droits de l'homme et les risques environnementaux imputables aux fournisseurs directs ou indirects, ainsi que les violations des droits de l'homme et des obligations environnementales en vertu de la loi sur le devoir de diligence dans la chaîne d'approvisionnement (LkSG). Il s'agit notamment des violations du code de conduite des OSI, de la législation antitrust, de la corruption, du vol, de la discrimination, du non-respect de la santé et de la sécurité au travail, du travail des enfants, de la pollution du sol, de l'eau ou de l'air, des émissions sonores nocives, de la consommation inacceptable d'eau, de la production ou de l'utilisation de certains polluants organiques persistants et de l'importation et de l'exportation non autorisées de déchets.

3. l' accès au système:

Les dénonciateurs ont accès au système de signalement géré en externe dans différentes langues:

EthicsPoint - OSI Group, LLC

- sous forme de texte via un formulaire dans le portail en ligne ou
- par téléphone (appel gratuit depuis plusieurs pays)

III. Traitement des rapports:

1. réception et évaluation initiale:

Lorsqu'un rapport est reçu par le biais des canaux de signalement externes gérés par le système de dénonciation, il est d'abord documenté et un numéro de dossier individuel lui est attribué. L'OSI Compliance reçoit tous les rapports et procède à une évaluation initiale pour déterminer leur plausibilité et leur validité.

2. Enquête:

Une enquête approfondie, objective et confidentielle sera menée sur les informations pertinentes. Si cela s'avère nécessaire pour recevoir des rapports ou prendre des mesures, d'autres services seront consultés ou invités à apporter leur aide. Des informations supplémentaires peuvent également être demandées au dénonciateur.

La durée d'une enquête jusqu'à sa conclusion dépend de la complexité de l'affaire, des mesures d'enquête requises et de la disponibilité des informations ou des parties impliquées dans l'affaire. Tout sera mis en œuvre pour mener à bien l'enquête de la manière la plus efficace et la plus rapide possible.

3. le retour d'information au dénonciateur:

Le dénonciateur recevra un retour d'information sur la réception de son signalement dans un délai de 7 jours, dans la mesure du possible et sans compromettre l'anonymat.

Si le dénonciateur a soumis son rapport en ligne ou par téléphone, il recevra des informations de connexion qui lui permettront d'assurer le suivi du rapport et de recevoir un retour d'information anonyme (s'il le souhaite). En particulier, il peut être nécessaire de poser des questions de compréhension et d'obtenir des informations complémentaires.

Au cours de l'enquête (au plus tard trois mois après la réception de l'accusé de réception), des informations seront fournies sur l'état d'avancement de l'enquête en ce qui concerne les mesures prévues ou déjà engagées ou, si les soupçons sont insuffisants, sur l'arrêt de l'enquête.

IV. Protection des dénonciateurs:

1. la non-représailles:

L'OSI déploie tous les efforts raisonnables pour s'assurer que les dénonciateurs seront protégés contre toute forme de représailles, de désavantages ou d'autres mesures de rétorsion.

Les mesures disciplinaires fondées sur des dénonciations à l'encontre de personnes qui coopèrent de bonne foi aux enquêtes sont interdites et ne seront pas tolérées.

2. la confidentialité:

Les personnes impliquées dans l'enquête sont tenues à une stricte confidentialité.

V. Documentation et stockage:

1. Documentation:

Toutes les étapes de l'enquête sont soigneusement documentées.

La documentation sert à la transparence et à la traçabilité de la procédure.

2. période de conservation:

La documentation est conservée conformément aux exigences légales et aux lignes directrices internes.

VI. Révision et ajustement:

Ces règles de procédure sont régulièrement réexaminées et adaptées si nécessaire afin de garantir qu'elles sont conformes aux exigences légales en vigueur et aux objectifs de l'entreprise.

II. Informations conformément à l'art. 13 GDPR (pour les personnes fournissant des informations):

Nom et coordonnées du responsable du traitement: Voir les mentions légales sur le site web. Coordonnées du délégué à la protection des données et, le cas échéant, du représentant: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Munich, Allemagne. Finalités du traitement des données à caractère personnel et base juridique du traitement: Respect de la loi sur la protection des dénonciateurs (HinSchG) et de la loi sur la diligence raisonnable dans la chaîne d'approvisionnement (LkSG) ; la base juridique est l'article 6, paragraphe 1, point c), du RGPD. 6 (1) (c) GDPR en conjonction avec les sections 8, 9 LkSG et la section 10 HinSchG, dans la mesure où cela est nécessaire pour remplir les tâches spécifiées dans les sections 13 et 24 HinSchG, ainsi que le respect de la directive (UE) 2019/1937 sur la protection des personnes signalant des violations du droit de l'Union et le droit national des États membres qui en découle, et le respect de la législation applicable d'autres pays. Destinataires ou catégories de destinataires des données à caractère personnel: Les autorités chargées de l'application de la loi, les autorités chargées des amendes et d'autres autorités, ainsi que les avocats, les sociétés du groupe ou les employeurs. Transfert prévu vers des pays tiers: Entrée dans le système en ligne Navex et transfert ultérieur à des entités du groupe, à des employeurs ou à des avocats. Les clauses contractuelles types de l'UE et l'addendum britannique aux clauses contractuelles types de l'UE ont été conclus avec Navex. Navex est également membre du cadre de protection des données UE-États-Unis, du cadre de protection des données Suisse-États-Unis et de l'extension britannique du cadre de protection des données UE-États-Unis. Pour les autres transferts, il se peut qu'il n'y ait pas de décision d'adéquation. Les clauses contractuelles types de l'UE et l'addendum britannique aux clauses contractuelles types de l'UE sont utilisés pour ces transferts. Critères de détermination de la période de conservation: La documentation est supprimée trois ans après la fin de la procédure. La documentation peut être conservée plus longtemps pour satisfaire aux exigences de la législation applicable si cela est nécessaire et proportionné.

En vertu du règlement général sur la protection des données, vous disposez d'un droit d'accès aux données à caractère personnel vous concernant et d'un droit de rectification, d'effacement ou de limitation du traitement ou d'un droit d'opposition au traitement et d'un droit à la portabilité des données. Vous avez le droit d'introduire une réclamation auprès de l'autorité de contrôle compétente en matière de protection des données en ce qui concerne le traitement. La fourniture de données à caractère personnel n'est pas exigée par la loi ou par un contrat et n'est pas nécessaire à la conclusion d'un contrat, c'est pourquoi vous n'êtes pas obligé de fournir des données à caractère personnel à la ligne d'alerte. Les conséquences possibles de la non-fourniture sont que le rapport ne sera pas traité ou le sera avec retard, ou qu'il sera rejeté, et qu'aucune information ou information relative au rapport ne pourra vous être fournie. Il n'y a pas de prise de décision automatisée.

III. Informations conformément à l'art. 14 du GDPR (pour les autres personnes concernées):

Nom et coordonnées du responsable du traitement: Voir les mentions légales sur le site web. Coordonnées du délégué à la protection des données et, le cas échéant, du représentant: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Munich, Allemagne. Finalités du traitement des données à caractère personnel et base juridique du traitement: Respect de la loi sur la protection des dénonciateurs (HinSchG) et de la loi sur la diligence raisonnable dans la chaîne d'approvisionnement (LkSG) ; la base juridique est l'article 6, paragraphe 1, point c), du RGPD. 6 (1) (c) GDPR en conjonction avec les sections 8, 9 LkSG et la section 10 HinSchG, dans la mesure où cela est nécessaire pour remplir les tâches spécifiées dans les sections 13 et 24 HinSchG, ainsi que le respect de la directive (UE) 2019/1937 sur la protection des personnes signalant des violations du droit de l'Union et le droit national des États membres qui en découle, ainsi que le respect de la législation applicable d'autres pays. Catégories de données à caractère personnel traitées: Données de signalement. Destinataires ou catégories de destinataires des données à caractère personnel: Les autorités chargées de l'application de la loi, les autorités chargées des amendes et d'autres autorités, ainsi que les avocats, les sociétés du groupe ou les employeurs. Transfert prévu vers des pays tiers: Entrée dans le système en ligne Navex et transfert ultérieur aux entités du groupe, aux employeurs ou aux avocats. Les clauses contractuelles types de l'UE et l'addendum britannique aux clauses contractuelles types de l'UE ont été conclus avec Navex. Navex est également membre du cadre de protection des données UE-États-Unis, du cadre de protection des données Suisse-États-Unis et de l'extension britannique du cadre de protection des données UE-États-Unis. Pour les autres transferts, il se peut qu'il n'y ait pas de décision d'adéquation. Les clauses contractuelles types de l'UE et l'addendum britannique aux clauses contractuelles types de l'UE sont utilisés pour ces transferts. Critères de détermination de la période de conservation: La documentation est supprimée trois ans après la fin de la procédure. La documentation peut être conservée plus longtemps pour répondre aux exigences de la législation applicable si cela est nécessaire et proportionné. La source des données à caractère personnel est le dénonciateur et/ou l'entreprise concernée.

En vertu du règlement général sur la protection des données, vous pouvez avoir le droit d'accéder aux données à caractère personnel vous concernant et le droit de rectification, d'effacement ou de limitation du traitement ou le droit de vous opposer au traitement et le droit à la portabilité des données. Vous avez le droit d'introduire une réclamation auprès de l'autorité de contrôle compétente en matière de protection des données en ce qui concerne le traitement. Il n'y a pas de prise de décision automatisée. La fourniture d'informations complémentaires s'avère impossible.

ITALIAN: Sistema di whistleblower (canali di segnalazione interni)

I nostri valori sono alla base delle nostre pratiche commerciali e riflettono il nostro impegno per l'integrità, la trasparenza e una cultura aziendale positiva. Il nostro sistema di whistleblowing è uno strumento essenziale per promuovere la responsabilità e garantire operazioni commerciali etiche. Il presente regolamento interno serve a rendere trasparenti il processo e i principi delle nostre indagini e a garantire che tutte le segnalazioni ricevute attraverso il nostro sistema siano gestite in modo appropriato e professionale.

OSI è impegnata in un dialogo aperto e riconosce l'importanza degli informatori come partner chiave nei nostri sforzi per mantenere gli standard più elevati in tutte le aree della nostra attività.

I. Regolamento interno del sistema di segnalazione OSI

I. Scopo e ambito di applicazione:

1. Scopo: Il presente regolamento interno disciplina la gestione e l'indagine delle segnalazioni ricevute attraverso il sistema di whistleblowing della Make It Right Global Hotline. L'obiettivo è garantire che tutte le segnalazioni ricevute siano gestite in modo trasparente, efficiente e in conformità con gli standard etici di OSI.

2. Ambito di applicazione: Il presente regolamento interno si applica a tutti i dipendenti, partner commerciali, fornitori e altre parti interessate lungo la catena del valore che utilizzano il sistema di whistleblower per condividere indicazioni specifiche su possibili comportamenti scorretti, preoccupazioni o suggerimenti. Il sistema di whistleblower non è destinato all'elaborazione di problemi relativi a prodotti e servizi. Tali domande o problemi possono essere affrontati direttamente tramite il modulo di contatto sul sito web dell'azienda.

II. Presentazione delle informazioni:

1. Anonimato e riservatezza:

Il sistema di whistleblower consente, tra l'altro, l'invio anonimo di segnalazioni, nella misura consentita dalle leggi nazionali.

Tutte le informazioni trattate nell'ambito del sistema di whistleblower sono soggette a una rigorosa riservatezza.

2. Tipi di rapporti:

Il sistema consente ai whistleblower di presentare segnalazioni in presenza di indicazioni concrete di possibili comportamenti scorretti, preoccupazioni o indizi in tal senso. Si tratta di violazioni da parte di dipendenti o partner commerciali di leggi, regolamenti ecc. applicabili (in particolare quelli citati nella

sezione 2 della legge sulla protezione degli informatori o nella direttiva UE 2019/1937) o di regolamenti aziendali interni (in particolare violazioni del Codice di condotta) o di rischi per i diritti umani e l'ambiente attribuibili a fornitori diretti o indiretti, nonché di violazioni degli obblighi in materia di diritti umani e ambiente ai sensi della legge sulla due diligence della catena di fornitura (LkSG). Questi includono violazioni del Codice di Condotta OSI, delle leggi antitrust, corruzione, furto, discriminazione, mancato rispetto della salute e della sicurezza sul lavoro, lavoro minorile, inquinamento del suolo, dell'acqua o dell'aria, emissioni acustiche nocive, consumo inaccettabile di acqua, produzione o utilizzo di determinati inquinanti organici persistenti e importazione ed esportazione non autorizzata di rifiuti.

3. Accesso al sistema:

Gli informatori hanno accesso al sistema di segnalazione gestito esternamente in diverse lingue all'indirizzo:

EthicsPoint - OSI Group, LLC

- in forma testuale tramite un modulo nel portale online o
- per telefono (numero verde da vari paesi)

III. Elaborazione dei rapporti:

1. Ricevimento e valutazione iniziale:

Una volta ricevuta una segnalazione attraverso i canali di segnalazione esterni gestiti dal sistema di whistleblower, essa viene innanzitutto documentata e le viene assegnato un numero di pratica individuale. OSI Compliance riceve tutte le segnalazioni ed effettua una valutazione iniziale per determinarne la plausibilità e la validità.

2. Indagine:

Per le segnalazioni pertinenti verrà avviata un'indagine approfondita, obiettiva e riservata. Se necessario, per ricevere le segnalazioni o prendere provvedimenti, verranno consultati o chiesta l'assistenza di altri dipartimenti. Possono essere richieste ulteriori informazioni all'informatore.

La durata di un'indagine fino alla sua conclusione dipende dalla complessità del caso, dalle misure investigative richieste e dalla disponibilità di informazioni o di parti coinvolte nel singolo caso. Si farà il possibile per completare l'indagine nel modo più efficiente e rapido possibile.

3. Feedback all'informatore:

L'informatore riceverà un riscontro sulla ricezione della sua segnalazione entro 7 giorni, ove possibile e senza compromettere l'anonimato.

Se l'informatore ha presentato la segnalazione online o per telefono, riceverà le informazioni di accesso che gli consentiranno di dare seguito alla segnalazione e di ricevere un feedback anonimo (se lo desidera). In particolare, potrebbe essere necessario porre domande di comprensione e ottenere ulteriori informazioni.

Nel prosieguo dell'indagine (non oltre 3 mesi dal ricevimento della conferma di ricezione), verranno fornite informazioni sullo stato dell'indagine in merito alle misure previste o già avviate o, in caso di sospetti insufficienti, sull'interruzione dell'indagine.

IV. Protezione degli informatori:

1. Non ritorsione:

OSI compie ogni ragionevole sforzo per garantire che gli informatori siano protetti da qualsiasi forma di ritorsione, svantaggio o altra rappresaglia.

Le azioni disciplinari basate sulla denuncia di irregolarità nei confronti di persone che collaborano in buona fede alle indagini sono vietate e non saranno tollerate.

2. Riservatezza:

Le persone coinvolte nell'indagine sono tenute alla massima riservatezza.

V. Documentazione e conservazione:

1. Documentazione:

Tutte le fasi dell'indagine sono accuratamente documentate.

La documentazione serve alla trasparenza e alla tracciabilità della procedura.

2. Periodo di conservazione:

La documentazione viene conservata in conformità ai requisiti legali e alle linee guida interne.

VI. Revisione e adeguamento:

Queste regole procedurali vengono regolarmente riviste e adattate, se necessario, per garantire che siano conformi agli attuali requisiti legali e agli obiettivi aziendali.

II. Informazioni ai sensi dell'art. 13 GDPR (per le persone che forniscono informazioni):

Nome e dati di contatto del responsabile del trattamento: Vedere l'impronta sul sito web. Dati di contatto del responsabile della protezione dei dati e, se del caso, del rappresentante: Prof. Dr. h.c. Heiko Jonny

Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Monaco, Germania. Finalità del trattamento dei dati personali e base giuridica del trattamento: Conformità alla legge sulla protezione degli informatori (HinSchG) e alla legge sulla due diligence della catena di approvvigionamento (LkSG); la base giuridica è l'art. 6 (1) (c) GD. 6 (1) (c) GDPR in combinato disposto con gli artt. 8, 9 LkSG e l'art. 10 HinSchG, nella misura in cui ciò sia necessario per adempiere ai compiti specificati negli artt. 13 e 24 HinSchG, nonché per il rispetto della Direttiva (UE) 2019/1937 sulla protezione delle persone che segnalano violazioni del diritto dell'Unione e del conseguente diritto nazionale degli Stati membri e per il rispetto della legislazione applicabile di altri paesi. Destinatari o categorie di destinatari dei dati personali: Autorità di polizia, autorità sanzionatorie e altre autorità, nonché avvocati, società del gruppo o datori di lavoro. Trasferimento previsto verso paesi terzi: Inserimento nel sistema online di Navex e successivo trasferimento a entità del gruppo, datori di lavoro o avvocati. Le Clausole contrattuali standard dell'UE e l'Addendum britannico alle Clausole contrattuali standard dell'UE sono stati stipulati con Navex. Navex è anche membro dell'EU-U.S. Data Privacy Framework, dell'Swiss-U.S. Data Privacy Framework e dell'UK Extension to the EU-U.S. Data Privacy Framework. Per altri trasferimenti, potrebbe non esserci una decisione di adeguatezza. Per tali trasferimenti vengono utilizzate le Clausole contrattuali standard dell'UE e l'Addendum britannico alle Clausole contrattuali standard dell'UE. Criteri per determinare il periodo di conservazione: La documentazione viene cancellata tre anni dopo la fine della procedura. La documentazione può essere conservata più a lungo per soddisfare i requisiti della legislazione applicabile, se ciò è necessario e proporzionato.

Ai sensi del Regolamento generale sulla protezione dei dati, avete il diritto di accedere ai dati personali che vi riguardano e il diritto di rettifica o cancellazione o limitazione del trattamento o il diritto di opporsi al trattamento e il diritto alla portabilità dei dati. Avete il diritto di presentare un reclamo all'autorità di controllo della protezione dei dati competente in materia di trattamento. Il conferimento dei dati personali non è richiesto dalla legge o dal contratto e non è necessario per la conclusione di un contratto; per questo motivo non siete obbligati a fornire dati personali alla hotline whistleblowing. Le possibili conseguenze del mancato conferimento sono che la segnalazione non sarà elaborata o sarà elaborata con ritardo, o che sarà rifiutata, e che non sarà possibile fornirvi informazioni o informazioni relative alla segnalazione. Non esiste un processo decisionale automatizzato.

III. Informazioni ai sensi dell'art. 14 del GDPR (per gli altri interessati):

Nome e dati di contatto del responsabile del trattamento: Vedere l'impronta sul sito web. Dati di contatto del responsabile della protezione dei dati e, se del caso, del rappresentante: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Monaco, Germania. Finalità del trattamento dei dati personali e base giuridica del trattamento: Conformità alla legge sulla protezione degli informatori (HinSchG) e alla legge sulla due diligence della catena di approvvigionamento (LkSG); la base giuridica è l'art. 6 (1) (c) GD. 6 (1) (c) GDPR in combinato disposto con gli artt. 8, 9 LkSG e l'art. 10 HinSchG, nella misura in cui ciò sia necessario per adempiere ai compiti specificati negli artt. 13 e 24 HinSchG, nonché per il rispetto della Direttiva (UE) 2019/1937 sulla protezione delle persone che

segnalano violazioni del diritto dell'Unione e del conseguente diritto nazionale degli Stati membri e per il rispetto della legislazione applicabile di altri Paesi. Categorie di dati personali trattati: Dati relativi al whistleblowing. Destinatari o categorie di destinatari dei dati personali: Autorità di polizia, autorità sanzionatorie e altre autorità, nonché avvocati, società del gruppo o datori di lavoro. Trasferimento previsto verso paesi terzi: Inserimento nel sistema online di Navex e successivo trasferimento a entità del gruppo, datori di lavoro o avvocati. Le Clausole contrattuali standard dell'UE e l'Addendum britannico alle Clausole contrattuali standard dell'UE sono stati stipulati con Navex. Navex è anche membro dell'EU-U.S. Data Privacy Framework, dell'Swiss-U.S. Data Privacy Framework e dell'UK Extension to the EU-U.S. Data Privacy Framework. Per altri trasferimenti, potrebbe non esserci una decisione di adeguatezza. Per tali trasferimenti vengono utilizzate le Clausole contrattuali standard dell'UE e l'Addendum britannico alle Clausole contrattuali standard dell'UE. Criteri per determinare il periodo di conservazione: La documentazione viene cancellata tre anni dopo la fine della procedura. La documentazione può essere conservata più a lungo per soddisfare i requisiti della legislazione applicabile, se ciò è necessario e proporzionato. La fonte dei dati personali è l'autore della denuncia e/o la società interessata.

Ai sensi del Regolamento generale sulla protezione dei dati, l'utente può avere il diritto di accesso ai dati personali che lo riguardano e il diritto di rettifica o cancellazione o limitazione del trattamento o il diritto di opporsi al trattamento e il diritto alla portabilità dei dati. Avete il diritto di presentare un reclamo all'autorità di controllo della protezione dei dati competente in relazione al trattamento. Non esiste un processo decisionale automatizzato. Il conferimento di ulteriori informazioni si rivela impossibile.

HUNGARIAN: Whistleblower-rendszer (belső bejelentési csatornák)

Értékeink képezik üzleti gyakorlatunk alapját, és tükrözik elkötelezettségünket az integritás, az átláthatóság és a pozitív vállalati kultúra iránt. Bejelentő rendszerünk alapvető eszköz az elszámoltathatóság előmozdításában és az etikus üzleti működés biztosításában. Ez az eljárási szabályzat arra szolgál, hogy átláthatóvá tegye a vizsgálati folyamatainkat és elveinket, és biztosítsa, hogy a rendszerünkön keresztül beérkező összes bejelentést megfelelően és szakszerűen kezeljük.

Az OSI elkötelezett a nyílt párbeszéd mellett, és elismeri a bejelentők fontosságát, akik kulcsfontosságú partnerként vesznek részt az üzleti tevékenységünk minden területén a legmagasabb színvonal fenntartására irányuló erőfeszítéseinkben.

I. Az OSI Whistleblower-rendszer eljárási szabályzata

I. Cél és hatály:

1. Cél: Ez az eljárási szabályzat szabályozza a Make It Right Global Hotline bejelentő rendszerén keresztül beérkező bejelentések kezelését és kivizsgálását. A cél annak biztosítása, hogy minden beérkezett bejelentést átláthatóan, hatékonyan és az OSI etikai normáinak megfelelően kezeljenek.

2. Ez az eljárási szabályzat az értéklánc minden olyan alkalmazottjára, üzleti partnerére, beszállítójára és egyéb érdekeltjére vonatkozik, aki a bejelentő rendszert használja a lehetséges visszaélésekre, aggályokra vagy tippekre vonatkozó konkrét jelzések megosztására. A bejelentő rendszer nem a termékekkel és szolgáltatásokkal kapcsolatos aggályok feldolgozására szolgál. Az ilyen kérdéseket vagy problémákat közvetlenül a vállalat honlapján található kapcsolatfelvételi űrlapon keresztül lehet feltenni.

II. Az információk benyújtása:

1. Anonimitás és bizalmasság:

A bejelentő rendszer többek között lehetővé teszi a bejelentések névtelen benyújtását, a nemzeti jogszabályok által megengedett mértékben.

A bejelentő rendszer keretében kezelt minden információ szigorúan bizalmasan kezelendő.

2 :

A rendszer lehetővé teszi a bejelentők számára, hogy bejelentéseket tegyenek, ha konkrét jelek utalnak lehetséges kötelességszegésre, aggályokra vagy ilyenekre utaló jelekre. Ez vonatkozik az alkalmazottak vagy üzleti partnerek által elkövetett, az alkalmazandó törvények, jogszabályok stb. megsértésére (különösen a bejelentők védelméről szóló törvény 2. szakaszában vagy a 2019/1937/EU irányelvben említettekre) vagy a vállalat belső szabályzataira (különösen a magatartási kódex megsértésére), illetve

a közvetlen vagy közvetett beszállítóknak tulajdonítható emberi jogi és környezeti kockázatokra, valamint az ellátási lánc átvilágításáról szóló törvény (LkSG) szerinti emberi jogi és környezetvédelmi kötelezettségek megsértésére. Ezek közé tartozik az OSI magatartási kódex, a trösztellenes törvények, a korrupció, a lopás, a megkülönböztetés, a munkahelyi egészség és biztonság figyelmen kívül hagyása, a gyermekmunka, a talaj-, víz- vagy levegőszennyezés, a káros zajkibocsátás, az elfogadhatatlan vízfogyasztás, egyes tartósan megmaradó szerves szennyező anyagok előállítása vagy felhasználása, valamint a hulladék engedély nélküli behozatala és kivitele.

3. Hozzáférés a rendszerhez:

A bejelentők különböző nyelveken férhetnek hozzá a külsőleg kezelt bejelentési rendszerhez a következő címen:

EthicsPoint - OSI Group, LLC

- szöveges formában az online portálon található űrlapon keresztül vagy
- telefonon (több országból díjmentesen)

III. A jelentések feldolgozása:

1. Átvétel és kezdeti értékelés:

Amint a bejelentés a bejelentő rendszer által kezelt külső bejelentési csatornákon keresztül beérkezik, először dokumentálják és egyedi iktatószámmal látják el. Az OSI Compliance megkapja az összes bejelentést, és elvégzi az első értékelést, hogy megállapítsa azok hihetőségét és érvényességét.

2. Vizsgálat:

A vonatkozó tippek alapján alapos, objektív és bizalmas vizsgálatot indítunk. Ha a bejelentések fogadásához vagy az intézkedések meghozatalához szükséges, más osztályokkal konzultálnak vagy kérnek segítséget. A bejelentőtől további információkat is kérhetnek.

A nyomozás időtartama a lezárásig az ügy összetettségétől, a szükséges nyomozati intézkedésektől, valamint az adott ügyben érintett információk vagy felek rendelkezésre állásától függ. Minden erőfeszítést megtesznek annak érdekében, hogy a vizsgálatot a lehető leghatékonyabban és leggyorsabban fejezzék be.

3. Visszajelzés a bejelentőnek:

A bejelentő 7 napon belül visszajelzést kap a bejelentés beérkezéséről, amennyiben lehetséges, és az anonimitás veszélyeztetése nélkül.

Ha a bejelentő online vagy telefonon nyújtotta be a bejelentést, akkor bejelentkezési adatokat kap, amelyek lehetővé teszik számára, hogy nyomon kövesse a bejelentést, és névtelen visszajelzést kapjon

(ha kívánja). Különösen szükség lehet a megértési kérdések feltevésére és további információk beszerzésére.

A vizsgálat további szakaszában (legkésőbb az átvételi elismervény kézhezvételét követő 3 hónapon belül) tájékoztatást adnak a vizsgálat állásáról a tervezett vagy már megkezdett intézkedések tekintetében, vagy ha nem áll fenn elegendő gyanú, a vizsgálat megszüntetéséről.

IV. A bejelentők védelme:

1. Non-Retaliation:

Az OSI minden ésszerű erőfeszítést megtesz annak érdekében, hogy a bejelentőket megvédje a megtorlás, hátrányos megkülönböztetés vagy egyéb megtorlás bármely formájától.

A vizsgálatokban jóhiszeműen együttműködő személyekkel szemben a bejelentésen alapuló fegyelmi eljárás tilos, és nem tűrhető.

2. A vizsgálatban részt vevő személyeket szigorú titoktartási kötelezettség terheli.

V. Dokumentáció és tárolás:

1. Dokumentáció:

A vizsgálat minden lépését gondosan dokumentálják.

A dokumentáció az eljárás átláthatóságát és nyomon követhetőségét szolgálja.

2. A dokumentációt a jogi követelményeknek és a belső iránymutatásoknak megfelelően őrzik meg.

VI. Felülvizsgálat és kiigazítás:

Ezeket az eljárási szabályokat rendszeresen felülvizsgálják és szükség szerint kiigazítják annak érdekében, hogy megfeleljenek az aktuális jogi követelményeknek és a vállalati célkitűzéseknek.

II. Az információ a következő cikk szerint. GDPR 13. cikke (az információt nyújtó személyek esetében):

Az adatkezelő neve és elérhetőségei: Lásd a honlapon található impresszumot. Az adatvédelmi tisztviselő és adott esetben a képviselő elérhetőségei: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 München, Németország. A személyes adatok feldolgozásának céljai és a feldolgozás jogalapja: A bejelentők védelméről szóló törvény (HinSchG) és az ellátási lánc átvilágításáról szóló törvény (LkSG) betartása, jogalapja az Art. GDPR 6. cikk (1) bekezdés c) pontja, összefüggésben a LkSG 8. és 9. §-ával és a HinSchG 10. §-ával, amennyiben ez

a HinSchG 13. és 24. §-ában meghatározott feladatok teljesítéséhez szükséges, valamint az uniós jog megsértését bejelentő személyek védelméről szóló (EU) 2019/1937 irányelvnek és a tagállamok ebből eredő nemzeti jogának, valamint más országok alkalmazandó jogszabályainak való megfelelés. A személyes adatok címzettjei vagy a címzettek kategóriái: Bűnüldöző hatóságok, bírságoló hatóságok és egyéb hatóságok, valamint ügyvédek, csoportvállalatok vagy munkáltatók. Tervezett továbbítás harmadik országokba: A Navex online rendszerébe való belépés és továbbítás a csoporton belüli jogalanyok, munkáltatók vagy ügyvédek részére. A Navexszel megkötötték az EU szabványos szerződési feltételeket és az EU szabványos szerződési feltételek brit kiegészítését. A Navex tagja az EU és az Egyesült Államok közötti adatvédelmi keretrendszernek, a svájci és az Egyesült Államok közötti adatvédelmi keretrendszernek és az EU és az Egyesült Államok közötti adatvédelmi keretrendszer brit kiterjesztésének is. Más adattovábbítások esetében előfordulhat, hogy nem születik megfelelőségi határozat. Az ilyen adattovábbításokra az uniós általános szerződési feltételeket és az uniós általános szerződési feltételek brit kiegészítését alkalmazzák. A tárolási időszak meghatározásának kritériumai: A dokumentációt az eljárás befejezése után három évvel törlik. A dokumentáció hosszabb ideig is megőrizhető az alkalmazandó jogszabályok követelményeinek teljesítése érdekében, ha ez szükséges és arányos.

Az általános adatvédelmi rendelet értelmében Önnek joga van hozzáférni az Önre vonatkozó személyes adatokhoz, és joga van a helyesbítéshez, törléshez vagy a feldolgozás korlátozásához, illetve joga van tiltakozni a feldolgozás ellen, valamint joga van az adatok hordozhatóságához. Önnek joga van panaszt tenni az illetékes adatvédelmi felügyeleti hatóságnál a feldolgozással kapcsolatban. A személyes adatok megadását nem írja elő jogszabály vagy szerződés, és nem szükséges a szerződés megkötéséhez, ezért Ön nem köteles személyes adatokat megadni a bejelentő forródrótnak. A meg nem adás lehetséges következményei közé tartozik, hogy a bejelentést nem, vagy csak késedelmesen dolgozzák fel, vagy elutasítják, és hogy a bejelentéssel kapcsolatban nem kaphat tájékoztatást vagy információt. Nincs automatizált döntéshozatal.

III. A tájékoztatás a következő cikk szerint. GDPR 14. cikke alapján (egyéb érintettek esetében):

Az adatkezelő neve és elérhetőségei: Lásd a honlapon található impresszumot. Az adatvédelmi tisztviselő és adott esetben a képviselő elérhetőségei: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 München, Németország. A személyes adatok feldolgozásának céljai és a feldolgozás jogalapja: A bejelentők védelméről szóló törvény (HinSchG) és az ellátási lánc átvilágításáról szóló törvény (LkSG) betartása, jogalapja az Art. GDPR 6. cikk (1) bekezdés c) pontja, összefüggésben a LkSG 8. és 9. §-ával és a HinSchG 10. §-ával, amennyiben ez a HinSchG 13. és 24. §-ában meghatározott feladatok teljesítéséhez szükséges, valamint az uniós jog megsértését bejelentő személyek védelméről szóló (EU) 2019/1937 irányelvnek és a tagállamok ebből eredő nemzeti jogának, valamint más országok alkalmazandó jogszabályainak való megfelelés. A feldolgozott személyes adatok kategóriái: Bejelentő adatok. A személyes adatok címzettjei vagy a

címzettek kategóriái: Bűnüldöző hatóságok, bírságoló hatóságok és egyéb hatóságok, valamint ügyvédek, csoporthoz tartozó vállalatok vagy munkáltatók. Tervezett továbbítás harmadik országokba: A Navex online rendszerébe való belépés és továbbítás a csoporton belüli szervezetek, munkáltatók vagy ügyvédek részére. A Navexszel megkötötték az EU szabványos szerződési feltételeket és az EU szabványos szerződési feltételek brit kiegészítését. A Navex tagja az EU és az Egyesült Államok közötti adatvédelmi keretrendszernek, a svájci és az Egyesült Államok közötti adatvédelmi keretrendszernek és az EU és az Egyesült Államok közötti adatvédelmi keretrendszer brit kiterjesztésének is. Más adattovábbítások esetében előfordulhat, hogy nem születik megfelelőségi határozat. Az ilyen adattovábbításokra az uniós általános szerződési feltételeket és az uniós általános szerződési feltételek brit kiegészítését alkalmazzák. A tárolási időszak meghatározásának kritériumai: A dokumentációt az eljárás befejezése után három évvel törlik. A dokumentáció hosszabb ideig is megőrizhető az alkalmazandó jogszabályok követelményeinek teljesítése érdekében, ha ez szükséges és arányos. A személyes adatok forrása a bejelentő és/vagy az érintett vállalat.

Az általános adatvédelmi rendelet értelmében Ön jogosult lehet az Önre vonatkozó személyes adatokhoz való hozzáférésre, valamint az adatkezelés helyesbítéséhez, törléséhez vagy korlátozásához, illetve az adatkezelés elleni tiltakozáshoz és az adathordozhatósághoz való jogra. Ön jogosult arra, hogy panaszt tegyen az illetékes adatvédelmi felügyeleti hatóságnál a feldolgozással kapcsolatban. Nincs automatizált döntéshozatal. A további információk szolgáltatása lehetetlennek bizonyul.

DUTCH: Klokkenluidersregeling (interne meldkanalen)

Onze waarden vormen de basis voor onze bedrijfspraktijken en weerspiegelen ons streven naar integriteit, transparantie en een positieve bedrijfscultuur. Ons klokkenluidersysteem is een essentieel instrument voor het bevorderen van verantwoordingsplicht en het garanderen van een ethische bedrijfsvoering. Deze procedureregels dienen om het proces en de principes van onze onderzoeksprocessen transparant te maken en ervoor te zorgen dat alle meldingen die via ons systeem binnenkomen op gepaste en professionele wijze worden behandeld.

OSI zet zich in voor een open dialoog en erkent het belang van klokkenluiders als belangrijke partners in onze inspanningen om de hoogste normen te handhaven op alle gebieden van ons bedrijf.

I. Reglement voor het OSI-Klokkenluidersregeling

I. Doel en toepassingsgebied:

1. Doel: Dit reglement regelt de behandeling en het onderzoek van meldingen die binnenkomen via het klokkenluiderssysteem van de Make It Right Global Hotline. Het doel is ervoor te zorgen dat alle ontvangen meldingen transparant, efficiënt en in overeenstemming met de ethische normen van OSI worden behandeld.

2. Toepassingsgebied: Deze procedureregels zijn van toepassing op alle werknemers, zakelijke partners, leveranciers en andere belanghebbenden in de gehele waardeketen die gebruik maken van het klokkenluidersysteem om specifieke aanwijzingen van mogelijk wangedrag, zorgen of tips te delen. Het klokkenluidersysteem is niet bedoeld voor het verwerken van product- en servicegerelateerde kwesties. Dergelijke vragen of kwesties kunnen rechtstreeks worden aangepakt via het contactformulier op de website van het bedrijf.

II. Indienen van informatie:

1. Anonimiteit en vertrouwelijkheid:

De klokkenluidersregeling maakt het onder andere mogelijk om anoniem klokkenluidersrapporten in te dienen, voor zover de nationale wetgeving dit toestaat.

Alle informatie die in het kader van de klokkenluidersregeling wordt behandeld, is onderworpen aan strikte vertrouwelijkheid.

2. Soorten rapporten:

Het systeem stelt klokkenluiders in staat om meldingen in te dienen wanneer er concrete aanwijzingen zijn van mogelijk wangedrag, zorgen, of indicaties daarvan. Dit betreft schendingen door werknemers of zakenpartners van toepasselijke wet- en regelgeving etc. (in het bijzonder die genoemd in artikel 2 van

de Klokkenluidersbeschermingswet of EU-richtlijn 2019/1937) of interne bedrijfsvoorschriften (in het bijzonder schendingen van de Gedragscode) of mensenrechten- en milieurisico's die toe te schrijven zijn aan directe of indirecte leveranciers, evenals schendingen van mensenrechten- en milieuverplichtingen onder de Supply Chain Due Diligence Act (LkSG). Hieronder vallen schendingen van de OSI Gedragscode, antitrustwetgeving, corruptie, diefstal, discriminatie, veronachtzaming van gezondheid en veiligheid op het werk, kinderarbeid, bodem-, water- of luchtverontreiniging, schadelijke geluidsemissies, onaanvaardbaar waterverbruik, de productie of het gebruik van bepaalde persistente organische verontreinigende stoffen en de ongeoorloofde import en export van afval.

3. Toegang tot het systeem:

Klokkenluiders hebben toegang tot het extern beheerde meldsysteem in verschillende talen op:

EthicsPoint - OSI Group, LLC

- in tekstvorm via een formulier in het online portaal of
- per telefoon (gratis vanuit verschillende landen)

III. Verwerking van rapporten:

1. Ontvangst en eerste beoordeling:

Zodra een melding wordt ontvangen via de externe meldkanalen die door het klokkenluidersysteem worden beheerd, wordt deze eerst gedocumenteerd en krijgt de melding een individueel dossiernummer. OSI Compliance ontvangt alle meldingen en voert een eerste beoordeling uit om de plausibiliteit en geldigheid ervan vast te stellen.

2. Onderzoek:

Bij relevante tips wordt een grondig, objectief en vertrouwelijk onderzoek ingesteld. Als het nodig is om meldingen te ontvangen of actie te ondernemen, worden andere afdelingen geraadpleegd of om hulp gevraagd. Er kan ook aanvullende informatie worden gevraagd aan de klokkenluider.

Hoe lang een onderzoek duurt tot het is afgerond, hangt af van de complexiteit van de zaak, de vereiste onderzoeksmaatregelen en de beschikbaarheid van informatie of partijen die bij de individuele zaak betrokken zijn. Alles zal in het werk worden gesteld om het onderzoek zo efficiënt en snel mogelijk af te ronden.

3. Feedback aan de klokkenluider:

De klokkenluider ontvangt binnen 7 dagen feedback over de ontvangst van zijn tip, waar mogelijk en zonder de anonimiteit in gevaar te brengen.

Als de klokkenluider de melding online of telefonisch heeft ingediend, ontvangt hij/zij inloggegevens waarmee hij/zij de melding kan opvolgen en anonieme feedback kan ontvangen (als hij/zij dat wenst). Het kan met name nodig zijn om begripsvragen te stellen en meer informatie te verkrijgen.

In het verdere verloop van het onderzoek (uiterlijk 3 maanden na ontvangst van de ontvangstbevestiging) zal informatie worden verstrekt over de status van het onderzoek met betrekking tot geplande of reeds geïnitieerde maatregelen of, als er onvoldoende verdenking is, over het stopzetten van het onderzoek.

IV. Bescherming van klokkenluiders:

1. Geen represailles:

OSI doet alle redelijke inspanningen om ervoor te zorgen dat klokkenluiders worden beschermd tegen elke vorm van vergelding, benadeling of andere represailles.

Disciplinaire maatregelen op basis van klokkenluiden tegen personen die te goeder trouw meewerken aan onderzoeken zijn verboden en worden niet getolereerd.

2. Vertrouwelijkheid:

Personen die betrokken zijn bij het onderzoek zijn gebonden aan strikte vertrouwelijkheid.

V. Documentatie en opslag:

1. Documentatie:

Alle stappen van het onderzoek worden zorgvuldig gedocumenteerd.

De documentatie dient de transparantie en traceerbaarheid van de procedure.

2. Bewaartermijn:

Documentatie wordt bewaard in overeenstemming met wettelijke vereisten en interne richtlijnen.

VI. Herziening en aanpassing:

Deze procedureregels worden regelmatig herzien en waar nodig aangepast om ervoor te zorgen dat ze voldoen aan de huidige wettelijke vereisten en bedrijfsdoelstellingen.

II. Informatie volgens Art. 13 GDPR (voor personen die informatie verstrekken):

Naam en contactgegevens van de voor de verwerking verantwoordelijke: Zie opdruk op de website. Contactgegevens van de functionaris voor gegevensbescherming en, indien van toepassing, de vertegenwoordiger: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str.

11, 80801 München, Duitsland. Doeleinden waarvoor de persoonsgegevens worden verwerkt en de rechtsgrondslag voor de verwerking: Naleving van de klokkenluidersbeschermingswet (HinSchG) en de Supply Chain Due Diligence Act (LkSG), rechtsgrondslag is Art. 6 (1) (c) GDPR in samenhang met Sections 8, 9 LkSG en Section 10 HinSchG, voor zover dit noodzakelijk is om de taken te vervullen die zijn gespecificeerd in Sections 13 en 24 HinSchG, evenals naleving van Richtlijn (EU) 2019/1937 betreffende de bescherming van personen die schendingen van het recht van de Unie melden en het daaruit voortvloeiende nationale recht van de lidstaten en naleving van toepasselijke wetgeving van andere landen. Ontvangers of categorieën ontvangers van de persoonsgegevens: Rechtshandhavingsinstanties, boeteautoriteiten en andere autoriteiten, evenals advocaten, groepsmaatschappijen of werkgevers. Geplande overdracht naar derde landen: Invoer in het online systeem van Navex en verdere doorgifte aan entiteiten binnen de groep, werkgevers of advocaten. De EU Standaard Contractuele Clausules en het UK Addendum bij de EU Standaard Contractuele Clausules zijn afgesloten met Navex. Navex is ook lid van het EU-VS Data Privacy Framework, het Swiss-U.S. Data Privacy Framework en de UK Extension to the EU-U.S. Data Privacy Framework. Voor andere doorgiften is er mogelijk geen adequaatheidsbesluit. Voor dergelijke doorgiften worden de EU Standard Contractual Clauses en het UK Addendum to the EU Standard Contractual Clauses gebruikt. Criteria voor het bepalen van de bewaartermijn: De documentatie wordt drie jaar na het einde van de procedure verwijderd. De documentatie kan langer worden bewaard om te voldoen aan de vereisten van de toepasselijke wetgeving als dit noodzakelijk en proportioneel is.

Op grond van de Algemene Verordening Gegevensbescherming heeft u recht op toegang tot uw persoonsgegevens en het recht op rectificatie, wissing of beperking van de verwerking of het recht om bezwaar te maken tegen de verwerking en het recht op gegevensoverdraagbaarheid. U hebt het recht om een klacht in te dienen bij de bevoegde toezichthoudende autoriteit voor gegevensbescherming met betrekking tot de verwerking. Het verstrekken van persoonsgegevens is niet wettelijk of contractueel verplicht en is niet noodzakelijk voor het sluiten van een contract, daarom bent u niet verplicht persoonsgegevens te verstrekken aan het meldpunt. Mogelijke gevolgen van het niet verstrekken zijn dat de melding niet of vertraagd wordt verwerkt, of dat de melding wordt afgewezen en dat er geen informatie of informatie met betrekking tot de melding aan u kan worden verstrekt. Er is geen sprake van geautomatiseerde besluitvorming.

III. Informatie op grond van Art. 14 van de GDPR (voor andere betrokkenen):

Naam en contactgegevens van de voor de verwerking verantwoordelijke: Zie opdruk op de website. Contactgegevens van de functionaris voor gegevensbescherming en, indien van toepassing, de vertegenwoordiger: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 München, Duitsland. Doeleinden waarvoor de persoonsgegevens worden verwerkt en de rechtsgrondslag voor de verwerking: Naleving van de klokkenluidersbeschermingswet (HinSchG) en de Supply Chain Due Diligence Act (LkSG), rechtsgrondslag is Art. 6 (1) (c) GDPR in samenhang met

Sections 8, 9 LkSG en Section 10 HinSchG, voor zover dit noodzakelijk is om de taken te vervullen die zijn gespecificeerd in Sections 13 en 24 HinSchG, evenals naleving van Richtlijn (EU) 2019/1937 betreffende de bescherming van personen die schendingen van het recht van de Unie melden en het daaruit voortvloeiende nationale recht van de lidstaten en naleving van toepasselijke wetgeving van andere landen. Categorieën verwerkte persoonsgegevens: Klokkenluidersgegevens. Ontvangers of categorieën ontvangers van de persoonsgegevens: Rechtshandhavingsinstanties, boeteautoriteiten en andere autoriteiten, evenals advocaten, groepsmaatschappijen of werkgevers. Geplande overdracht naar derde landen: Invoer in het online systeem van Navex en verdere doorgifte aan entiteiten binnen de groep, werkgevers of advocaten. De EU Standaard Contractuele Clausules en het UK Addendum bij de EU Standaard Contractuele Clausules zijn afgesloten met Navex. Navex is ook lid van het EU-VS Data Privacy Framework, het Swiss-U.S. Data Privacy Framework en de UK Extension to the EU-U.S. Data Privacy Framework. Voor andere doorgiften is er mogelijk geen adequaatheidsbesluit. Voor dergelijke doorgiften worden de EU Standard Contractual Clauses en het UK Addendum to the EU Standard Contractual Clauses gebruikt. Criteria voor het bepalen van de bewaartermijn: De documentatie wordt drie jaar na het einde van de procedure verwijderd. De documentatie kan langer worden bewaard om te voldoen aan de vereisten van de toepasselijke wetgeving als dit noodzakelijk en proportioneel is. De bron van de persoonsgegevens is de klokkenluider en/of het betrokken bedrijf.

Op grond van de Algemene Verordening Gegevensbescherming kunt u recht hebben op toegang tot uw persoonsgegevens en het recht op rectificatie, wissing of beperking van de verwerking of het recht om bezwaar te maken tegen de verwerking en het recht op gegevensoverdraagbaarheid. U hebt het recht om een klacht in te dienen bij de bevoegde toezichthoudende autoriteit voor gegevensbescherming met betrekking tot de verwerking. Er is geen sprake van geautomatiseerde besluitvorming. Verdere informatieverstrekking blijkt onmogelijk.

UKRAINIAN: Система викривачів (внутрішні канали повідомлень)

Наші цінності формують основу нашої ділової практики та відображають нашу відданість принципам доброчесності, прозорості та позитивної корпоративної культури. Наша система повідомлень про порушення є важливим інструментом сприяння підзвітності та забезпечення етичного ведення бізнесу. Ці правила процедури слугують для того, щоб зробити процес і принципи наших розслідувань прозорими і гарантувати, що всі повідомлення, отримані через нашу систему, обробляються належним чином і професійно.

OSI прагне до відкритого діалогу та визнає важливість викривачів як ключових партнерів у наших зусиллях щодо дотримання найвищих стандартів у всіх сферах нашого бізнесу.

I. Правила процедури для Системи викривачів ICI

I. Мета та сфера застосування:

1. Мета: Ці Правила процедури регулюють обробку та розслідування повідомлень, отриманих через Глобальну гарячу лінію Ініціативи "Make It Right". Мета полягає в тому, щоб забезпечити прозору, ефективну обробку всіх отриманих повідомлень відповідно до етичних стандартів ICI.

2. сфера застосування: Ці правила процедури поширюються на всіх працівників, ділових партнерів, постачальників та інших зацікавлених осіб по всьому ланцюжку створення вартості, які використовують систему викривачів, щоб поділитися конкретними ознаками можливих неправомірних дій, побоюваннями або порадами. Система повідомлень не призначена для обробки питань, пов'язаних із продукцією та послугами. З такими питаннями або проблемами можна звертатися безпосередньо через контактну форму на веб-сайті компанії.

II. Подання інформації:

1. анонімність та конфіденційність:

Система викривачів дозволяє, серед іншого, анонімне подання повідомлень про корупцію в межах, дозволених національним законодавством.

Вся інформація, що обробляється в рамках системи викривачів, підлягає суворій конфіденційності.

2. Типи звітів:

Система дозволяє викривачам подавати повідомлення, якщо є конкретні вказівки на можливі порушення, побоювання або ознаки таких порушень. Це стосується порушень працівниками або діловими партнерами чинного законодавства, нормативно-правових актів тощо (зокрема тих, що

згадуються в розділі 2 Закону про захист викривачів або Директиві ЄС 2019/1937) або внутрішніх правил компанії (зокрема порушень Кодексу поведінки), або ризиків для прав людини та довкілля, пов'язаних із прямими чи опосередкованими постачальниками, а також порушень прав людини та екологічних зобов'язань відповідно до Закону про комплексну перевірку ланцюгів постачання (LkSG). До них належать порушення Кодексу поведінки OSI, антимонопольного законодавства, корупція, крадіжки, дискримінація, нехтування нормами охорони праці, дитяча праця, забруднення ґрунту, води або повітря, шкідливі шумові викиди, неприйнятне споживання води, виробництво або використання певних стійких органічних забруднювачів, а також несанкціонований імпорт і експорт відходів.

3. доступ до системи:

Викривачі мають доступ до зовнішньої системи звітності різними мовами за адресою:

EthicsPoint - OSI Group, LLC

- у текстовому вигляді через форму на онлайн-порталі або
- по телефону (безкоштовно з різних країн)

III. Обробка звітів:

1. Отримання та первинна оцінка:

Після отримання повідомлення зовнішніми каналами, якими керує система повідомлень, воно спочатку документується та отримує індивідуальний номер файлу. Відділ комплаєнсу OSI отримує всі повідомлення та проводить первинну оцінку, щоб визначити їхню достовірність та обґрунтованість.

2. Розслідування:

За відповідними повідомленнями буде розпочато ретельне, об'єктивне та конфіденційне розслідування. У разі необхідності отримання повідомлень або вжиття заходів, будуть проведені консультації з іншими відділами або звернені до них за допомогою. У викривача також може бути запитана додаткова інформація.

Тривалість розслідування до його завершення залежить від складності справи, необхідних слідчих дій, а також наявності інформації або сторін, залучених до конкретної справи. Буде докладено всіх зусиль, щоб завершити розслідування якомога ефективніше та швидше.

3. зворотній зв'язок з Викривачем:

Викривач отримає зворотній зв'язок про отримання його повідомлення протягом 7 днів, якщо це можливо і не загрожує анонімності.

Якщо викривач подав повідомлення онлайн або телефоном, він отримає інформацію для входу в систему, яка дозволить йому відстежувати повідомлення та отримувати анонімний зворотній зв'язок (за бажанням). Зокрема, може виникнути необхідність поставити уточнюючі запитання та отримати додаткову інформацію.

У подальшому ході розслідування (не пізніше ніж через 3 місяці після отримання підтвердження про отримання) буде надана інформація про стан розслідування щодо запланованих або вже розпочатих заходів або, за відсутності достатніх підстав для підозри, про припинення розслідування.

IV. Захист викривачів:

1. Невідплата:

Ініціатива "Відкритий Діалог" докладає всіх розумних зусиль, щоб забезпечити захист викривачів від будь-яких форм помсти, несприятливого ставлення або інших репресій.

Дисциплінарні стягнення на підставі викриття проти осіб, які добросовісно співпрацюють зі слідством, заборонені і не допускатимуться.

2. конфіденційність:

Особи, які беруть участь у розслідуванні, зобов'язані дотримуватися суворої конфіденційності.

V. Документація та зберігання:

1. Документація:

Всі етапи розслідування ретельно документуються.

Документація забезпечує прозорість і простежуваність процедури.

2. період зберігання:

Документація зберігається відповідно до вимог законодавства та внутрішніх інструкцій.

VI. Перегляд та коригування:

Ці процедурні правила регулярно переглядаються та адаптуються за необхідності, щоб забезпечити їх відповідність чинним законодавчим вимогам та корпоративним цілям.

II. Інформація відповідно до ст. 13 GDPR (для осіб, які надають інформацію):

Ім'я та контактні дані контролера: Див. напис на веб-сайті. Контактні дані відповідального за захист даних та, за необхідності, представника: Професор, доктор Хайко Джонні Маньєро, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Мюнхен, Німеччина. Цілі, для яких обробляються персональні дані, та правові підстави для обробки: Дотримання Закону про захист інформаторів (HinSchG) та Закону про належну перевірку постачальників (LkSG), правова підстава - ст. 6 (1) (c) GDPR у поєднанні зі статтями 8, 9 LkSG та статтею 10 HinSchG, якщо це необхідно для виконання завдань, зазначених у статтях 13 та 24 HinSchG, а також дотримання Директиви (ЄС) 2019/1937 про захист осіб, які повідомляють про порушення законодавства Союзу, та випливаючого з неї національного законодавства держав-членів і дотримання чинного законодавства інших країн. Одержувачі або категорії одержувачів персональних даних: Правоохоронні органи, органи, що накладають штрафи, та інші органи влади, а також адвокати, компанії групи або роботодавці. Запланована передача до третіх країн: Введення в онлайн-систему Navex і подальша передача компаніям групи, роботодавцям або юристам. З Navex укладено Стандартні договірні умови ЄС та Британське доповнення до Стандартних договірних умов ЄС. Navex також є членом Рамкової угоди про захист даних між ЄС та США, Швейцарсько-американської угоди про захист даних та Британського доповнення до Рамкової угоди про захист даних між ЄС та США. Для інших передач рішення про адекватність може не прийматися. Для таких передач застосовуються Стандартні договірні умови ЄС та Британське доповнення до Стандартних договірних умов ЄС. Критерії для визначення терміну зберігання: Документація видаляється через три роки після завершення процедури. Документація може зберігатися довше, щоб відповідати вимогам чинного законодавства, якщо це є необхідним і пропорційним.

Відповідно до Загального регламенту захисту даних, ви маєте право на доступ до персональних даних, що стосуються вас, а також право на виправлення, видалення або обмеження обробки, право на заперечення проти обробки та право на перенесення даних. Ви маєте право подати скаргу до компетентного наглядового органу з питань захисту даних щодо обробки. Надання персональних даних не вимагається законом або договором і не є необхідним для укладення договору, тому ви не зобов'язані надавати персональні дані на гарячу лінію викривачів. Можливими наслідками ненадання є те, що повідомлення не буде оброблено або буде оброблено із затримкою, або його буде відхилено, а також те, що вам не буде надано жодної інформації або відомостей, пов'язаних із повідомленням. Автоматизованого прийняття рішень не існує.

III. Інформація відповідно до ст. 14 GDPR (для інших суб'єктів даних):

Ім'я та контактні дані контролера: Див. напис на веб-сайті. Контактні дані відповідального за захист даних та, за необхідності, представника: Професор, доктор Хайко Джонні Маньєро, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Мюнхен, Німеччина. Цілі, для яких обробляються

персональні дані, та правові підстави для обробки: Дотримання Закону про захист інформаторів (HinSchG) та Закону про належну перевірку постачальників (LkSG), правова підстава - ст. 6 (1) (c) GDPR у поєднанні зі статтями 8, 9 LkSG та статтею 10 HinSchG, якщо це необхідно для виконання завдань, зазначених у статтях 13 та 24 HinSchG, а також дотримання Директиви (ЄС) 2019/1937 про захист осіб, які повідомляють про порушення законодавства Союзу, та випливаючого з неї національного законодавства держав-членів, а також дотримання чинного законодавства інших країн. Категорії оброблюваних персональних даних: Дані про викриття. Одержувачі або категорії одержувачів персональних даних: Правоохоронні органи, органи, що накладають штрафи, та інші органи влади, а також адвокати, компанії групи або роботодавці. Запланована передача в треті країни: Введення в онлайн-систему Navex і подальша передача компаніям групи, роботодавцям або юристам. З Navex укладено Стандартні договірні умови ЄС та Британське доповнення до Стандартних договірних умов ЄС. Navex також є членом Рамкової угоди про захист даних між ЄС та США, Швейцарсько-американської угоди про захист даних та Британського доповнення до Рамкової угоди про захист даних між ЄС та США. Для інших передач рішення про адекватність може не прийматися. Для таких передач застосовуються Стандартні договірні умови ЄС та Британське доповнення до Стандартних договірних умов ЄС. Критерії для визначення терміну зберігання: Документація видаляється через три роки після завершення процедури. Документація може зберігатися довше, щоб відповідати вимогам чинного законодавства, якщо це необхідно і пропорційно. Джерелом персональних даних є викривач та/або відповідна компанія.

Відповідно до Загального регламенту про захист даних, ви можете мати право на доступ до персональних даних, що стосуються вас, а також право на виправлення, видалення або обмеження обробки, право на заперечення проти обробки та право на перенесення даних. Ви маєте право подати скаргу до компетентного наглядового органу з питань захисту даних щодо обробки. Автоматизованого прийняття рішень не відбувається. Надання додаткової інформації виявляється неможливим.

BULGARIAN: Система за подаване на сигнали за нередности (вътрешни канали за докладване)

Нашите ценности са в основата на бизнес практиките ни и отразяват ангажимента ни за почтеност, прозрачност и позитивна корпоративна култура. Нашата система за подаване на сигнали за нередности е основен инструмент за насърчаване на отчетността и осигуряване на етични бизнес операции. Тези процедурни правила служат за прозрачност на процеса и принципите на нашите процеси на разследване и гарантират, че всички доклади, получени чрез нашата система, се обработват по подходящ и професионален начин.

OSI се ангажира с открит диалог и признава значението на лицата, подаващи сигнали за нарушения, като ключови партньори в усилията ни да поддържаме най-високи стандарти във всички области на нашата дейност.

I. Процедурен правилник на системата за подаване на сигнали за нередности на OSI

I. Цел и обхват:

1. Цел: Настоящите процедурни правила уреждат обработката и разследването на сигнали, получени чрез системата за подаване на сигнали за нередности Make It Right Global Hotline. Целта е да се гарантира, че всички получени доклади се обработват прозрачно, ефикасно и в съответствие с етичните стандарти на OSI.

2. Обхват на приложение: Настоящият процедурен правилник се прилага за всички служители, бизнес партньори, доставчици и други заинтересовани страни по цялата верига на стойността, които използват системата за подаване на сигнали за нередности, за да споделят конкретни индикации за възможни нарушения, опасения или съвети. Системата за подаване на сигнали не е предназначена за обработване на опасения, свързани с продукти и услуги. Такива въпроси или проблеми могат да бъдат адресирани директно чрез формуляра за контакт на уебсайта на компанията.

II. Предоставяне на информация:

1. Анонимност и поверителност:

Системата за подаване на сигнали за нередности позволява, наред с другото, анонимно подаване на сигнали за нередности, доколкото това е разрешено от националното законодателство.

Цялата информация, обработвана в рамките на системата за подаване на сигнали, е предмет на строга поверителност.

2. Видове отчети:

Системата дава възможност на лицата, подаващи сигнали за нарушения, да подават сигнали, когато има конкретни данни за възможни нарушения, опасения или признаци за такива. Това се отнася до нарушения от страна на служители или бизнес партньори на приложимите закони, наредби и т.н. (по-специално тези, посочени в член 2 от Закона за защита на лицата, подаващи сигнали за нарушения или Директива 2019/1937 на ЕС) или вътрешнофирмени разпоредби (по-специално нарушения на Кодекса за поведение) или рискове за правата на човека и околната среда, които могат да се припишат на преки или непреки доставчици, както и нарушения на задълженията за правата на човека и околната среда съгласно Закона за комплексна проверка на веригата на доставки (LkSG). Те включват нарушения на Кодекса за поведение на OSI, антитръстовото законодателство, корупция, кражба, дискриминация, пренебрегване на здравето и безопасността на работното място, детски труд, замърсяване на почвата, водата или въздуха, вредни шумови емисии, неприемливо потребление на вода, производство или използване на определени устойчиви органични замърсители и неразрешен внос и износ на отпадъци.

3. Достъп до системата:

Лицата, подаващи сигнали за нередности, имат достъп до външно управляваната система за докладване на различни езици на адрес:

EthicsPoint - OSI Group, LLC

- в текстова форма чрез формуляр в онлайн портала или
- по телефона (безплатно от различни страни)

III. Обработка на докладите:

1. Получаване и първоначална оценка:

След като докладът бъде получен чрез външните канали за докладване, управлявани от системата за сигнализиране, той първо се документира и му се присвоява индивидуален номер на досието. OSI Compliance получава всички доклади и извършва първоначална оценка, за да определи тяхната правдоподобност и валидност.

2. Разследване:

За съответните сигнали ще бъде започнато задълбочено, обективно и поверително разследване. Ако е необходимо да се получат сигнали или да се предприемат действия, ще бъдат консултирани други отдели или ще бъде поискана помощ от тях. От подателя на сигнала може да бъде поискана и допълнителна информация.

Продължителността на разследването до неговото приключване зависи от сложността на случая, необходимите следствени действия и наличието на информация или страни, участващи в конкретния случай. Ще бъдат положени всички усилия за възможно най-ефективно и бързо приключване на разследването.

3. Обратна връзка с подателя на сигнала:

Подателят на сигнала ще получи обратна информация за получаването му в рамките на 7 дни, когато това е възможно и без да се застрашава анонимността.

Ако подателят на сигнала е подал сигнала онлайн или по телефона, той ще получи информация за вход, която му позволява да проследи действията по сигнала и да получи анонимна обратна връзка (ако желае). По-специално, може да се наложи да се зададат въпроси за разбиране и да се получи допълнителна информация.

В по-нататъшния ход на разследването (не по-късно от 3 месеца след получаване на потвърждението за получаване) ще бъде предоставена информация за състоянието на разследването по отношение на планираните или вече предприетите мерки или, ако няма достатъчно подозрения, за прекратяването на разследването.

IV. Защита на лицата, подаващи сигнали за нередности:

1. Недопускане на репресии:

OSI полага всички разумни усилия, за да гарантира, че лицата, подаващи сигнали за нередности, ще бъдат защитени от всякакви форми на отмъщение, неблагоприятно положение или други репресии.

Дисциплинарните действия, основани на подаване на сигнали за нередности срещу лица, които добросъвестно сътрудничат на разследванията, са забранени и няма да бъдат толерирани.

2. Конфиденциалност:

Лицата, участващи в разследването, са задължени да спазват строга поверителност.

V. Документиране и съхранение:

1. Документация:

Всички етапи на разследването се документират внимателно.

Документацията служи за прозрачност и проследимост на процедурата.

2. Период на съхранение:

Документацията се съхранява в съответствие със законовите изисквания и вътрешните насоки.

VI. Преглед и корекция:

Тези процедурни правила редовно се преразглеждат и при необходимост се адаптират, за да се гарантира, че те отговарят на действащите правни изисквания и корпоративните цели.

II. Информация съгласно чл. 13 от ОРЗД (за лицата, които предоставят информация):

Име и данни за контакт на администратора: Вижте отпечатъка на уебсайта. Данни за контакт на длъжностното лице по защита на данните и, ако е приложимо, на представителя: Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Мюнхен, Германия. Цели, за които ще се обработват личните данни, и правно основание за обработката: Спазване на Закона за защита на лицата, подаващи сигнали за нередности (HinSchG) и Закона за надлежна проверка на веригата на доставки (LkSG), правното основание е чл. 6, параграф 1, буква в) от ОРЗД във връзка с чл. 8, 9 от LkSG и чл. 10 от HinSchG, доколкото това е необходимо за изпълнение на задачите, посочени в чл. 13 и 24 от HinSchG, както и спазването на Директива (ЕС) 2019/1937 относно защитата на лицата, които подават сигнали за нарушения на правото на Съюза и произтичащото от нея национално законодателство на държавите членки и спазването на приложимото законодателство на други държави. Получатели или категории получатели на лични данни: Правоприлагащи органи, органи за налагане на глоби и други органи, както и адвокати, дружества от групата или работодатели. Планирано предаване на данни на трети държави: Въвеждане в онлайн системата на Navex и последващо предаване на структури в рамките на групата, работодатели или адвокати. Стандартните договорни клаузи на ЕС и допълнението на Обединеното кралство към стандартните договорни клаузи на ЕС са сключени с Navex. Navex също така е член на Рамката за защита на личните данни между ЕС и САЩ, Рамката за защита на личните данни между Швейцария и САЩ и Разширението на Обединеното кралство към Рамката за защита на личните данни между ЕС и САЩ. За други предавания на данни може да няма решение за адекватност. За такива предавания се използват Стандартните договорни клаузи на ЕС и допълнението на Обединеното кралство към Стандартните договорни клаузи на ЕС. Критерии за определяне на периода на съхранение: Документацията се заличава три години след приключване на процедурата. Документацията може да се съхранява по-дълго, за да се изпълнят изискванията на приложимото законодателство, ако това е необходимо и пропорционално.

Съгласно Общия регламент относно защитата на данните имате право на достъп до личните данни, които ви засягат, и право на коригиране, изтриване или ограничаване на обработката, или право на възражение срещу обработката, както и право на преносимост на данните. Имате право да подадете жалба до компетентния надзорен орган за защита на данните във връзка с обработването. Предоставянето на лични данни не се изисква по закон или договор и не е

необходимо за сключването на договор, поради което не сте задължени да предоставяте лични данни на горещата линия за подаване на сигнали. Възможните последици от непредоставянето на данни са, че сигналът няма да бъде обработен или ще бъде обработен със закъснение, или ще бъде отхвърлен, както и че няма да може да ви бъде предоставена информация или информация, свързана със сигнала. Няма автоматизирано вземане на решения.

III. Информация съгласно чл. 14 от ОРЗД (за други субекти на данни):

Име и данни за контакт на администратора: Вижте отпечатъка на уебсайта. Данни за контакт на длъжностното лице по защита на данните и, ако е приложимо, на представителя: Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Мюнхен, Германия. Цели, за които ще се обработват личните данни, и правно основание за обработката: Спазване на Закона за защита на лицата, подаващи сигнали за нередности (HinSchG) и Закона за надлежна проверка на веригата на доставки (LkSG), правното основание е чл. 6, параграф 1, буква в) от ОРЗД във връзка с чл. 8, 9 от LkSG и чл. 10 от HinSchG, доколкото това е необходимо за изпълнение на задачите, посочени в чл. 13 и 24 от HinSchG, както и спазването на Директива (ЕС) 2019/1937 относно защитата на лицата, които подават сигнали за нарушения на правото на Съюза и произтичащото от нея национално законодателство на държавите членки и спазването на приложимото законодателство на други държави. Категории обработвани лични данни: Данни за подаване на сигнали за нередности. Получатели или категории получатели на лични данни: Правоприлагащи органи, органи за налагане на глоби и други органи, както и адвокати, дружества от групата или работодатели. Планирано предаване на данни на трети държави: Въвеждане в онлайн системата на Navex и последващо предаване на структури в рамките на групата, работодатели или адвокати. Стандартните договорни клаузи на ЕС и допълнението на Обединеното кралство към стандартните договорни клаузи на ЕС са сключени с Navex. Navex също така е член на Рамката за защита на личните данни между ЕС и САЩ, Рамката за защита на личните данни между Швейцария и САЩ и Разширението на Обединеното кралство към Рамката за защита на личните данни между ЕС и САЩ. За други предавания на данни може да няма решение за адекватност. За такива предавания се използват Стандартните договорни клаузи на ЕС и допълнението на Обединеното кралство към Стандартните договорни клаузи на ЕС. Критерии за определяне на периода на съхранение: Документацията се заличава три години след приключване на процедурата. Документацията може да се съхранява по-дълго, за да се изпълнят изискванията на приложимото законодателство, ако това е необходимо и пропорционално. Източникът на личните данни е подателят на сигнала и/или съответното дружество.

Съгласно Общия регламент относно защитата на данните може да имате право на достъп до личните данни, които се отнасят до вас, и право на коригиране, изтриване или ограничаване на обработката, или право на възражение срещу обработката и право на преносимост на данните. Имате право да подадете жалба до компетентния надзорен орган за защита на данните във

връзка с обработването. Няма автоматизирано вземане на решения. Предоставянето на допълнителна информация се оказва невъзможно.

CZECH: Systém pro oznamovatele (interní kanály pro podávání zpráv)

Naše hodnoty tvoří základ našich obchodních postupů a odrážejí náš závazek k integritě, transparentnosti a pozitivní firemní kultuře. Náš systém oznamování je základním nástrojem pro podporu odpovědnosti a zajištění etických obchodních operací. Tento jednací řád slouží k tomu, aby proces a zásady našich vyšetřovacích postupů byly transparentní a aby bylo zajištěno, že všechna oznámení přijatá prostřednictvím našeho systému budou zpracována vhodně a profesionálně.

Společnost OSI se zavázala k otevřenému dialogu a uznává význam oznamovatelů jako klíčových partnerů v našem úsilí o zachování nejvyšších standardů ve všech oblastech našeho podnikání.

I. Jednací řád systému OSI pro oznamovatele

I. Účel a oblast působnosti:

1. Účel: Tento jednací řád upravuje zpracování a vyšetřování oznámení přijatých prostřednictvím systému globální horké linky Make It Right. Cílem je zajistit, aby všechna přijatá oznámení byla vyřizována transparentně, efektivně a v souladu s etickými normami společnosti OSI.

2. Oblast použití: Tento jednací řád se vztahuje na všechny zaměstnance, obchodní partnery, dodavatele a další zúčastněné strany v celém hodnotovém řetězci, kteří využívají systém oznamovatelů ke sdílení konkrétních informací o možném pochybení, obav nebo tipů. Systém whistleblowerů není určen pro zpracování obav týkajících se produktů a služeb. Takové dotazy nebo problémy lze řešit přímo prostřednictvím kontaktního formuláře na webových stránkách společnosti.

II. Předkládání informací:

1. Anonymita a důvěrnost:

Systém pro oznamovatele umožňuje mimo jiné anonymní podávání oznámení v rozsahu povoleném vnitrostátními právními předpisy.

Veškeré informace zpracovávané v rámci systému pro oznamovatele podléhají přísné důvěrnosti.

2. Typy zpráv:

Systém umožňuje oznamovatelům podávat oznámení v případě, že existují konkrétní náznaky možného pochybení, obavy nebo náznaky takového pochybení. Jedná se o porušení platných zákonů, předpisů atd. ze strany zaměstnanců nebo obchodních partnerů (zejména těch, které jsou uvedeny v § 2 zákona o ochraně oznamovatelů nebo ve směrnici EU 2019/1937) nebo interních předpisů společnosti (zejména porušení etického kodexu) nebo o rizika v oblasti lidských práv a životního prostředí, která lze přičíst přímým nebo nepřímým dodavatelům, jakož i o porušení povinností v oblasti lidských práv a životního

prostředí podle zákona o náležité péči v dodavatelském řetězci (LkSG). Patří mezi ně porušení Kodexu chování OSI, antimonopolního zákona, korupce, krádeže, diskriminace, nedodržování bezpečnosti a ochrany zdraví při práci, dětská práce, znečištění půdy, vody nebo ovzduší, škodlivé emise hluku, nepřijatelná spotřeba vody, výroba nebo používání některých perzistentních organických znečišťujících látek a neoprávněný dovoz a vývoz odpadu.

3. Přístup do systému:

Oznamovatelé mají přístup k externě spravovanému systému oznamování v různých jazycích na adrese:

EthicsPoint - OSI Group, LLC

- v textové podobě prostřednictvím formuláře na online portálu nebo
- telefonicky (bezplatně z různých zemí).

III. Zpracování zpráv:

1. Příjem a prvotní posouzení:

Jakmile je hlášení přijato prostřednictvím externích kanálů pro podávání hlášení spravovaných systémem pro oznamovatele, je nejprve zdokumentováno a je mu přiděleno individuální číslo spisu. OSI Compliance obdrží všechna hlášení a provede prvotní posouzení, aby určil jejich věrohodnost a platnost.

2. Vyšetřování:

V případě relevantních tipů bude zahájeno důkladné, objektivní a důvěrné vyšetřování. V případě potřeby přijetí oznámení nebo přijetí opatření budou konzultovány nebo požádány o pomoc další útvary. Od oznamovatele mohou být rovněž vyžádány další informace.

Doba trvání vyšetřování až do jeho ukončení závisí na složitosti případu, potřebných vyšetřovacích opatřeních a dostupnosti informací nebo stran zapojených do konkrétního případu. Bude vyvinuto veškeré úsilí, aby bylo vyšetřování dokončeno co nejefektivněji a nejrychleji.

3. Zpětná vazba pro oznamovatele:

Oznamovatel obdrží zpětnou vazbu o přijetí svého tipu do 7 dnů, pokud je to možné a bez ohrožení anonymity.

Pokud oznamovatel podal oznámení online nebo telefonicky, obdrží přihlašovací údaje, které mu umožní na oznámení navázat a získat anonymní zpětnou vazbu (pokud si to přeje). Zejména může být nutné klást otázky na porozumění a získat další informace.

V dalším průběhu šetření (nejpozději do 3 měsíců od obdržení potvrzení o přijetí) budou poskytnuty informace o stavu šetření, pokud jde o plánovaná nebo již zahájená opatření, nebo v případě nedostatečného podezření o zastavení šetření.

IV. Ochrana oznamovatelů:

1. Zákaz odvetných opatření:

Společnost OSI vyvíjí veškeré přiměřené úsilí, aby zajistila, že oznamovatelé budou chráněni před jakoukoli formou odplaty, znevýhodnění nebo jiné odvety.

Disciplinární opatření na základě whistleblowingu proti osobám, které v dobré víře spolupracují při vyšetřování, jsou zakázána a nebudou tolerována.

2. Důvěrnost:

Osoby zapojené do vyšetřování jsou vázány přísnou mlčenlivostí.

V. Dokumentace a skladování:

1. Dokumentace:

Všechny kroky šetření jsou pečlivě zdokumentovány.

Dokumentace slouží k transparentnosti a sledovatelnosti postupu.

2. Doba uchovávání:

Dokumentace je uchovávána v souladu s právními požadavky a interními pokyny.

VI. Přezkum a úprava:

Tato procesní pravidla jsou pravidelně revidována a podle potřeby upravována, aby byla v souladu s aktuálními právními požadavky a podnikovými cíli.

II. Informace podle čl. 13 GDPR (pro osoby poskytující informace):

Jméno a kontaktní údaje správce: Kontaktní údaje: viz otisk na webových stránkách. Kontaktní údaje pověřence pro ochranu osobních údajů a případně zástupce: Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Mnichov, Německo. Účely, pro které mají být osobní údaje zpracovávány, a právní základ pro zpracování: Dodržování zákona o ochraně oznamovatelů (HinSchG) a zákona o náležité péči v dodavatelském řetězci (LkSG), právním základem je čl. 2 odst. 1 písm. a) zákona o ochraně osobních údajů. 6 odst. 1 písm. c) GDPR ve spojení s § 8, 9 LkSG a § 10 HinSchG, pokud je to nezbytné pro plnění úkolů uvedených v § 13 a 24 HinSchG, jakož i dodržování směrnice (EU) 2019/1937 o ochraně osob podávajících oznámení o porušení práva Unie a z ní vyplývajícího vnitrostátního práva členských států a dodržování platných právních předpisů jiných zemí. Příjemci nebo kategorie příjemců osobních údajů: Orgány činné v trestním řízení, orgány ukládající pokuty a další orgány, jakož i advokáti, společnosti ve skupině nebo zaměstnavatelé. Plánované předání do

třetích zemí: Vložení do online systému Navex a následné předání subjektům v rámci skupiny, zaměstnavatelům nebo právníkům. Se společností Navex byly uzavřeny standardní smluvní doložky EU a dodatek Spojeného království ke standardním smluvním doložkám EU. Společnost Navex je rovněž členem Rámce pro ochranu osobních údajů mezi EU a USA, Rámce pro ochranu osobních údajů mezi Švýcarskem a USA a Rozšíření Rámce pro ochranu osobních údajů mezi EU a USA ve Spojeném království. V případě jiných předávání nemusí být rozhodnutí o odpovídající ochraně vydáno. Pro taková předávání se používají standardní smluvní doložky EU a dodatek Spojeného království ke standardním smluvním doložkám EU. Kritéria pro určení doby uchovávání: Dokumentace se vymaže tři roky po ukončení řízení. Dokumentace může být uchovávána déle, aby byly splněny požadavky platných právních předpisů, pokud je to nezbytné a přiměřené.

Podle obecného nařízení o ochraně osobních údajů máte právo na přístup k osobním údajům, které se vás týkají, a právo na opravu nebo výmaz nebo omezení zpracování nebo právo vznést námitku proti zpracování a právo na přenositelnost údajů. Máte právo podat stížnost na zpracování u příslušného dozorového úřadu pro ochranu osobních údajů. Poskytnutí osobních údajů není vyžadováno zákonem ani smlouvou a není nezbytné pro uzavření smlouvy, proto nejste povinni poskytnout osobní údaje na horkou linku pro oznamování. Možné důsledky neposkytnutí údajů spočívají v tom, že oznámení nebude zpracováno nebo bude zpracováno se zpožděním, případně bude odmítnuto a že vám nebudou moci být poskytnuty žádné informace nebo informace týkající se oznámení. Neexistuje žádné automatizované rozhodování.

III. Informace podle čl. 14 GDPR (pro ostatní subjekty údajů):

Jméno a kontaktní údaje správce: Kontaktní údaje: viz otisk na webových stránkách. Kontaktní údaje pověřence pro ochranu osobních údajů a případně zástupce: Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Mnichov, Německo. Účely, pro které mají být osobní údaje zpracovávány, a právní základ pro zpracování: Dodržování zákona o ochraně oznamovatelů (HinSchG) a zákona o náležité péči v dodavatelském řetězci (LkSG), právním základem je čl. 4 odst. 1 písm. a) zákona o ochraně osobních údajů. 6 odst. 1 písm. c) GDPR ve spojení s § 8, 9 LkSG a § 10 HinSchG, pokud je to nezbytné pro plnění úkolů uvedených v § 13 a 24 HinSchG, jakož i dodržování směrnice (EU) 2019/1937 o ochraně osob podávajících oznámení o porušení práva Unie a z ní vyplývajícího vnitrostátního práva členských států a dodržování platných právních předpisů jiných zemí. Kategorie zpracovávaných osobních údajů: Údaje o whistleblowingu. Příjemci nebo kategorie příjemců osobních údajů: Orgány činné v trestním řízení, orgány ukládající pokuty a další orgány, jakož i právníci, společnosti ve skupině nebo zaměstnavatelé. Plánované předání do třetích zemí: Vložení do online systému Navex a následné předání subjektům v rámci skupiny, zaměstnavatelům nebo právníkům. Se společností Navex byly uzavřeny standardní smluvní doložky EU a dodatek Spojeného království ke standardním smluvním doložkám EU. Společnost Navex je rovněž členem Rámce pro ochranu osobních údajů mezi EU a USA, Rámce pro ochranu osobních údajů mezi Švýcarskem a USA a Rozšíření Rámce pro ochranu osobních údajů mezi EU a USA ve Spojeném království. V případě jiných

předávání nemusí být rozhodnutí o odpovídající ochraně vydáno. Pro taková předávání se používají standardní smluvní doložky EU a dodatek Spojeného království ke standardním smluvním doložkám EU. Kritéria pro určení doby uchovávání: Dokumentace se vymaže tři roky po ukončení řízení. Dokumentace může být uchovávána déle, aby byly splněny požadavky platných právních předpisů, pokud je to nezbytné a přiměřené. Zdrojem osobních údajů je oznamovatel a/nebo dotčená společnost.

Podle obecného nařízení o ochraně osobních údajů můžete mít právo na přístup k osobním údajům, které se vás týkají, a právo na opravu nebo výmaz nebo omezení zpracování nebo právo vznést námitku proti zpracování a právo na přenositelnost údajů. V souvislosti se zpracováním máte právo podat stížnost u příslušného dozorového úřadu pro ochranu osobních údajů. Neexistuje žádné automatizované rozhodování. Poskytnutí dalších informací se ukáže jako nemožné.

DANISH: Whistleblower-system (interne rapporteringskanaler)

Vores værdier danner grundlaget for vores forretningspraksis og afspejler vores engagement i integritet, gennemsigtighed og en positiv virksomhedskultur. Vores whistleblowing-system er et vigtigt redskab til at fremme ansvarlighed og sikre etisk forretningsdrift. Disse procedureregler tjener til at gøre processen og principperne for vores undersøgelsesprocesser gennemsigtige og sikre, at alle rapporter, der modtages gennem vores system, håndteres korrekt og professionelt.

OSI er forpligtet til åben dialog og anerkender vigtigheden af whistleblowere som vigtige partnere i vores bestræbelser på at opretholde de højeste standarder inden for alle områder af vores forretning.

I. Forretningsorden for OSI's whistleblower-system

I. Formål og anvendelsesområde:

1. Formål: Denne forretningsorden regulerer håndteringen og undersøgelsen af rapporter, der modtages via Make It Right Global Hotline whistleblowing-systemet. Formålet er at sikre, at alle modtagne rapporter håndteres gennemsigtigt, effektivt og i overensstemmelse med OSI's etiske standarder.

2. Anvendelsesområde: Denne forretningsorden gælder for alle medarbejdere, forretningspartnere, leverandører og andre interessenter i hele værdikæden, som bruger whistleblower-systemet til at dele specifikke indikationer på mulig forseelse, bekymringer eller tips. Whistleblower-systemet er ikke beregnet til behandling af produkt- og servicerelaterede bekymringer. Sådanne spørgsmål eller problemer kan adresseres direkte via kontaktformularen på virksomhedens hjemmeside.

II. Indsendelse af oplysninger:

1. anonymitet og fortrolighed:

Whistleblower-ordningen giver blandt andet mulighed for anonym indsendelse af whistleblower-rapporter, i det omfang det er tilladt i henhold til national lovgivning.

Alle oplysninger, der håndteres inden for rammerne af whistleblower-ordningen, er underlagt streng fortrolighed.

2. Typer af rapporter:

Systemet gør det muligt for whistleblowere at indsende rapporter, hvor der er konkrete indikationer på mulige forseelser, bekymringer eller indikationer på sådanne. Det drejer sig om medarbejderes eller forretningspartneres overtrædelser af gældende love, bestemmelser osv. (især dem, der er nævnt i § 2 i Whistleblower Protection Act eller EU-direktiv 2019/1937) eller interne virksomhedsregler (især overtrædelser af Code of Conduct) eller menneskerettigheds- og miljørisici, der kan tilskrives direkte eller

indirekte leverandører, samt overtrædelser af menneskerettigheds- og miljøforpligtelser i henhold til Supply Chain Due Diligence Act (LkSG). Disse omfatter overtrædelser af OSI's adfærdskodeks, antitrustlovgivning, korruption, tyveri, diskrimination, tilsidesættelse af sundhed og sikkerhed på arbejdspladsen, børnearbejde, jord-, vand- eller luftforurening, skadelige støjemissioner, uacceptabelt vandforbrug, produktion eller brug af visse persistente organiske forurenende stoffer og uautoriseret import og eksport af affald.

3. adgang til systemet:

Whistleblowere har adgang til det eksternt administrerede rapporteringssystem på forskellige sprog på:

EthicsPoint - OSI Group, LLC

- i tekstform via en formular i onlineportalen eller
- via telefon (gratis fra forskellige lande)

III. Behandling af rapporter:

1. Modtagelse og indledende vurdering:

Når en indberetning er modtaget via de eksterne indberetningskanaler, der administreres af whistleblowersystemet, bliver den først dokumenteret og tildelt et individuelt sagsnummer. OSI Compliance modtager alle indberetninger og foretager en indledende vurdering for at fastslå deres troværdighed og gyldighed.

2. Undersøgelse:

Der iværksættes en grundig, objektiv og fortrolig undersøgelse af relevante tips. Hvis det er nødvendigt for at modtage rapporter eller træffe foranstaltninger, vil andre afdelinger blive konsulteret eller bedt om hjælp. Der kan også blive bedt om yderligere oplysninger fra whistlebloweren.

Varigheden af en undersøgelse indtil dens afslutning afhænger af sagens kompleksitet, de nødvendige undersøgelsesforanstaltninger og tilgængeligheden af oplysninger eller parter, der er involveret i den enkelte sag. Der vil blive gjort alt for at afslutte undersøgelsen så effektivt og hurtigt som muligt.

3. Feedback til whistlebloweren:

Whistlebloweren vil modtage feedback om modtagelsen af deres tip inden for 7 dage, hvor det er muligt og uden at bringe anonymiteten i fare.

Hvis whistlebloweren har indsendt rapporten online eller via telefon, vil de modtage login-oplysninger, der gør det muligt for dem at følge op på rapporten og modtage anonym feedback (hvis de ønsker det). Det kan især være nødvendigt at stille forståelsesspørgsmål og indhente yderligere oplysninger.

I det videre forløb af undersøgelsen (senest 3 måneder efter modtagelsen af bekræftelsen på modtagelsen) vil der blive givet oplysninger om status for undersøgelsen med hensyn til planlagte eller allerede iværksatte foranstaltninger eller, hvis der ikke er tilstrækkelig mistanke, om afbrydelse af undersøgelsen.

IV. Beskyttelse af whistleblowere:

1. Ingen repressalier:

OSI gør alt, hvad der er rimeligt for at sikre, at whistleblowere beskyttes mod enhver form for repressalier, ulempe eller andre repressalier.

Disciplinære foranstaltninger baseret på whistleblowing mod personer, der samarbejder i god tro med undersøgelser, er forbudt og vil ikke blive tolereret.

2. fortrolighed:

Personer, der er involveret i undersøgelsen, er bundet af streng fortrolighed.

V. Dokumentation og opbevaring:

1. Dokumentation:

Alle trin i undersøgelsen dokumenteres omhyggeligt.

Dokumentationen tjener procedurens gennemsigtighed og sporbarhed.

2. Opbevaringsperiode:

Dokumentation opbevares i overensstemmelse med lovkrav og interne retningslinjer.

VI. Gennemgang og justering:

Disse procedureregler gennemgås regelmæssigt og tilpasses efter behov for at sikre, at de er i overensstemmelse med gældende lovkrav og virksomhedens mål.

II. Oplysninger i henhold til art. 13 GDPR (for personer, der giver oplysninger):

Navn og kontaktoplysninger på den dataansvarlige: Se aftryk på hjemmesiden. Kontaktoplysninger på den databeskyttelsesansvarlige og, hvis relevant, repræsentanten: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 München, Tyskland. Formål, som personoplysningerne skal behandles til, og retsgrundlaget for behandlingen: Overholdelse af loven om beskyttelse af whistleblowere (HinSchG) og loven om due diligence i forsyningskæden (LkSG), retsgrundlaget er Art. 6 (1) (c) GDPR i forbindelse med §§ 8, 9 LkSG og § 10 HinSchG, for så vidt dette

er nødvendigt for at udføre de opgaver, der er angivet i §§ 13 og 24 HinSchG, samt overholdelse af direktiv (EU) 2019/1937 om beskyttelse af personer, der indberetter overtrædelser af EU-retten, og den deraf følgende nationale lovgivning i medlemsstaterne og overholdelse af gældende lovgivning fra andre lande. Modtagere eller kategorier af modtagere af personoplysningerne: Retshåndhævende myndigheder, bødemyndigheder og andre myndigheder samt advokater, koncernselskaber eller arbejdsgivere. Planlagt overførsel til tredjelande: Indtastning i Navex' onlinesystem og videre overførsel til enheder inden for koncernen, arbejdsgivere eller advokater. EU's standardkontraktbestemmelser og det britiske tillæg til EU's standardkontraktbestemmelser er indgået med Navex. Navex er også medlem af EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework og UK Extension to the EU-U.S. Data Privacy Framework. For andre overførsler er der muligvis ingen afgørelse om tilstrækkeligheden af beskyttelsesniveauet. EU's standardkontraktbestemmelser og det britiske tillæg til EU's standardkontraktbestemmelser anvendes til sådanne overførsler. Kriterier for bestemmelse af opbevaringsperioden: Dokumentationen slettes tre år efter afslutningen af proceduren. Dokumentationen kan opbevares i længere tid for at opfylde kravene i den gældende lovgivning, hvis det er nødvendigt og proportionelt.

I henhold til den generelle forordning om databeskyttelse har du ret til adgang til personoplysninger om dig og ret til berigtigelse eller sletning eller begrænsning af behandling eller ret til at gøre indsigelse mod behandling og ret til dataportabilitet. Du har ret til at indgive en klage til den kompetente tilsynsmyndighed for databeskyttelse vedrørende behandlingen. Levering af personoplysninger er ikke påkrævet ved lov eller kontrakt og er ikke nødvendig for indgåelse af en kontrakt, hvorfor du ikke er forpligtet til at levere personoplysninger til whistleblowing-hotlinen. Mulige konsekvenser af ikke at give oplysninger er, at rapporten ikke vil blive behandlet eller vil blive behandlet med forsinkelse, eller at den vil blive afvist, og at ingen oplysninger eller oplysninger vedrørende rapporten kan gives til dig. Der er ingen automatiseret beslutningstagning.

III. Oplysninger i henhold til art. 14 i GDPR (for andre registrerede):

Navn og kontaktoplysninger på den dataansvarlige: Se aftryk på hjemmesiden. Kontaktoplysninger på den databeskyttelsesansvarlige og, hvis relevant, repræsentanten: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 München, Tyskland. Formål, som personoplysningerne skal behandles til, og retsgrundlaget for behandlingen: Overholdelse af Whistleblower Protection Act (HinSchG) og Supply Chain Due Diligence Act (LkSG), retsgrundlaget er Art. 6 (1) (c) GDPR i forbindelse med §§ 8, 9 LkSG og § 10 HinSchG, for så vidt dette er nødvendigt for at udføre de opgaver, der er angivet i §§ 13 og 24 HinSchG, samt overholdelse af direktiv (EU) 2019/1937 om beskyttelse af personer, der indberetter overtrædelser af EU-retten, og den deraf følgende nationale lovgivning i medlemsstaterne og overholdelse af gældende lovgivning fra andre lande. Kategorier af behandlede personoplysninger: Oplysninger om whistleblowing. Modtagere eller kategorier af modtagere af personoplysningerne: Retshåndhævende myndigheder, bødemyndigheder og andre myndigheder samt advokater, koncernselskaber eller arbejdsgivere. Planlagt overførsel til

tredjelande: Indtastning i Navex' onlinesystem og videreoverførsel til enheder i koncernen, arbejdsgivere eller advokater. EU's standardkontraktbestemmelser og det britiske tillæg til EU's standardkontraktbestemmelser er indgået med Navex. Navex er også medlem af EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework og UK Extension to the EU-U.S. Data Privacy Framework. For andre overførsler er der muligvis ingen afgørelse om tilstrækkeligheden af beskyttelsesniveauet. EU's standardkontraktbestemmelser og det britiske tillæg til EU's standardkontraktbestemmelser anvendes til sådanne overførsler. Kriterier for bestemmelse af opbevaringsperioden: Dokumentationen slettes tre år efter afslutningen af proceduren. Dokumentationen kan opbevares i længere tid for at opfylde kravene i gældende lovgivning, hvis dette er nødvendigt og proportionelt. Kilden til de personlige data er whistleblowerens og/eller den pågældende virksomhed.

I henhold til den generelle forordning om databeskyttelse kan du have ret til adgang til personoplysninger om dig og ret til berigtigelse eller sletning eller begrænsning af behandling eller ret til at gøre indsigelse mod behandling og ret til dataportabilitet. Du har ret til at indgive en klage til den kompetente tilsynsmyndighed for databeskyttelse med hensyn til behandlingen. Der er ingen automatiseret beslutningstagning. Det viser sig at være umuligt at give yderligere oplysninger.

GREEK: Σύστημα καταγγελιών (εσωτερικοί δίαυλοι αναφοράς)

Οι αξίες μας αποτελούν το θεμέλιο για τις επιχειρηματικές μας πρακτικές και αντανακλούν τη δέσμευσή μας για ακεραιότητα, διαφάνεια και θετική εταιρική κουλτούρα. Το σύστημά μας για την καταγγελία είναι ένα ουσιαστικό εργαλείο για την προώθηση της λογοδοσίας και τη διασφάλιση ηθικών επιχειρηματικών δραστηριοτήτων. Αυτοί οι διαδικαστικοί κανόνες χρησιμεύουν για να καταστήσουν τη διαδικασία και τις αρχές των διαδικασιών διερεύνησής μας διαφανείς και να διασφαλίσουν ότι όλες οι αναφορές που λαμβάνονται μέσω του συστήματός μας αντιμετωπίζονται κατάλληλα και επαγγελματικά.

Η OSI δεσμεύεται για ανοικτό διάλογο και αναγνωρίζει τη σημασία των πληροφοριοδοτών ως βασικών εταίρων στις προσπάθειές μας να διατηρήσουμε τα υψηλότερα πρότυπα σε όλους τους τομείς της επιχείρησής μας.

I. Διαδικαστικός κανονισμός για το σύστημα καταγγελιών του OSI

I. Σκοπός και πεδίο εφαρμογής:

1. Σκοπός: Ο παρών εσωτερικός κανονισμός διέπει το χειρισμό και τη διερεύνηση των αναφορών που λαμβάνονται μέσω του συστήματος καταγγελίας καταγγελιών Make It Right Global Hotline. Στόχος είναι να διασφαλιστεί ότι όλες οι αναφορές που λαμβάνονται αντιμετωπίζονται με διαφάνεια, αποτελεσματικότητα και σύμφωνα με τα δεοντολογικά πρότυπα της OSI.

2. Οι παρόντες διαδικαστικοί κανόνες ισχύουν για όλους τους εργαζόμενους, τους επιχειρηματικούς εταίρους, τους προμηθευτές και άλλους ενδιαφερόμενους φορείς σε όλη την αλυσίδα αξίας που χρησιμοποιούν το σύστημα καταγγελιών για να μοιραστούν συγκεκριμένες ενδείξεις πιθανών παραπτωμάτων, ανησυχίες ή συμβουλές. Το σύστημα καταγγελιών δεν προορίζεται για την επεξεργασία ανησυχιών που σχετίζονται με προϊόντα και υπηρεσίες. Τέτοιες ερωτήσεις ή ζητήματα μπορούν να απευθύνονται απευθείας μέσω της φόρμας επικοινωνίας στον ιστότοπο της εταιρείας.

II. Υποβολή πληροφοριών:

1. Ανωνυμία και εμπιστευτικότητα:

Το σύστημα καταγγελιών επιτρέπει, μεταξύ άλλων, την ανώνυμη υποβολή αναφορών καταγγελιών, στο βαθμό που επιτρέπεται από την εθνική νομοθεσία.

Όλες οι πληροφορίες που διαχειρίζονται στο πλαίσιο του συστήματος καταγγελίας υπόκεινται σε αυστηρή εμπιστευτικότητα.

2. Τύποι εκθέσεων:

Το σύστημα δίνει τη δυνατότητα στους πληροφοριοδότες να υποβάλλουν αναφορές όταν υπάρχουν συγκεκριμένες ενδείξεις για πιθανό παράπτωμα, ανησυχίες ή ενδείξεις για κάτι τέτοιο. Αυτό αφορά

παραβιάσεις από εργαζόμενους ή επιχειρηματικούς εταίρους των εφαρμοστέων νόμων, κανονισμών κ.λπ. (ιδίως εκείνων που αναφέρονται στο άρθρο 2 του νόμου περί προστασίας των πληροφοριοδοτών ή στην οδηγία 2019/1937 της ΕΕ) ή εσωτερικών κανονισμών της εταιρείας (ιδίως παραβιάσεις του κώδικα δεοντολογίας) ή των ανθρωπίνων δικαιωμάτων και των περιβαλλοντικών κινδύνων που οφείλονται σε άμεσους ή έμμεσους προμηθευτές, καθώς και παραβιάσεις των υποχρεώσεων για τα ανθρώπινα δικαιώματα και το περιβάλλον βάσει του νόμου περί δέουσας επιμέλειας στην εφοδιαστική αλυσίδα (LkSG). Αυτές περιλαμβάνουν παραβιάσεις του Κώδικα Δεοντολογίας της OSI, του αντιμονοπωλιακού δικαίου, της διαφθοράς, της κλοπής, των διακρίσεων, της περιφρόνησης της επαγγελματικής υγείας και ασφάλειας, της παιδικής εργασίας, της ρύπανσης του εδάφους, του νερού ή του αέρα, των επιβλαβών εκπομπών θορύβου, της απαράδεκτης κατανάλωσης νερού, της παραγωγής ή χρήσης ορισμένων έμμονων οργανικών ρύπων και της μη εξουσιοδοτημένης εισαγωγής και εξαγωγής αποβλήτων.

3. Πρόσβαση στο σύστημα:

Οι καταγγέλλοντες έχουν πρόσβαση στο εξωτερικά διαχειριζόμενο σύστημα αναφοράς σε διάφορες γλώσσες στη διεύθυνση:

EthicsPoint - OSI Group, LLC

- σε μορφή κειμένου μέσω φόρμας στην ηλεκτρονική πύλη ή
- μέσω τηλεφώνου (χωρίς χρέωση από διάφορες χώρες)

III. Επεξεργασία των εκθέσεων:

1. Παραλαβή και αρχική αξιολόγηση:

Μόλις παραληφθεί μια αναφορά μέσω των εξωτερικών διαύλων αναφοράς που διαχειρίζεται το σύστημα καταγγελιών, καταρχάς τεκμηριώνεται και της αποδίδεται ατομικός αριθμός φακέλου. Η OSI Compliance λαμβάνει όλες τις αναφορές και διενεργεί μια αρχική αξιολόγηση για να προσδιορίσει την αληθοφάνεια και την εγκυρότητά τους.

2. Έρευνα:

Για τις σχετικές πληροφορίες θα ξεκινήσει μια ενδελεχής, αντικειμενική και εμπιστευτική έρευνα. Εάν είναι απαραίτητο για τη λήψη αναφορών ή τη λήψη μέτρων, θα ζητείται η γνώμη ή η συνδρομή άλλων υπηρεσιών. Μπορεί επίσης να ζητηθούν πρόσθετες πληροφορίες από τον καταγγέλλοντα.

Η διάρκεια μιας έρευνας μέχρι την ολοκλήρωσή της εξαρτάται από την πολυπλοκότητα της υπόθεσης, τα απαιτούμενα ερευνητικά μέτρα και τη διαθεσιμότητα των πληροφοριών ή των εμπλεκόμενων μερών στην εκάστοτε υπόθεση. Θα καταβληθεί κάθε δυνατή προσπάθεια για την όσο το δυνατόν αποτελεσματικότερη και ταχύτερη ολοκλήρωση της έρευνας.

3. Ανατροφοδότηση του πληροφοριοδότη:

Ο πληροφοριοδότης θα λάβει ανατροφοδότηση σχετικά με την παραλαβή της πληροφορίας του εντός 7 ημερών, όπου είναι δυνατόν και χωρίς να τίθεται σε κίνδυνο η ανωνυμία.

Εάν ο καταγγέλλων έχει υποβάλει την αναφορά ηλεκτρονικά ή τηλεφωνικά, θα λάβει πληροφορίες σύνδεσης που θα του επιτρέψουν να παρακολουθήσει την αναφορά και να λάβει ανώνυμα σχόλια (εάν το επιθυμεί). Ειδικότερα, ενδέχεται να χρειαστεί να θέσει ερωτήσεις κατανόησης και να λάβει περαιτέρω πληροφορίες.

Στην περαιτέρω πορεία της έρευνας (το αργότερο 3 μήνες μετά την παραλαβή της επιβεβαίωσης παραλαβής), θα παρέχονται πληροφορίες σχετικά με την κατάσταση της έρευνας όσον αφορά τα σχεδιαζόμενα ή ήδη δρομολογημένα μέτρα ή, εάν δεν υπάρχουν επαρκείς υποψίες, σχετικά με τη διακοπή της έρευνας.

IV. Προστασία των πληροφοριοδοτών:

1. Μη επιβολή αντιποίνων:

Η OSI αναλαμβάνει όλες τις εύλογες προσπάθειες για να διασφαλίσει ότι οι πληροφοριοδότες θα προστατεύονται από οποιαδήποτε μορφή αντιποίνων, μειονεξίας ή άλλων αντιποίνων.

Απαγορεύεται και δεν θα γίνει ανεκτή η λήψη πειθαρχικών μέτρων λόγω καταγγελίας κατά ατόμων που συνεργάζονται καλόπιστα στις έρευνες.

2. Εμπιστευτικότητα:

Τα πρόσωπα που συμμετέχουν στην έρευνα δεσμεύονται από αυστηρή εχεμύθεια.

V. Τεκμηρίωση και αποθήκευση:

1. Τεκμηρίωση:

Όλα τα στάδια της έρευνας τεκμηριώνονται προσεκτικά.

Η τεκμηρίωση εξυπηρετεί τη διαφάνεια και την ιχνηλασιμότητα της διαδικασίας.

2. Η τεκμηρίωση διατηρείται σύμφωνα με τις νομικές απαιτήσεις και τις εσωτερικές κατευθυντήριες γραμμές.

VI. Επανεξέταση και προσαρμογή:

Οι εν λόγω διαδικαστικοί κανόνες επανεξετάζονται τακτικά και προσαρμόζονται ανάλογα με τις ανάγκες, ώστε να διασφαλίζεται η συμμόρφωσή τους με τις τρέχουσες νομικές απαιτήσεις και τους εταιρικούς στόχους.

II. Πληροφορίες σύμφωνα με το άρθρο. 13 ΓΚΠΔ (για τα πρόσωπα που παρέχουν πληροφορίες):

Όνομα και στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας: Βλέπε αποτύπωμα στον ιστότοπο. Στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων και, κατά περίπτωση, του εκπροσώπου: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Μόναχο, Γερμανία. Σκοποί για τους οποίους τα δεδομένα προσωπικού χαρακτήρα πρόκειται να υποβληθούν σε επεξεργασία και νομική βάση για την επεξεργασία: Συμμόρφωση με τον νόμο περί προστασίας των πληροφοριοδοτών (HinSchG) και τον νόμο περί δέουσας επιμέλειας της αλυσίδας εφοδιασμού (LkSG), νομική βάση είναι το άρθρο 1 του νόμου. 6 παράγραφος 1 στοιχείο γ) ΓΚΠΔ σε συνδυασμό με τα άρθρα 8, 9 LkSG και 10 HinSchG, εφόσον αυτό είναι απαραίτητο για την εκπλήρωση των καθηκόντων που ορίζονται στα άρθρα 13 και 24 HinSchG, καθώς και συμμόρφωση με την οδηγία (ΕΕ) 2019/1937 σχετικά με την προστασία των προσώπων που αναφέρουν παραβάσεις του δικαίου της Ένωσης και το συνακόλουθο εθνικό δίκαιο των κρατών μελών και συμμόρφωση με την ισχύουσα νομοθεσία άλλων χωρών. Αποδέκτες ή κατηγορίες αποδεκτών των προσωπικών δεδομένων: Αρχές επιβολής του νόμου, αρχές επιβολής προστίμων και άλλες αρχές καθώς και δικηγόροι, εταιρείες του ομίλου ή εργοδότες. Προγραμματισμένη διαβίβαση σε τρίτες χώρες: Καταχώρηση στο ηλεκτρονικό σύστημα Navex και περαιτέρω διαβίβαση σε οντότητες του ομίλου, εργοδότες ή δικηγόρους. Οι τυποποιημένες συμβατικές ρήτρες της ΕΕ και η προσθήκη του Ηνωμένου Βασιλείου στις τυποποιημένες συμβατικές ρήτρες της ΕΕ έχουν συναφθεί με τη Navex. Η Navex είναι επίσης μέλος του πλαισίου προστασίας δεδομένων ΕΕ-ΗΠΑ, του πλαισίου προστασίας δεδομένων Ελβετίας-ΗΠΑ και της επέκτασης του πλαισίου προστασίας δεδομένων ΕΕ-ΗΠΑ στο Ηνωμένο Βασίλειο. Για άλλες διαβιβάσεις, ενδέχεται να μην υπάρχει απόφαση επάρκειας. Για τις εν λόγω διαβιβάσεις χρησιμοποιούνται οι τυποποιημένες συμβατικές ρήτρες της ΕΕ και η προσθήκη του Ηνωμένου Βασιλείου στις τυποποιημένες συμβατικές ρήτρες της ΕΕ. Κριτήρια για τον καθορισμό της περιόδου αποθήκευσης: Η τεκμηρίωση διαγράφεται τρία έτη μετά τη λήξη της διαδικασίας. Η τεκμηρίωση μπορεί να διατηρηθεί για μεγαλύτερο χρονικό διάστημα προκειμένου να πληρούνται οι απαιτήσεις της ισχύουσας νομοθεσίας, εάν αυτό είναι αναγκαίο και αναλογικό.

Σύμφωνα με τον Γενικό Κανονισμό για την Προστασία Δεδομένων, έχετε το δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα που σας αφορούν και το δικαίωμα διόρθωσης ή διαγραφής ή περιορισμού της επεξεργασίας ή το δικαίωμα εναντίωσης στην επεξεργασία και το δικαίωμα φορητότητας των δεδομένων. Έχετε το δικαίωμα να υποβάλετε καταγγελία στην αρμόδια εποπτική αρχή προστασίας δεδομένων σχετικά με την επεξεργασία. Η παροχή δεδομένων προσωπικού χαρακτήρα δεν απαιτείται από το νόμο ή τη σύμβαση και δεν είναι απαραίτητη για τη σύναψη σύμβασης, γι' αυτό και δεν είστε υποχρεωμένοι να παρέχετε δεδομένα προσωπικού χαρακτήρα στην τηλεφωνική γραμμή καταγγελιών. Πιθανές συνέπειες της μη παροχής είναι ότι η αναφορά δεν θα επεξεργαστεί ή θα επεξεργαστεί με καθυστέρηση ή ότι θα απορριφθεί και ότι δεν μπορούν να σας παρασχεθούν πληροφορίες ή πληροφορίες σχετικά με την αναφορά. Δεν υπάρχει αυτοματοποιημένη λήψη αποφάσεων.

III. Πληροφορίες σύμφωνα με το άρθρο. 14 του ΓΚΠΔ (για άλλα υποκείμενα των δεδομένων):

Όνομα και στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας: Βλέπε αποτύπωμα στον ιστότοπο. Στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων και, κατά περίπτωση, του εκπροσώπου: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Μόναχο, Γερμανία. Σκοποί για τους οποίους τα δεδομένα προσωπικού χαρακτήρα πρόκειται να υποβληθούν σε επεξεργασία και νομική βάση για την επεξεργασία: Συμμόρφωση με τον νόμο περί προστασίας των πληροφοριοδοτών (HinSchG) και τον νόμο περί δέουσας επιμέλειας της αλυσίδας εφοδιασμού (LkSG), νομική βάση είναι το άρθρο 1 του νόμου. 6 παράγραφος 1 στοιχείο γ) ΓΚΠΔ σε συνδυασμό με τα άρθρα 8, 9 LkSG και 10 HinSchG, εφόσον αυτό είναι απαραίτητο για την εκπλήρωση των καθηκόντων που ορίζονται στα άρθρα 13 και 24 HinSchG, καθώς και συμμόρφωση με την οδηγία (ΕΕ) 2019/1937 σχετικά με την προστασία των προσώπων που αναφέρουν παραβάσεις του δικαίου της Ένωσης και το συνακόλουθο εθνικό δίκαιο των κρατών μελών και συμμόρφωση με την ισχύουσα νομοθεσία άλλων χωρών. Κατηγορίες δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία: Δεδομένα σχετικά με την καταγγελία. Αποδέκτες ή κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα: Αρχές επιβολής του νόμου, αρχές επιβολής προστίμων και άλλες αρχές, καθώς και δικηγόροι, εταιρείες του ομίλου ή εργοδότες. Προγραμματισμένη διαβίβαση σε τρίτες χώρες: Καταχώρηση στο ηλεκτρονικό σύστημα Navex και περαιτέρω διαβίβαση σε οντότητες του ομίλου, εργοδότες ή δικηγόρους. Οι τυποποιημένες συμβατικές ρήτρες της ΕΕ και η προσθήκη του Ηνωμένου Βασιλείου στις τυποποιημένες συμβατικές ρήτρες της ΕΕ έχουν συναφθεί με τη Navex. Η Navex είναι επίσης μέλος του πλαισίου προστασίας δεδομένων ΕΕ-ΗΠΑ, του πλαισίου προστασίας δεδομένων Ελβετίας-ΗΠΑ και της επέκτασης του πλαισίου προστασίας δεδομένων ΕΕ-ΗΠΑ στο Ηνωμένο Βασίλειο. Για άλλες διαβιβάσεις, ενδέχεται να μην υπάρχει απόφαση επάρκειας. Για τις εν λόγω διαβιβάσεις χρησιμοποιούνται οι τυποποιημένες συμβατικές ρήτρες της ΕΕ και η προσθήκη του Ηνωμένου Βασιλείου στις τυποποιημένες συμβατικές ρήτρες της ΕΕ. Κριτήρια για τον καθορισμό της περιόδου αποθήκευσης: Η τεκμηρίωση διαγράφεται τρία έτη μετά τη λήξη της διαδικασίας. Η τεκμηρίωση μπορεί να διατηρηθεί για μεγαλύτερο χρονικό διάστημα προκειμένου να πληρούνται οι απαιτήσεις της ισχύουσας νομοθεσίας, εφόσον αυτό είναι αναγκαίο και αναλογικό. Η πηγή των προσωπικών δεδομένων είναι ο καταγγέλλων ή/και η ενδιαφερόμενη εταιρεία.

Σύμφωνα με τον Γενικό Κανονισμό για την Προστασία Δεδομένων, έχετε το δικαίωμα πρόσβασης σε δεδομένα προσωπικού χαρακτήρα που σας αφορούν και το δικαίωμα διόρθωσης ή διαγραφής ή περιορισμού της επεξεργασίας ή το δικαίωμα εναντίωσης στην επεξεργασία και το δικαίωμα φορητότητας των δεδομένων. Έχετε το δικαίωμα να υποβάλετε καταγγελία στην αρμόδια εποπτική αρχή προστασίας δεδομένων σχετικά με την επεξεργασία. Δεν υπάρχει αυτοματοποιημένη λήψη αποφάσεων. Η παροχή περαιτέρω πληροφοριών αποδεικνύεται αδύνατη.

ESTONIAN: Teavitussüsteem (sisemised aruandluskanalid)

Meie väärtused on meie äritegevuse aluseks ja peegeldavad meie pühendumust aususele, läbipaistvusele ja positiivsele ettevõtluskultuurile. Meie rikkumisest teatamise süsteem on oluline vahend vastutuse edendamiseks ja eetilise äritegevuse tagamiseks. Need protseduurireeglid aitavad muuta meie uurimisprotsessi ja -põhimõtted läbipaistvaks ning tagavad, et kõiki meie süsteemi kaudu saadud teateid käsitletakse asjakohaselt ja professionaalselt.

OSI on pühendunud avatud dialoogile ja tunnustab rikkumisest teatajate kui peamiste partnerite tähtsust meie püüdlustes säilitada kõrgeimad standardid kõigis meie ärivaldkondades.

I. OSI rikkumisest teatamise süsteemi töökord

I. Eesmärk ja reguleerimisala:

1. Eesmärk: Käesolev töökord reguleerib Make It Right Global Hotline'i kaudu saadud teadete käsitlemist ja uurimist. Eesmärgiks on tagada, et kõiki saadud teateid käsitletakse läbipaistvalt, tõhusalt ja kooskõlas OSI eetikanormidega.

2. Käesolevat töökorda kohaldatakse kõigi töötajate, äripartnerite, tarnijate ja muude sidusrühmade suhtes kogu väärtusahelas, kes kasutavad rikkumisest teatamise süsteemi, et jagada konkreetseid viiteid võimalikest rikkumistest, probleemidest või vihjetest. Teavitussüsteem ei ole mõeldud toodete ja teenustega seotud probleemide töötlemiseks. Selliste küsimuste või probleemidega saab pöörduda otse ettevõtte veebisaidil oleva kontaktvormi kaudu.

II. Teabe esitamine:

1. Anonüümsus ja konfidentsiaalsus:

Teavitussüsteem võimaldab muu hulgas anonüümset teavitamist, kui see on siseriiklike õigusaktidega lubatud.

Kogu teave, mida käsitletakse rikkumisest teatamise süsteemi raames, on rangelt konfidentsiaalne.

2 :

Süsteem võimaldab teavitajatel esitada teateid, kui on konkreetseid viiteid võimalikele rikkumistele, muredele või märkidele nende kohta. See puudutab töötajate või äripartnerite poolt kohaldatavate seaduste, määruste jms (eelkõige need, mis on nimetatud rikkumisest teavitamise seaduse 2. jaos või ELi direktiivis 2019/1937) või ettevõtte sisemiste eeskirjade (eelkõige käitumisjuhendi rikkumised) või otseste või kaudsete tarnijate põhjustatud inimõiguste ja keskkonnariskide ning tarneahela hoolsuskohustuse seaduse (LkSG) kohaste inimõiguste ja keskkonnakohustuste rikkumisi. Nende hulka kuuluvad OSI tegevusjuhendi, konkurentsiseaduse, korruptsiooni, varguse, diskrimineerimise,

töötervishoiu ja tööohutuse eiramise, lapstööjõu, pinnase, vee või õhu saastamise, kahjuliku müra, lubamatu veetarbimise, teatavate püsivate orgaaniliste saasteainete tootmise või kasutamise ning jäätmete lubamatu impordi ja ekspordi rikkumised.

3. Juurdepääs süsteemile:

Teavitajatel on juurdepääs väliselt hallatavale aruandlussüsteemile erinevates keeltes aadressil:

EthicsPoint - OSI Group, LLC

- tekstina veebiportaalis oleva vormi kaudu või
- telefoni teel (eri riikidest tasuta)

III. Aruannete töötlemine:

1. Vastuvõtmine ja esialgne hindamine:

Kui rikkumisest teatamine saabub süsteemi hallatavate väliste teatamiskanalite kaudu, dokumenteeritakse see esmalt ja sellele antakse individuaalne toimiku number. OSI Compliance võtab kõik aruanded vastu ja viib läbi esialgse hindamise, et teha kindlaks nende usutavus ja kehtivus.

2. Uurimine:

Asjakohaste vihjete kohta algatatakse põhjalik, objektiivne ja konfidentsiaalne uurimine. Vajaduse korral konsulteeritakse või palutakse abi teistelt osakondadelt, et saada teateid või võtta meetmeid. Teavitajalt võidakse nõuda ka lisateavet.

Uurimise kestus kuni selle lõpetamiseni sõltub juhtumi keerukusest, vajalikest uurimismeetmetest ja konkreetse juhtumi puhul teabe või asjaosaliste kättesaadavusest. Uurimise võimalikult tõhusaks ja kiireks lõpuleviimiseks tehakse kõik endast olenev.

3. Tagasiside teavitajale:

Teavitaja saab võimaluse korral ja anonüümsust ohustamata 7 päeva jooksul tagasisidet oma vihje kättesaamise kohta.

Kui rikkumisest teavitaja on esitanud teate internetis või telefoni teel, saab ta sisselogimisandmed, mis võimaldavad tal teate järelmeetmete võtmist ja (soovi korral) anonüümse tagasiside saamist. Eelkõige võib olla vaja esitada arusaadavaid küsimusi ja saada lisateavet.

Uurimise edasisel käigus (hiljemalt 3 kuu jooksul pärast vastuvõtukinnituse saamist) antakse teavet uurimise seisu kohta seoses kavandatud või juba algatatud meetmetega või, kui kahtlus ei ole piisav, uurimise lõpetamise kohta.

IV. Teavitajate kaitse:

1. OSI teeb kõik mõistlikud jõupingutused tagamaks, et rikkumisest teatajad oleksid kaitstud mis tahes liiki kättemaksu, ebasoodsa kohtlemise või muude repressioonide eest.

Distsiplinaarmeetmed, mis põhinevad rikkumisest teatamisel isikute vastu, kes teevad uurimise käigus heas usus koostööd, on keelatud ja neid ei sallita.

2. Konfidentsiaalsus:

Uurimises osalevad isikud on kohustatud hoidma oma andmeid rangelt konfidentsiaalsena.

V. Dokumentatsioon ja ladustamine:

1. Dokumentatsioon:

Kõik uurimise etapid dokumenteeritakse hoolikalt.

Dokumentatsioon teenib menetluse läbipaistvust ja jälgitavust.

2. Dokumentatsiooni säilitatakse vastavalt õiguslikele nõuetele ja sisemistele suunistele.

VI. Läbivaatamine ja kohandamine:

Need protseduurireeglid vaadatakse korrapäraselt läbi ja neid kohandatakse vastavalt vajadusele, et tagada nende vastavus kehtivatele õiguslikele nõuetele ja ettevõtte eesmärkidele.

II. Teave vastavalt artiklile. 13 GDPR (teavet esitavate isikute puhul):

Vastutava töötleja nimi ja kontaktandmed: Vt jäljend veebilehel. Andmekaitseametniku ja vajaduse korral esindaja kontaktandmed: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 München, Saksamaa. Isikuandmete töötlemise eesmärgid ja õiguslik alus: Teavitajate kaitse seaduse (HinSchG) ja tarneahela hoolsuskohustuse seaduse (LkSG) täitmine, õiguslik alus on art. 6 lõike 1 punkt c GDPR koostoimes LkSG §-dega 8, 9 ja 10 HinSchG, kuivõrd see on vajalik HinSchG §-des 13 ja 24 sätestatud ülesannete täitmiseks, samuti direktiivi (EL) 2019/1937 (liidu õiguse rikkumistest teatanud isikute kaitse kohta) ja sellest tuleneva liikmesriikide siseriikliku õiguse ning teiste riikide kohaldatavate õigusaktide järgimine. Isikuandmete vastuvõtjad või vastuvõtjate kategooriad: Õiguskaitseasutused, trahviasutused ja muud asutused, samuti advokaadid, kontserni ettevõtted või tööandjad. Kavandatav edastamine kolmandatele riikidele: Sisestamine Navexi veebisüsteemi ja edasine edastamine kontserni kuuluvatele üksustele, tööandjatele või advokaatidele. Navexiga on sõlmitud ELi lepingu tüüptingimused ja ELi lepingu tüüptingimuste Ühendkuningriigi lisa. Navex on ka ELi-USA andmekaitseraamistiku, Šveitsi-USA andmekaitseraamistiku ja ELi-USA andmekaitseraamistiku Ühendkuningriigi laienduse liige. Muude andmeedastuste puhul ei pruugi

adekvaatsuse otsus puududa. Selliste andmeedastuste puhul kasutatakse ELi lepingu tüüptingimusi ja ELi lepingu tüüptingimuste Ühendkuningriigi lisa. Säilitamisperioodi määramise kriteeriumid: Dokumentatsioon kustutatakse kolm aastat pärast menetluse lõppu. Dokumentatsiooni võib säilitada kauem, et täita kohaldatavate õigusaktide nõudeid, kui see on vajalik ja proportsionaalne.

Vastavalt isikuandmete kaitse üldmäärusele on teil õigus tutvuda teid puudutavate isikuandmetega ning õigus neid parandada või kustutada või nende töötlemist piirata või õigus esitada vastuväiteid töötlemisele ning õigus andmete ülekantavusele. Teil on õigus esitada pädevale andmekaitse järelevalveasutusele kaebus töötlemise kohta. Isikuandmete esitamine ei ole seadusest või lepingust tulenevalt nõutav ega lepingu sõlmimiseks vajalik, mistõttu te ei ole kohustatud esitama isikuandmeid vihjetelefonile. Andmete esitamata jätmise võimalikud tagajärjed on see, et teatist ei töödelda või töödeldakse viivitusega või et see lükatakse tagasi ning et teile ei saa anda teatisega seotud teavet või teavet. Automatiseeritud otsuste tegemine puudub.

III. Teave vastavalt artiklile. 14 (teiste andmesubjektide puhul):

Vastutava töötleja nimi ja kontaktandmed: Vt jäljend veebilehel. Andmekaitseametniku ja vajaduse korral esindaja kontaktandmed: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 München, Saksamaa. Isikuandmete töötlemise eesmärgid ja õiguslik alus: Teavitajate kaitse seaduse (HinSchG) ja tarneahela hoolsuskohustuse seaduse (LkSG) täitmine, õiguslik alus on art. 6 lõike 1 punkt c GDPR koostoimes LkSG §-dega 8, 9 ja 10 HinSchG, kuivõrd see on vajalik HinSchG §-des 13 ja 24 sätestatud ülesannete täitmiseks, samuti direktiivi (EL) 2019/1937 (liidu õiguse rikkumistest teatanud isikute kaitse kohta) ja sellest tuleneva liikmesriikide siseriikliku õiguse ning teiste riikide kohaldatavate õigusaktide järgimine. Töödeldavate isikuandmete kategooriad: Teavitamise andmed. Isikuandmete vastuvõtjad või vastuvõtjate kategooriad: Õiguskaitseasutused, trahviasutused ja muud asutused ning advokaadid, kontserni kuuluvad äriühingud või tööandjad. Kavandatav edastamine kolmandatele riikidele: Sisestamine Navexi veebisüsteemi ja edasine edastamine kontserni kuuluvatele üksustele, tööandjatele või advokaatidele. Navexiga on sõlmitud ELi lepingu tüüptingimused ja ELi lepingu tüüptingimuste Ühendkuningriigi lisa. Navex on ka ELi-USA andmekaitseraamistiku, Šveitsi-USA andmekaitseraamistiku ja ELi-USA andmekaitseraamistiku Ühendkuningriigi laienduse liige. Muude andmeedastuste puhul ei pruugi adekvaatsuse otsus puududa. Selliste andmeedastuste puhul kasutatakse ELi lepingu tüüptingimusi ja ELi lepingu tüüptingimuste Ühendkuningriigi lisa. Säilitamisperioodi määramise kriteeriumid: Dokumentatsioon kustutatakse kolm aastat pärast menetluse lõppu. Dokumentatsiooni võib säilitada kauem, et täita kohaldatavate õigusaktide nõudeid, kui see on vajalik ja proportsionaalne. Isikuandmete allikas on teavitaja ja/või asjaomane ettevõte.

Vastavalt isikuandmete kaitse üldmäärusele võib teil olla õigus tutvuda teid puudutavate isikuandmetega ning õigus neid parandada või kustutada või nende töötlemist piirata või õigus esitada vastuväiteid töötlemisele ning õigus andmete ülekantavusele. Teil on õigus esitada kaebus pädevale

andmekaitse järelevalveasutusele seoses töötlemisega. Automatiseeritud otsuste tegemine puudub. Täiendava teabe esitamine osutub võimatuks.

FINISH: Whistleblower-järjestelmä (sisäiset ilmoituskanavat)

Arvomme muodostavat liiketoimintakäytäntöjemme perustan ja heijastavat sitoutumistamme rehellisyyteen, avoimuuteen ja myönteiseen yrityskulttuuriin. Ilmoitusjärjestelmämme on tärkeä väline vastuullisuuden edistämisessä ja eettisen liiketoiminnan varmistamisessa. Näiden menettelysääntöjen tarkoituksena on tehdä tutkintamenettelymme prosessi ja periaatteet läpinäkyviksi ja varmistaa, että kaikki järjestelmämme kautta vastaanotetut ilmoitukset käsitellään asianmukaisesti ja ammattimaisesti.

OSI on sitoutunut avoimeen vuoropuheluun ja tunnustaa ilmiantajien merkityksen tärkeinä kumppaneina pyrkimyksissämme ylläpitää korkeimpia standardeja kaikilla liiketoimintamme osa-alueilla.

I. OSI:n ilmiantajajärjestelmän menettelysäännöt

I. Tarkoitus ja soveltamisala:

1. Tarkoitus: Näillä menettelysäännöillä säännellään Make It Right Global Hotline -ilmoitusjärjestelmän kautta vastaanotettujen ilmoitusten käsittelyä ja tutkintaa. Tavoitteena on varmistaa, että kaikki vastaanotetut ilmoitukset käsitellään avoimesti, tehokkaasti ja OSI:n eettisten normien mukaisesti.

2. Soveltamisala: Näitä menettelysääntöjä sovelletaan kaikkiin työntekijöihin, liikekumppaneihin, tavarantoimittajiin ja muihin sidosryhmiin koko arvoketjussa, jotka käyttävät ilmiantajajärjestelmää kertoakseen erityisistä viitteistä mahdollisista väärinkäytöksistä, huolenaiheista tai vihjeistä. Ilmiantajajärjestelmää ei ole tarkoitettu tuotteisiin ja palveluihin liittyvien huolenaiheiden käsittelyyn. Tällaiset kysymykset tai ongelmat voi esittää suoraan yrityksen verkkosivustolla olevan yhteydenottolomakkeen kautta.

II. Tietojen toimittaminen:

1. Anonymiteetti ja luottamuksellisuus:

Ilmoitusjärjestelmä mahdollistaa muun muassa ilmiantojen nimettömän tekemisen kansallisten lakien sallimissa rajoissa.

Kaikki ilmiantajajärjestelmän puitteissa käsiteltävät tiedot ovat ehdottoman luottamuksellisia.

2. Raporttien tyypit:

Järjestelmän avulla ilmiantajat voivat tehdä ilmoituksia, jos on konkreettisia viitteitä mahdollisista väärinkäytöksistä, huolenaiheista tai viitteistä. Tämä koskee työntekijöiden tai liikekumppaneiden tekemiä sovellettavien lakien, asetusten jne. rikkomuksia (erityisesti ilmiantajien suojelusta annetun lain 2 §:ssä tai EU-direktiivissä 2019/1937 mainittuja) tai yrityksen sisäisiä määräyksiä (erityisesti käytännesääntöjen rikkomuksia) tai suorista tai välillisistä toimittajista johtuvia ihmisoikeus- ja

ympäristöriskejä sekä toimitusketjujen huolellisuuslain (LkSG) mukaisten ihmisoikeus- ja ympäristövelvoitteiden rikkomuksia. Tällaisia ovat muun muassa OSI:n käytännesääntöjen, kilpailulainsäädännön, korruption, varkauksien, syrjinnän, työterveyden ja -turvallisuuden laiminlyönnin, lapsityövoiman käytön, maaperän, veden tai ilman pilaantumisen, haitallisten melupäästöjen, kohtuuttoman vedenkulutuksen, tiettyjen pysyvien orgaanisten yhdisteiden tuotannon tai käytön sekä jätteiden luvattoman maahantuonnin ja maastaviennin rikkomukset.

3. Pääsy järjestelmään:

Ilmiantajilla on pääsy ulkoisesti hallinnoituun raportointijärjestelmään eri kielillä osoitteessa:

EthicsPoint - OSI Group, LLC

- tekstimuodossa verkkoportaalissa olevan lomakkeen kautta tai
- puhelimitse (maksutta eri maista)

III. Raporttien käsittely:

1. Vastaanotto ja alustava arviointi:

Kun ilmoitus on vastaanotettu ilmiantajajärjestelmän hallinnoimien ulkoisten ilmoituskanavien kautta, se dokumentoidaan ensin ja sille annetaan yksilöllinen tiedostonumero. OSI Compliance vastaanottaa kaikki ilmoitukset ja suorittaa alustavan arvioinnin niiden uskottavuuden ja pätevyyden määrittämiseksi.

2. Tutkimus:

Asiaan liittyvien vihjeiden perusteella käynnistetään perusteellinen, puolueeton ja luottamuksellinen tutkinta. Tarvittaessa ilmoitusten vastaanottamiseksi tai toimenpiteiden toteuttamiseksi kuullaan tai pyydetään apua muilta yksiköiltä. Ilmiantajalta voidaan myös pyytää lisätietoja.

Tutkinnan kesto sen päättymiseen asti riippuu tapauksen monimutkaisuudesta, tarvittavista tutkintatoimenpiteistä ja yksittäisen tapauksen tietojen tai asianosaisten saatavuudesta. Tutkinta pyritään saamaan päätökseen mahdollisimman tehokkaasti ja nopeasti.

3. Palaute ilmiantajalle:

Ilmiantaja saa palautetta vihjeen vastaanottamisesta 7 päivän kuluessa mahdollisuuksien mukaan ja nimettömyyttä vaarantamatta.

Jos ilmiantaja on tehnyt ilmoituksen verkossa tai puhelimitse, hän saa kirjautumistiedot, joiden avulla hän voi seurata ilmoitusta ja saada nimettömän palautteen (jos hän haluaa). Erityisesti voi olla tarpeen esittää ymmärryskysymyksiä ja saada lisätietoja.

Tutkimuksen myöhemmässä vaiheessa (viimeistään kolmen kuukauden kuluessa vastaanottovahvistuksen vastaanottamisesta) annetaan tietoja tutkimuksen tilanteesta suunniteltujen tai jo aloitettujen toimenpiteiden osalta tai, jos epäilyjä ei ole riittävästi, tutkimuksen lopettamisesta.

IV. Ilmiantajien suojelu:

1. OSI pyrkii kaikin kohtuullisin keinoin varmistamaan, että ilmiantajia suojellaan kaikenlaisilta kostotoimilta, epäedulliselta kohtelulta tai muilta kostotoimilta.

Kurinpitotoimet, jotka perustuvat ilmiantoon ja kohdistuvat tutkimuksissa vilpittömässä mielessä yhteistyötä tekeviin henkilöihin, ovat kiellettyjä, eikä niitä suvaita.

2. Luottamuksellisuus:

Tutkintaan osallistuvia henkilöitä sitoo tiukka vaitiolovelvollisuus.

V. Dokumentointi ja varastointi:

1. Asiakirjat:

Kaikki tutkinnan vaiheet dokumentoidaan huolellisesti.

Asiakirjojen avulla varmistetaan menettelyn avoimuus ja jäljitettävyys.

2. Säilytysaika:

Asiakirjat säilytetään oikeudellisten vaatimusten ja sisäisten ohjeiden mukaisesti.

VI. Tarkistaminen ja mukauttaminen:

Menettelysääntöjä tarkistetaan säännöllisesti ja mukautetaan tarvittaessa sen varmistamiseksi, että ne ovat nykyisten oikeudellisten vaatimusten ja yrityksen tavoitteiden mukaisia.

II. Tietojen antaminen asetuksen (EY) N:o 2100/94 3 artiklan mukaisesti. 13 yleisen tietosuoja-asetuksen mukaisesti (tietoja antavien henkilöiden osalta):

Rekisterinpitäjän nimi ja yhteystiedot: Katso verkkosivujen jäljennös. Tietosuojavastaavan ja tarvittaessa edustajan yhteystiedot: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 München, Saksa. Henkilötietojen käsittelyn tarkoitus ja käsittelyn oikeusperusta: Ilmiantajien suojelua koskevan lain (HinSchG) ja toimitusketjun huolellisuutta koskevan lain (LkSG) noudattaminen, oikeusperusta on Art. 6 artiklan 1 kohdan c alakohta GDPR yhdessä LkSG:n 8 ja 9 §:n sekä HinSchG:n 10 §:n kanssa, sikäli kuin se on tarpeen HinSchG:n 13 ja 24 §:ssä määriteltyjen tehtävien suorittamiseksi, sekä unionin oikeuden rikkomisesta ilmoittavien henkilöiden

suojelusta annetun direktiivin (EU) 2019/1937 ja siitä johtuvan jäsenvaltioiden kansallisen lainsäädännön noudattaminen ja muiden maiden sovellettavan lainsäädännön noudattaminen. Henkilötietojen vastaanottajat tai vastaanottajaryhmät: Lainvalvontaviranomaiset, sakkoviranomaiset ja muut viranomaiset sekä asianajajat, konserniyhtiöt tai työnantajat. Suunniteltu siirto kolmansiin maihin: Kirjaaminen Navexin online-järjestelmään ja edelleen siirto konserniin kuuluville yksiköille, työnantajille tai asianajajille. Navexin kanssa on tehty EU:n vakiosopimuslausekkeet ja Yhdistyneen kuningaskunnan lisäys EU:n vakiosopimuslausekkeisiin. Navex on myös jäsenenä EU:n ja Yhdysvaltojen välisessä tietosuojakehyksessä, Sveitsin ja Yhdysvaltojen välisessä tietosuojakehyksessä ja EU:n ja Yhdysvaltojen välisen tietosuojakehyksen Yhdistyneen kuningaskunnan laajennuksessa. Muiden siirtojen osalta ei välttämättä tehdä päätöstä tietosuojan riittävyydestä. Tällaisissa siirroissa käytetään EU:n vakiosopimuslausekkeita ja EU:n vakiosopimuslausekkeiden Yhdistyneen kuningaskunnan lisäystä. Säilytysajan määrittämisperusteet: Asiakirjat poistetaan kolmen vuoden kuluttua menettelyn päättymisestä. Asiakirjoja voidaan säilyttää pidempään sovellettavan lainsäädännön vaatimusten täyttämiseksi, jos se on tarpeen ja oikeasuhteista.

Yleisen tietosuoja-asetuksen mukaan sinulla on oikeus tutustua itseäsi koskeviin henkilötietoihin ja oikeus oikaista tai poistaa ne tai rajoittaa niiden käsittelyä tai oikeus vastustaa käsittelyä ja oikeus siirtää tiedot muualle. Sinulla on oikeus tehdä valitus käsittelystä toimivaltaiselle tietosuojaviranomaiselle. Henkilötietojen toimittamista ei edellytetä laissa tai sopimuksessa eikä se ole tarpeen sopimuksen tekemistä varten, minkä vuoksi sinun ei ole pakko toimittaa henkilötietoja whistleblowing-hotlineen. Toimittamatta jättämisen mahdollisia seurauksia ovat, että ilmoitusta ei käsitellä tai käsitellään viiveellä tai että se hylätään ja että sinulle ei voida antaa tietoja tai ilmoitukseen liittyviä tietoja. Automaattista päätöksentekoa ei tehdä.

III. Tietojen antaminen asetuksen (EY) N:o 2100/94 3 artiklan mukaisesti. GDPR:n 14 artiklan mukaisesti (muiden rekisteröityjen osalta):

Rekisterinpitäjän nimi ja yhteystiedot: Katso verkkosivujen jäljennös. Tietosuojavastaavan ja tarvittaessa edustajan yhteystiedot: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 München, Saksa. Henkilötietojen käsittelyn tarkoitukset ja käsittelyn oikeusperusta: Ilmiantajien suojelua koskevan lain (HinSchG) ja toimitusketjun huolellisuutta koskevan lain (LkSG) noudattaminen, oikeusperusta on Art. 6 artiklan 1 kohdan c alakohta GDPR yhdessä LkSG:n 8 ja 9 §:n sekä HinSchG:n 10 §:n kanssa, sikäli kuin se on tarpeen HinSchG:n 13 ja 24 §:ssä määriteltyjen tehtävien suorittamiseksi, sekä unionin oikeuden rikkomisesta ilmoittavien henkilöiden suojelusta annetun direktiivin (EU) 2019/1937 ja siitä johtuvan jäsenvaltioiden kansallisen lainsäädännön noudattaminen ja muiden maiden sovellettavan lainsäädännön noudattaminen. Käsiteltävien henkilötietojen luokat: Ilmoitustiedot. Henkilötietojen vastaanottajat tai vastaanottajaryhmät: Lainvalvontaviranomaiset, sakkoviranomaiset ja muut viranomaiset sekä asianajajat, konserniyhtiöt tai työnantajat. Suunniteltu siirto kolmansiin maihin: Kirjaaminen Navexin online-järjestelmään ja edelleen siirto konserniin kuuluville yksiköille, työnantajille tai asianajajille.

Navexin kanssa on tehty EU:n vakiosopimuslausekkeet ja Yhdistyneen kuningaskunnan lisäys EU:n vakiosopimuslausekkeisiin. Navex on myös jäsenenä EU:n ja Yhdysvaltojen välisessä tietosuojakehyksessä, Sveitsin ja Yhdysvaltojen välisessä tietosuojakehyksessä ja EU:n ja Yhdysvaltojen välisen tietosuojakehyksen Yhdistyneen kuningaskunnan laajennuksessa. Muiden siirtojen osalta ei välttämättä tehdä päätöstä tietosuojan riittävyydestä. Tällaisissa siirroissa käytetään EU:n vakiosopimuslausekkeita ja EU:n vakiosopimuslausekkeiden Yhdistyneen kuningaskunnan lisäystä. Säilytysajan määrittämisperusteet: Asiakirjat poistetaan kolmen vuoden kuluttua menettelyn päättymisestä. Asiakirjoja voidaan säilyttää pidempään sovellettavan lainsäädännön vaatimusten täyttämiseksi, jos se on tarpeen ja oikeasuhteista. Henkilötietojen lähde on ilmiantaja ja/tai asianomainen yritys.

Yleisen tietosuoja-asetuksen mukaan sinulla voi olla oikeus tutustua itseäsi koskeviin henkilötietoihin ja oikeus oikaista tai poistaa ne tai rajoittaa niiden käsittelyä tai oikeus vastustaa käsittelyä ja oikeus tietojen siirrettävyyteen. Sinulla on oikeus tehdä valitus toimivaltaiselle tietosuojaa valvovalle viranomaiselle käsittelystä. Automaattista päätöksentekoa ei tehdä. Lisätietojen antaminen osoittautuu mahdottomaksi.

LITHUANIAN: Pranešėjų apie pažeidimus sistema (vidiniai pranešimų kanalai)

Mūsų vertybės sudaro mūsų verslo praktikos pagrindą ir atspindi mūsų įsipareigojimą laikytis sąžiningumo, skaidrumo ir teigiamos įmonės kultūros. Mūsų pranešimų apie pažeidimus sistema yra esminė priemonė, skatinanti atskaitomybę ir užtikrinanti etišką verslo veiklą. Šiomis darbo tvarkos taisyklėmis siekiama, kad mūsų tyrimo procesai ir principai būtų skaidrūs, ir užtikrinti, kad visi per mūsų sistemą gauti pranešimai būtų tinkamai ir profesionaliai išnagrinėti.

OSI yra įsipareigojusi palaikyti atvirą dialogą ir pripažįsta, kad pranešėjai yra svarbūs mūsų partneriai siekiant išlaikyti aukščiausius standartus visose mūsų verslo srityse.

I. OSI pranešėjų sistemos darbo tvarkos taisyklės

I. Tikslas ir taikymo sritis:

1. Tikslas: Šios darbo tvarkos taisyklės reglamentuoja pranešimų, gautų per Pasaulinės karštosios linijos "Make It Right" pranešimų apie pažeidimus sistemą, tvarkymą ir tyrimą. Tikslas - užtikrinti, kad visi gauti pranešimai būtų tvarkomi skaidriai, veiksmingai ir laikantis OSI etikos standartų.

2. Taikymo sritis: Šios darbo tvarkos taisyklės taikomos visiems darbuotojams, verslo partneriams, tiekėjams ir kitiems suinteresuotiesiems subjektams visoje vertės grandinėje, kurie naudojasi pranešėjų sistema, kad pasidalytų konkrečiais galimo netinkamo elgesio požymiais, abejonėmis ar patarimais. Pranešėjų apie pažeidimus sistema nėra skirta su produktais ir paslaugomis susijusiems susirūpinimą keliantiems klausimams nagrinėti. Į tokius klausimus ar problemas galima kreiptis tiesiogiai per įmonės interneto svetainėje esančią kontaktinę formą.

II. Informacijos pateikimas:

1. Anonimiškumas ir konfidencialumas:

Pranešėjų sistema, be kita ko, suteikia galimybę anonimiškai teikti pranešimus apie pažeidimus tiek, kiek tai leidžiama pagal nacionalinius įstatymus.

Visai pagal pranešėjų sistemą tvarkomai informacijai taikomas griežtas konfidencialumo reikalavimas.

2. Ataskaitų tipai:

Sistema suteikia galimybę pranešėjams teikti pranešimus, kai yra konkrečių duomenų apie galimą netinkamą elgesį, susirūpinimą keliančius dalykus ar jų požymius. Tai susiję su darbuotojų ar verslo partnerių taikomų įstatymų, kitų teisės aktų ir pan. pažeidimais (visų pirma nurodytais Pranešėjų apsaugos įstatymo 2 straipsnyje arba ES direktyvoje (ES) 2019/1937) arba įmonės vidaus teisės aktų (visų pirma Elgesio kodekso pažeidimais), arba su žmogaus teisių ir aplinkosaugos rizika, priskiriama

tiesioginiams ar netiesioginiams tiekėjams, taip pat su žmogaus teisių ir aplinkosaugos įsipareigojimų pažeidimais pagal Tiekimo grandinės deramo patikrinimo įstatymą (LkSG). Tai apima OSI elgesio kodekso, antimonopolinių įstatymų, korupcijos, vagystės, diskriminacijos, darbuotojų sveikatos ir saugos nepaisymo, vaikų darbo, dirvožemio, vandens ar oro taršos, kenksmingo triukšmo, neleistino vandens suvartojimo, tam tikrų patvariųjų organinių teršalų gamybos ar naudojimo ir neleistino atliekų importo ir eksporto pažeidimus.

3. Prieiga prie sistemos:

Pranešėjai gali naudotis išoriškai valdoma pranešimų sistema įvairiomis kalbomis adresu:

EthicsPoint - OSI Group, LLC

- teksto forma per internetiniame portale esančią formą arba
- telefonu (nemokamai iš įvairių šalių)

III. Ataskaitų tvarkymas:

1. Gavimas ir pirminis įvertinimas:

Gavus pranešimą išoriniais pranešimų kanalais, kuriuos valdo pranešėjų sistema, jis pirmiausia dokumentuojamas ir jam suteikiamas atskiras bylos numeris. OSI atitikties užtikrinimo tarnyba gauna visus pranešimus ir atlieka pirminį vertinimą, kad nustatytų jų tikėtinumą ir pagrįstumą.

2. Tyrimas:

Bus pradėtas išsamus, objektyvus ir konfidencialus tyrimas dėl atitinkamų patarimų. Prireikus priimti pranešimus ar imtis veiksmų, bus konsultuojamasi su kitais skyriais arba prašoma jų pagalbos. Taip pat gali būti prašoma papildomos informacijos iš pranešėjo.

Tyrimo trukmė iki jo pabaigos priklauso nuo bylos sudėtingumo, reikalingų tyrimo priemonių, turimos informacijos ar su konkrečia byla susijusių šalių. Bus dedamos visos pastangos, kad tyrimas būtų baigtas kuo veiksmingiau ir greičiau.

3. Grįžtamasis ryšys su pranešėju:

Jei įmanoma, per 7 dienas pranešėjas gaus grįžtamąjį ryšį apie gautą pranešimą, nepažeidžiant jo anonimiškumo.

Jei pranešėjas pateikė pranešimą internetu arba telefonu, jis gaus prisijungimo informaciją, kad galėtų tęsti su pranešimu susijusią veiklą ir gauti anoniminę grįžtamąją informaciją (jei pageidauja). Visų pirma gali prireikti užduoti suprantamus klausimus ir gauti papildomos informacijos.

Tolesnėje tyrimo eigoje (ne vėliau kaip per 3 mėnesius nuo gavimo patvirtinimo gavimo) bus pateikta informacija apie tyrimo eigą, susijusią su planuojamomis ar jau pradėtomis priemonėmis, arba, jei įtarimų nepakanka, apie tyrimo nutraukimą.

IV. Pranešėjų apsauga:

1 :

OSI imasi visų pagrįstų pastangų užtikrinti, kad pranešėjai būtų apsaugoti nuo bet kokio persekiojimo, nepalankių sąlygų sudarymo ar kitokių atsakomųjų veiksmų.

Drausminės nuobaudos dėl pranešimų apie pažeidimus asmenims, kurie sąžiningai bendradarbiauja atliekant tyrimus, yra draudžiamos ir nebus toleruojamos.

2. Konfidencialumas:

Tyrime dalyvaujantys asmenys privalo laikytis griežto konfidencialumo.

V. Dokumentacija ir saugojimas:

1. Dokumentai:

Visi tyrimo etapai kruopščiai dokumentuojami.

Dokumentacija padeda užtikrinti procedūros skaidrumą ir atsekamumą.

2. Saugojimo laikotarpis:

Dokumentai saugomi laikantis teisinių reikalavimų ir vidaus gairių.

VI. Peržiūra ir koregavimas:

Šios procedūrinės taisyklės reguliariai peržiūrimos ir prireikus pritaikomos siekiant užtikrinti, kad jos atitiktų galiojančius teisinius reikalavimus ir įmonės tikslus.

II. Informacija pagal CK 6.2 straipsnį. 13 BDAR (informaciją teikiantiems asmenims):

Duomenų valdytojo pavadinimas ir kontaktiniai duomenys: Kontaktiniai duomenys ir kontaktiniai duomenys: Žr. atspaudą svetainėje. Duomenų apsaugos pareigūno ir, jei taikoma, atstovo kontaktiniai duomenys: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Miunchenas, Vokietija. Asmens duomenų tvarkymo tikslai ir tvarkymo teisinis pagrindas: Atitiktis Pranešėjų apsaugos įstatymui (HinSchG) ir Tiekimo grandinės deramo patikrinimo įstatymui (LkSG), teisinis pagrindas - Įstatymo 2 str. 6 straipsnio 1 dalies c punktas BDAR kartu su LkSG 8, 9 straipsniais ir HinSchG 10 straipsniu, jei tai būtina HinSchG 13 ir 24 straipsniuose nurodytoms užduotims atlikti,

taip pat atitiktis Direktyvai (ES) 2019/1937 dėl asmenų, pranešančių apie Sąjungos teisės pažeidimus, apsaugos ir iš jos kylančiai valstybių narių nacionalinei teisei bei atitiktis taikytiniems kitų šalių teisės aktams. Asmens duomenų gavėjai arba gavėjų kategorijos: Teisėsaugos institucijos, baudas skiriančios institucijos ir kitos institucijos, taip pat advokatai, grupės įmonės arba darbdaviai. Planuojamas perdavimas į trečiąsias šalis: Įvedimas į "Navex" internetinę sistemą ir tolesnis perdavimas grupės subjektams, darbdaviams arba advokatams. Su "Navex" sudarytos ES standartinės sutarčių sąlygos ir ES standartinių sutarčių sąlygų JK papildymas. Be to, "Navex" yra ES ir JAV duomenų privatumo sistemos, Šveicarijos ir JAV duomenų privatumo sistemos ir ES ir JAV duomenų privatumo sistemos JK papildymo narė. Kitų duomenų perdavimo atveju sprendimas dėl tinkamumo gali būti nepriimtas. Tokiems duomenų perdavimams taikomos ES standartinės sutarčių sąlygos ir JK ES standartinių sutarčių sąlygų papildymas. Saugojimo laikotarpio nustatymo kriterijai: Dokumentai ištrinami praėjus trejiems metams nuo procedūros pabaigos. Dokumentai gali būti saugomi ilgiau, kad atitiktų taikomų teisės aktų reikalavimus, jei tai būtina ir proporcinga.

Pagal Bendrąjį duomenų apsaugos reglamentą turite teisę susipažinti su savo asmens duomenimis ir teisę juos ištaisyti, ištrinti ar apriboti jų tvarkymą arba teisę nesutikti, kad duomenys būtų tvarkomi, ir teisę į duomenų perkeliamumą. Turite teisę pateikti skundą dėl duomenų tvarkymo kompetentingai duomenų apsaugos priežiūros institucijai. Asmens duomenų pateikti nereikalaujama pagal įstatymą ar sutartį ir jie nėra būtini sutarčiai sudaryti, todėl jūs neprivalote pateikti asmens duomenų į Pranešimų apie pažeidimus karštąją liniją. Galimos nepateikimo pasekmės yra tai, kad pranešimas nebus tvarkomas arba bus tvarkomas pavėluotai, arba bus atmestas, ir kad jums nebus galima suteikti jokios informacijos ar su pranešimu susijusios informacijos. Automatizuoto sprendimų priėmimo nėra.

III. Informacija pagal CK 6.2 str. 14 BDAR (kitiems duomenų subjektams):

Duomenų valdytojo pavadinimas ir kontaktiniai duomenys: Kontaktiniai duomenys ir kontaktiniai duomenys: Žr. atspaudą svetainėje. Duomenų apsaugos pareigūno ir, jei taikoma, atstovo kontaktiniai duomenys: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Miunchenas, Vokietija. Asmens duomenų tvarkymo tikslai ir tvarkymo teisinis pagrindas: Atitiktis Pranešėjų apsaugos įstatymui (HinSchG) ir Tiekimo grandinės deramo patikrinimo įstatymui (LkSG), teisinis pagrindas - Įstatymo 2 str. 6 straipsnio 1 dalies c punktas BDAR kartu su LkSG 8, 9 straipsniais ir HinSchG 10 straipsniu, jei tai būtina HinSchG 13 ir 24 straipsniuose nurodytoms užduotims atlikti, taip pat atitiktis Direktyvai (ES) 2019/1937 dėl asmenų, pranešančių apie Sąjungos teisės pažeidimus, apsaugos ir iš jos kylančiai valstybių narių nacionalinei teisei bei atitiktis taikytiniems kitų šalių teisės aktams. Tvarkomų asmens duomenų kategorijos: Duomenys apie pranešimus apie pažeidimus. Asmens duomenų gavėjai arba gavėjų kategorijos: Teisėsaugos institucijos, baudas skiriančios institucijos ir kitos institucijos, taip pat teisininkai, grupės įmonės arba darbdaviai. Planuojamas perdavimas į trečiąsias šalis: Įvedimas į "Navex" internetinę sistemą ir tolesnis perdavimas grupės subjektams, darbdaviams arba advokatams. Su "Navex" sudarytos ES standartinės sutarčių sąlygos ir ES standartinių sutarčių sąlygų JK papildymas. Be to, "Navex" yra ES ir JAV duomenų privatumo

sistemos, Šveicarijos ir JAV duomenų privatumo sistemos ir ES ir JAV duomenų privatumo sistemos JK papildymo narė. Kitų duomenų perdavimo atveju sprendimas dėl tinkamumo gali būti nepriimtas. Tokiems duomenų perdavimams taikomos ES standartinės sutarčių sąlygos ir JK ES standartinių sutarčių sąlygų papildymas. Saugojimo laikotarpio nustatymo kriterijai: Dokumentai ištrinami praėjus trejiems metams nuo procedūros pabaigos. Dokumentai gali būti saugomi ilgiau, kad atitiktų taikomų teisės aktų reikalavimus, jei tai būtina ir proporcinga. Asmens duomenų šaltinis yra pranešėjas ir (arba) atitinkama įmonė.

Pagal Bendrąjį duomenų apsaugos reglamentą galite turėti teisę susipažinti su savo asmens duomenimis ir teisę juos ištaisyti, ištrinti ar apriboti jų tvarkymą arba teisę nesutikti, kad duomenys būtų tvarkomi, ir teisę į duomenų perkeliamumą. Turite teisę pateikti skundą dėl duomenų tvarkymo kompetentingai duomenų apsaugos priežiūros institucijai. Automatizuoto sprendimų priėmimo nėra. Paaiškėjo, kad papildomos informacijos pateikti neįmanoma.

LATVIAN: Ziņotāju sistēma (iekšējie ziņošanas kanāli)

Mūsu vērtības veido mūsu uzņēmējdarbības prakses pamatu un atspoguļo mūsu apņemšanos ievērot godīgumu, pārredzamību un pozitīvu korporatīvo kultūru. Mūsu trauksmes celšanas sistēma ir būtisks rīks, lai veicinātu atbildību un nodrošinātu ētisku uzņēmējdarbību. Šis reglaments kalpo tam, lai padarītu mūsu izmeklēšanas procesu procesu un principus pārredzamus un nodrošinātu, ka visi mūsu sistēmā saņemtie ziņojumi tiek pienācīgi un profesionāli apstrādāti.

OSI ir apņēmusies uzturēt atklātu dialogu un atzīst trauksmes cēlēju kā galveno partneru nozīmi mūsu centienos saglabāt visaugstākos standartus visās mūsu uzņēmējdarbības jomās.

I. OSI ziņotāju sistēmas darba kārtības noteikumi

I. Mērķis un darbības joma:

1. Mērķis: Šis reglaments reglamentē to ziņojumu izskatīšanu un izmeklēšanu, kas saņemti, izmantojot Make It Right Global Hotline trauksmes celšanas sistēmu. Mērķis ir nodrošināt, lai visi saņemtie ziņojumi tiktu izskatīti pārredzami, efektīvi un saskaņā ar OSI ētikas standartiem.

2. Piemērošanas joma: 2.2. Procedūras noteikumi 2.2.1. Šis reglaments attiecas uz visiem darbiniekiem, darījumu partneriem, piegādātājiem un citām ieinteresētajām personām visā vērtību ķēdē, kas izmanto ziņotāju sistēmu, lai dalītos ar konkrētām norādēm par iespējamiem pārkāpumiem, bažām vai padomiem. Trauksmes cēlēju sistēma nav paredzēta ar produktiem un pakalpojumiem saistītu bažu apstrādei. Šādus jautājumus vai problēmas var risināt tieši, izmantojot kontaktformu uzņēmuma tīmekļa vietnē.

II. Informācijas iesniegšana:

1. Anonimitāte un konfidencialitāte:

Ziņotāju sistēma cita starpā ļauj anonīmi iesniegt ziņojumus par pārkāpumiem, ciktāl to pieļauj valsts tiesību akti.

Uz visu informāciju, kas tiek apstrādāta trauksmes cēlēju sistēmas ietvaros, attiecas stingra konfidencialitāte.

2. Ziņojumu veidi:

Sistēma ļauj ziņotājiem iesniegt ziņojumus, ja ir konkrētas norādes par iespējamiem pārkāpumiem, bažām vai pazīmēm. Tas attiecas uz darbinieku vai sadarbības partneru pieļautiem piemērojamo likumu, noteikumu u. c. pārkāpumiem (jo īpaši tiem, kas minēti Likuma par trauksmes cēlēju aizsardzību 2. pantā vai ES Direktīvā 2019/1937) vai uzņēmuma iekšējiem noteikumiem (jo īpaši uzvedības kodeksa pārkāpumiem), vai uz cilvēktiesību un vides riskiem, kas saistīti ar tiešajiem vai netiešajiem

piegādātājiem, kā arī uz cilvēktiesību un vides aizsardzības pienākumu pārkāpumiem saskaņā ar Piegādes ķēdes uzticamības pārbaudes likumu (LkSG). Tie ietver OSI Rīcības kodeksa, pretmonopola tiesību aktu, korupcijas, zādzību, diskriminācijas, darba drošības un veselības aizsardzības neievērošanas, bērnu darba, augsnes, ūdens vai gaisa piesārņojuma, kaitīga trokšņa emisijas, nepieļaujama ūdens patēriņa, noteiktu noturīgu organisko piesārņotāju ražošanas vai izmantošanas un neatļauta atkritumu importa un eksporta pārkāpumus.

3. Piekļuve sistēmai:

Ziņotājiem ir piekļuve ārēji pārvaldītai ziņošanas sistēmai dažādās valodās:

EthicsPoint - OSI Group, LLC

- teksta formā, izmantojot tiešsaistes portālā esošo veidlapu vai
- pa tālruni (bezmaksas no dažādām valstīm).

III. Ziņojumu apstrāde:

1. Saņemšana un sākotnējais novērtējums:

Kad ziņojums ir saņemts, izmantojot ārējos ziņošanas kanālus, ko pārvalda ziņotāju sistēma, tas vispirms tiek dokumentēts un tam tiek piešķirts individuāls lietas numurs. OSI Compliance saņem visus ziņojumus un veic sākotnējo novērtējumu, lai noteiktu to ticamību un pamatotību.

2. Izmeklēšana:

Tiks uzsākta rūpīga, objektīva un konfidenciāla izmeklēšana par attiecīgajiem padomiem. Ja būs nepieciešams saņemt ziņojumus vai veikt pasākumus, tiks konsultēts ar citām struktūrvienībām vai lūgta palīdzība. No ziņotāja var pieprasīt arī papildu informāciju.

Izmeklēšanas ilgums līdz tās pabeigšanai ir atkarīgs no lietas sarežģītības, nepieciešamajiem izmeklēšanas pasākumiem, kā arī no informācijas pieejamības vai konkrētajā lietā iesaistītajām pusēm. Tiks pieliktas visas pūles, lai izmeklēšanu pabeigtu pēc iespējas efektīvāk un ātrāk.

3. Atgriezeniskā saite ziņotājam:

Ja iespējams, un neapdraudot anonimitāti, ziņotājs 7 dienu laikā saņems atgriezenisko saiti par sava ziņojuma saņemšanu.

Ja trauksmes cēlājs ziņojumu ir iesniedzis tiešsaistē vai pa tālruni, viņš saņems pieteikšanās informāciju, kas viņam ļaus veikt turpmākus pasākumus saistībā ar ziņojumu un saņemt anonīmu atgriezenisko saiti (ja viņš vēlas). Jo īpaši var būt nepieciešams uzdot jautājumus par izpratni un iegūt papildu informāciju.

Turpmākajā izmeklēšanas gaitā (ne vēlāk kā 3 mēnešus pēc saņemšanas apstiprinājuma saņemšanas) tiks sniegta informācija par izmeklēšanas statusu attiecībā uz plānotajiem vai jau uzsāktajiem pasākumiem vai, ja nav pietiekamu aizdomu, par izmeklēšanas pārtraukšanu.

IV. Ziņotāju aizsardzība:

1. Atriebības aizliegums:

OSI apņemas darīt visu iespējamo, lai nodrošinātu, ka trauksmes cēlēji ir aizsargāti pret jebkāda veida atriebību, neizdevīgu stāvokli vai cita veida represijām.

Disciplinārsods, kas pamatojas uz ziņošanu par pārkāpumiem pret personām, kuras godprātīgi sadarbojas izmeklēšanā, ir aizliegts un netiks pieļauts.

2. Konfidencialitāte:

Izmeklēšanā iesaistītajām personām ir jāievēro stingra konfidencialitāte.

V. Dokumentācija un glabāšana:

1. Dokumentācija:

Visi izmeklēšanas posmi tiek rūpīgi dokumentēti.

Dokumentācija kalpo procedūras pārredzamībai un izsekojamībai.

2. Uzglabāšanas periods:

Dokumentācija tiek saglabāta saskaņā ar juridiskajām prasībām un iekšējām vadlīnijām.

VI. Pārskatīšana un koriģēšana:

Šie procesuālie noteikumi tiek regulāri pārskatīti un pēc vajadzības pielāgoti, lai nodrošinātu to atbilstību pašreizējām juridiskajām prasībām un korporatīvajiem mērķiem.

II. Informācija saskaņā ar Regulas (EK) Nr. 13 VDAR (personām, kas sniedz informāciju):

Pārziņa nosaukums un kontaktinformācija: Skatīt nospiedumu tīmekļa vietnē. Datu aizsardzības speciālista un attiecīgā gadījumā pārstāvja kontaktinformācija: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Minhene, Vācija. Personas datu apstrādes nolūki un apstrādes juridiskais pamats: Atbilstība Likumam par trauksmes cēlēju aizsardzību (HinSchG) un Likumam par uzticamības pārbaudi piegādes ķēdē (LkSG), juridiskais pamats ir Likuma par uzticamības pārbaudi (LkSG) 3. pants. 6. panta 1. punkta c) apakšpunkts VDAR saistībā ar 8. un 9. pantu LkSG un 10. pantu HinSchG, ciktāl tas ir nepieciešams, lai izpildītu HinSchG 13. un 24. pantā

noteiktos uzdevumus, kā arī atbilstība Direktīvai (ES) 2019/1937 par to personu aizsardzību, kuras ziņo par Savienības tiesību aktu pārkāpumiem, un no tās izrietošajiem dalībvalstu tiesību aktiem un atbilstība piemērojamiem citu valstu tiesību aktiem. Personas datu saņēmēji vai saņēmēju kategorijas: Tiesībaizsardzības iestādes, naudas sodu uzlikšanas iestādes un citas iestādes, kā arī juristi, grupas uzņēmumi vai darba devēji. Plānotā pārsūtīšana uz trešām valstīm: Ievadīšana Navex tiešsaistes sistēmā un turpmāka nosūtīšana grupas struktūrām, darba devējiem vai juristiem. Ar Navex ir noslēgtas ES standarta līguma klauzulas un ES standarta līguma klauzulu Apvienotās Karalistes papildinājums. Navex ir arī ES un ASV datu privātuma sistēmas, Šveices un ASV datu privātuma sistēmas un ES un ASV datu privātuma sistēmas Apvienotās Karalistes paplašinājuma dalībniece. Attiecībā uz citiem datu nosūtīšanas gadījumiem lēmums par atbilstību var netikt pieņemts. Šādai datu pārsūtīšanai izmanto ES standarta līguma klauzulas un Apvienotās Karalistes papildinājumu ES standarta līguma klauzulām. Kritēriji glabāšanas perioda noteikšanai: Dokumentāciju dzēš trīs gadus pēc procedūras beigām. Dokumentāciju var glabāt ilgāk, lai izpildītu piemērojamo tiesību aktu prasības, ja tas ir nepieciešams un samērīgi.

Saskaņā ar Vispārīgo datu aizsardzības regulu jums ir tiesības piekļūt personas datiem, kas attiecas uz jums, un tiesības labot vai dzēst, vai ierobežot apstrādi, vai tiesības iebilst pret apstrādi un tiesības uz datu pārnesamību. Jums ir tiesības iesniegt sūdzību kompetentajai datu aizsardzības uzraudzības iestādei par apstrādi. Personas datu sniegšana nav prasīta ar likumu vai līgumu un nav nepieciešama līguma noslēgšanai, tāpēc jums nav pienākuma sniegt personas datus ziņošanas uzticības dienestam. Iespējamās ziņojuma nesniegšanas sekas ir tādas, ka ziņojums netiks apstrādāts vai tiks apstrādāts ar kavēšanos, vai arī tas tiks noraidīts, un jums nevarēs sniegt nekādu informāciju vai ar ziņojumu saistītu informāciju. Automatizēta lēmumu pieņemšana netiek veikta.

III. Informācija saskaņā ar Regulas (EK) Nr. 14 (citiem datu subjektiem):

Pārziņa nosaukums un kontaktinformācija: Skatīt nospiedumu tīmekļa vietnē. Datu aizsardzības speciālista un attiecīgā gadījumā pārstāvja kontaktinformācija: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Minhene, Vācija. Personas datu apstrādes nolūki un apstrādes juridiskais pamats: Atbilstība Likumam par trauksmes cēlēju aizsardzību (HinSchG) un Likumam par uzticamības pārbaudi piegādes ķēdē (LkSG), juridiskais pamats ir Likuma par uzticamības pārbaudi (LkSG) 3. pants. 6. panta 1. punkta c) apakšpunkts VDAR saistībā ar 8. un 9. pantu LkSG un 10. pantu HinSchG, ciktāl tas ir nepieciešams, lai izpildītu HinSchG 13. un 24. pantā noteiktos uzdevumus, kā arī atbilstība Direktīvai (ES) 2019/1937 par to personu aizsardzību, kuras ziņo par Savienības tiesību aktu pārkāpumiem, un no tās izrietošajiem dalībvalstu tiesību aktiem un atbilstība piemērojamiem citu valstu tiesību aktiem. Apstrādāto personas datu kategorijas: Ziņošanas dati. Personas datu saņēmēji vai saņēmēju kategorijas: Tiesībaizsardzības iestādes, naudas sodu uzlikšanas iestādes un citas iestādes, kā arī juristi, grupas uzņēmumi vai darba devēji. Plānotā pārsūtīšana uz trešām valstīm: Ienākšana Navex tiešsaistes sistēmā un tālāka nodošana grupas struktūrām, darba devējiem vai juristiem. Ar Navex ir noslēgtas ES standarta līguma klauzulas un ES

standarta līguma klauzulu Apvienotās Karalistes papildinājums. Navex ir arī ES un ASV datu privātuma sistēmas, Šveices un ASV datu privātuma sistēmas un ES un ASV datu privātuma sistēmas Apvienotās Karalistes paplašinājuma dalībniece. Attiecībā uz citiem datu nosūtīšanas gadījumiem lēmums par atbilstību var netikt pieņemts. Šādai datu pārsūtīšanai izmanto ES standarta līguma klauzulas un Apvienotās Karalistes papildinājumu ES standarta līguma klauzulām. Kritēriji glabāšanas perioda noteikšanai: Dokumentāciju dzēš trīs gadus pēc procedūras beigām. Dokumentāciju var glabāt ilgāk, lai izpildītu piemērojamo tiesību aktu prasības, ja tas ir nepieciešams un samērīgi. Personas datu avots ir ziņotājs un/vai attiecīgais uzņēmums.

Saskaņā ar Vispārīgo datu aizsardzības regulu jums var būt tiesības piekļūt personas datiem, kas attiecas uz jums, un tiesības uz datu labošanu, dzēšanu vai apstrādes ierobežošanu, vai tiesības iebilst pret apstrādi un tiesības uz datu pārnesamību. Jums ir tiesības iesniegt sūdzību kompetentajai datu aizsardzības uzraudzības iestādei par apstrādi. Automatizēta lēmumu pieņemšana nenotiek. Papildu informācijas sniegšana izrādās neiespējama.

PORTUGUESE: Sistema de denúncia de irregularidades (canais de comunicação internos)

Os nossos valores constituem a base das nossas práticas comerciais e reflectem o nosso compromisso com a integridade, a transparência e uma cultura empresarial positiva. O nosso sistema de denúncia de irregularidades é uma ferramenta essencial para promover a responsabilização e garantir operações comerciais éticas. Estas regras de procedimento servem para tornar transparente o processo e os princípios dos nossos processos de investigação e garantir que todas as denúncias recebidas através do nosso sistema são tratadas de forma adequada e profissional.

A OSI está empenhada num diálogo aberto e reconhece a importância dos denunciantes como parceiros fundamentais nos nossos esforços para manter os mais elevados padrões em todas as áreas da nossa atividade.

I. Regulamento interno do sistema de denúncia de irregularidades da ISC

I. Objetivo e âmbito de aplicação:

1. Objetivo: O presente Regulamento Interno rege o tratamento e a investigação das denúncias recebidas através do sistema de denúncia de irregularidades da Linha Direta Global Make It Right. O objetivo é garantir que todas as denúncias recebidas sejam tratadas de forma transparente, eficiente e de acordo com os padrões éticos da OSI.

2. Âmbito de aplicação: As presentes regras de procedimento aplicam-se a todos os colaboradores, parceiros comerciais, fornecedores e outras partes interessadas ao longo da cadeia de valor que utilizem o sistema de denúncia de irregularidades para partilhar indicações específicas de possíveis condutas incorrectas, preocupações ou dicas. O sistema de denúncia de irregularidades não se destina ao tratamento de questões relacionadas com produtos e serviços. Essas questões ou problemas podem ser abordados diretamente através do formulário de contacto no sítio Web da empresa.

II. Apresentação de informações:

1. anonimato e confidencialidade:

O sistema de denúncia de irregularidades permite, entre outras coisas, a apresentação anónima de relatórios de denúncia, na medida em que a legislação nacional o permita.

Todas as informações tratadas no âmbito do sistema de denúncia de irregularidades estão sujeitas a uma confidencialidade rigorosa.

2. tipos de relatórios:

O sistema permite que os denunciantes apresentem relatórios sempre que existam indicações concretas de uma possível conduta incorrecta, preocupações ou indícios de tal. Isto diz respeito a violações, por parte de funcionários ou parceiros comerciais, de leis, regulamentos, etc. aplicáveis (em particular os mencionados na Secção 2 da Lei de Proteção de Denúncias ou na Diretiva da UE 2019/1937) ou regulamentos internos da empresa (em particular violações do Código de Conduta) ou direitos humanos e riscos ambientais atribuíveis a fornecedores directos ou indirectos, bem como violações de direitos humanos e obrigações ambientais ao abrigo da Lei de Diligência Prévia da Cadeia de Fornecimento (LkSG). Estas incluem violações do Código de Conduta da OSI, da legislação antitrust, corrupção, roubo, discriminação, desrespeito pela saúde e segurança no trabalho, trabalho infantil, poluição do solo, da água ou do ar, emissões sonoras nocivas, consumo inaceitável de água, produção ou utilização de determinados poluentes orgânicos persistentes e importação e exportação não autorizadas de resíduos.

3. acesso ao sistema:

Os denunciantes têm acesso ao sistema de comunicação de informações gerido externamente, em diferentes línguas, no seguinte endereço

EthicsPoint - OSI Group, LLC

- em forma de texto através de um formulário no portal em linha ou
- por telefone (gratuito a partir de vários países)

III. Processamento dos relatórios:

1) Receção e avaliação inicial:

Assim que uma denúncia é recebida através dos canais de denúncia externos geridos pelo sistema de denúncia, é primeiro documentada e é-lhe atribuído um número de processo individual. A OSI Compliance recebe todas as denúncias e efectua uma avaliação inicial para determinar a sua plausibilidade e validade.

2. Investigação:

Será iniciada uma investigação minuciosa, objetiva e confidencial sobre as denúncias relevantes. Se necessário, para receber denúncias ou tomar medidas, serão consultados ou solicitada a assistência de outros departamentos. Poderão também ser solicitadas informações adicionais ao autor da denúncia.

A duração de um inquérito até à sua conclusão depende da complexidade do caso, das medidas de investigação necessárias e da disponibilidade de informações ou das partes envolvidas no caso individual. Serão envidados todos os esforços para concluir o inquérito da forma mais eficiente e expedita possível.

3. reacções ao denunciante:

O autor da denúncia receberá um feedback sobre a receção da sua denúncia no prazo de 7 dias, sempre que possível e sem pôr em causa o anonimato.

Se o autor da denúncia tiver apresentado a denúncia em linha ou por telefone, receberá informações de início de sessão que lhe permitirão dar seguimento à denúncia e receber um feedback anónimo (se assim o desejar). Em particular, pode ser necessário fazer perguntas de compreensão e obter mais informações.

No decurso do inquérito (o mais tardar 3 meses após a receção do aviso de receção), serão fornecidas informações sobre a situação do inquérito no que se refere às medidas previstas ou já iniciadas ou, se não houver suspeitas suficientes, sobre a interrupção do inquérito.

IV. Proteção dos autores de denúncias:

1. não retaliação:

A OSI envida todos os esforços razoáveis para garantir que os denunciantes sejam protegidos contra qualquer forma de retaliação, desvantagem ou outras represálias.

As acções disciplinares baseadas em denúncias contra pessoas que cooperam de boa fé com as investigações são proibidas e não serão toleradas.

2. confidencialidade:

As pessoas envolvidas no inquérito estão vinculadas a um sigilo absoluto.

V. Documentação e armazenamento:

1. Documentação:

Todas as etapas do inquérito são cuidadosamente documentadas.

A documentação serve a transparência e a rastreabilidade do procedimento.

2. período de conservação:

A documentação é conservada em conformidade com os requisitos legais e as directrizes internas.

VI. Revisão e ajustamento:

Estas regras processuais são regularmente revistas e adaptadas, se necessário, para garantir a sua conformidade com os requisitos legais em vigor e os objectivos da empresa.

II. Informação nos termos do Art. 13 do RGPD (para pessoas que fornecem informações):

Nome e dados de contacto do responsável pelo tratamento: Ver impressão no sítio Web. Dados de contacto do responsável pela proteção de dados e, se aplicável, do representante: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Munique, Alemanha. Finalidades para as quais os dados pessoais serão processados e a base legal para o processamento: Conformidade com a Lei de Proteção de Denúncias (HinSchG) e a Lei de Diligência Devida da Cadeia de Fornecimento (LkSG), a base legal é o Art. 6 (1) (c) do RGPD em conjunto com os §§ 8, 9 da LkSG e o § 10 da HinSchG, na medida em que tal seja necessário para cumprir as tarefas especificadas nos §§ 13 e 24 da HinSchG, bem como o cumprimento da Diretiva (UE) 2019/1937 relativa à proteção das pessoas que denunciam violações do direito da União e do direito nacional dos Estados-Membros daí resultante e o cumprimento da legislação aplicável de outros países. Destinatários ou categorias de destinatários dos dados pessoais: Autoridades responsáveis pela aplicação da lei, autoridades responsáveis pela aplicação de coimas e outras autoridades, bem como advogados, empresas do grupo ou empregadores. Transferência planeada para países terceiros: Entrada no sistema online Navex e posterior transferência para entidades do grupo, entidades patronais ou advogados. As cláusulas contratuais-tipo da UE e a adenda do Reino Unido às cláusulas contratuais-tipo da UE foram celebradas com a Navex. A Navex é também membro do Quadro de Privacidade de Dados UE-EUA, do Quadro de Privacidade de Dados Suíça-EUA e da Extensão do Reino Unido ao Quadro de Privacidade de Dados UE-EUA. Para outras transferências, pode não haver uma decisão de adequação. As cláusulas contratuais-tipo da UE e a adenda do Reino Unido às cláusulas contratuais-tipo da UE são utilizadas para essas transferências. Critérios para determinar o período de conservação: A documentação é eliminada três anos após a conclusão do procedimento. A documentação pode ser conservada durante mais tempo para cumprir os requisitos da legislação aplicável, se tal for necessário e proporcionado.

Nos termos do Regulamento Geral sobre a Proteção de Dados, tem o direito de aceder aos dados pessoais que lhe dizem respeito e o direito de retificar ou apagar ou restringir o tratamento ou o direito de se opor ao tratamento e o direito à portabilidade dos dados. Tem o direito de apresentar uma queixa à autoridade de controlo competente em matéria de proteção de dados relativamente ao tratamento. O fornecimento de dados pessoais não é exigido por lei ou por contrato e não é necessário para a celebração de um contrato, razão pela qual não é obrigado a fornecer dados pessoais à linha direta de denúncias. As possíveis consequências do não fornecimento são que o relatório não será processado ou será processado com um atraso, ou que será rejeitado, e que nenhuma informação ou informação relacionada com o relatório lhe poderá ser fornecida. Não existem decisões automatizadas.

III. Informações nos termos do Art. 14 do RGPD (para outros titulares de dados):

Nome e dados de contacto do responsável pelo tratamento: Ver impressão no sítio Web. Dados de contacto do responsável pela proteção de dados e, se aplicável, do representante: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Munique, Alemanha. Finalidades para as quais os dados pessoais serão processados e a base legal para o processamento: Conformidade com a Lei de Proteção de Denúncias (HinSchG) e a Lei de Diligência Devida da Cadeia de Fornecimento (LkSG), a base legal é o Art. 6 (1) (c) do RGPD em conjunto com os §§ 8, 9 da LkSG e o § 10 da HinSchG, na medida em que tal seja necessário para cumprir as tarefas especificadas nos §§ 13 e 24 da HinSchG, bem como o cumprimento da Diretiva (UE) 2019/1937 relativa à proteção das pessoas que denunciam violações do direito da União e do direito nacional dos Estados-Membros daí resultante e o cumprimento da legislação aplicável de outros países. Categorias de dados pessoais tratados: Dados de denúncia de irregularidades. Destinatários ou categorias de destinatários dos dados pessoais: Autoridades responsáveis pela aplicação da lei, autoridades responsáveis pela aplicação de coimas e outras autoridades, bem como advogados, empresas do grupo ou empregadores. Transferência planeada para países terceiros: Entrada no sistema online Navex e posterior transferência para entidades do grupo, entidades patronais ou advogados. As cláusulas contratuais-tipo da UE e a adenda do Reino Unido às cláusulas contratuais-tipo da UE foram celebradas com a Navex. A Navex é também membro do Quadro de Privacidade de Dados UE-EUA, do Quadro de Privacidade de Dados Suíça-EUA e da Extensão do Reino Unido ao Quadro de Privacidade de Dados UE-EUA. Para outras transferências, pode não haver uma decisão de adequação. As cláusulas contratuais-tipo da UE e a adenda do Reino Unido às cláusulas contratuais-tipo da UE são utilizadas para essas transferências. Critérios para determinar o período de conservação: A documentação é eliminada três anos após a conclusão do procedimento. A documentação pode ser conservada durante mais tempo para cumprir os requisitos da legislação aplicável, se tal for necessário e proporcionado. A fonte dos dados pessoais é o autor da denúncia e/ou a empresa em causa.

Ao abrigo do Regulamento Geral sobre a Proteção de Dados, pode ter o direito de acesso aos dados pessoais que lhe dizem respeito e o direito de retificação, apagamento ou limitação do tratamento ou o direito de se opor ao tratamento e o direito à portabilidade dos dados. Tem o direito de apresentar uma queixa à autoridade de controlo competente em matéria de proteção de dados relativamente ao tratamento. Não existem decisões automatizadas. O fornecimento de mais informações revela-se impossível.

ROMANIAN: Sistemul de denunțare a neregulilor (canale interne de raportare)

Valorile noastre constituie fundamentul practicilor noastre de afaceri și reflectă angajamentul nostru față de integritate, transparență și o cultură corporativă pozitivă. Sistemul nostru de denunțare a neregulilor este un instrument esențial pentru promovarea responsabilității și asigurarea unor operațiuni comerciale etice. Acest regulament de procedură servește la transparentizarea procesului și a principiilor proceselor noastre de investigare și asigură faptul că toate rapoartele primite prin intermediul sistemului nostru sunt tratate în mod corespunzător și profesionist.

OSI se angajează în favoarea unui dialog deschis și recunoaște importanța denunțătorilor ca parteneri cheie în eforturile noastre de a menține cele mai înalte standarde în toate domeniile de activitate.

I. Regulamentul de procedură pentru sistemul de sesizare a informatorilor OSI

I. Scopul și domeniul de aplicare:

1. Scop: Prezentul regulament de procedură reglementează tratarea și investigarea rapoartelor primite prin intermediul sistemului de denunțare a neregulilor de la Make It Right Global Hotline. Scopul este de a se asigura că toate rapoartele primite sunt tratate în mod transparent, eficient și în conformitate cu standardele etice ale OSI.

2. Domeniul de aplicare: Prezentul regulament de procedură se aplică tuturor angajaților, partenerilor de afaceri, furnizorilor și altor părți interesate din întregul lanț valoric care utilizează sistemul de denunțare a neregulilor pentru a împărtăși indicii specifice privind posibile abateri, preocupări sau sugestii. Sistemul de denunțare a neregulilor nu este destinat procesării preocupărilor legate de produse și servicii. Astfel de întrebări sau probleme pot fi adresate direct prin intermediul formularului de contact de pe site-ul web al companiei.

II. Prezentarea informațiilor:

1. Anonimatul și confidențialitatea:

Sistemul de denunțare a neregulilor permite, printre altele, transmiterea anonimă a rapoartelor de denunțare a neregulilor, în măsura în care acest lucru este permis de legislația națională.

Toate informațiile tratate în cadrul sistemului de denunțare a neregulilor sunt strict confidențiale.

2. Tipuri de rapoarte:

Sistemul permite avertizorilor de integritate să transmită rapoarte atunci când există indicii concrete ale unor posibile abateri, preocupări sau indicii în acest sens. Este vorba despre încălcări de către angajați

sau parteneri de afaceri ale legilor, reglementărilor etc. aplicabile (în special cele menționate în secțiunea 2 din Legea privind protecția denunțătorilor sau în Directiva UE 2019/1937) sau ale reglementărilor interne ale companiei (în special încălcări ale Codului de conduită) sau ale drepturilor omului și ale riscurilor de mediu imputabile furnizorilor direcți sau indirecți, precum și încălcări ale obligațiilor privind drepturile omului și de mediu în temeiul Legii privind diligența necesară în lanțul de aprovizionare (LkSG). Printre acestea se numără încălcări ale Codului de conduită OSI, ale legislației antitrust, corupția, furtul, discriminarea, nerespectarea sănătății și siguranței la locul de muncă, munca copiilor, poluarea solului, a apei sau a aerului, emisiile de zgomot dăunătoare, consumul inacceptabil de apă, producerea sau utilizarea anumitor poluanți organici persistenți și importul și exportul neautorizat de deșeuri.

3. Accesul la sistem:

Denunțătorii au acces la sistemul de raportare gestionat extern în diferite limbi la adresa:

EthicsPoint - OSI Group, LLC

- sub formă de text prin intermediul unui formular din portalul online sau
- prin telefon (gratuit din diferite țări)

III. Prelucrarea rapoartelor:

1. Primire și evaluare inițială:

Odată ce un raport este primit prin intermediul canalelor de raportare externe gestionate de sistemul de denunțare a neregulilor, acesta este mai întâi documentat și i se atribuie un număr de dosar individual. OSI Compliance primește toate rapoartele și efectuează o evaluare inițială pentru a determina plauzibilitatea și validitatea acestora.

2. Investigarea:

Se va iniția o investigație amănunțită, obiectivă și confidențială în cazul unor informații relevante. Dacă este necesar pentru a primi rapoarte sau pentru a lua măsuri, vor fi consultate sau va fi solicitată asistența altor departamente. De asemenea, pot fi solicitate informații suplimentare de la persoana care a făcut denunțul.

Durata unei investigații până la încheierea acesteia depinde de complexitatea cazului, de măsurile de investigare necesare și de disponibilitatea informațiilor sau a părților implicate în cazul respectiv. Se vor depune toate eforturile pentru a finaliza investigația cât mai eficient și mai rapid posibil.

3. Feedback către denunțător:

Denunțătorul va primi un feedback cu privire la primirea pontului său în termen de 7 zile, în măsura în care este posibil și fără a pune în pericol anonimatul.

În cazul în care denunțătorul a transmis raportul online sau telefonic, acesta va primi informații de conectare care îi vor permite să dea curs raportului și să primească feedback anonim (dacă dorește). În special, poate fi necesar să pună întrebări de înțelegere și să obțină informații suplimentare.

În cursul anchetei (în termen de cel mult 3 luni de la primirea confirmării de primire), se vor furniza informații privind stadiul anchetei în ceea ce privește măsurile planificate sau deja inițiate sau, în cazul în care nu există suspiciuni suficiente, privind încetarea anchetei.

IV. Protecția denunțătorilor:

1. Non-represalii:

OSI depune toate eforturile rezonabile pentru a se asigura că denunțătorii vor fi protejați de orice formă de represalii, dezavantaje sau alte represalii.

Acțiunile disciplinare bazate pe denunțare împotriva persoanelor care cooperează cu bună credință în cadrul investigațiilor sunt interzise și nu vor fi tolerate.

2. Confidențialitate:

Persoanele implicate în investigație sunt obligate să respecte o strictă confidențialitate.

V. Documentare și depozitare:

1. Documentație:

Toate etapele investigației sunt atent documentate.

Documentația servește la transparența și trasabilitatea procedurii.

2. Perioada de păstrare:

Documentația este păstrată în conformitate cu cerințele legale și cu orientările interne.

VI. Revizuire și ajustare:

Aceste norme procedurale sunt revizuite în mod regulat și adaptate, după caz, pentru a se asigura că sunt conforme cu cerințele legale actuale și cu obiectivele corporative.

II. Informații în temeiul art. 13 GDPR (pentru persoanele care furnizează informații):

Numele și datele de contact ale operatorului: A se vedea amprenta de pe site-ul web. Datele de contact ale responsabilului cu protecția datelor și, dacă este cazul, ale reprezentantului: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 München, Germania. Scopurile

pentru care datele cu caracter personal urmează să fie prelucrate și temeiul juridic al prelucrării: Conformitatea cu Legea privind protecția denunțătorilor (HinSchG) și cu Legea privind diligența în lanțul de aprovizionare (LkSG), temeiul juridic este art. 6 (1) (c) GDPR coroborat cu secțiunile 8, 9 LkSG și secțiunea 10 HinSchG, în măsura în care acest lucru este necesar pentru a îndeplini sarcinile specificate în secțiunile 13 și 24 HinSchG, precum și conformitatea cu Directiva (UE) 2019/1937 privind protecția persoanelor care raportează încălcări ale dreptului Uniunii și cu legislația națională a statelor membre care rezultă din aceasta și conformitatea cu legislația aplicabilă din alte țări. Destinatarii sau categoriile de destinatari ai datelor cu caracter personal: Autoritățile de aplicare a legii, autoritățile de aplicare a amenzilor și alte autorități, precum și avocații, societățile din grup sau angajatorii. Transferul planificat către țări terțe: Introducerea în sistemul online Navex și transferul ulterior către entități din cadrul grupului, angajatori sau avocați. Clauzele contractuale standard ale UE și addendumul britanic la clauzele contractuale standard ale UE au fost încheiate cu Navex. Navex este, de asemenea, membră a Cadrului de confidențialitate a datelor UE-SUA, a Cadrului de confidențialitate a datelor Elveția-SUA și a Extinderii din Regatul Unit la Cadrul de confidențialitate a datelor UE-SUA. Pentru alte transferuri, este posibil să nu existe o decizie de adecvare. Pentru astfel de transferuri se utilizează clauzele contractuale standard ale UE și addendumul britanic la clauzele contractuale standard ale UE. Criterii pentru determinarea perioadei de stocare: Documentația este ștearsă la trei ani de la încheierea procedurii. Documentația poate fi păstrată mai mult timp pentru a îndeplini cerințele legislației aplicabile, dacă acest lucru este necesar și proporțional.

În conformitate cu Regulamentul general privind protecția datelor, aveți dreptul de acces la datele cu caracter personal care vă privesc și dreptul la rectificarea, ștergerea sau restricționarea prelucrării sau dreptul de a vă opune prelucrării și dreptul la portabilitatea datelor. Aveți dreptul de a depune o plângere la autoritatea de supraveghere competentă în materie de protecție a datelor cu privire la prelucrare. Furnizarea de date cu caracter personal nu este impusă prin lege sau contract și nu este necesară pentru încheierea unui contract, motiv pentru care nu sunteți obligat să furnizați date cu caracter personal la linia telefonică de sesizare a neregulilor. Posibilele consecințe ale neprezentării datelor sunt faptul că raportul nu va fi prelucrat sau va fi prelucrat cu întârziere sau că va fi respins și că nu vă pot fi furnizate informații sau informații referitoare la raport. Nu există un proces decizional automatizat.

III. Informații în temeiul art. 14 din GDPR (pentru alte persoane vizate):

Numele și datele de contact ale operatorului: A se vedea amprenta de pe site-ul web. Datele de contact ale responsabilului cu protecția datelor și, dacă este cazul, ale reprezentantului: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 München, Germania. Scopurile în care datele cu caracter personal urmează să fie prelucrate și temeiul juridic al prelucrării: Respectarea Legii privind protecția denunțătorilor (HinSchG) și a Legii privind diligența în lanțul de aprovizionare (LkSG), temeiul juridic este art. 6 (1) (c) GDPR coroborat cu secțiunile 8, 9 LkSG și secțiunea 10 HinSchG, în măsura în care acest lucru este necesar pentru a îndeplini sarcinile specificate în secțiunile 13 și 24 HinSchG, precum și conformitatea cu Directiva (UE) 2019/1937 privind

protecția persoanelor care raportează încălcări ale dreptului Uniunii și cu legislația națională a statelor membre care rezultă din aceasta și conformitatea cu legislația aplicabilă din alte țări. Categorii de date cu caracter personal prelucrate: Date privind denunțarea. Destinatarii sau categoriile de destinatari ai datelor cu caracter personal: Autoritățile de aplicare a legii, autoritățile de aplicare a amenzilor și alte autorități, precum și avocații, societățile din grup sau angajatorii. Transfer planificat către țări terțe: Introducerea în sistemul online Navex și transferul ulterior către entități din cadrul grupului, angajatori sau avocați. Clauzele contractuale standard ale UE și addendumul britanic la clauzele contractuale standard ale UE au fost încheiate cu Navex. Navex este, de asemenea, membră a Cadrului de confidențialitate a datelor UE-SUA, a Cadrului de confidențialitate a datelor Elveția-SUA și a Extinderii din Regatul Unit la Cadrul de confidențialitate a datelor UE-SUA. Pentru alte transferuri, este posibil să nu existe o decizie de adecvare. Pentru astfel de transferuri se utilizează clauzele contractuale standard ale UE și addendumul britanic la clauzele contractuale standard ale UE. Criterii pentru determinarea perioadei de stocare: Documentația este ștearsă la trei ani de la încheierea procedurii. Documentația poate fi păstrată mai mult timp pentru a îndeplini cerințele legislației aplicabile, dacă acest lucru este necesar și proporțional. Sursa datelor cu caracter personal este denunțătorul și/sau compania în cauză.

În conformitate cu Regulamentul general privind protecția datelor, este posibil să aveți dreptul de acces la datele cu caracter personal care vă privesc și dreptul de rectificare, ștergere sau restricționare a prelucrării sau dreptul de a vă opune prelucrării și dreptul la portabilitatea datelor. Aveți dreptul de a depune o plângere la autoritatea de supraveghere competentă în materie de protecție a datelor cu privire la prelucrare. Nu există un proces decizional automatizat. Furnizarea de informații suplimentare se dovedește a fi imposibilă.

SLOVAK: Systém oznamovania nekalých praktík (interné kanály oznamovania)

Naše hodnoty tvoria základ našich obchodných postupov a odrážajú náš záväzok k integrite, transparentnosti a pozitívnej firemnej kultúre. Náš systém oznamovania nekalých praktík je základným nástrojom na podporu zodpovednosti a zabezpečenie etických obchodných operácií. Tieto pravidlá postupu slúžia na to, aby boli proces a zásady našich vyšetrovacích postupov transparentné a aby sa zabezpečilo, že všetky oznámenia prijaté prostredníctvom nášho systému budú spracované primerane a profesionálne.

Spoločnosť OSI sa zaviazala k otvorenému dialógu a uznáva význam oznamovateľov ako kľúčových partnerov v našom úsilí o zachovanie najvyšších štandardov vo všetkých oblastiach nášho podnikania.

I. Rokovací poriadok systému OSI pre oznamovateľov

I. Účel a rozsah pôsobnosti:

1. Účel: Tento rokovací poriadok upravuje spracovanie a vyšetrovanie hlásení prijatých prostredníctvom globálnej horúcej linky Make It Right. Cieľom je zabezpečiť, aby všetky prijaté oznámenia boli spracované transparentne, efektívne a v súlade s etickými normami spoločnosti OSI.

2. Rozsah použitia: Tento rokovací poriadok sa vzťahuje na všetkých zamestnancov, obchodných partnerov, dodávateľov a iné zainteresované strany v celom hodnotovom reťazci, ktorí využívajú systém oznamovateľov, aby sa podelili o konkrétne náznaky možného pochybenia, obavy alebo tipy. Systém oznamovateľov nie je určený na spracovanie obáv týkajúcich sa produktov a služieb. Takéto otázky alebo problémy je možné adresovať priamo prostredníctvom kontaktného formulára na webovej stránke spoločnosti.

II. Predkladanie informácií:

1. Anonymita a dôvernosť:

Systém oznamovateľov okrem iného umožňuje anonymné podávanie oznámení v rozsahu povolenom vnútroštátnymi právnymi predpismi.

Všetky informácie spracúvané v rámci systému oznamovateľov podliehajú prísnej dôvernosti.

2. Typy správ:

Systém umožňuje oznamovateľom podávať oznámenia v prípade, že existujú konkrétne náznaky možného pochybenia, obavy alebo náznaky takéhoto pochybenia. Týka sa to porušení platných zákonov, predpisov atď. zo strany zamestnancov alebo obchodných partnerov (najmä tých, ktoré sú uvedené v § 2 zákona o ochrane oznamovateľov alebo v smernici EÚ 2019/1937) alebo interných

predpisov spoločnosti (najmä porušenia etického kódexu) alebo rizík v oblasti ľudských práv a životného prostredia, ktoré možno pripísať priamym alebo nepriamym dodávateľom, ako aj porušení povinností v oblasti ľudských práv a životného prostredia podľa zákona o náležitej starostlivosti v dodávateľskom reťazci (LkSG). Patrí sem porušenie Kódexu správania OSI, protimonopolného práva, korupcia, krádež, diskriminácia, nerešpektovanie bezpečnosti a ochrany zdravia pri práci, detská práca, znečistenie pôdy, vody alebo ovzdušia, škodlivé emisie hluku, neprijateľná spotreba vody, výroba alebo používanie určitých perzistentných organických znečisťujúcich látok a nepovolený dovoz a vývoz odpadu.

3. Prístup do systému:

Oznamovatelia majú prístup k externe spravovanému systému oznamovania v rôznych jazykoch na adrese:

EthicsPoint - OSI Group, LLC

- v textovej forme prostredníctvom formulára na online portáli alebo
- telefonicky (bezplatne z rôznych krajín)

III. Spracovanie správ:

1. Prijatie a úvodné posúdenie:

Po prijatí hlásenia prostredníctvom externých oznamovacích kanálov spravovaných systémom pre oznamovateľov sa hlásenie najprv zdokumentuje a pridelí sa mu individuálne číslo spisu. OSI Compliance prijíma všetky hlásenia a vykonáva počiatočné posúdenie s cieľom určiť ich hodnovernosť a platnosť.

2. Vyšetrovanie:

V prípade relevantných tipov sa začne dôkladné, objektívne a dôverné vyšetrovanie. Ak to bude potrebné na prijatie hlásení alebo opatrení, budú konzultované alebo požiadané o pomoc iné oddelenia. Od oznamovateľa sa môžu vyžiadať aj ďalšie informácie.

Trvanie vyšetrovania až do jeho ukončenia závisí od zložitosti prípadu, potrebných vyšetrovacích opatrení a dostupnosti informácií alebo strán zapojených do konkrétneho prípadu. Vynaloží sa maximálne úsilie na čo najefektívnejšie a najrýchlejšie ukončenie vyšetrovania.

3. Spätná väzba pre oznamovateľa:

Oznamovateľ dostane spätnú väzbu o prijatí svojho tipu do 7 dní, ak je to možné a bez ohrozenia anonymity.

Ak oznamovateľ podal oznámenie online alebo telefonicky, dostane prihlasovacie údaje, ktoré mu umožnia nadviazať na oznámenie a získať anonymnú spätnú väzbu (ak si to želá). Môže byť potrebné najmä položiť otázky na pochopenie a získať ďalšie informácie.

V ďalšom priebehu vyšetrovania (najneskôr do 3 mesiacov od prijatia potvrdenia o prijatí) sa poskytnú informácie o stave vyšetrovania týkajúceho sa plánovaných alebo už začatých opatrení alebo, ak neexistuje dostatočné podozrenie, o zastavení vyšetrovania.

IV. Ochrana oznamovateľov:

1. Zákaz odvetných opatrení:

Spoločnosť OSI vynakladá všetko primerané úsilie na zabezpečenie toho, aby boli oznamovatelia chránení pred akoukoľvek formou odvety, znevýhodnenia alebo inej represie.

Disciplinárne opatrenia na základe whistleblowingu voči osobám, ktoré v dobrej viere spolupracujú pri vyšetrovaní, sú zakázané a nebudú tolerované.

2. Dôvernosť:

Osoby zapojené do vyšetrovania sú viazané prísnou mlčanlivosťou.

V. Dokumentácia a skladovanie:

1. Dokumentácia:

Všetky kroky vyšetrovania sú starostlivo zdokumentované.

Dokumentácia slúži na transparentnosť a sledovateľnosť postupu.

2. Doba uchovávania:

Dokumentácia sa uchováva v súlade s právnymi požiadavkami a internými smernicami.

VI. Preskúmanie a úprava:

Tieto procesné pravidlá sa pravidelne prehodnocujú a podľa potreby upravujú, aby boli v súlade s aktuálnymi právnymi požiadavkami a podnikovými cieľmi.

II. Informácie podľa čl. 13 GDPR (pre osoby poskytujúce informácie):

Názov a kontaktné údaje prevádzkovateľa: Kontaktné údaje: pozri odtlačok na webovej stránke. Kontaktné údaje úradníka pre ochranu údajov a prípadne zástupcu: Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Mníchov, Nemecko. Účely, na ktoré sa majú osobné údaje spracúvať, a právny základ spracúvania: Dodržiavanie zákona o ochrane oznamovateľov

(HinSchG) a zákona o náležitej starostlivosti v dodávateľskom reťazci (LkSG), právnym základom je čl. 6 ods. 1 písm. c) GDPR v spojení s § 8, 9 LkSG a § 10 HinSchG, pokiaľ je to potrebné na plnenie úloh uvedených v § 13 a 24 HinSchG, ako aj dodržiavanie smernice (EÚ) 2019/1937 o ochrane osôb oznamujúcich porušenie práva Únie a z nej vyplývajúcich vnútroštátnych právnych predpisov členských štátov a dodržiavanie platných právnych predpisov iných krajín. Príjemcovia alebo kategórie príjemcov osobných údajov: Orgány činné v trestnom konaní, orgány ukladajúce pokuty a iné orgány, ako aj advokáti, spoločnosti v skupine alebo zamestnávatelia. Plánovaný prenos do tretích krajín: Vloženie do online systému Navex a následný prenos subjektom v rámci skupiny, zamestnávateľom alebo právnikom. Štandardné zmluvné doložky EÚ a dodatok Spojeného kráľovstva k štandardným zmluvným doložkám EÚ boli uzavreté so spoločnosťou Navex. Spoločnosť Navex je tiež členom rámca EÚ - USA pre ochranu osobných údajov, švajčiarsko-amerického rámca pre ochranu osobných údajov a rozšírenia Spojeného kráľovstva k rámcu EÚ - USA pre ochranu osobných údajov. V prípade iných prenosov nemusí byť vydané rozhodnutie o primeranosti. Na takéto prenosy sa používajú štandardné zmluvné doložky EÚ a dodatok Spojeného kráľovstva k štandardným zmluvným doložkám EÚ. Kritériá na určenie doby uchovávania: Dokumentácia sa vymaže tri roky po ukončení postupu. Dokumentácia sa môže uchovávať dlhšie, aby sa splnili požiadavky platných právnych predpisov, ak je to potrebné a primerané.

Podľa všeobecného nariadenia o ochrane údajov máte právo na prístup k osobným údajom, ktoré sa vás týkajú, a právo na opravu, vymazanie alebo obmedzenie spracovania alebo právo namietať proti spracovaniu a právo na prenosnosť údajov. V súvislosti so spracovaním máte právo podať sťažnosť príslušnému dozornému orgánu na ochranu údajov. Poskytnutie osobných údajov sa nevyžaduje na základe zákona alebo zmluvy a nie je nevyhnutné na uzavretie zmluvy, preto nie ste povinný poskytnúť osobné údaje na linku pre oznamovanie nekalých praktík. Možnými dôsledkami neposkytnutia údajov je, že oznámenie nebude spracované alebo bude spracované s oneskorením, prípadne bude zamietnuté a že vám nebudú môcť byť poskytnuté žiadne informácie alebo informácie týkajúce sa oznámenia. Neexistuje žiadne automatizované rozhodovanie.

III. Informácie podľa čl. 14 GDPR (pre ostatné dotknuté osoby):

Názov a kontaktné údaje prevádzkovateľa: Kontaktné údaje: pozri odtlačok na webovej stránke. Kontaktné údaje úradníka pre ochranu údajov a prípadne zástupcu: Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 Mníchov, Nemecko. Účely, na ktoré sa majú osobné údaje spracúvať, a právny základ spracúvania: Dodržiavanie zákona o ochrane oznamovateľov (HinSchG) a zákona o náležitej starostlivosti v dodávateľskom reťazci (LkSG), právny základ je čl. 6 ods. 1 písm. c) GDPR v spojení s § 8, 9 LkSG a § 10 HinSchG, pokiaľ je to potrebné na plnenie úloh uvedených v § 13 a 24 HinSchG, ako aj dodržiavanie smernice (EÚ) 2019/1937 o ochrane osôb oznamujúcich porušenie práva Únie a z nej vyplývajúcich vnútroštátnych právnych predpisov členských štátov a dodržiavanie platných právnych predpisov iných krajín. Kategórie spracúvaných osobných údajov: Údaje o oznamovateľoch. Príjemcovia alebo kategórie príjemcov osobných údajov: Orgány

činné v trestnom konaní, orgány ukladajúce pokuty a iné orgány, ako aj právnici, spoločnosti v skupine alebo zamestnávatelia. Plánovaný prenos do tretích krajín: Vloženie do online systému Navex a následný prenos subjektom v rámci skupiny, zamestnávateľom alebo právnikom. Štandardné zmluvné doložky EÚ a dodatok Spojeného kráľovstva k štandardným zmluvným doložkám EÚ boli uzavreté so spoločnosťou Navex. Spoločnosť Navex je tiež členom rámca EÚ - USA pre ochranu osobných údajov, švajčiarsko-amerického rámca pre ochranu osobných údajov a rozšírenia Spojeného kráľovstva k rámcu EÚ - USA pre ochranu osobných údajov. V prípade iných prenosov nemusí byť vydané rozhodnutie o primeranosti. Na takéto prenosy sa používajú štandardné zmluvné doložky EÚ a dodatok Spojeného kráľovstva k štandardným zmluvným doložkám EÚ. Kritériá na určenie doby uchovávania: Dokumentácia sa vymaže tri roky po ukončení postupu. Dokumentácia sa môže uchovávať dlhšie, aby sa splnili požiadavky platných právnych predpisov, ak je to potrebné a primerané. Zdrojom osobných údajov je oznamovateľ a/alebo príslušná spoločnosť.

Podľa všeobecného nariadenia o ochrane údajov môžete mať právo na prístup k osobným údajom, ktoré sa vás týkajú, a právo na opravu, vymazanie alebo obmedzenie spracovania alebo právo namietať proti spracovaniu a právo na prenosnosť údajov. V súvislosti so spracovaním máte právo podať sťažnosť príslušnému dozornému orgánu na ochranu údajov. Neexistuje žiadne automatizované rozhodovanie. Poskytnutie ďalších informácií sa ukazuje ako nemožné.

SLOVENIAN: Sistem za prijavo nepravilnosti (notranji kanali za poročanje)

Naše vrednote so temelj naših poslovnih praks in odražajo našo zavezanost integriteti, preglednosti in pozitivni korporativni kulturi. Naš sistem obveščanja o nepravilnostih je bistveno orodje za spodbujanje odgovornosti in zagotavljanje etičnega poslovanja. Ta poslovnik služi preglednosti postopkov in načel naših preiskovalnih postopkov ter zagotavlja, da so vsa poročila, prejeta prek našega sistema, ustrezno in strokovno obravnavana.

Družba OSI je zavezana odprtemu dialogu in priznava pomen prijaviteljev nepravilnosti kot ključnih partnerjev pri naših prizadevanjih za ohranjanje najvišjih standardov na vseh področjih našega poslovanja.

I. Pravila postopka za sistem OSI za prijavitelje nepravilnosti

I. Namen in področje uporabe:

1. Namen: Ta poslovnik ureja obravnavo in preiskavo prijav, prejetih prek sistema za prijavo nepravilnosti Make It Right Global Hotline. Cilj je zagotoviti, da se vsa prejeta poročila obravnavajo pregledno, učinkovito in v skladu z etičnimi standardi družbe OSI.

2. Področje uporabe: Ta poslovnik velja za vse zaposlene, poslovne partnerje, dobavitelje in druge zainteresirane strani v celotni vrednostni verigi, ki uporabljajo sistem za prijavo nepravilnosti, da bi sporočili posebne navedbe o morebitnih kršitvah, pomisleke ali nasvete. Sistem za prijavo nepravilnosti ni namenjen obravnavi pomislekov v zvezi z izdelki in storitvami. Takšna vprašanja ali težave lahko naslovite neposredno prek kontaktnega obrazca na spletni strani podjetja.

II. Predložitev informacij:

1. Anonimnost in zaupnost:

Sistem za prijavo nepravilnosti med drugim omogoča anonimno prijavo nepravilnosti, kolikor to dopušča nacionalna zakonodaja.

Za vse informacije, ki se obravnavajo v okviru sistema prijaviteljev, velja stroga zaupnost.

2. Vrste poročil:

Sistem omogoča prijaviteljem, da predložijo prijave, če obstajajo konkretni znaki morebitnega nepravilnega ravnanja, pomisleki ali indici o njem. Gre za kršitve veljavnih zakonov, predpisov itd. s strani zaposlenih ali poslovnih partnerjev (zlasti tistih, ki so navedeni v 2. členu Zakona o zaščiti žvižgačev ali Direktivi EU 2019/1937) ali notranjih predpisov podjetja (zlasti kršitve Kodeksa ravnanja) ali za kršitve človekovih pravic in okoljskih tveganj, ki jih je mogoče pripisati neposrednim ali posrednim dobaviteljem,

ter za kršitve obveznosti glede človekovih pravic in okolja na podlagi Zakona o skrbnem pregledu dobavne verige (LkSG). Te vključujejo kršitve Kodeksa ravnanja OSI, protimonopolne zakonodaje, korupcije, kraje, diskriminacije, neupoštevanja zdravja in varnosti pri delu, otroškega dela, onesnaževanja tal, vode ali zraka, škodljivih emisij hrupa, nesprejemljive porabe vode, proizvodnje ali uporabe nekaterih obstojnih organskih onesnaževal ter nedovoljenega uvoza in izvoza odpadkov.

3. Dostop do sistema:

Žvižgači imajo dostop do zunanjega sistema za poročanje v različnih jezikih na naslovu:

EthicsPoint - OSI Group, LLC

- v besedilni obliki prek obrazca na spletnem portalu ali
- po telefonu (brezplačno iz različnih držav).

III. Obdelava poročil:

1. Prejem in začetna ocena:

Ko je prijava prejeta prek zunanjih kanalov za prijavo, ki jih upravlja sistem za prijavo nepravilnosti, se najprej dokumentira in ji dodeli individualna številka spisa. Organizacija OSI Compliance prejme vsa poročila in opravi začetno oceno, da ugotovi njihovo verodostojnost in veljavnost.

2. Preiskava:

Za ustrezne nasvete se bo začela temeljita, objektivna in zaupna preiskava. Če bo to potrebno za sprejemanje poročil ali ukrepanje, se bodo posvetovali z drugimi oddelki ali jih prosili za pomoč. Od prijavitelja se lahko zahtevajo tudi dodatne informacije.

Trajanje preiskave do njenega zaključka je odvisno od zapletenosti primera, potrebnih preiskovalnih ukrepov in razpoložljivosti informacij ali strank, ki so vpletene v posamezen primer. Storjeno bo vse, da se preiskava zaključi čim bolj učinkovito in hitro.

3. Povratne informacije prijavitelju:

Žvižgač bo prejel povratne informacije o prejemu svoje prijave v sedmih dneh, če bo to mogoče in ne bo ogrožena njegova anonimnost.

Če je prijavitelj podal prijavo prek spleta ali telefona, bo prejel prijavne podatke, ki mu bodo omogočili nadaljnje ukrepanje v zvezi s prijavo in anonimno povratno informacijo (če želi). Morda bo treba zastaviti zlasti vprašanja za razumevanje in pridobiti dodatne informacije.

V nadaljnjem poteku preiskave (najpozneje v treh mesecih po prejemu potrdila o prejemu) bodo zagotovljene informacije o stanju preiskave v zvezi z načrtovanimi ali že začetimi ukrepi ali, če ni zadostnega suma, o prekinitvi preiskave.

IV. Zaščita žvižgačev:

1. Prepoved povračilnih ukrepov:

Družba OSI si po najboljših močeh prizadeva zagotoviti, da bodo žvižgači zaščiteni pred vsemi oblikami povračilnih ukrepov, prikrajšanjem ali drugimi povračilnimi ukrepi.

Disciplinski ukrepi na podlagi prijavljanja nepravilnosti zoper posameznike, ki v dobri veri sodelujejo pri preiskavah, so prepovedani in se ne bodo dopuščali.

2. Zaupnost:

Osebe, vključene v preiskavo, so zavezane k strogi zaupnosti.

V. Dokumentacija in shranjevanje:

1. Dokumentacija:

Vsi koraki preiskave so skrbno dokumentirani.

Dokumentacija služi preglednosti in sledljivosti postopka.

2. Rok hrambe:

Dokumentacija se hrani v skladu z zakonskimi zahtevami in notranjimi smernicami.

VI. Pregled in prilagoditev:

Ta postopkovna pravila se redno pregledujejo in po potrebi prilagajajo, da se zagotovi njihova skladnost z veljavnimi zakonskimi zahtevami in cilji podjetja.

II. Informacije v skladu s čl. 13 Splošne uredbe o varstvu podatkov (za osebe, ki posredujejo informacije):

Ime in kontaktni podatki upravljavca: Kontaktni podatki: glej odtis na spletni strani. Kontaktni podatki pooblaščene osebe za varstvo podatkov in, če je primerno, predstavnika: Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 München, Nemčija. Nameni obdelave osebnih podatkov in pravna podlaga za obdelavo: Skladnost z Zakonom o zaščiti žvižgačev (HinSchG) in Zakonom o skrbnosti v dobavni verigi (LkSG), pravna podlaga je čl. 6(1)(c) GDPR v povezavi s členoma 8, 9 LkSG in členom 10 HinSchG, če je to potrebno za izpolnjevanje nalog, določenih v členih 13 in 24 HinSchG, ter skladnost z Direktivo (EU) 2019/1937 o zaščiti oseb, ki prijavljajo kršitve prava Unije, in posledično nacionalno zakonodajo držav članic ter skladnost z veljavno zakonodajo drugih držav. Prejemniki ali kategorije prejemnikov osebnih podatkov: Organi pregona, organi za izrekanje glob in drugi organi ter odvetniki, družbe v skupini ali delodajalci. Načrtovani prenos v tretje države: Vnos v

spletni sistem Navex in nadaljnji prenos subjektom v skupini, delodajalcem ali odvetnikom. S podjetjem Navex sta bila sklenjena standardna pogodbena določila EU in dodatek Združenega kraljestva k standardnim pogodbenim določilom EU. Podjetje Navex je tudi član okvira za varstvo zasebnosti podatkov med EU in ZDA, okvira za varstvo zasebnosti podatkov med Švico in ZDA ter dodatka Združenega kraljestva k okviru za varstvo zasebnosti podatkov med EU in ZDA. Za druge prenose morda ne bo sprejet sklep o ustreznosti. Za take prenose se uporabljajo standardna pogodbena določila EU in dodatek Združenega kraljestva k standardnim pogodbenim določilom EU. Merila za določitev obdobja hrambe: Dokumentacija se izbriše tri leta po koncu postopka. Dokumentacija se lahko hrani dlje, da se izpolnijo zahteve veljavne zakonodaje, če je to potrebno in sorazmerno.

V skladu s Splošno uredbo o varstvu podatkov imate pravico do dostopa do osebnih podatkov v zvezi z vami in pravico do popravka ali izbrisa ali omejitve obdelave ali pravico do ugovora obdelavi in pravico do prenosljivosti podatkov. Glede obdelave imate pravico vložiti pritožbo pri pristojnem nadzornem organu za varstvo podatkov. Zagotavljanje osebnih podatkov ni zakonsko ali pogodbeno zahtevano in ni potrebno za sklenitev pogodbe, zato niste dolžni posredovati osebnih podatkov na telefonsko številko za prijavo nepravilnosti. Možne posledice opustitve posredovanja podatkov so, da prijava ne bo obdelana ali bo obdelana z zamudo ali da bo zavrnjena ter da vam ne bo mogoče posredovati nobenih informacij ali podatkov v zvezi s prijavo. Avtomatiziranega odločanja ni.

III. Informacije v skladu s čl. 14 Splošne uredbe o varstvu podatkov (za druge posameznike, na katere se nanašajo osebni podatki):

Ime in kontaktni podatki upravljavca: Kontaktni podatki: glej odtis na spletni strani. Kontaktni podatki pooblaščene osebe za varstvo podatkov in, če je primerno, predstavnika: Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 München, Nemčija. Nameni obdelave osebnih podatkov in pravna podlaga za obdelavo: Skladnost z Zakonom o zaščiti žvižgačev (HinSchG) in Zakonom o skrbnosti v dobavni verigi (LkSG), pravna podlaga je čl. 6(1)(c) GDPR v povezavi s členoma 8, 9 LkSG in členom 10 HinSchG, če je to potrebno za izpolnjevanje nalog, določenih v členih 13 in 24 HinSchG, ter skladnost z Direktivo (EU) 2019/1937 o zaščiti oseb, ki prijavljajo kršitve prava Unije, in posledično nacionalno zakonodajo držav članic ter skladnost z veljavno zakonodajo drugih držav. Kategorije osebnih podatkov, ki se obdelujejo: Podatki o prijavah nepravilnosti. Prejemniki ali kategorije prejemnikov osebnih podatkov: Organi pregona, organi za izrekanje glob in drugi organi ter odvetniki, družbe v skupini ali delodajalci. Načrtovani prenos v tretje države: Vnos v spletni sistem Navex in nadaljnji prenos subjektom v skupini, delodajalcem ali odvetnikom. S podjetjem Navex sta bila sklenjena standardna pogodbena določila EU in dodatek Združenega kraljestva k standardnim pogodbenim določilom EU. Podjetje Navex je tudi član okvira za varstvo zasebnosti podatkov med EU in ZDA, okvira za varstvo zasebnosti podatkov med Švico in ZDA ter dodatka Združenega kraljestva k okviru za varstvo zasebnosti podatkov med EU in ZDA. Za druge prenose morda ne bo sprejet sklep o ustreznosti. Za take prenose se uporabljajo standardna pogodbena določila EU in dodatek Združenega kraljestva k standardnim pogodbenim določilom EU. Merila za določitev obdobja hrambe: Dokumentacija se izbriše

tri leta po koncu postopka. Dokumentacija se lahko hrani dlje, da se izpolnijo zahteve veljavne zakonodaje, če je to potrebno in sorazmerno. Vir osebnih podatkov je prijavitelj in/ali zadevno podjetje.

V skladu s Splošno uredbo o varstvu podatkov imate lahko pravico do dostopa do osebnih podatkov v zvezi z vami in pravico do popravka ali izbrisa ali omejitve obdelave ali pravico do ugovora obdelavi in pravico do prenosljivosti podatkov. V zvezi z obdelavo imate pravico vložiti pritožbo pri pristojnem nadzornem organu za varstvo podatkov. Avtomatiziranega sprejemanja odločitev ni. Zagotavljanje dodatnih informacij se izkaže za nemogoče.

SWEDISH: Visselblåsarsystem (interna rapporteringskanaler)

Våra värderingar utgör grunden för våra affärsmetoder och återspeglar vårt engagemang för integritet, öppenhet och en positiv företagskultur. Vårt visselblåsarsystem är ett viktigt verktyg för att främja ansvarstagande och säkerställa en etisk affärsverksamhet. Denna arbetsordning syftar till att göra processen och principerna för våra utredningsprocesser transparenta och säkerställa att alla rapporter som tas emot via vårt system hanteras på ett lämpligt och professionellt sätt.

OSI strävar efter en öppen dialog och erkänner vikten av visselblåsare som viktiga partners i våra ansträngningar att upprätthålla de högsta standarderna inom alla områden av vår verksamhet.

I. Arbetsordning för OSI:s system för visselblåsare

I. Syfte och tillämpningsområde:

1. Syfte: Denna arbetsordning reglerar hanteringen och utredningen av rapporter som tas emot via Make It Right Global Hotlines visselblåsarsystem. Syftet är att säkerställa att alla inkomna rapporter hanteras transparent, effektivt och i enlighet med OSI:s etiska standarder.

2. Tillämpningsområde: Denna arbetsordning gäller för alla anställda, affärspartners, leverantörer och andra intressenter i hela värdekedjan som använder visselblåsarsystemet för att dela specifika indikationer på eventuella missförhållanden, farhågor eller tips. Visselblåsarsystemet är inte avsett för hantering av produkt- och servicerelaterade problem. Sådana frågor eller problem kan tas upp direkt via kontaktformuläret på företagets webbplats.

II. Inlämnande av information:

1. Anonymitet och konfidentialitet:

Visselblåsarsystemet gör det bland annat möjligt att anonymt lämna in visselblåsarrapporter, i den utsträckning som tillåts enligt nationell lagstiftning.

All information som hanteras inom ramen för visselblåsarsystemet omfattas av strikt sekretess.

2. Typer av rapporter:

Systemet gör det möjligt för visselblåsare att lämna in rapporter där det finns konkreta indikationer på möjliga missförhållanden, farhågor eller indikationer på sådana. Detta gäller överträdelser av anställda eller affärspartner av tillämpliga lagar, förordningar etc. (särskilt de som nämns i avsnitt 2 i Whistleblower Protection Act eller EU-direktiv 2019/1937) eller interna företagsbestämmelser (särskilt överträdelser av uppförandekoden) eller mänskliga rättigheter och miljörisker som kan hänföras till direkta eller indirekta leverantörer samt överträdelser av mänskliga rättigheter och miljöskyldigheter enligt lagen om due diligence i leveranskedjan (LkSG). Dessa inkluderar brott mot OSI:s uppförandekod, antitrustlagstiftning,

korruption, stöld, diskriminering, bristande respekt för hälsa och säkerhet på arbetsplatsen, barnarbete, förorening av mark, vatten eller luft, skadliga ljudutsläpp, oacceptabel vattenförbrukning, produktion eller användning av vissa långlivade organiska föroreningar samt obehörig import och export av avfall.

3. Tillgång till systemet:

Visselblåsare har tillgång till det externt hanterade rapporteringssystemet på olika språk på:

EthicsPoint - OSI Group, LLC

- i textform via ett formulär i onlineportalen eller
- per telefon (avgiftsfritt från olika länder)

III. Behandling av rapporter:

1. Mottagande och inledande bedömning:

När en rapport har tagits emot via de externa rapporteringskanaler som hanteras av visselblåsarsystemet, dokumenteras den först och tilldelas ett individuellt ärendenummer. OSI Compliance tar emot alla rapporter och gör en första bedömning för att fastställa om de är rimliga och giltiga.

2. Undersökning:

En grundlig, objektiv och konfidentiell undersökning kommer att inledas för relevanta tips. Om det är nödvändigt för att ta emot rapporter eller vidta åtgärder kommer andra avdelningar att konsulteras eller ombes om hjälp. Ytterligare information kan också begäras från visselblåsaren.

Hur lång tid en utredning tar innan den avslutas beror på hur komplicerat ärendet är, vilka utredningsåtgärder som krävs och tillgången till information eller vilka parter som är inblandade i det enskilda ärendet. Alla ansträngningar kommer att göras för att slutföra utredningen så effektivt och skyndsamt som möjligt.

3. Återkoppling till visselblåsaren:

Visselblåsaren kommer att få återkoppling om mottagandet av deras tips inom 7 dagar, om möjligt och utan att äventyra anonymiteten.

Om visselblåsaren har lämnat in rapporten online eller via telefon kommer de att få inloggningsuppgifter som gör det möjligt för dem att följa upp rapporten och få anonym feedback (om de så önskar). I synnerhet kan det vara nödvändigt att ställa förståelsefrågor och inhämta ytterligare information.

Under den fortsatta utredningen (senast 3 månader efter mottagandet av mottagningsbeviset) kommer information att lämnas om utredningens status när det gäller planerade eller redan inledda åtgärder eller, om det inte finns tillräckliga misstankar, om utredningen läggs ned.

IV. Skydd av visselblåsare:

1. Ingen vedergällning:

OSI vidtar alla rimliga åtgärder för att säkerställa att visselblåsare skyddas från alla former av repressalier, nackdelar eller andra repressalier.

Disciplinära åtgärder baserade på visselblåsning mot personer som i god tro samarbetar med utredningar är förbjudna och kommer inte att tolereras.

2. Konfidentialitet:

Personer som deltar i undersökningen är bundna av strikt sekretess.

V. Dokumentation och lagring:

1. Dokumentation:

Alla steg i utredningen dokumenteras noggrant.

Dokumentationen bidrar till transparens och spårbarhet i förfarandet.

2. Förvaringsperiod:

Dokumentationen bevaras i enlighet med rättsliga krav och interna riktlinjer.

VI. Översyn och justering:

Dessa förfaranderegler ses regelbundet över och anpassas vid behov för att säkerställa att de överensstämmer med gällande rättsliga krav och företagets mål.

II. Information i enlighet med Art. 13 GDPR (för personer som tillhandahåller information):

Namn och kontaktuppgifter till den personuppgiftsansvarige: Se avtryck på webbplatsen. Kontaktuppgifter till dataskyddsombudet och, i förekommande fall, till ombudet: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 München, Tyskland. Ändamål för vilka personuppgifterna ska behandlas och den rättsliga grunden för behandlingen: Överensstämmelse med lagen om skydd av visselblåsare (HinSchG) och lagen om due diligence i leveranskedjan (LkSG), rättslig grund är art. 6 (1) (c) GDPR i kombination med §§ 8, 9 LkSG och § 10 HinSchG, i den mån detta är nödvändigt för att utföra de uppgifter som anges i §§ 13 och 24 HinSchG, samt överensstämmelse med direktiv (EU) 2019/1937 om skydd för personer som rapporterar överträdelser av unionsrätten och den nationella lagstiftning i medlemsstaterna som följer av detta och överensstämmelse med tillämplig lagstiftning från andra länder. Mottagare eller kategorier av mottagare

av personuppgifterna: Brottsbekämpande myndigheter, bötfällande myndigheter och andra myndigheter samt advokater, koncernföretag eller arbetsgivare. Planerad överföring till tredje land: Registrering i Navex onlinesystem och vidare överföring till enheter inom koncernen, arbetsgivare eller advokater. EU:s standardavtalsklausuler och det brittiska tillägget till EU:s standardavtalsklausuler har ingåtts med Navex. Navex är också medlem i EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework och UK Extension to the EU-U.S. Data Privacy Framework. För andra överföringar kanske det inte finns något beslut om adekvat skyddsnivå. EU:s standardavtalsklausuler och det brittiska tillägget till EU:s standardavtalsklausuler används för sådana överföringar. Kriterier för att fastställa lagringsperioden: Dokumentationen raderas tre år efter det att förfarandet avslutats. Dokumentationen får bevaras längre för att uppfylla kraven i tillämplig lagstiftning om detta är nödvändigt och proportionerligt.

Enligt den allmänna dataskyddsförordningen har du rätt att få tillgång till personuppgifter som rör dig och rätt till rättelse eller radering eller begränsning av behandlingen eller rätt att invända mot behandlingen och rätt till dataportabilitet. Du har rätt att lämna in ett klagomål till den behöriga tillsynsmyndigheten för dataskydd angående behandlingen. Tillhandahållande av personuppgifter krävs inte enligt lag eller avtal och är inte nödvändigt för att ingå ett avtal, vilket är anledningen till att du inte är skyldig att tillhandahålla personuppgifter till visselblåsarjouren. Möjliga konsekvenser av att inte lämna uppgifter är att rapporten inte kommer att behandlas eller kommer att behandlas med fördröjning, eller att den kommer att avvisas, och att ingen information eller information som rör rapporten kan tillhandahållas till dig. Det förekommer inget automatiserat beslutsfattande.

III. Information i enlighet med Art. 14 i GDPR (för andra registrerade personer):

Namn och kontaktuppgifter till den personuppgiftsansvarige: Se avtryck på webbplatsen. Kontaktuppgifter till dataskyddsombudet och, i förekommande fall, till ombudet: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 München, Tyskland. Ändamål för vilka personuppgifterna ska behandlas och den rättsliga grunden för behandlingen: Överensstämmelse med lagen om skydd av visselblåsare (HinSchG) och lagen om due diligence i leveranskedjan (LkSG), rättslig grund är art. 6 (1) (c) GDPR i kombination med §§ 8, 9 LkSG och § 10 HinSchG, i den mån detta är nödvändigt för att utföra de uppgifter som anges i §§ 13 och 24 HinSchG, samt överensstämmelse med direktiv (EU) 2019/1937 om skydd för personer som rapporterar överträdelser av unionsrätten och den nationella lagstiftning i medlemsstaterna som följer av detta och överensstämmelse med tillämplig lagstiftning från andra länder. Kategorier av personuppgifter som behandlas: Uppgifter om visselblåsare. Mottagare eller kategorier av mottagare av personuppgifterna: Polismyndigheter, bötfällande myndigheter och andra myndigheter samt advokater, koncernföretag eller arbetsgivare. Planerad överföring till tredje land: Registrering i Navex onlinesystem och vidare överföring till enheter inom koncernen, arbetsgivare eller advokater. EU:s standardavtalsklausuler och det brittiska tillägget till EU:s standardavtalsklausuler har ingåtts med Navex. Navex är också medlem

i EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework och UK Extension to the EU-U.S. Data Privacy Framework. För andra överföringar kanske det inte finns något beslut om adekvat skyddsnivå. EU:s standardavtalsklausuler och det brittiska tillägget till EU:s standardavtalsklausuler används för sådana överföringar. Kriterier för att fastställa lagringsperioden: Dokumentationen raderas tre år efter det att förfarandet avslutats. Dokumentationen får bevaras längre för att uppfylla kraven i tillämplig lagstiftning om detta är nödvändigt och proportionerligt. Källan till personuppgifterna är visselblåsaren och/eller det berörda företaget.

Enligt den allmänna dataskyddsförordningen kan du ha rätt att få tillgång till personuppgifter som rör dig och rätt till rättelse eller radering eller begränsning av behandlingen eller rätt att invända mot behandlingen och rätt till dataportabilitet. Du har rätt att lämna in ett klagomål till den behöriga tillsynsmyndigheten för dataskydd med avseende på behandlingen. Det förekommer inget automatiserat beslutsfattande. Det visar sig vara omöjligt att tillhandahålla ytterligare information.

NORWEGIAN: Varslingssystem (interne rapporteringskanaler)

Våre verdier danner grunnlaget for vår forretningspraksis og gjenspeiler vår forpliktelse til integritet, åpenhet og en positiv bedriftskultur. Varslingssystemet vårt er et viktig verktøy for å fremme ansvarlighet og sikre etisk forretningsdrift. Denne forretningsordenen har til hensikt å gjøre prosessen og prinsippene for granskingsprosessene våre transparente og sikre at alle varsler som mottas gjennom systemet vårt, håndteres på en hensiktsmessig og profesjonell måte.

OSI er opptatt av åpen dialog og anerkjenner betydningen av varslere som viktige partnere i arbeidet med å opprettholde de høyeste standardene i alle deler av virksomheten.

I. Prosedyreregler for OSI Whistleblower System

I. Formål og omfang:

1. Formål: Denne forretningsordenen regulerer håndteringen og etterforskningen av rapporter som mottas gjennom varslingssystemet Make It Right Global Hotline. Målet er å sikre at alle mottatte varsler håndteres åpent, effektivt og i samsvar med OSIs etiske standarder.

2. Anvendelsesområde: Disse reglene gjelder for alle ansatte, forretningspartnere, leverandører og andre interessenter i hele verdikjeden som bruker varslingssystemet til å dele konkrete indikasjoner på mulige kritikkverdige forhold, bekymringer eller tips. Varslingssystemet er ikke ment for behandling av produkt- og tjenesterelaterte bekymringer. Slike spørsmål eller problemer kan tas opp direkte via kontaktskjemaet på selskapets nettside.

II. Innsending av informasjon:

1. anonymitet og konfidensialitet:

Varslingssystemet gjør det blant annet mulig å varsle anonymt, i den grad det er tillatt i henhold til nasjonal lovgivning.

All informasjon som håndteres innenfor rammen av varslingssystemet, er underlagt streng konfidensialitet.

2. typer rapporter:

Systemet gjør det mulig for varslere å sende inn rapporter der det foreligger konkrete indikasjoner på mulige kritikkverdige forhold, bekymringer eller indikasjoner på slike. Dette gjelder ansattes eller forretningspartneres brudd på gjeldende lover, forskrifter osv. (særlig de som er nevnt i § 2 i Whistleblower Protection Act eller EU-direktiv 2019/1937) eller bedriftsinterne forskrifter (særlig brudd på de etiske retningslinjene) eller menneskerettighets- og miljørisikoer som kan tilskrives direkte eller indirekte leverandører, samt brudd på menneskerettighets- og miljøforpliktelser i henhold til loven om

aktsomhet i leverandørkjeden (LkSG). Dette omfatter brudd på OSIs etiske retningslinjer, antitrustlovgivning, korrupsjon, tyveri, diskriminering, manglende respekt for helse og sikkerhet på arbeidsplassen, barnearbeid, jord-, vann- eller luftforurensning, skadelige støyutslipp, uakseptabelt vannforbruk, produksjon eller bruk av visse persistente organiske miljøgifter og uautorisert import og eksport av avfall.

3. tilgang til systemet:

Varslere har tilgang til det eksternt administrerte rapporteringssystemet på flere språk på:

EthicsPoint - OSI Group, LLC

- i tekstform via et skjema i den elektroniske portalen, eller
- per telefon (gratis fra flere land)

III. Behandling av rapporter:

1. Mottak og innledende vurdering:

Når en rapport mottas via de eksterne rapporteringskanalene som administreres av varslingssystemet, blir den først dokumentert og tildelt et individuelt saksnummer. OSI Compliance mottar alle varsler og foretar en innledende vurdering for å fastslå om de er sannsynlige og gyldige.

2. Undersøkelse:

Det vil bli iverksatt en grundig, objektiv og konfidensiell undersøkelse av relevante tips. Hvis det er nødvendig for å motta rapporter eller iverksette tiltak, vil andre avdelinger bli konsultert eller bedt om hjelp. Det kan også bli bedt om ytterligere informasjon fra varsleren.

Hvor lang tid det tar fra etterforskningen starter til den er avsluttet, avhenger av sakens kompleksitet, hvilke etterforskningstiltak som er nødvendige, samt tilgjengeligheten av informasjon eller involverte parter i den enkelte sak. Alle anstrengelser vil bli gjort for å fullføre etterforskningen så effektivt og raskt som mulig.

3. Tilbakemelding til varsleren:

Varsleren vil få tilbakemelding om mottakelsen av tipset innen 7 dager, så langt det er mulig og uten at anonymiteten settes i fare.

Hvis varsleren har sendt inn varselet via Internett eller telefon, vil vedkommende motta påloggingsinformasjon som gjør det mulig å følge opp varselet og få anonym tilbakemelding (hvis vedkommende ønsker det). Det kan være nødvendig å stille utdypende spørsmål og innhente ytterligere informasjon.

I løpet av den videre etterforskningen (senest 3 måneder etter mottak av mottaksbekreftelsen) vil det bli gitt informasjon om status for etterforskningen med hensyn til planlagte eller allerede iverksatte tiltak, eller, dersom det ikke foreligger tilstrekkelig mistanke, om henleggelse av etterforskningen.

IV. Beskyttelse av varslere:

1. Ingen gjengjeldelse:

OSI gjør alle rimelige anstrengelser for å sikre at varslere beskyttes mot enhver form for gjengjeldelse, ulempe eller andre represalier.

Disiplinærtiltak basert på varsling mot personer som samarbeider i god tro i forbindelse med undersøkelser, er forbudt og vil ikke bli tolerert.

2. konfidensialitet:

Personer som er involvert i etterforskningen, er underlagt streng taushetsplikt.

V. Dokumentasjon og lagring:

1. Dokumentasjon:

Alle trinn i etterforskningen dokumenteres nøye.

Dokumentasjonen bidrar til transparens og sporbarhet i prosedyren.

2. oppbevaringsperiode:

Dokumentasjon oppbevares i samsvar med lovkrav og interne retningslinjer.

VI. Gjennomgang og justering:

Prosedyrereglene gjennomgås jevnlig og tilpasses etter behov for å sikre at de er i samsvar med gjeldende lovkrav og selskapets mål.

II. Informasjon i henhold til art. 13 GDPR (for personer som gir opplysninger):

Navn og kontaktinformasjon til den behandlingsansvarlige: Se avtrykk på nettstedet. Kontaktinformasjon til personvernombudet og, hvis aktuelt, representanten: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 München, Tyskland. Formålene med behandlingen av personopplysningene og det rettslige grunnlaget for behandlingen: Overholdelse av lov om beskyttelse av varslere (HinSchG) og lov om aktsomhet i leverandørkjeden (LkSG), rettslig grunnlag er art. 6 (1) (c) GDPR. 6 (1) (c) GDPR i forbindelse med §§ 8, 9 LkSG og § 10 HinSchG, i den grad dette er nødvendig for å oppfylle oppgavene som er spesifisert i §§ 13 og 24 HinSchG, samt

overholdelse av direktiv (EU) 2019/1937 om beskyttelse av personer som rapporterer brudd på unionsretten og den resulterende nasjonale lovgivningen i medlemsstatene og overholdelse av gjeldende lovgivning fra andre land. Mottakere eller kategorier av mottakere av personopplysningene: Politimyndigheter, bøteleggende myndigheter og andre myndigheter samt advokater, konsernselskaper eller arbeidsgivere. Planlagt overføring til tredjeland: Registrering i Navex' online-system og videre overføring til enheter i konsernet, arbeidsgivere eller advokater. EUs standardkontraktsklausuler og det britiske tillegget til EUs standardkontraktsklausuler er inngått med Navex. Navex er også medlem av EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework og UK Extension to the EU-U.S. Data Privacy Framework. For andre overføringer kan det være at det ikke foreligger noen beslutning om tilstrekkelig beskyttelsesnivå. EUs standardkontraktsklausuler og det britiske tillegget til EUs standardkontraktsklausuler brukes for slike overføringer. Kriterier for fastsettelse av lagringsperioden: Dokumentasjonen slettes tre år etter at prosedyren er avsluttet. Dokumentasjonen kan oppbevares lenger for å oppfylle kravene i gjeldende lovgivning hvis dette er nødvendig og forholdsmessig.

I henhold til personvernforordningen har du rett til innsyn i personopplysningene dine og rett til retting eller sletting eller begrensning av behandlingen eller rett til å protestere mot behandlingen og rett til dataportabilitet. Du har rett til å sende inn en klage på behandlingen til den kompetente tilsynsmyndigheten for databeskyttelse. Levering av personopplysninger er ikke lov- eller avtalefestet og er ikke nødvendig for å inngå en avtale, og du er derfor ikke forpliktet til å levere personopplysninger til varslingstelefonen. Mulige konsekvenser av ikke å oppgi personopplysninger er at varselet ikke vil bli behandlet eller vil bli behandlet med forsinkelse, eller at det vil bli avvist, og at ingen informasjon eller opplysninger knyttet til varselet kan gis til deg. Det er ingen automatisert beslutningstaking.

III. Informasjon i henhold til art. 14 i GDPR (for andre registrerte):

Navn og kontaktinformasjon til den behandlingsansvarlige: Se avtrykk på nettstedet. Kontaktinformasjon til personvernombudet og, hvis aktuelt, representanten: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., Franz-Joseph-Str. 11, 80801 München, Tyskland. Formålene med behandlingen av personopplysningene og det rettslige grunnlaget for behandlingen: Overholdelse av lov om beskyttelse av varslere (HinSchG) og lov om aktsomhet i leverandørkjeden (LkSG), rettslig grunnlag er art. 6 (1) (c) GDPR. 6 (1) (c) i GDPR sammenholdt med §§ 8, 9 i LkSG og § 10 i HinSchG, i den grad dette er nødvendig for å utføre oppgavene som er spesifisert i §§ 13 og 24 i HinSchG, samt overholdelse av direktiv (EU) 2019/1937 om beskyttelse av personer som varsler om brudd på unionsretten og den nasjonale lovgivningen i medlemsstatene som følger av dette, og overholdelse av gjeldende lovgivning i andre land. Kategorier av personopplysninger som behandles: Opplysninger om varsling. Mottakere eller kategorier av mottakere av personopplysninger: Politimyndigheter, bøteleggende myndigheter og andre myndigheter samt advokater, konsernselskaper eller arbeidsgivere. Planlagt overføring til tredjeland: Registrering i Navex' online-system og videre overføring til enheter i konsernet, arbeidsgivere eller advokater. EUs standardkontraktsklausuler og det

britiske tillegget til EUs standardkontraktsklausuler er inngått med Navex. Navex er også medlem av EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework og UK Extension to the EU-U.S. Data Privacy Framework. For andre overføringer kan det være at det ikke foreligger noen beslutning om tilstrekkelig beskyttelsesnivå. EUs standardkontraktsklausuler og det britiske tillegget til EUs standardkontraktsklausuler brukes for slike overføringer. Kriterier for fastsettelse av lagringsperioden: Dokumentasjonen slettes tre år etter at prosedyren er avsluttet. Dokumentasjonen kan oppbevares lenger for å oppfylle kravene i gjeldende lovgivning hvis dette er nødvendig og forholdsmessig. Kilden til personopplysningene er varsleren og/eller det berørte selskapet.

I henhold til personvernforordningen kan du ha rett til innsyn i personopplysningene dine og rett til retting eller sletting eller begrensning av behandlingen eller rett til å protestere mot behandlingen og rett til dataportabilitet. Du har rett til å klage på behandlingen til den kompetente tilsynsmyndigheten for personvern. Det er ingen automatisert beslutningstaking. Det viser seg å være umulig å gi ytterligere informasjon.

MALTESE: Sistema ta’ whistleblower (kanali interni ta’ rappurtar)

Il-valuri tagħna jiffurmaw il-pedament għall-prattiki tan-negozju tagħna u jirriflettu l-impenn tagħna għall-integrità, it-trasparenza u l-kultura korporattiva pożittiva. Is-sistema tagħna ta’ whistleblowing hija għodda essenzjali għall-promozzjoni tar-responsabbiltà u l-iżgurar ta’ operazzjonijiet kummerċjali etiċi. Dawn ir-regoli ta' proċedura jservu biex jagħmlu l-proċess u l-prinċipji tal-proċessi ta' investigazzjoni tagħna trasparenti u jiżguraw li r-rapporti kollha riċevuti permezz tas-sistema tagħna jiġu ttrattati b'mod xieraq u professjonali.

L-OSI hija impenjata li tiftaħ djalogu u tagħraf l-importanza tal-whistleblowers bħala msieħba ewlenin fl-isforzi tagħna biex inżommu l-ogħla standards fl-oqsma kollha tan-negozju tagħna.

I. Regoli ta' Proċedura għas-Sistema ta' Whistleblower OSI

I. Għan u skop:

1. Għan: Dawn ir-Regoli ta’ Proċedura jirregolaw l-immaniġġjar u l-investigazzjoni tar-rapporti riċevuti permezz tas-sistema ta’ whistleblowing tal-Whistleblowing Globali Make It Right. L-għan huwa li jiġi żgurat li r-rapporti kollha riċevuti jiġu ttrattati b'mod trasparenti, effiċjenti u skont l-istandards etiċi tal-OSI.

2. Skop ta' applikazzjoni: Dawn ir-regoli ta' proċedura japplikaw għall-impjegati kollha, imsieħba fin-negozju, fornituri u partijiet interessati oħra tul il-katina tal-valur kollha li jużaw is-sistema ta' whistleblower biex jaqsmu indikazzjonijiet speċifiċi ta' kondotta ħażina possibbli, tħassib, jew pariri. Is-sistema tal-whistleblower mhijiex maħsuba għall-ipproċessar ta' tħassib relatat mal-prodott u s-servizz. Mistoqsijiet jew kwistjonijiet bħal dawn jistgħu jiġu indirizzati direttament permezz tal-formola ta’ kuntatt fuq il-websajt tal-kumpanija.

II. Sottomissjoni ta' informazzjoni:

1. Anonimat u Kunfidenzjalità:

Is-sistema ta’ whistleblower tippermetti, fost affarijiet oħra, is-sottomissjoni anonima ta’ rapporti ta’ whistleblower, sal-punt permess mil-liġijiet nazzjonali.

L-informazzjoni kollha ttrattata fil-qafas tas-sistema tal-whistleblower hija suġġetta għal kunfidenzjalità stretta.

2. Tipi ta' rapporti:

Is-sistema tippermetti lill-informaturi biex jissottomettu rapporti fejn ikun hemm indikazzjonijiet konkreti ta’ kondotta ħażina possibbli, tħassib, jew indikazzjonijiet ta’ tali. Dan jikkonċerna ksur minn impjegati jew imsieħba fin-negozju tal-liġijiet, regolamenti, eċċ applikabbli. (b'mod partikolari dawk imsemmija fit-

Taqsima 2 tal-Att dwar il-Protezzjoni tal-Whistleblower jew id-Direttiva tal-UE 2019/1937) jew regolamenti interni tal-kumpanija (b'mod partikolari ksur tal-Kodiċi ta' Kondotta) jew drittijiet tal-bniedem u riskji ambjentali attribwibbli għal forniturі diretti jew indiretti kif ukoll ksur tad-drittijiet tal-bniedem u l-obbligi ambjentali taħt l- Att dwar id-Diliġenza dovuta tal-Katina tal-Provvista (LkSG). Dawn jinkludu ksur tal-Kodiċi ta' Kondotta OSI, liġi tal-antitrust, korruzzjoni, serq, diskriminazzjoni, nuqqas ta' attenzjoni għas-saħħa u s-sigurtà fuq il-post tax-xogħol, xogħol tat-tfal, tniġġis tal-ħamrija, tal-ilma jew tal-arja, emissjonijiet ta' ħsejjes ta' ħsara, konsum inaċċettabbli tal-ilma, il-produzzjoni jew l-użu ta' ċerti pollutanti organiċi persistenti u l-importazzjoni u l-esportazzjoni mhux awtorizzati ta 'skart.

3. Aċċess għas-sistema:

L-informaturi għandhom aċċess għas-sistema ta' rappurtar ġestita esternament f'lingwi differenti fuq:

EthicsPoint - OSI Group, LLC

- f'forma ta' test permezz ta' formola fil-portal onlajn jew
- bit-telefon (bla ħlas minn diversi pajjiżi)

III. Ipproċessar tar-rapporti:

1. Irċevuta u Valutazzjoni Inizjali:

Ladarba rapport jasal permezz tal-kanali ta' rappurtar esterni ġestiti mis-sistema tal-whistleblower, l-ewwel jiġi ddokumentat u assenjat numru ta' fajl individwali. OSI Compliance tirċievi r-rapporti kollha u twettaq valutazzjoni inizjali biex tiddetermina l-plawżibbiltà u l-validità tagħhom.

2.Investigazzjoni :

Se tinbeda investigazzjoni bir-reqqa, oġġettiva u kunfidenzjali għal pariri rilevanti. Jekk meħtieġ biex jirċievu rapporti jew tieħu azzjoni , dipartimenti oħra jiġu kkonsultati jew mitluba għall-għajnuna. Informazzjoni addizzjonali tista' tintalab ukoll mingħand il-whistleblower.

It-tul ta' investigazzjoni sal-konklużjoni tagħha jiddependi fuq il-kumplessità tal-każ, il-miżuri investigattivi meħtieġa, u d-disponibbiltà ta' informazzjoni jew partijiet involuti fil-każ individwali. Se jsir kull sforz biex titlesta l-investigazzjoni b'mod effiċjenti u malajr kemm jista' jkun.

3. Feedback lill-Whistleblower:

Il-whistleblower se jirċievi feedback dwar l-irċevuta tal-ponta tiegħu fi żmien 7 ijiem, fejn possibbli u mingħajr ma jipperikola l-anonimità.

Jekk il-whistleblower issottometta r-rapport online jew bit-telefon, jirċievi informazzjoni ta' login li tippermettilhom isegwu r-rapport u jirċievu feedback anonimu (jekk jixtiequ). B'mod partikolari, jista' jkun meħtieġ li wieħed jistaqsi mistoqsijiet ta' komprensjoni u jikseb aktar informazzjoni.

Fil-kors ulterjuri tal-investigazzjoni (mhux aktar tard minn 3 xhur wara l-wasla tal-konferma tal-wasla), se tiġi pprovduta informazzjoni dwar l-istatus tal-investigazzjoni rigward miżuri ppjanati jew diġà mibdija jew, jekk ma jkunx hemm suspett biżżejjed, dwar it-twaqqif tal-investigazzjoni. l-investigazzjoni.

IV. Protezzjoni tal-Whistleblowers:

1.Non -Ritaljazzjoni:

L-OSI tagħmel l-isforzi raġonevoli kollha biex tiżgura li l-informaturi jkunu protetti minn kwalunkwe forma ta' ritaljazzjoni, żvantaġġ, jew ritaljazzjoni oħra.

Azzjoni dixxiplinarja bbażata fuq whistleblowing kontra individwi li jikkooperaw in bona fede ma' investigazzjonijiet hija pprojbita u mhux se tkun ittollerata.

2. Kunfidenzjalità:

Persuni involuti fl-investigazzjoni huma marbuta għal kunfidenzjalità stretta.

V. Dokumentazzjoni u ħażna:

1.Dokumentazzjoni :

Il-passi kollha tal-investigazzjoni huma dokumentati bir-reqqa.

Id-dokumentazzjoni sservi t-trasparenza u t-traċċabilità tal-proċedura.

2. Perjodu ta' żamma:

Id-dokumentazzjoni tinżamm skont ir-rekwiżiti legali u l-linji gwida interni.

INTI. Reviżjoni u aġġustament:

Dawn ir-regoli proċedurali jiġu riveduti u adattati regolarment kif meħtieġ biex jiġi żgurat li jikkonformaw mar-rekwiżiti legali attwali u l-għanijiet korporattivi.

II. Informazzjoni skont l-Artikolu 13 GDPR (għall-persuni li jipprovdu informazzjoni):

Isem u dettalji ta' kuntatt tal-kontrollur: Ara l-istampa fuq il-websajt. Dettalji ta' kuntatt tal-uffiċjal tal-protezzjoni tad-data u, jekk applikabbli, tar-rappreżentant: Prof Dr. hc Heiko Jonny Maniero, LL.B., LL.M. mult., MLE, Franz-Joseph-Str. 11, 80801 Munich, il-Ġermanja. Skopijiet li għalihom id-dejta personali għandha tiġi pproċessata u l-bażi legali għall-ipproċessar: Konformità mal-Att dwar il-Protezzjoni tal-Whistleblower (HinSchG) u l-Att dwar id-Diliġenza dovuta tal-Katina tal-Provvista (LkSG), il-bażi legali hija l-Art 6 (1) (c) GDPR flimkien mat-Taqsimiet 8, 9 LkSG u t-Taqsima 10 HinSchG, sa fejn dan ikun meħtieġ biex jitwettqu l-kompiti speċifikati fit-Taqsimiet 13 u 24 HinSchG, kif ukoll il-

konformità mad-Direttiva (UE) 2019/1937 dwar il-protezzjoni ta' persuni li jirrappurtaw ksur tal-liġi tal-Unjoni u l-liġi nazzjonali li tirriżulta tal-Istati Membri u l-konformità mal-leġiżlazzjoni applikabbli minn pajjiżi oħra. Riċevituri jew kategoriji ta' riċevituri tad-dejta personali: Awtoritajiet tal-infurzar tal-liġi, awtoritajiet tal-multi , u awtoritajiet oħra kif ukoll avukati, kumpaniji tal-grupp jew min iħaddem. Trasferiment ippjanat lejn pajjiżi terzi: Dħul fis-sistema online Navex u trasferiment bil-quddiem lil entitajiet fi ħdan il-grupp, min iħaddem, jew avukati. Il-Klawżoli Kuntrattwali Standard tal-UE u l-Addendum tar-Renju Unit għall-Klawżoli Kuntrattwali Standard tal-UE ġew konklużi ma' Navex. Navex huwa wkoll membru tal-Qafas tal-Privatezza tad-Dejta bejn l-UE u l-Istati Uniti, il-Qafas tal-Privatezza tad-Dejta bejn l-Iżvizzera u l-Istati Uniti, u l-Estensjoni tar-Renju Unit għall-Qafas tal-Privatezza tad-Data bejn l-UE u l-Istati Uniti. Għal trasferimenti oħra, jista' ma jkun hemm l-ebda deċiżjoni ta' adegwatezza. Il-Klawżoli Kuntrattwali Standard tal-UE u l-Addendum tar-Renju Unit għall-Klawżoli Kuntrattwali Standard tal-UE jintużaw għal tali trasferimenti. Kriterji għad-determinazzjoni tal-perjodu tal-ħażna: Id-dokumentazzjoni titħassar tliet snin wara t-tmiem tal-proċedura. Id-dokumentazzjoni tista' tinżamm għal aktar żmien biex tissodisfa r-rekwiżiti tal-leġiżlazzjoni applikabbli jekk dan ikun meħtieġ u proporzjonat.

Skont ir-Regolament Ġenerali dwar il-Protezzjoni tad-Dejta, għandek id-dritt ta' aċċess għal data personali li tikkonċernak u d-dritt għal rettifika jew tħassir jew restrizzjoni tal-ipproċessar jew id-dritt li toġġezzjona għall-ipproċessar u d-dritt għall-portabbiltà tad-data. Għandek id-dritt li tressaq ilment mal-awtorità kompetenti ta' sorveljanza tal-protezzjoni tad-data dwar l-ipproċessar. Il-provvista ta' data personali mhijiex meħtieġa bil-liġi jew bil-kuntratt u mhix meħtieġa għall-konklużjoni ta' kuntratt, u għalhekk m'intix obbligat li tipprovdi data personali lill-hotline tal-whistleblowing. Konsegwenzi possibbli ta' nuqqas ta' provvediment huma li r-rapport mhux se jiġi pproċessat jew se jiġi pproċessat b'dewmien, jew li se jiġi rrifjutat, u li l-ebda informazzjoni jew informazzjoni relatata mar-rapport ma tista' tingħatalek. M'hemm l-ebda teħid ta' deċiżjonijiet awtomatizzat.

III. Informazzjoni skont l-Artikolu 14 tal-GDPR (għal suġġetti oħra tad-dejta):

Isem u dettalji ta' kuntatt tal-kontrollur: Ara l-istampa fuq il-websajt. Dettalji ta' kuntatt tal-uffiċjal tal-protezzjoni tad-data u, jekk applikabbli, tar-rappreżentant: Prof Dr. hc Heiko Jonny Maniero, LL.B., LL.M. mult., MLE, Franz-Joseph-Str. 11, 80801 Munich, il-Ġermanja. Skopijiet li għalihom id-dejta personali għandha tiġi pproċessata u l-bażi legali għall-ipproċessar: Konformità mal-Att dwar il-Protezzjoni tal-Whistleblower (HinSchG) u l-Att dwar id-Diliġenza dovuta tal-Katina tal-Provvista (LkSG), il-bażi legali hija l-Art 6 (1) (c) GDPR flimkien mat-Taqsimiet 8, 9 LkSG u t-Taqsima 10 HinSchG, sa fejn dan ikun meħtieġ biex jitwettqu l-kompiti speċifikati fit-Taqsimiet 13 u 24 HinSchG, kif ukoll il-konformità mad-Direttiva (UE) 2019/1937 dwar il-protezzjoni ta' persuni li jirrappurtaw ksur tal-liġi tal-Unjoni u l-liġi nazzjonali li tirriżulta tal-Istati Membri u l-konformità mal-leġiżlazzjoni applikabbli minn pajjiżi oħra. Kategoriji ta' data personali pproċessata: Dejta ta' whistleblowing. Riċevituri jew kategoriji ta' riċevituri tad-dejta personali: Awtoritajiet tal-infurzar tal-liġi, awtoritajiet tal-multi, u awtoritajiet oħra

kif ukoll avukati, kumpaniji tal-grupp jew min iħaddem. Trasferiment ippjanat lejn pajjiżi terzi: Dħul fis-sistema online Navex u trasferiment bil-quddiem lil entitajiet fi ħdan il-grupp, min iħaddem, jew avukati. Il-Klawżoli Kuntrattwali Standard tal-UE u l-Addendum tar-Renju Unit għall-Klawżoli Kuntrattwali Standard tal-UE ġew konklużi ma' Navex. Navex huwa wkoll membru tal-Qafas tal-Privatezza tad-Dejta bejn l-UE u l-Istati Uniti, il-Qafas tal-Privatezza tad-Dejta bejn l-Iżvizzera u l-Istati Uniti, u l-Estensjoni tar-Renju Unit għall-Qafas tal-Privatezza tad-Data bejn l-UE u l-Istati Uniti. Għal trasferimenti oħra, jista' ma jkun hemm l-ebda deċiżjoni ta' adegwatezza. Il-Klawżoli Kuntrattwali Standard tal-UE u l-Addendum tar-Renju Unit għall-Klawżoli Kuntrattwali Standard tal-UE jintużaw għal tali trasferimenti. Kriterji għad-determinazzjoni tal-perjodu tal-ħażna: Id-dokumentazzjoni titħassar tliet snin wara t-tmiem tal-proċedura. Id-dokumentazzjoni tista' tinżamm għal aktar żmien biex tissodisfa r-rekwiżiti tal-leġiżlazzjoni applikabbli jekk dan ikun meħtieġ u proporzjonat. Is-sors tad-dejta personali huwa l-whistleblower u/jew il-kumpanija kkonċernata.

Skont ir-Regolament Ġenerali dwar il-Protezzjoni tad-Dejta, jista' jkollok id-dritt ta' aċċess għal data personali li tikkonċernak u d-dritt għal rettifika jew tħassir jew restrizzjoni tal-ipproċessar jew id-dritt li toġġezzjona għall-ipproċessar u d-dritt għall-portabbiltà tad-data. Għandek id-dritt li tressaq ilment mal-awtorità kompetenti ta' sorveljanza tal-protezzjoni tad-dejta fir-rigward tal-ipproċessar. M'hemm l-ebda teħid ta' deċiżjonijiet awtomatizzat. L-għoti ta' aktar informazzjoni jirriżulta li huwa impossibbli.

IRISH: Córas sceithire (bealaí tuairiscithe inmheánacha)

Tá ár luachanna mar bhunús dár gcleachtais ghnó agus léiríonn siad ár dtiomantas d'ionracas, trédhearcacht, agus cultúr corparáideach dearfach. Is uirlis riachtanach é ár gcóras sceithireachta chun cuntasacht a chur chun cinn agus chun oibríochtaí gnó eiticiúla a chinntiú. Feidhmíonn na rialacha nós imeachta seo chun próiseas agus prionsabail ár bpróisis imscrúdaithe a dhéanamh trédhearcach agus a chinntiú go láimhseáiltear gach tuairisc a fhaightear tríd ár gcóras go cuí agus go gairmiúil.

Tá OSI tiomanta d'idirphlé oscailte agus aithníonn sé an tábhacht a bhaineann le sceithirí mar phríomh-chomhpháirtithe inár n-iarrachtaí na caighdeáin is airde a choinneáil i ngach réimse dár ngnó.

I. Rialacha Nós Imeachta maidir le Córas sceithire OSI

I. Aidhm agus raon feidhme:

1. Aidhm: Rialaíonn na Rialacha Nós Imeachta seo láimhseáil agus imscrúdú tuairiscí a fhaightear tríd an gcóras sceithireachta Beolíne Dhomhanda Make It Right. Is é an aidhm a chinntiú go láimhseáiltear gach tuairisc a fhaightear ar bhealach trédhearcach, éifeachtach agus de réir chaighdeáin eiticiúla an OSI.

2. Raon feidhme: Tá feidhm ag na rialacha nós imeachta seo maidir le gach fostaí, comhpháirtí gnó, soláthraí agus geallsealbhóir eile ar fud an tslabhra luacha a úsáideann an córas sceithireachta chun tásca sonracha a roinnt maidir le mí-iompar, imní nó leideanna féideartha. Níl an córas sceithireachta beartaithe chun ábhair imní a bhaineann le táirgí agus seirbhísí a phróiseáil. Is féidir dul i ngleic le ceisteanna nó ceisteanna den sórt sin go díreach tríd an bhfoirm teagmhála ar shuíomh Gréasáin na cuideachta.

II. Cur isteach faisnéise:

1. Anaithnideacht agus Rúndacht:

Ceadaíonn an córas sceithireachta, i measc rudaí eile, tuairiscí sceithireachta a chur isteach gan ainm, a mhéid a cheadaítear le dlíthe náisiúnta.

Tá an fhaisnéis go léir a láimhseáiltear faoi chuimsiú an chórais sceithireachta faoi réir rúndachta docht.

2. Cineálacha tuarascálacha:

Cuireann an córas ar chumas sceithirí tuarascálacha a chur isteach nuair a bhíonn tásca nithiúla ann maidir le mí-iompar, imní nó comharthaí dá leithéid. Baineann sé seo le sáruithe ag fostaithe nó comhpháirtithe gnó ar dhlíthe, rialacháin is infheidhme etc. (go háirithe iad sin a luaitear i Roinn 2 den Acht um Chosaint sceithirí nó Treoir 2019/1937 an AE) nó rialacháin inmheánacha cuideachtaí (go háirithe sáruithe ar an gCód Iompair) nó rioscaí cearta daonna agus comhshaoil atá inchurtha i leith

soláthraithe díreacha nó indíreacha chomh maith le sáruithe. cearta daonna agus oibleagáidí comhshaoil faoin Acht um Dhícheall Cuí sa tSlabhra Soláthair (LkSG). Ina measc seo tá sáruithe ar Chód Iompraíochta an OSI, dlí frith-iontaobhais, éilliú, goid, idirdhealú, neamhaird ar shláinte agus sábháilteacht ceirde, saothair leanaí, truailliú ithreach, uisce nó aeir, astuithe díobhálacha torainn, tomhaltas uisce do-ghlactha, táirgeadh nó úsáid áirithe truailleáin orgánacha marthanacha agus allmhairiú agus onnmhairiú neamhúdaraithe dramhaíola.

3. Rochtain ar an gcóras:

Tá rochtain ag sceithirí ar an gcóras tuairiscithe a bhainistítear go seachtrach i dteangacha éagsúla ag:

EthicsPoint - OSI Group, LLC

- i bhfoirm téacs trí fhoirm sa tairseach ar líne nó
- ar an teileafón (saor ó dola ó thíortha éagsúla)

III. Próiseáil tuarascálacha:

1. Admháil agus Measúnú Tosaigh:

Nuair a fhaightear tuairisc trí na bealaí tuairiscithe seachtracha arna mbainistiú ag an gcóras sceithireachta, déantar é a dhoiciméadú ar dtús agus sanntar uimhir comhaid aonair í. Faigheann Comhlíonadh OSI gach tuairisc agus déanann sé measúnú tosaigh chun a n-inchreidteacht agus a mbailíocht a chinneadh.

2.Imscrúdú :

Cuirfear tús le himscrúdú críochnúil, oibiachtúil agus rúnda le haghaidh leideanna ábhartha. Más gá tuarascálacha a fháil nó beart a dhéanamh , rachfar i gcomhairle le ranna eile nó iarrfar cúnamh orthu. Féadfar faisnéis bhreise a iarraidh ar an sceithire freisin.

Braitheann fad an imscrúdaithe go dtí go dtabharfar chun críche é ar chastacht an cháis, ar na bearta imscrúdaithe is gá, agus ar infhaighteacht na faisnéise nó na bpáirtithe a bhfuil baint acu leis an gcás aonair. Déanfar gach iarracht an t-imscrúdú a chríochnú chomh héifeachtach agus chomh gasta agus is féidir.

3. Aiseolas chuig an sceithire:

Gheobhaidh an sceithire aiseolas ar a leid a fháil laistigh de 7 lá, nuair is féidir agus gan anaithnideacht a chur i gcontúirt.

Más rud é go bhfuil an tuairisc curtha isteach ag an sceithire ar líne nó ar an teileafón, gheobhaidh siad faisnéis logáil isteach a chuirfidh ar a gcumas leanúint ar aghaidh leis an tuairisc agus aiseolas gan ainm

a fháil (más mian leo). D'fhéadfadh go mbeadh gá go háirithe ceisteanna tuisceana a chur agus tuilleadh faisnéise a fháil.

I gcúrsa an imscrúdaithe (tráth nach déanaí ná 3 mhí tar éis an deimhniú fála a fháil), cuirfear faisnéis ar fáil maidir le stádas an imscrúdaithe maidir le bearta atá beartaithe nó atá tionscanta cheana féin nó, mura bhfuil dóthain amhrais ann, maidir le scor de. an t-imscrúdú.

IV. Cosaint do sceithirí:

1.Neamh -Retaliation:

Déanann OSI gach iarracht réasúnach lena chinntiú go gcosnófar sceithirí ó aon chineál frithbheartaíochta, míbhuntáiste nó díoltais eile.

Tá cosc ar ghníomh araíonachta bunaithe ar sceithireacht i gcoinne daoine aonair a chomhoibríonn de mheon macánta le himscrúduithe agus ní ghlacfar léi.

2. Rúndacht:

daoine a bhfuil baint acu leis an imscrúdú faoi cheangal rúndachta docht.

V. Doiciméadú agus stóráil:

1.Documentation :

Déantar gach céim den imscrúdú a dhoiciméadú go cúramach.

Freastalaíonn an doiciméadacht ar thrédhearcacht agus ar inrianaitheacht an nós imeachta.

2. Tréimhse coinneála:

Coinnítear an doiciméadú de réir na gceanglas dlí agus na dtreoirlínte inmheánacha.

TÚ. Athbhreithniú agus coigeartú:

Déantar na rialacha nós imeachta seo a athbhreithniú go rialta agus a oiriúnú de réir mar is gá chun a áirithiú go gcomhlíonann siad na ceanglais dhlíthiúla reatha agus na cuspóirí corparáideacha.

II. Faisnéis de bhun Airteagal 13 den GDPR (do dhaoine a sholáthraíonn faisnéis):

Ainm agus sonraí teagmhála an rialaitheora: Féach an rian ar an suíomh Gréasáin. Sonraí teagmhála an oifigigh cosanta sonraí agus, más infheidhme, an ionadaí: An tOllamh Dr. hc Heiko Jonny Maniero, LL.B., LL.M. il., MLE, Franz-Joseph-Str. 11, 80801 München, an Ghearmáin. Na cuspóirí a bhfuil na sonraí pearsanta le próiseáil ina leith agus an bunús dlí don phróiseáil: Comhlíonadh an Achta um

Chosaint sceithirí (HinSchG) agus an tAcht um Dhícheall Cuí sa tSlabhra Soláthair (LkSG), is é Airteagal 6(1)(c) an bunús dlí. GDPR i gcomhar le hAilt 8, 9 LkSG agus Alt 10 HinSchG, a mhéid is gá sin chun na cúraimí a shonraítear i Ranna 13 agus 24 HinSchG a chomhlíonadh, chomh maith le comhlíonadh Threoir (AE) 2019/1937 maidir le cosaint daoine a thuairiscíonn sáruithe. ar dhlí an Aontais agus ar dhlí náisiúnta na mBallstát dá bharr agus ar chomhlíonadh na reachtaíochta is infheidhme ó thíortha eile. Faighteoirí nó catagóirí faighteoirí na sonraí pearsanta: Údaráis forghníomhaithe an dlí, údaráis fíneáil , agus údaráis eile chomh maith le dlíodóirí, cuideachtaí grúpa nó fostóirí. Aistriú pleanáilte go tríú tíortha: Teacht isteach i gcóras ar líne Navex agus aistriú ar aghaidh chuig aonáin laistigh den ghrúpa, fostóirí nó dlíodóirí. Tá Clásail Chaighdeánacha Conarthacha an AE agus Aguisín na RA a ghabhann le Clásail Chaighdeánacha Conarthacha an AE tugtha chun críche le Navex. Tá Navex ina bhall freisin de Chreat Príobháideachta Sonraí AE-SAM, de Chreat Príobháideachta Sonraí na hEilvéise-SAM, agus Síneadh an RA ar Chreat Príobháideachta Sonraí AE-SAM. I gcás aistrithe eile, d'fhéadfadh nach mbeadh aon chinneadh leordhóthanachta. Úsáidtear Clásail Chaighdeánacha Conarthacha an AE agus Aguisín na RA a ghabhann le Clásail Chaighdeánacha Conarthacha an AE le haghaidh aistrithe den sórt sin. Critéir chun an tréimhse stórála a chinneadh: Scriostar an doiciméadú trí bliana tar éis dheireadh an nós imeachta. Féadfar an doiciméadú a choinneáil ar feadh tréimhse níos faide chun ceanglais na reachtaíochta is infheidhme a chomhlíonadh má tá sé sin riachtanach agus comhréireach.

Faoin Rialachán Ginearálta um Chosaint Sonraí, tá sé de cheart agat rochtain a fháil ar shonraí pearsanta a bhaineann leat agus an ceart chun próiseáil a cheartú nó a scriosadh nó a shrianadh nó an ceart agóid a dhéanamh i gcoinne próiseála agus an ceart chun iniomparthacht sonraí. Tá sé de cheart agat gearán a dhéanamh leis an údarás inniúil maoirseachta um chosaint sonraí maidir leis an bpróiseáil. Níl gá le soláthar sonraí pearsanta de réir dlí nó conartha agus níl sé riachtanach chun conradh a thabhairt i gcrích, agus is é sin an fáth nach bhfuil ort sonraí pearsanta a sholáthar don bheolíne sceithireachta. Is iad na hiarmhairtí a d'fhéadfadh a bheith ag neamhsholáthar ná nach bpróiseálfar an tuarascáil nó nach bpróiseálfar í le moill, nó go ndiúltófar í, agus nach féidir aon fhaisnéis nó faisnéis a bhaineann leis an tuarascáil a sholáthar duit. Níl aon chinnteoireacht uathoibrithe ann.

III. Faisnéis de bhun Airteagal 14 den GDPR (le haghaidh ábhair sonraí eile):

Ainm agus sonraí teagmhála an rialaitheora: Féach an rian ar an suíomh Gréasáin. Sonraí teagmhála an oifigigh cosanta sonraí agus, más infheidhme, an ionadaí: An tOllamh Dr. hc Heiko Jonny Maniero, LL.B., LL.M. il., MLE, Franz-Joseph-Str. 11, 80801 München, an Ghearmáin. Na cuspóirí a bhfuil na sonraí pearsanta le próiseáil ina leith agus an bunús dlí don phróiseáil: Comhlíonadh an Achta um Chosaint sceithirí (HinSchG) agus an tAcht um Dhícheall Cuí sa tSlabhra Soláthair (LkSG), is é Airteagal 6(1)(c) an bunús dlí. GDPR i gcomhar le hAilt 8, 9 LkSG agus Alt 10 HinSchG, a mhéid is gá sin chun na cúraimí a shonraítear i Ranna 13 agus 24 HinSchG a chomhlíonadh, chomh maith le comhlíonadh Threoir (AE) 2019/1937 maidir le cosaint daoine a thuairiscíonn sáruithe. ar dhlí an

Aontais agus ar dhlí náisiúnta na mBallstát dá bharr agus ar chomhlíonadh na reachtaíochta is infheidhme ó thíortha eile. Catagóirí sonraí pearsanta a próiseáladh: Sonraí sceithireachta. Faighteoirí nó catagóirí faighteoirí na sonraí pearsanta: Údaráis forghníomhaithe an dlí, údaráis fíneáil, agus údaráis eile chomh maith le dlíodóirí, cuideachtaí grúpa nó fostóirí. Aistriú pleanáilte go tríú tíortha: Teacht isteach i gcóras ar líne Navex agus aistriú ar aghaidh chuig aonáin laistigh den ghrúpa, fostóirí nó dlíodóirí. Tá Clásail Chaighdeánacha Conarthacha an AE agus Aguisín na RA a ghabhann le Clásail Chaighdeánacha Conarthacha an AE tugtha chun críche le Navex. Tá Navex ina bhall freisin de Chreat Príobháideachta Sonraí AE-SAM, de Chreat Príobháideachta Sonraí na hEilvéise-SAM, agus Síneadh an RA ar Chreat Príobháideachta Sonraí AE-SAM. I gcás aistrithe eile, d'fhéadfadh nach mbeadh aon chinneadh leordhóthanachta. Úsáidtear Clásail Chaighdeánacha Conarthacha an AE agus Aguisín na RA a ghabhann le Clásail Chaighdeánacha C an AE le haghaidh aistrithe den sórt sin. Critéir chun an tréimhse stórála a chinneadh: Scriostar an doiciméadú trí bliana tar éis dheireadh an nós imeachta. Féadfar an doiciméadú a choinneáil ar feadh tréimhse níos faide chun ceanglais na reachtaíochta is infheidhme a chomhlíonadh má tá sé sin riachtanach agus comhréireach. Is é foinse na sonraí pearsanta ná an sceithire agus/nó an chuideachta lena mbaineann.

Faoin Rialachán Ginearálta maidir le Cosaint Sonraí, féadfaidh sé go bhfuil an ceart agat chun rochtain a fháil ar shonraí pearsanta a bhaineann leat agus an ceart chun próiseáil a cheartú nó a scriosadh nó a shrianadh nó an ceart agóid a dhéanamh i gcoinne próiseála agus an ceart chun iniomparthacht sonraí. Tá sé de cheart agat gearán a dhéanamh leis an údarás inniúil maoirseachta um chosaint sonraí maidir leis an bpróiseáil. Níl aon chinnteoireacht uathoibrithe ann. Ní féidir tuilleadh faisnéise a sholáthar.

Gildi okkar mynda grunninn að viðskiptaháttum okkar og endurspegla skuldbindingu okkar um heiðarleika, gagnsæi og jákvæða fyrirtækjamenningu. Uppljóstrarakerfið okkar er nauðsynlegt tæki til að efla ábyrgð og tryggja siðferðilegan viðskiptarekstur. Þessar verklagsreglur þjóna til að gera ferlið og meginreglur rannsóknarferla okkar gagnsæjar og tryggja að allar tilkynningar sem berast í gegnum kerfið okkar séu meðhöndlaðar á viðeigandi og faglegan hátt.

OSI er skuldbundið til opinnar samræðu og viðurkennir mikilvægi uppljóstrara sem lykilaðila í viðleitni okkar til að viðhalda hæstu stöðlum á öllum sviðum viðskipta okkar.

I. Verklagsreglur fyrir OSI uppljóstrarakerfi

I. Tilgangur og umfang:

1. Tilgangur: Þessar verklagsreglur gilda um meðhöndlun og rannsókn á tilkynningum sem berast í gegnum uppljóstrarakerfið Make It Right Global Hotline. Markmiðið er að tryggja að allar tilkynningar sem berast séu meðhöndlaðar á gagnsæjan, skilvirkan hátt og í samræmi við siðareglur OSI.

2. Gildissvið: Þessar verklagsreglur eiga við um alla starfsmenn, viðskiptafélaga, birgja og aðra hagsmunaaðila í virðiskeðjunni sem nota uppljóstrarakerfið til að deila ákveðnum vísbendingum um hugsanlegt misferli, áhyggjur eða ábendingar. Uppljóstrarakerfið er ekki ætlað til að vinna úr vöru- og þjónustutengdum áhyggjum. Hægt er að bregðast við slíkum spurningum eða málum beint í gegnum tengiliðaeyðublaðið á heimasíðu fyrirtækisins.

II. Skil á upplýsingum:

1. Nafnleynd og trúnaður:

Uppljóstrarakerfið gerir meðal annars kleift að skila nafnlausum uppljóstrunum um uppljóstrara, að því marki sem landslög leyfa.

Allar upplýsingar sem meðhöndlaðar eru innan ramma uppljóstrarakerfisins eru háðar ströngum trúnaði.

2. Tegundir skýrslna:

Kerfið gerir uppljóstrarum kleift að skila inn skýrslum þar sem áþreifanlegar vísbendingar eru um hugsanlegt misferli, áhyggjur eða vísbendingar um slíkt. Þetta varðar brot starfsmanna eða viðskiptafélaga á gildandi lögum, reglugerðum o.fl. (sérstaklega þau sem nefnd eru í 2. hluta laga um vernd uppljóstrara eða tilskipun ESB 2019/1937) eða innri reglugerðum fyrirtækja (sérstaklega brot á siðareglum) eða mannréttinda- og umhverfisáhættu sem rekja má til beinna eða óbeinna birgja sem og brota. mannréttinda og umhverfisskyldna samkvæmt lögum um áreiðanleikakönnun á birgðakeðju (LkSG). Þetta felur í sér brot á siðareglum OSI, samkeppnislagalögum, spillingu, þjófnaði, mismunun,

virðingu fyrir heilsu og öryggi á vinnustöðum, barnavinnu, jarðvegs-, vatns- eða loftmengun, skaðlegan hávaða, óviðunandi vatnsnotkun, framleiðsla eða notkun ákveðinna þrávirk lífræn efni og óleyfilegur inn- og útflutningur úrgangs.

3. Aðgangur að kerfinu:

Uppljóstrarar hafa aðgang að utanaðkomandi skýrslukerfi á mismunandi tungumálum á:

EthicsPoint - OSI Group, LLC

- í textaformi í gegnum eyðublað í netgáttinni eða
- í síma (gjaldfrjálst frá ýmsum löndum)

III. Vinnsla skýrslna:

1. Kvittun og frummat:

Þegar tilkynning hefur borist í gegnum ytri tilkynningarleiðir sem stjórnað er af uppljóstrarakerfinu er hún fyrst skjalfest og henni úthlutað einstöku skráarnúmeri. OSI Compliance tekur við öllum skýrslum og framkvæmir frummat til að ákvarða trúverðugleika þeirra og réttmæti.

2. Rannsókn :

Ítarleg, hlutlæg og trúnaðarrannsókn verður hafin fyrir viðeigandi ábendingar. Ef nauðsyn krefur til að fá skýrslur eða grípa til aðgerða verður leitað til annarra deilda eða beðið um aðstoð. Einnig er hægt að óska eftir frekari upplýsingum frá uppljóstrara.

Lengd rannsókna þar til henni lýkur fer eftir því hversu flókið mál er, hvaða rannsóknaraðgerðir eru nauðsynlegar og hvort upplýsingar eða aðilar sem koma að einstökum málum liggja fyrir. Leitast verður við að ljúka rannsókninni á eins skilvirkan og skjótan hátt og hægt er.

3. Endurgjöf til uppljóstrara:

Uppljóstrarinn mun fá endurgjöf um móttöku ábendingarinnar innan 7 daga, þar sem það er hægt og án þess að tefla nafnleynd í hættu.

Ef uppljóstrarinn hefur skilað skýrslunni á netinu eða símleiðis mun hann fá innskráningarupplýsingar sem gera þeim kleift að fylgjast með tilkynningunni og fá nafnlaus endurgjöf (ef hann vill). Einkum getur verið nauðsynlegt að spyrja skilningsspurninga og afla frekari upplýsinga.

Í framhaldi rannsóknarinnar (ekki síðar en 3 mánuðum eftir móttöku staðfestingar) verða veittar upplýsingar um stöðu rannsóknarinnar varðandi fyrirhugaðar eða þegar hafin aðgerðir eða, ef ekki er nægilegur grunur, um stöðvun aðgerða. rannsókninni.

IV. Vernd uppljóstrara:

1.Ekki hefndaraðgerðir:

OSI tekur að sér allar sanngjarnar tilraunir til að tryggja að uppljóstrarar verði verndaðir fyrir hvers kyns hefndum, óhagræði eða öðrum hefndaraðgerðum.

Agaaðgerðir sem byggja á uppljóstrun gegn einstaklingum sem vinna í góðri trú við rannsóknir eru bannaðar og verða ekki liðnar.

2. Trúnaður:

Þeir sem taka þátt í rannsókninni eru bundnir ströngum trúnaði.

V. Skjöl og geymsla:

1. Skjöl :

Öll skref rannsóknarinnar eru vandlega skjalfest.

Skjölin þjóna gagnsæi og rekjanleika málsmeðferðarinnar.

2. Varðveislutími:

Skjöl eru varðveitt í samræmi við lagaskilyrði og innri leiðbeiningar.

ÞÚ. Skoðun og aðlögun:

Þessar verklagsreglur eru reglulega endurskoðaðar og aðlagaðar eftir þörfum til að tryggja að þær séu í samræmi við gildandi lagakröfur og markmið fyrirtækja.

II. Upplýsingar skv. 13. gr. GDPR (fyrir þá sem veita upplýsingar):

Nafn og tengiliðaupplýsingar ábyrgðaraðila: Sjá áletrun á vefsíðunni. Samskiptaupplýsingar gagnaverndarfulltrúa og, ef við á, fulltrúa: Prófessor Dr. hc Heiko Jonny Maniero, LL.B., LL.M. mult., MLE, Franz-Joseph-Str. 11, 80801 München, Þýskalandi. Tilgangur með því að vinna persónuupplýsingarnar og lagagrundvöllur vinnslunnar: Fylgni lögum um vernd uppljóstrara (HinSchG) og lögum um áreiðanleikakönnun á birgðakeðju (LkSG), lagagrundvöllur er c-liður 6. mgr. GDPR í tengslum við 8., 9. LkSG og 10. kafla HinSchG, að því marki sem það er nauðsynlegt til að uppfylla þau verkefni sem tilgreind eru í 13. og 24. köflum HinSchG, sem og samræmi við tilskipun (ESB) 2019/1937 um vernd einstaklinga sem tilkynna brot. laga sambandsins og landslaga aðildarríkjanna sem af því leiðir og að farið sé að gildandi lögum frá öðrum löndum. Viðtakendur eða flokkar viðtakenda persónuupplýsinganna: Löggæsluyfirvöld, sektayfirvöld og önnur yfirvöld sem og lögfræðingar, samstæðufyrirtæki eða vinnuveitendur. Fyrirhugaður flutningur til þriðju landa: Inngangur í Navex

netkerfið og framsenda flutningur til aðila innan samstæðunnar, vinnuveitenda eða lögfræðinga. Staðlaða samningsákvæði ESB og viðauki í Bretlandi við staðlaða samningsákvæði ESB hafa verið gerðir við Navex. Navex er einnig aðili að EU-US Data Privacy Framework, Swiss-US Data Privacy Framework og UK Framlengingu á EU-US Data Privacy Framework. Að því er varðar aðra flutning kann að vera engin ákvörðun um hæfi. Staðlaður samningsákvæði ESB og viðauki í Bretlandi við staðlaða samningsákvæði ESB eru notuð fyrir slíkar millifærslur. Skilyrði til að ákvarða geymslutíma: Gögnunum er eytt þremur árum eftir að aðgerð lýkur. Heimilt er að geyma gögnin lengur til að uppfylla kröfur gildandi laga ef það er nauðsynlegt og í réttu hlutfalli við það.

Samkvæmt almennu persónuverndarreglugerðinni átt þú rétt á aðgangi að persónuupplýsingum um þig og rétt til leiðréttingar eða eyðingar eða takmörkunar á vinnslu eða rétt til að andmæla vinnslu og rétt til gagnaflutnings. Þú hefur rétt til að leggja fram kvörtun til þar til bærra gagnaverndareftirlitsaðila vegna vinnslunnar. Veiting persónuupplýsinga er hvorki skylda samkvæmt lögum né samningum og er ekki nauðsynleg við gerð samnings, þess vegna er þér ekki skylt að veita persónuupplýsingar til uppljóstrara. Hugsanlegar afleiðingar af vanskilum eru þær að skýrslan verður ekki afgreidd eða verður afgreidd með töf eða að henni verði hafnað og að engar upplýsingar eða upplýsingar er varða skýrsluna er hægt að veita þér. Það er engin sjálfvirk ákvarðanataka.

III. Upplýsingar skv. 14. gr. GDPR (fyrir aðra skráða einstaklinga):

Nafn og tengiliðaupplýsingar ábyrgðaraðila: Sjá áletrun á vefsíðunni. Samskiptaupplýsingar gagnaverndarfulltrúa og, ef við á, fulltrúa: Prófessor Dr. hc Heiko Jonny Maniero, LL.B., LL.M. mult., MLE, Franz-Joseph-Str. 11, 80801 München, Þýskalandi. Tilgangur með því að vinna persónuupplýsingarnar og lagagrundvöllur vinnslunnar: Fylgni lögum um vernd uppljóstrara (HinSchG) og lögum um áreiðanleikakönnun á birgðakeðju (LkSG), lagagrundvöllur er c-liður 6. mgr. GDPR í tengslum við 8., 9. LkSG og 10. kafla HinSchG, að því marki sem það er nauðsynlegt til að uppfylla þau verkefni sem tilgreind eru í 13. og 24. köflum HinSchG, sem og samræmi við tilskipun (ESB) 2019/1937 um vernd einstaklinga sem tilkynna brot. laga sambandsins og landslaga aðildarríkjanna sem af því leiðir og að farið sé að gildandi lögum frá öðrum löndum. Flokkar persónuupplýsinga sem unnið er með: Upplýsingar um uppljóstrara. Viðtakendur eða flokkar viðtakenda persónuupplýsinganna: Löggæsluyfirvöld, sektayfirvöld og önnur yfirvöld sem og lögfræðingar, samstæðufyrirtæki eða vinnuveitendur. Fyrirhugaður flutningur til þriðju landa: Inngangur í Navex netkerfið og framsenda flutningur til aðila innan samstæðunnar, vinnuveitenda eða lögfræðinga. Staðlaða samningsákvæði ESB og viðauki í Bretlandi við staðlaða samningsákvæði ESB hafa verið gerðir við Navex. Navex er einnig aðili að EU-US Data Privacy Framework, Swiss-US Data Privacy Framework og UK Framlengingu á EU-US Data Privacy Framework. Að því er varðar aðra flutning kann að vera engin ákvörðun um hæfi. Staðlaður samningsákvæði ESB og viðauki í Bretlandi við samningsákvæði ESB staðalsins eru notuð fyrir slíkar millifærslur. Skilyrði til að ákvarða geymslutíma: Gögnunum er eytt þremur árum eftir að aðgerð lýkur. Heimilt er að geyma gögnin lengur til að uppfylla kröfur gildandi laga

ef það er nauðsynlegt og í réttu hlutfalli við það. Uppruni persónuupplýsinganna er uppljóstrari og/eða hlutaðeigandi fyrirtæki.

Samkvæmt almennu persónuverndarreglugerðinni gætir þú átt rétt á aðgangi að persónuupplýsingum um þig og rétt á leiðréttingu eða eyðingu eða takmörkun á vinnslu eða rétt til að andmæla vinnslu og rétt til gagnaflutnings. Þú hefur rétt til að leggja fram kvörtun til þar til bærra gagnaverndareftirlitsaðila vegna vinnslunnar. Það er engin sjálfvirk ákvarðanataka. Það reynist ómögulegt að veita frekari upplýsingar.

CROATIAN: Sustav zviždača (interni kanali za prijavu)

Naše vrijednosti čine temelj naše poslovne prakse i odražavaju našu predanost integritetu, transparentnosti i pozitivnoj korporativnoj kulturi. Naš sustav za prijavu zviždača bitan je alat za promicanje odgovornosti i osiguravanje etičkog poslovanja. Ova pravila postupka služe kako bi proces i načela naših istražnih procesa bili transparentni i osigurali da se sa svim prijavama primljenim putem našeg sustava postupa na odgovarajući i profesionalan način.

OSI je predan otvorenom dijalogu i prepoznaje važnost zviždača kao ključnih partnera u našim nastojanjima da održimo najviše standarde u svim područjima našeg poslovanja.

I. Pravila postupka za OSI Whistleblower System

I. Svrha i opseg:

1. Svrha: Ova Pravila postupka uređuju postupanje i istragu prijava primljenih putem sustava za prijavu zviždača Make It Right Global Hotline. Cilj je osigurati da se sa svim primljenim prijavama postupa transparentno, učinkovito iu skladu s etičkim standardima OSI-ja.

2. Opseg primjene: Ova pravila postupka primjenjuju se na sve zaposlenike, poslovne partnere, dobavljače i druge dionike u cijelom lancu vrijednosti koji koriste sustav za prijavu zviždača za dijeljenje specifičnih naznaka mogućeg nedoličnog ponašanja, zabrinutosti ili savjeta. Sustav za zviždače nije namijenjen za obradu pitanja vezanih uz proizvode i usluge. Takva pitanja ili problemi mogu se uputiti izravno putem obrasca za kontakt na web stranici tvrtke.

II. Podnošenje informacija:

1. Anonimnost i povjerljivost:

Sustav za prijavu zviždača omogućuje, između ostalog, anonimno podnošenje prijava o zviždačima, u mjeri u kojoj to dopuštaju nacionalni zakoni.

Sve informacije s kojima se postupa u okviru sustava zviždača podliježu strogoj povjerljivosti.

2. Vrste izvješća:

Sustav omogućuje zviždačima podnošenje prijava ako postoje konkretne naznake o mogućem nedoličnom ponašanju, zabrinutosti ili naznake takvog ponašanja. To se odnosi na kršenja primjenjivih zakona, propisa itd. od strane zaposlenika ili poslovnih partnera. (osobito onih navedenih u odjeljku 2. Zakona o zaštiti zviždača ili Direktivi EU 2019/1937) ili internim propisima tvrtke (posebno kršenjima Kodeksa ponašanja) ili ljudskim pravima i rizicima za okoliš koji se mogu pripisati izravnim ili neizravnim dobavljačima, kao i kršenjima ljudskih prava i ekoloških obveza prema Zakonu o dužoj pažnji u lancu opskrbe (LkSG). To uključuje kršenja Kodeksa ponašanja OSI-ja, antimonopolskog zakona, korupciju,

krađu, diskriminaciju, nepoštivanje zdravlja i sigurnosti na radu, dječji rad, onečišćenje tla, vode ili zraka, štetne emisije buke, neprihvatljivu potrošnju vode, proizvodnju ili korištenje određenih postojanih organskih onečišćivača te neovlaštenog uvoza i izvoza otpada.

3. Pristup sustavu:

Zviždači imaju pristup sustavu za prijavu kojim se upravlja izvana na različitim jezicima na:

EthicsPoint - OSI Group, LLC

- u tekstualnom obliku putem obrasca na online portalu ili
- telefonom (besplatno iz raznih zemalja)

III. Obrada izvješća:

1. Prijem i početna procjena:

Nakon što se prijava primi putem vanjskih kanala za prijavu kojima upravlja sustav za prijavu zviždača, ona se najprije dokumentira i dodjeljuje joj se pojedinačni broj datoteke. OSI Compliance prima sva izvješća i provodi početnu procjenu kako bi utvrdila njihovu vjerodostojnost i valjanost.

2. Istraga :

Za relevantne savjete bit će pokrenuta temeljita, objektivna i povjerljiva istraga. Ako je potrebno za primanje izvješća ili poduzimanje radnji , drugi će se odjeli konzultirati ili zatražiti pomoć. Od zviždača se također mogu zatražiti dodatne informacije.

Trajanje istrage do njezina završetka ovisi o složenosti predmeta, potrebnim istražnim radnjama i dostupnosti informacija odnosno stranama uključenim u pojedini slučaj. Učinit će se sve kako bi se istraga završila što je moguće učinkovitije i ekspeditivnije.

3. Povratne informacije zviždaču:

Zviždač će dobiti povratnu informaciju o primitku dojave u roku od 7 dana, gdje je to moguće i bez ugrožavanja anonimnosti.

Ako je zviždač podnio prijavu putem interneta ili telefonom, dobit će podatke za prijavu koji mu omogućuju praćenje prijave i primanje anonimne povratne informacije (ako želi). Konkretno, možda će biti potrebno postaviti pitanja o razumijevanju i dobiti dodatne informacije.

U daljnjem tijeku istrage (najkasnije u roku od 3 mjeseca od primitka potvrde o primitku) dostavit će se podaci o statusu istrage u vezi s planiranim ili već započetim mjerama ili, ako postoji nedostatna sumnja, o obustavi istrage. istraga.

IV. Zaštita zviždača:

1. Neodmazda:

OSI poduzima sve razumne napore kako bi osigurao da će zviždači biti zaštićeni od bilo kojeg oblika odmazde, nepovoljnog položaja ili drugih odmazdi.

Zabranjeno je i neće se tolerirati disciplinske mjere temeljene na zviždanju protiv pojedinaca koji u dobroj vjeri surađuju s istragama.

2. Povjerljivost:

Osobe uključene u istragu obvezuju se na strogu povjerljivost.

V. Dokumentacija i skladištenje:

1. Dokumentacija :

Svi koraci istrage pažljivo su dokumentirani.

Dokumentacija služi transparentnosti i sljedivosti postupka.

2. Razdoblje čuvanja:

Dokumentacija se čuva u skladu sa zakonskim odredbama i internim uputama.

VAS. Pregled i podešavanje:

Ova se proceduralna pravila redovito pregledavaju i po potrebi prilagođavaju kako bi se osiguralo da su u skladu s trenutnim zakonskim zahtjevima i korporativnim ciljevima.

II. Informacije u skladu s člankom 13. GDPR (za osobe koje daju informacije):

Ime i kontakt podaci kontrolora: Vidi impresum na web stranici. Kontakt podaci službenika za zaštitu podataka i, ako je primjenjivo, predstavnika: prof. dr. hc Heiko Jonny Maniero, LL.B., LL.M. mult., MLE, Franz-Joseph-Str. 11, 80801 München, Njemačka. Svrhe za koje se osobni podaci trebaju obrađivati i pravna osnova za obradu: Usklađenost sa Zakonom o zaštiti zviždača (HinSchG) i Zakonom o dubinskoj provjeri lanca opskrbe (LkSG), pravna osnova je članak 6. stavak 1. točka (c) GDPR u vezi s Odjeljcima 8, 9 LkSG i Odjeljkom 10 HinSchG, u onoj mjeri u kojoj je to potrebno za ispunjavanje zadataka navedenih u Odjeljcima 13 i 24 HinSchG, kao i usklađenost s Direktivom (EU) 2019/1937 o zaštiti osoba koje prijavljuju kršenja prava Unije i proizlazećeg nacionalnog prava država članica te usklađenosti s primjenjivim zakonodavstvom iz drugih zemalja. Primatelji ili kategorije primatelja osobnih podataka: Tijela za provođenje zakona, tijela za izricanje novčanih kazni i druga tijela, kao i

odvjetnici, društva grupe ili poslodavci. Planirani transfer u treće zemlje: Ulazak u Navex online sustav i prosljeđivanje transfera subjektima unutar grupe, poslodavcima ili odvjetnicima. S tvrtkom Navex sklopljene su EU standardne ugovorne klauzule i UK Dodatak EU standardnim ugovornim klauzulama. Navex je također član EU-SAD okvira za privatnost podataka, Švicarsko-američkog okvira za privatnost podataka i britanskog proširenja EU-SAD okvira za privatnost podataka. Za druge prijenose možda neće biti odluke o primjerenosti. Za takve prijenose koriste se Standardne ugovorne klauzule EU-a i dodatak UK-a Standardnim ugovornim klauzulama EU-a. Kriteriji za određivanje roka čuvanja: Dokumentacija se briše tri godine nakon završetka postupka. Dokumentacija se može čuvati dulje kako bi se ispunili zahtjevi primjenjivog zakonodavstva ako je to nužno i razmjerno.

Prema Općoj uredbi o zaštiti podataka imate pravo na pristup osobnim podacima koji se odnose na Vas i pravo na ispravak ili brisanje ili ograničenje obrade ili pravo na prigovor na obradu i pravo na prenosivost podataka. Imate pravo podnijeti pritužbu nadležnom tijelu za nadzor zaštite podataka u vezi s obradom. Davanje osobnih podataka nije propisano zakonom ili ugovorom te nije nužno za sklapanje ugovora, zbog čega niste dužni davati osobne podatke na telefon za prijavu zviždača. Moguće posljedice nedostavljanja su da prijava neće biti obrađena ili će biti obrađena sa zakašnjenjem, ili da će biti odbijena, te da vam se ne mogu dostaviti nikakve informacije ili informacije koje se odnose na prijavu. Ne postoji automatizirano donošenje odluka.

III. Informacije u skladu s člankom 14. GDPR-a (za druge subjekte podataka):

Ime i kontakt podaci kontrolora: Vidi impresum na web stranici. Kontakt podaci službenika za zaštitu podataka i, ako je primjenjivo, predstavnika: prof. dr. hc Heiko Jonny Maniero, LL.B., LL.M. mult., MLE, Franz-Joseph-Str. 11, 80801 München, Njemačka. Svrhe za koje se osobni podaci trebaju obrađivati i pravna osnova za obradu: Usklađenost sa Zakonom o zaštiti zviždača (HinSchG) i Zakonom o dubinskoj provjeri lanca opskrbe (LkSG), pravna osnova je članak 6. stavak 1. točka (c) GDPR u vezi s Odjeljcima 8, 9 LkSG i Odjeljkom 10 HinSchG, u onoj mjeri u kojoj je to potrebno za ispunjavanje zadataka navedenih u Odjeljcima 13 i 24 HinSchG, kao i usklađenost s Direktivom (EU) 2019/1937 o zaštiti osoba koje prijavljuju kršenja prava Unije i proizlazećeg nacionalnog prava država članica te usklađenosti s primjenjivim zakonodavstvom iz drugih zemalja. Kategorije osobnih podataka koji se obrađuju: Podaci o zviždačima. Primatelji ili kategorije primatelja osobnih podataka: Tijela za provođenje zakona, tijela za izricanje novčanih kazni i druga tijela, kao i odvjetnici, društva grupe ili poslodavci. Planirani transfer u treće zemlje: Ulazak u Navex online sustav i prosljeđivanje transfera subjektima unutar grupe, poslodavcima ili odvjetnicima. S tvrtkom Navex sklopljene su EU standardne ugovorne klauzule i UK Dodatak EU standardnim ugovornim klauzulama. Navex je također član EU-SAD okvira za privatnost podataka, Švicarsko-američkog okvira za privatnost podataka i britanskog proširenja EU-SAD okvira za privatnost podataka. Za druge prijenose možda neće biti odluke o primjerenosti. Za takve prijenose koriste se Standardne ugovorne klauzule EU-a i dodatak UK Standardnim ugovornim klauzulama EU-a . Kriteriji za određivanje roka čuvanja: Dokumentacija se

briše tri godine nakon završetka postupka. Dokumentacija se može čuvati dulje kako bi se ispunili zahtjevi primjenjivog zakonodavstva ako je to nužno i razmjerno. Izvor osobnih podataka je zviždač i/ili dotična tvrtka.

Prema Općoj uredbi o zaštiti podataka, možete imati pravo na pristup osobnim podacima koji se odnose na vas i pravo na ispravak ili brisanje ili ograničenje obrade ili pravo na prigovor na obradu i pravo na prenosivost podataka. Imate pravo podnijeti pritužbu nadležnom tijelu za nadzor zaštite podataka u vezi s obradom. Ne postoji automatizirano donošenje odluka. Pružanje daljnjih informacija pokazalo se nemogućim.