DISS-CO

WHITE PAPER

DIE EU-HINWEISGEBERRICHTLINIE UND PRAXISTIPPS ZUR RICHTIGEN IMPLEMENTIERUNG

Inhaltsverzeichnis

1. Einleitung

Mit der **EU-Richtlinie 2019/1937 vom 23. Oktober 2019** zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden („EU Hinweisgeberrichtlinie"), werden die EU-Mitgliedsstaaten aufgefordert, die teils sehr detaillierten Anforderungen bis Ende 2021 in nationales Recht umzusetzen. Die Implementierung eines Hinweisgebersystems kann für internationale Konzerne komplex und aufwendig sein, auch wenn das Erwerben und Einrichten eines Hinweisgeber Tools simpel ist. Für die KMU ist die Implementierung keine große Hürde. Erfahrungsgemäß gehen nur wenige Meldungen pro Jahr bei Unternehmen mit <1000 Mitarbeitern ein, so dass die Aufklärung der Meldungen ebenfalls keine große administrative Belastung darstellen sollte.

2. Der Kreis der Verpflichteten

- Staatliche und private Unternehmen und Organisationen mit mehr als 250 Mitarbeitern ab dem 17. Dezember 2021
- Unternehmen mit mehr als 50 Mitarbeitern ab dem 17. Dezember 2023
- Gemeinden und Kommunen ab 10.000 Einwohner

3. Pflichten

1. **Einrichtung einer vertraulichen Meldestelle in mündlicher und schriftlicher Form**. Unternehmen sind nicht verpflichtet, anonymen Meldungen nachzugehen. Gehen sie jedoch der Meldung nach, was wir ausdrücklich empfehlen und wird die Identität des Hinweisgebers festgestellt, muss der Hinweisgeber vor Repressalien geschützt werden. Es wird den Mitgliedsstaaten selbst überlassen, ob sie die Einrichtung einer anonymen Meldestelle als verpflichtend vorgeben möchten. Jedoch sind in einigen Sektoren längst andere national und extraterritoriale Gesetze in Kraft, die eine anonyme Beschwerdeführung vorsehen, wie das Wertpapierhandelsgesetz und das Patientenrechtegesetz in Deutschland. Zudem haben externe Meldestellen wie das LKA einiger Bundesländer sowie die BAFIN eine anonyme Meldestelle eingerichtet.
2. **Rückmeldung an den Hinweisgeber** innerhalb von 7 Tagen nach Eingang der Meldung.
3. **Schutz der betroffenen Personen**, sofern ihnen kein Verstoß nachgewiesen werden kann.
4. **Schutz des Hinweisgebers vor Repressalien**, sofern der Hinweisgeber gutgläubig handelt und nicht wissentlich falsche Informationen übermittelt.
5. **Rückmeldung über den Status** an den Hinweisgeber nach 3 Monaten ab Bestätigung des Eingangs der Meldung, in wenigen Fällen kann die Rückmeldung auch innerhalb von 6 Monaten erfolgen.

4. Was soll gemeldet werden?

- Grundsätzlich sollen **Verstöße gegen das Unionsrecht** gemeldet werden. Zu erwarten ist die Erweiterung auf **Verstöße gegen das nationale Recht** durch die Mitgliedsstaaten im Rahmen der Umsetzung der Direktive.

- Der Begriff „Verstoß" wird ausgeweitet auf missbräuchliche Praktiken im Sinne der Rechtsprechung des Gerichtshofs, also Handlungen oder Unterlassungen, die in formaler Hinsicht nicht als rechtswidrig erscheinen, die jedoch mit dem Ziel oder Zweck der einschlägigen Rechtsvorschriften unvereinbar sind.

- Hinweisgeber können auch folgendes melden:
  - Informationen, die zur Aufdeckung von bereits eingetretenen Verstößen notwendig sind
  - Verstöße, die zwar noch nicht eingetreten sind, aber mit deren Eintreten mit hoher Wahrscheinlichkeit zu rechnen ist
  - Handlungen oder Unterlassungen, die der Hinweisgeber aus hinreichendem Grund als Verstöße erachtet
  - Versuche zur Verschleierung von Verstößen

5. Das Einrichten einer internen Meldestelle

- Hinweisgeber sollten grundsätzlich darin bestärkt werden, zunächst die internen Meldekanäle zu nutzen und ihrem Arbeitgeber Meldung zu erstatten, sofern ihnen derartige Kanäle zur Verfügung stehen und vernünftigerweise erwartet werden kann, dass sie funktionieren. Dies gilt insbesondere, wenn die Hinweisgeber der Meinung sind, dass **in der betreffenden Organisation wirksam gegen den Verstoß vorgegangen werden kann** und keine Repressalien drohen.

- Folglich sollten juristische Personen des privaten und öffentlichen Sektors **geeignete interne Verfahren für die Entgegennahme von Meldungen und entsprechende Folgemaßnahmen** einrichten.

- Die Förderung einer **Kultur der guten Kommunikation und der sozialen Verantwortung** soll dazu beitragen, dass (gutgläubig handelnde) Hinweisgeber als Personen gelten, die wesentlich zu Selbstverbesserung und herausragender Kompetenz innerhalb der Organisation beitragen. (Nr. 47 Direktive)

6. Die Schutzbedürftigen

a) Arbeitnehmer

- Schutz sollte zuallererst für „Arbeitnehmer“, d. h. für Personen, die während eines bestimmten Zeitraums Dienstleistungen, für die sie eine Vergütung erhalten, für und unter der Leitung einer anderen Person erbringen.
- Schutz sollte daher auch Arbeitnehmern in atypischen Beschäftigungsverhältnissen, einschließlich Teilzeitbeschäftigten und befristet Beschäftigten, sowie Personen gewährt werden, die einen Arbeitsvertrag oder ein Arbeitsverhältnis mit einem Leiharbeitsunternehmen geschlossen haben; bei prekären Vertragsbeziehungen ist es häufig schwierig, Standardschutzbestimmungen gegen unfaire Behandlung anzuwenden.
- Der Begriff „Arbeitnehmer“ schließt auch Beamte, öffentliche Bedienstete und andere Personen, die im öffentlichen Sektor arbeiten, ein. (Nr. 38 Direktive)
- Die Arbeitnehmer sind vor Repressalien zu schützen. Die Liste der Maßnahmen, die als Repressalien gelten, ist lang. Dazu gehören Kündigung, Versetzung, Übergehung bei Beförderung, Degradierung, Rufschädigung, negative Leistungsbeurteilung etc.

b) Freiberufler, Geschäftspartner und sonstige Dritte, die in einem Abhängigkeitsverhältnis zum Verpflichteten stehen

Zu schützen sind darüber hinaus die folgenden Personengruppen, die in einer Beziehung zu den Verpflichteten stehen und Verstöße melden:

- Berater
- Selbstständige, die Dienstleistungen erbringen
- Freiberufler
- Auftragnehmer und Unterauftragnehmer
- Lieferanten
- Anteilseigner
- Personen in Leitungsgremien
- Ehemaligen Mitarbeitern
- Bewerbern

Repressalien in Form von vorzeitiger Kündigung der Dienstleistungsverträge, Beendigung von Lizenzen oder Bewilligungen, so dass die o.g. Gruppen Auftrags- oder Einkommensverluste erleiden, Nötigung, Einschüchterung oder Mobbing, Aufnahme auf „schwarze Listen“ bzw. geschäftliche Boykottierung und Rufschädigungen sind verboten. (Nr. 39 Direktive)

c) Freiwillige, bezahlte oder unbezahlte Praktikanten

Auch Personengruppen, die zwar auf ihre berufliche Tätigkeit nicht wirtschaftlich angewiesen sind, aber infolge einer Meldung von Verstößen dennoch Repressalien erleiden können, sind zu schützen. Dazu gehören Freiwillige, bezahlte und unbezahlte Praktikanten.

Repressalien in Form von der Beendigung des Praktikums oder der freiwilligen Tätigkeit, das Ausstellen von negativen Arbeitszeugnissen oder Rufschädigungen sind verboten. (Nr. 40 Direktive)

d) Personen, die dem Hinweisgeber nahestehen

- Geschützt werden auch Mittler, Kollegen oder Verwandte des Hinweisgebers, die ebenfalls in einer beruflichen Verbindung zum Arbeitgeber des Hinweisgebers, zu einem Kunden des Hinweisgebers oder zu einem Empfänger vom Hinweisgeber erbrachter Dienstleistungen stehen.

- Verboten sind auch indirekte Repressalien, z.B. Maßnahmen wie Verweigerung von Dienstleistungen, Erfassung auf „schwarzen Listen" oder Geschäftsboykott gegen die juristische Person, die im Eigentum des Hinweisgebers steht, für die er arbeitet oder mit der er in einem beruflichen Kontext anderweitig in Verbindung steht. (Nr. 41 Direktive)

7. Schutz auch bei begründetem Verdacht

- Wie oben dargestellt, können Hinweisgeber auch einen Verdacht melden, wenn dieser begründet ist. Daher ist der Schutz auch für Personen gerechtfertigt, die zwar keine eindeutigen Beweise beibringen, aber begründete Bedenken oder einen begründeten Verdacht äußern.

- Demgegenüber sollte Personen, die Informationen melden, die bereits öffentlich in vollem Umfang verfügbar sind oder bei denen es sich um unbegründete Spekulationen oder Gerüchte handelt, kein Schutz gewährt werden. (Nr. 43 Direktive)

8. Das Wahlrecht zwischen der internen und externen Meldestelle

- Die EU Hinweisgeberrichtlinie lässt ein Wahlrecht des Hinweisgebers zu, ob intern oder extern gemeldet wird. Der Schutz des Hinweisgebers vor Repressalien als Mittel zum Schutz der Freiheit der Meinungsäußerung und der Freiheit und der Pluralität der Medien sollte demnach trotzdem gewahrt werden.

- Extern bedeutet, dass die Informationen über Handlungen oder Unterlassungen an einer externen Behörde übermittelt werden (im Folgenden „externe Meldungen").

- Hinweisgeber können die Informationen auch direkt über Online-Plattformen und soziale Medien oder indirekt über die Medien, gewählte Amtsträger, zivilgesellschaftliche Organisationen, Gewerkschaften oder Berufsverbände veröffentlichen. (Nr. 45 Direktive)

- Auch wird die Informationsweitergabe an investigative Journalisten betont, da Hinweisgeber eine besonders wichtige Quelle sind. Der Schutz von Hinweisgebern trägt zur Wahrung der Überwachungsfunktion investigativer Journalisten in demokratischen Gesellschaften bei. (Nr. 46 Direktive)

9. Das Beschaffen von Informationen

- Hinweisgeber können für die Beschaffung, den Zugriff, die Offenlegung oder Meldung von betriebsinternen Informationen gemäß Artikel 21 der EU Hinweisgeberrichtlinie in keiner Weise haftbar gemacht werden. Für die Meldung oder Offenlegung reicht ein hinreichender Grund zu der Annahme, dass die Meldung oder Offenlegung der Information notwendig war, um einen Verstoß gemäß dieser Richtlinie aufzudecken.

- Dies gilt, sofern die Beschaffung oder der Zugriff nicht als solche bzw. solcher eine eigenständige Straftat dargestellt hat. Im Fall, dass die Beschaffung oder der Zugriff eine eigenständige Straftat darstellt, unterliegt die strafrechtliche Haftung weiterhin dem nationalen Recht.

a) Einschränkungen in der praktischen Umsetzung

- Fraglich ist nun, ob die Mitarbeiter, die meist keine Juristen sind, urteilen können, was ein "hinreichender Grund" ist und ob der Sachverhalt tatsächlich einen Verstoß darstellt.

- Es ist anzunehmen, dass die Mitgliedsstaaten die Richtlinie bei der Umsetzung ins nationale Recht um Verstöße gegen das nationale Recht erweitern werden. Die oben genannten Vorschriften implizieren, dass die Mitarbeiter eines Unternehmens oder auch die Bürger, die sich an die Behörden wenden, ausreichend Kenntnis über das nationale Recht besitzen. Es ist davon auszugehen, dass dies nicht der Fall ist. Es bleibt abzuwarten, wie etwaige Prozesse in Fällen der Offenlegung von Betriebsgeheimnissen verlaufen werden.

b) Nationales Recht

- Die weiteren nationalen Vorschriften sind ebenfalls zu beachten, die bereits heute einen gewissen Schutz für Hinweisgeber bieten. In Deutschland bieten Ausnahmen von Hinweisgebern im Geschäftsgeheimnisgesetz einen beschränkten Schutz für Hinweisgeber, wenn die Meldung vom öffentlichen Interesse ist. Die Beurteilung, ob eine Meldung vom öffentlichen Interesse ist, setzt eine rechtliche Bewertung der Informationen voraus. Dies bedeutet für den Hinweisgeber, dass er sich vorab und auf eigene Kosten an einen Rechtsanwalt wenden muss und die Informationen gegenüber seinem Anwalt offenlegen muss, was bereits einen Verstoß gegen das Geschäftsgeheimnisgesetz darstellen könnte.

- Demgegenüber stehen regelmäßig die Pflichten des Arbeitnehmers hinsichtlich der IT Sicherheit und Datenschutzrichtlinien des Unternehmens. Es ist davon auszugehen, dass betriebsinterne Informationen auch personenbezogene Informationen beinhalten, die nicht ohne weiteres weitergegeben werden dürfen.

- Wir empfehlen daher, eine anonyme interne Meldestelle einzurichten und den Betroffenen die Möglichkeit zu geben, sich intern zu informieren. Auch eine anonyme Chat Funktion erleichtert Rückfragen bei der Compliance Stelle erheblich.

10. Welcher Meldekanal ist der richtige?

- Gemäß der EU Hinweisgeberrichtlinie kann der Verpflichtete aussuchen, welche Kanäle er einrichtet, solange die Vertraulichkeit der Identität des Hinweisgebers gewahrt bleibt.
- Konkret sollten die Meldekanäle eine mündliche oder schriftliche Meldung ermöglichen. Ob auf dem Postweg, über einen Beschwerde-Briefkasten oder über eine Online-Plattform, sei es eine Plattform im Intranet oder im Internet, persönlich oder über eine Telefon-Hotline oder ein anderes System für gesprochene Nachrichten, wichtig ist die Wahrung der Vertraulichkeit. Einige Meldekanäle erfüllen dennoch die Anforderungen der Richtlinie nicht, wie im Folgenden ausführlich dargestellt wird.
- Auf Anfrage des Hinweisgebers sollte es auch möglich sein, innerhalb eines angemessenen Zeitraums im Rahmen von physischen Zusammenkünften Meldung zu erstatten.

11. Technische Hürden bei herkömmlichen Methoden

Werfen wir einen genauen Blick auf die herkömmlichen Meldekanäle, so werden die technischen und organisatorischen Schwachstellen deutlich:

Der Brief: die älteste aller Methoden weckt nostalgische Erinnerungen an die alten Zeiten, in den es Kummerkästen gab. Ein anonymer Brief ist bei dem undurchsichtigen technischen Dschungel für viele noch die Methode der Wahl. Leider kann man mit einem anonymen Briefabsender nicht in Kontakt treten, was einerseits keine Rückmeldungen an den Hinweisgeber und andererseits kein effizientes Aufarbeiten zulässt. Die Anforderungen gemäß der EU Hinweisgeberrichtlinie wären nicht erfüllt.

Das Telefon: beliebt sind telefonische Meldungen. Viele Menschen der älteren Generation vertrauen der "modernen Technik" nicht oder haben keinen Zugang zu Internet oder es fällt ihnen schwer so vertrauliche Informationen im Internet preiszugeben. Meldet sich der Hinweisgeber vertraulich, könnte der Bearbeiter der Meldung telefonisch Rückmeldung geben und die Rückmeldung dokumentieren, vorausgesetzt der Hinweisgeber ist erreichbar. Schwierig ist die Rückmeldung an anonyme Hinweisgeber und das Übermitteln von Dokumenten und Daten, die als Beweismittel dienen könnten. Die Anforderungen gemäß der EU Hinweisgeberrichtlinie wären nicht erfüllt.

Die E-Mail: betrachten wir die E-Mail-Option als nächste Alternative. Sicher kann fast jeder eine provisorische E-Mail-Adresse bei bei yahoo, gmail oder anderen Providern anlegen und mit einem Alias mit der internen Meldestelle kommunizieren.

- Der Hinweisgeber ist gezwungen, betriebsinterne Daten über einen externen E-Mail Provider an die interne Meldestelle zu senden, um anonym zu bleiben. Das bedeutet, dass er entweder die Endgeräte des Unternehmens nutzen muss oder die notwendigen Dateien auf ein Medium überträgt und diese der E-Mail anhängt. Beide Wege führen dazu, dass entweder gegen interne IT Richtlinien verstoßen wird oder/und die Spuren zurückverfolgt werden können. Die Anonymität ist somit nicht gewährleistet und der Hinweisgeber kann zivilrechtlich oder sogar strafrechtlich belangt werden.
- Die E-Mails sind gewöhnlich unverschlüsselt, was zu einem Sicherheitsrisiko für das Unternehmen führt.
- Die üblichen US E-Mail Provider wie Google und Yahoo übermitteln die Daten auf Servern in den USA oder an einem anderen Ort. Werden z.B. im Rahmen von externen Ermittlungen US Behörden eingeschaltet, sind die Provider zur Kooperation verpflichtet und müssen die Informationen und E-Mails der Zielperson herausgeben. Die Informationen können u.a. IP Adressen beinhalten, die die Anonymität des Hinweisgebers gefährden.

- Die Dateianhänge können über ihre Metadaten die Identität des Hinweisgebers offenlegen. Diese können mit den vorhandenen Daten im Unternehmen und auf diversen Endgeräten verglichen werden. So kann die Identität des Hinweisgebers auch offengelegt werden. Außer der Hinweisgeber ist versiert genug, um die Metadaten selbst zu entfernen. Aus der Praxis wissen wir, dass nur ein geringer Prozentsatz der Mitarbeiter dazu in der Lage ist und sich mit der Vorgehensweise sicher fühlt.
- Verwendet der Hinweisgeber das Endgerät des Unternehmens (Laptop oder Smartphone o.ä.), kann eine Auswertung der Browseraktivitäten zur Identifikation des Hinweisgebers führen.
- Zudem haben manche Unternehmen aus Sicherheitsgründen sogenannte Data Loss Prevention (DLP) Tools im Einsatz, die sämtliche Aktionen aufzeichnen und überwachen können. Die DLP Tools können präventiv zur Vorbeugung von Datendiebstahl eingesetzt werden, eignen sich jedoch auch sehr gut zur Mitarbeiterüberwachung und können die Anonymität des Hinweisgebers gefährden.

12. Webbasierte Systeme

Webbasierte Systeme wie die **Smart Integrity Platform (SIP)** von DISS-CO erfüllen alle technischen Anforderungen der EU Hinweisgeberrichtlinie und der DSGVO und unterstützen bei der effizienteren Bearbeitung von Meldungen.

Die SIP ist eine **white label Software as a Service** und bietet u.a.:

- eine **verschlüsselte externe Kommunikation** mit dem Hinweisgeber
- eine **verschlüsselte interne Kommunikation** zwischen den Bearbeitern der Meldungen
- eine **verschlüsselte Kommunikation mit Externen** (Ombudsleuten, Rechtsanwälten, Beratern)
- Eine **drei-Wege-Kommunikation**: Sie entscheiden, wann und wem Sie über welchen Zeitraum Zugriff auf die Informationen eines Falles gewähren; Ihre Berater können die Kommunikation mit dem Hinweisgeber teils oder ganz übernehmen oder Sie rechtlich beraten. Sie müssen die Plattform nicht verlassen, um z.B. per E-Mail intern oder extern über den Fall zu kommunizieren
- Hochgradig anpassbare Module, die die Prozesse und den Bedarf für Großunternehmen abdecken

- Ihre Daten werden auf einem ISO 27001 zertifizierten **Server in Deutschland** gehostet. Unter Beachtung der nationalen Datenschutzbestimmungen werden bei Tochtergesellschaften ähnliche Serverstrukturen in dem jeweiligen Land genutzt (u.a. in den USA, in China, Russland und Saudi Arabien). Die SIP kann auch auf Ihrem eigenen Server installiert werden.

a) Multiple Meldekanäle. Zentrale Erfassung.

Sie können verschiedene Meldekanäle einrichten und haben trotzdem die Möglichkeit, die Meldungen zentral zu erfassen und zu bearbeiten. Auch Ihr Ombudsmann kann die bei ihm eingegangenen Meldungen auf der SIP erfassen, mit Ihnen teilen und bearbeiten. Sie kommunizieren mit Ihrem Ombudsmann im internen Bereich vollkommen geschützt durch die Verschlüsselung.

b) Verschiedene Ansichten für Nutzer Rollen

- **Analyst Admin**: ist die zentrale Rolle für die Einrichtung des Systems, User Verwaltung und Zuweisung und/oder Bearbeitung der Meldungen; der Analyst Admin erhält zentral alle Meldungen und weist diese einzelnen Analysten zu.
- **Analyst**: ist der Bearbeiter der Meldungen, die ihm/ihr zugewiesen wurden. Diese Rolle kann auch teils oder ganz ausgelagert werden.
- **Mitarbeiter**: haben eine eigene Umgebung, in der sie vertraulich oder anonym melden und die Tutorials jederzeit einsehen können. Die Mitarbeiter können mit den Bearbeitern ihrer Meldung verschlüsselt kommunizieren. Das besondere an der Mitarbeiteransicht ist, dass sie eine Benachrichtigung bei vertraulichen Meldungen erhalten, wenn Rückmeldungen vom Bearbeiter da sind. So werden die Notwendigkeit des proaktiven Einloggens und damit zusammenhängenden Verzögerungen in der Bearbeitung vermieden.
- **Andere Nutzer**: Ihren Geschäftspartnern und anderen Personen, denen Sie die interne Meldestelle zur Verfügung stellen müssen, erreichen die Smart Integrity Platform über einen Link auf Ihre Homepage. Wir haben Nutzungs- und Datenschutzbestimmungen vorbereitet, die Sie nutzen und auf Ihr Unternehmen anpassen können.

c) Anonyme Live Chat Funktion

Über die anonyme Live Chat Funktion können Ihre Mitarbeiter und Externe Fragen stellen, ohne gleich eine Meldung abgeben zu müssen. So reduzieren Sie die Anzahl der nicht-gehaltvollen Meldungen und schaffen Vertrauen im Unternehmen. Sie können diese Funktion auch deaktivieren.

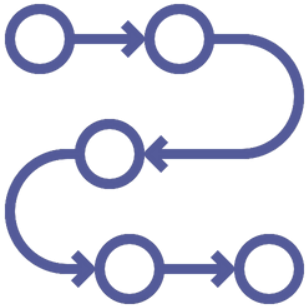
d) Managed Services

Sollten Sie nicht über die internen Kapazitäten für die Bearbeitung der Meldungen und die Erstellung der Maßnahmenpläne verfügen, unterstützen wir Sie mit einem Team an erfahrenen Mitarbeitern und attraktiven Paketpreisen mit Stundenkontingente.

13. Praxis Tipps: Implementierung

a) Die Implementierungsphase

- Die frühzeitige Einbindung des Datenschutzbeauftragten und des Betriebsrates sind ratsam, um sowohl eine Hinweisgeberrichtlinie als auch eine Betriebsvereinbarung zeitnah zu verabschieden.
- Dabei sollte beachtet werden, dass ein kleiner Kreis von Personen aus dem Unternehmen Zugang zu den Meldungen erhalten.
- Die Hinweisgeberrichtlinie sollte auch Prozesse vorschreiben, die einzuhalten sind, wenn die Meldeempfänger und -bearbeiter selbst betroffen sind.
- Auch sollten Prozesse festgelegt werden, wie mit Meldungen umzugehen ist, wenn das Management betroffen ist oder sein könnte.



- Der Betriebsrat würde spätestens durch Betroffene informiert und um Unterstützung gebeten werden. Es gilt die Unschuldsvermutung und die Betroffenen sind ebenfalls zu schützen bis ihre Schuld bewiesen wurde. Klären Sie frühzeitig, wie Sie in solchen Fällen mit den gemeldeten Informationen über den Stand der internen Untersuchung gegenüber den Betroffenen umgehen möchten. Es ist verständlich, dass Betroffene über den gesamten Fall und mögliche Konsequenzen informiert werden möchten. In solchen Fällen kommt es auf die richtige Balance zwischen Offenlegung und Zurückhaltung von wesentlichen Informationen an, um das Verdunkelungsrisiko zu reduzieren und die Vertraulichkeit der Identität des Hinweisgebers zu schützen. Der Einzelfall ist dahingehend zu prüfen.

b) Das Marketing

- Zur ordentlichen Implementierung eines Hinweisgebersystems gehört auch das Marketing. Mit den richtigen Maßnahmen, etwa durch Mailings, Plakate und vertrauenserweckenden Videobotschaften vom Management sensibilisieren Sie Ihre Mitarbeiter, mögliche Verstöße zu melden und somit die Risiken für das Unternehmen frühzeitig zu identifizieren.
- Veröffentlichen Sie Ihre Meldekanäle über Ihre Webseite an einer leicht zugänglichen Stelle.
- Bieten Sie Ihren Mitarbeitern über das eLearning hinaus, weiterbildende Schulungsmaßnahmen an und gehen Sie anonymisierte Fälle durch. So schaffen Sie eine Vertrauenskultur und reduzieren das Risiko der externen Meldungen.

14. Praxis Tipps: Durchführung

1

Wählen Sie das richtige Team

Die interne Meldestelle sollte über eine entsprechende Ausbildung verfügen, die sie befähigt, unabhängig intern untersuchen zu können. Eine unabhängige Stelle wie ein Ombudsmann oder das Team von DISS-CO könnten die Meldungen empfangen und eine erste Einschätzung vornehmen. Aus unserer Sicht sind jedoch weitreichende Kenntnisse über die internen Prozesse und Strukturen notwendig, um die Meldung effizient analysieren und bewerten zu können. Es empfiehlt sich daher, ein Team aus internen und externen Analysten für die Bearbeitung der Fälle zu stellen.

Unterlassen Sie Repressalien jeglicher Art

Auch wenn die Bewertung der Informationen und Ereignisse durch den Hinweisgeber zu einer falschen Schlussfolgerung geführt haben, darf der Hinweisgeber keine Nachteile durch seine Meldung haben. Der Begriff der Repressalien ist weit gefasst, dazu gehören unter anderem Übergehung bei Beförderungen, Mobbing, Versetzung etc. Sollten solche Maßnahmen erfolgen und im zeitlichen Zusammenhang mit der Meldung stehen, steht der Arbeitgeber in der Pflicht zu beweisen, dass die Maßnahmen nicht mit der Meldung im Zusammenhang stehen. Regelmäßig werden die Maßnahmen auf die Arbeitsleistung des Hinweisgebers abgestellt. Aber Vorsicht! Der Nachweis der mangelnden Leistung ist schwer zu erbringen. Die Beweislast liegt beim Arbeitsgeber, sofern ein zeitlicher Zusammenhang zwischen der Meldung und der Maßnahme besteht. Handeln Sie daher nicht zu vorschnell und bewerten Sie Ihre Risiken mit Ihrem Rechtsberater.

2

3

Versuchen Sie nicht den anonymen Hinweisgeber zu identifizieren

Ein Ausfindigmachen des anonymen Hinweisgebers ist nicht ratsam und sollte technisch nicht möglich sein, auch wenn die Inhalte der Meldung falsch sind. Diese Vorgabe sollte in den Hinweisgeber Richtlinien des Unternehmens festgehalten und die Mitarbeiter dahingehend geschult werden. Derartige Maßnahmen sorgen für Angst der Hinweisgeber, die gutwillig handeln, sich jedoch nicht sicher sind, ob ihr Verdacht korrekt ist.

Nutzen die Mitarbeiter eine webbasierte Hinweisgeberplattform, können Ihre IT Administratoren über die Browseraktivitäten und die Zeitpunkte der Kommunikation, den Kreis der möglichen Hinweisgeber eingrenzen. Wir empfehlen, solche Auswertungen über die internen Richtlinien zu untersagen.
Sollte die Vertraulichkeit der Identität des Hinweisgebers nicht gewahrt werden, laufen Sie Gefahr, Sanktionen gegen Ihr Unternehmen und die handelnden Personen zu erfahren.

4

Senden Sie klare Botschaften

Der Tone from the Top ist hinsichtlich der internen Bearbeitung und des Umgangs mit einem (neu) implementierten Hinweisgebersystem enorm wichtig. Das Management kann teilweise keinen Einfluss darauf nehmen, dass betroffene Kollegen den Hinweisgeber unfair behandeln, benachteiligen oder gar mobben. Es ist sogar vorgekommen, dass Betroffene mit Verleumdungsklagen gedroht und den Hinweisgeber einzuschüchtern versucht haben. Verstöße gegen Repressalien unter Kollegen sollten sanktioniert werden, beispielsweise mit mündlichen oder schriftlichen Ermahnungen oder gar Abmahnungen, sollte der Betroffene nicht von seinen Maßnahmen ablassen. Es kommt nicht selten vor, dass Betroffene, die eine höhere Position im Unternehmen bekleiden, den Drang verspüren, den „Verräter" ausfindig zu machen und Rache zu üben. Sorgen Sie dafür, dass solche Maßnahmen sofort und nachhaltig eingestellt werden. Das Hinweisgebersystem verliert sonst an Glaubwürdigkeit in der Belegschaft und wird nicht genutzt.

5

Motivieren Sie Ihre Mitarbeiter einen Verdacht zu melden

Auch wenn sie keine „harten Beweise" haben. Viele Korruptions- und Fraud-Fälle sind durch das Melden eines Verdachts aufgedeckt worden. Ihre Mitarbeiter sollten keine Angst haben, Meldungen abzugeben, auch wenn sich diese nach der internen Untersuchung als nicht korrekt herausstellen oder korrekt sind, jedoch nicht gegen Richtlinien oder Gesetze verstoßen. Denken Sie daran, dass Sie davon profitieren, wenn Risiken frühzeitig erkannt werden.

6

Starten Sie Umfragen

Wenn Sie ein Hinweisgebersystem implementiert haben und keine oder verhältnismäßig wenige Meldungen eingehen, ist das ein Zeichen dafür, dass Sie nicht genug getan haben, um das Vertrauen der Mitarbeiter in das Hinweisgebersystem zu stärken. Überlegen Sie sich neue Maßnahmen wie anonyme Umfragen und Workshops in kleineren Runden auf der operativen Ebene. So können Sie Meinungen einholen und die Implementierung des Systems verbessern.

7

Überwinden Sie Sprachbarrieren

Indem Sie lokalen Support anheuern und/oder kostenlose Rufnummern in der Landessprache für die Entgegennahme von Meldungen einrichten. Erfahrungsgemäß fühlen sich viele Hinweisgeber in ihrer Muttersprache wohler. Bei der Auswertung der Meldungen kommt es auf die Details und die sprachlichen Nuancen an.
Wir bieten mit internationalen Partnern in über 80 Ländern Support für Ihre interne Untersuchung.

8

Vermeiden Sie übereilte arbeitsrechtliche Maßnahmen

Z.B. die Beschuldigten frühzeitig zu sanktionieren, freizustellen oder zu entlassen, denn es besteht häufig Verdunkelungsgefahr. Sofern die interne Untersuchung ohne Verzögerung erfolgt, beginnt die Frist für die fristlose Kündigung erst nach Abschluss der Untersuchung. Nehmen Sie sich die Zeit, die notwendig ist, um den Fall vollumfänglich aufzuklären. Das DISS-CO Team unterstützt Sie gerne bei der Erstellung einer Untersuchungsstrategie. Die Reaktionszeiten spielen eine wesentliche Rolle.

9

Seien Sie vorbereitet

Auf den Fall einer externen Meldung. Gehen Sie vorab unterschiedliche Szenarien durch und bilden Sie eine Risikogruppe, die im Falle einer externen Meldung gerufen wird. Unsere erfahrenen Berater unterstützen Sie einen Risiko Mitigation Plan zu entwickeln, den Sie bei Bedarf heranziehen können.

10

Treffen Sie geeignete Folgemaßnahmen

Gemäß der EU Hinweisgeberrichtlinie sind Sie verpflichtet Folgemaßnahmen nach Meldungen zu treffen. Es wird offengelassen, welche Art Maßnahmen erwartet wird. Empfehlenswert sind Maßnahmen, die zur Schließung der internen Kontrolllücken und Prozessschwächen einerseits und zur Stärkung des Vertrauens der Belegschaft in das Compliance Management System andererseits geeignet sind.

Lassen Sie sich von unserem erfahrenen Team hierzu beraten!

15. Ihre Ansprechpartnerin

Sarah Afshari

Managing Director
und Erfinderin der Smart Integrity Platform

Frau Afshari verfügt über 18 Jahren Berufserfahrung und hat mehrere hundert internationale Fraud und Compliance Fälle für Unternehmen in unterschiedlichen Branchen untersucht. Vieler dieser Fälle stammten von Hinweisgebern, mit denen sie sich auch persönlich austauschte und dafür sorgte, dass ihre Identitäten im Laufe der Untersuchung geschützt blieben. Die Notwendigkeit für bestimmte Funktionen eines Hinweisgebersystems erkannte sie im Laufe Ihrer beruflichen Laufbahn und hat diese in der Smart Integrity Platform mit einem starken Entwicklerteam umgesetzt.

Sie war zudem als Compliance Officer zuständig für Compliance Audits und das Compliance Management Systems eines Bauunternehmens.

Vom Hintergrund ist sie Kriminologin (M.A.) und verfügt über einen MBA in Betriebswirtschaftslehre.

Kontaktdaten:

DISS-CO GmbH
Ottenser Hauptstraße 2
22765 Hamburg

Telefon: **+49 (0)40-226 392 51-0**

E-Mail: **info@diss-co.tech**
https://diss-co.tech

oder Sie melden Sich über das Kontaktformular auf der Webseite

ÜBER UNS

Entwickelt mit Erfahrung und Leidenschaft für Compliance und die frühzeitige Erkennung von Risiken.

DISS-CO ist ein Tech Start-Up mit starkem Fokus auf Legal Tech, eGRC und RegTech.
Entwickelt von Experten mit
mehr als 20 Jahre Erfahrung in Investigation, IT und Compliance.

WOFÜR WIR STEHEN

BESSERER SCHUTZ FÜR HINWEISGEBER

Wir sorgen dafür, dass Hinweisgeber anonym berichten können und besser vor Repressalien geschützt sind.

MEHR INTEGRITÄT IN UNTERNEHMEN

Je besser das Compliance-System implementiert ist, desto größer ist die Bereitschaft der Belegschaft, die Systeme zu nutzen.

KEINE STIGMATISIERUNG

In einer besseren Welt sollte die Meldung von Fehlverhalten nicht als Denunziantentum abgetan werden.

DISS-CO

E-Mail: info@diss-co.tech https://diss-co.tech

Titelbild von Rawpixel.com - stock.adobe.com
Weitere Bilder von canva.com
Icons von flaticon.com