

**Anleitung für die Ausarbeitung einer Hinweisgeber-Richtlinie und Beispiel für eine Hinweisgeber-Richtlinie**

Ein Unternehmen, auf das das HinweigeberInnenschutzgesetz (HSchG) anwendbar ist, ist verpflichtet, den potenziellen Whistleblowern (insbesondere deren Belegschaft) einfachen Zugang zu klaren Informationen über die Möglichkeit und das Verfahren der Hinweisgebung an die interne Stelle (innerhalb des Unternehmens errichtetes Hinweisgebersystem (und der Hinweisgebung an externe (behördliche) Stellen Um das zu erreichen, kann das Unternehmen z.B. eine Hinweisgeber-Richtline und ein schriftliches Verfahren für den Umgang mit Hinweisen ausarbeiten.

Auf Seite 8 geben wir ein Beispiel für eine Hinweisgeberichtlinie, die nach ein paar Anpassungen angewendet werden kann. Wenn Sie Ihre eigene Hinweisgeberrichtlinie ausarbeiten wollen, sollten Sie zumindest Folgendes berücksichtigen:

**1. Einleitende Beschreibung des Systems einschließlich seines Zwecks und Hintergrunds**

Eine allgemeine Beschreibung des Zwecks und des Hintergrunds der Schaffung des Systems sollte in einem einleitenden Abschnitt gegeben werden.

Darüber hinaus soll eine erste Beschreibung des Umgangs des Unternehmens mit den Anliegen der Mitarbeiter gegeben werden, und dass das Hinweisgebersystem als Ergänzung zur direkten, täglichen Kommunikation am Arbeitsplatz über Fehler und unbefriedigende Bedingungen gedacht ist.

**2. Wer kann Hinweise geben?**

Normalerweise steht allen Mitarbeitern und ehemaligen Mitarbeitern, Geschäftspartnern und Mitarbeitern von Geschäftspartnern ein System zur Verfügung, um in gutem Glauben begründete Verdachtsmomente und Bedenken über das Unternehmen und seine Mitarbeiter zu melden.

**3. Welche Hinweise können im Rahmen des Systems gegeben werden?**

In der Richtlinie sollte festgelegt werden, was im Rahmen des Systems an Hinweisen gegeben werden kann, einschließlich dessen, was und was nicht gemeldet werden darf.

Der Anwendungsbereich des HSchG umfasst Meldungen über Verletzungen einer Reihe von Vorschriften und Rechtsbereiche. Unter einer Rechtsverletzung ist nicht nur ein Rechtsverstoß gegen die unterstehenden Vorschriften bzw. Rechtsbereiche verstanden, Rechtsverstoß gegen die unterstehenden Vorschriften bzw. Rechtsbereiche verstanden, sondern vielmehr ein Verstoß gegen deren Ziel oder Zweck, erhebliche Missstände und Unregelmäßigkeiten in den genannten Bereichen oder darauf bezogene Verschleierungs- und versuchte Verschleierungshandlungen Auch bevorstehende Rechtsverletzungen (z.B. ein Versuch, Vorbereitungshandlungen) sind erfasst.

Erfasst sind Verletzungen von Vorschriften in einem der folgenden Bereiche:

* Öffentliches Auftragswesen,
* Finanzdienstleistungen, Finanzprodukte und Finanzmärkte sowie Verhinderung von Geldwäsche und Terrorismusfinanzierung,
* Produktsicherheit und -konformität,
* Verkehrssicherheit,
* Umweltschutz,
* Strahlenschutz und nukleare Sicherheit,
* Lebensmittel- und Futtermittelsicherheit, Tiergesundheit und Tierschutz,
* Öffentliche Gesundheit,
* Verbraucherschutz,
* Schutz der Privatsphäre und personenbezogener Daten sowie Sicherheit von Netz- und Informationssystemen,
* Verhinderung und Ahndung von Straftaten nach den §§ 302 bis 309 des Strafgesetzbuches (StGB) (verschiedene Korruptionsdelikte).

Weiters sind gemäß HSchG folgende Rechtsverletzungen erfasst:

* Rechtsverletzungen zum Nachteil der finanziellen Interessen der Union iSv Art 325 AEUV,
* Verletzungen von Binnenmarktvorschriften iSd Art 26 Abs 2 AEUV, sowie für Verletzungen von Unionsvorschriften über Wettbewerb und staatliche Beihilfen.
* Verletzungen von Binnenmarktvorschriften in Bezug auf Handlungen, die die Körperschaftsteuervorschriften verletzen oder in Bezug auf Vereinbarungen, die darauf abzielen, sich einen steuerlichen Vorteil zu verschaffen, der dem Ziel oder dem Zweck des Körperschaftsteuerrechts zuwiderläuft.

Darüber hinaus könnte je nach den Gegebenheiten des Unternehmens auch die Möglichkeit in Betracht gezogen werden, andere unerwünschte Verhaltensweisen zu melden. In solchen Fällen kann aber eine Betriebsvereinbarung oder (in betriebsratslosen Betrieben) eine Einzelzustimmung aller Mitarbeitenden erforderlich sein.

In diesem Zusammenhang könnte erwogen werden, eine Positivliste und eine Negativliste zu erstellen, aus denen hervorgeht, welche Situationen in den Anwendungsbereich der Richtline fallen und welche nicht.

Es könnte auch überlegt werden, wer gemeldet werden könnte. In der Regel handelt es sich dabei um Mitarbeiter des Unternehmens, einschließlich Geschäftsleitung, Aufsichtsrat, Wirtschaftsprüfer, Anwälte, Kunden, Berater, Lieferanten usw., sowie um sonstige Dritte, die mit dem Unternehmen in Verbindung stehen.

**4. Wie sollte das System organisiert werden?**

Es sollte überlegt werden, wie das System innerhalb des Unternehmens organisiert werden sollte. Die genaue Organisation hängt natürlich unter anderem von Standort, Struktur, Größe, Art und Branche des Unternehmens ab.

Dabei sollte auch überlegt werden, wer für den Empfang von Hinweisen zuständig ist. Oftmals besteht die Gefahr eines Interessenkonflikts, und daher ist es für ein Unternehmen oft angebracht, eine unabhängige externe Berichtsstelle zu beauftragen, die über das erforderliche Fachwissen und die Kompetenz zur Bearbeitung aller Arten von Hinweisen verfügt.

In der Regel ist es sinnvoll, innerhalb des Unternehmens ein spezielles Team oder eine Funktion auf geeigneter Ebene oder mit dem erforderlichen Hintergrund einzurichten, um mit einem externen Experten zusammenzuarbeiten, der sich mit den verschiedenen Arten der eingegangenen Hinweise befasst.

Es sollte ein Handbuch für den Umgang mit verschiedenen Arten von Hinweisen ausgearbeitet werden, damit die Hinweise optimal behandelt werden, je nachdem, von wem, worüber und über wen ein Hinweis gegeben wird.

**5. Wie können Hinweise über das Hinweisgebersystem gegeben werden?**

Zum Nutzen eines potenziellen Hinweisgebers sollte eine Hinweisgeberrichtlinie die praktischen Vorkehrungen für die Abgabe eines Hinweises über das Hinweisgebersystem detailliert beschreiben, z. B. wer die IT-Lösung bereitstellt, wie sie funktioniert, welche Sprachen gewählt werden können, ob der Hinweis anonym oder namentlich erfolgen soll und andere praktische Vorkehrungen.

Es sollte auch beschrieben werden, wie unterstützende Unterlagen vorgelegt werden können und wie die Kommunikation mit einem potenziellen Hinweisgeber erfolgt.

**6. Was sollte für Vertraulichkeit und Anonymität gelten?**

In einer Hinweisgeberrichtlinie sollten die Anforderungen an Vertraulichkeit für das System festgelegt werden. So sieht das Gesetz eine besondere Möglichkeit vor, personenbezogene Daten zu verarbeiten, wenn dies zur Bearbeitung von Hinweisen im Rahmen des Systems erforderlich ist. Dies sollte in einer Hinweisgeberrichtlinie beschrieben werden.

Unternehmen können nicht sensible Daten verarbeiten, wenn dies für die Bearbeitung von Hinweisen im Rahmen des Hinweisgebersystems erforderlich ist. Sensible personenbezogene Daten (besondere Kategorien von Daten iSd Art 9 DSGVO) dürfen nur dann verarbeitet werden, wenn die Verarbeitung im öffentlichen Interesse liegt und für die Erreichung des Zwecks des HSchG, Rechtsverletzungen zu verhindern oder zu ahnden, unbedingt erforderlich ist, das öffentliche Interesse erheblich ist und wirksame Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen getroffen werden. Informationen über Straftaten (Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen iSd Art 10 DSGVO) dürfen nur im Fall unbedingter Erforderlichkeit verarbeitet werden, was schriftlich zu dokumentieren ist.

Eine Hinweisgeberrichtlinie sollte auch beschreiben, dass die anderen regulatorischen Grundsätze der DSGVO, die weiterhin eingehalten werden müssen, auch in einer Hinweisgeber-Situation eingehalten werden. Dies gilt auch für die Verfahren, die bei etwaigen späteren Ermittlungen im Zusammenhang mit der Hinweisgebung einzuhalten sind. Eine Weitergabe ist jedoch unter bestimmten Bedingungen möglich, z.B. wenn sie zur Verhinderung von Straftaten usw. erforderlich ist.

In Österreich dürfen Unternehmen entscheiden, ob sie anonyme Meldungen zulassen möchten oder nicht. Sollten anonyme Meldungen zugelassen werden, sollten auch die entsprechenden Anforderungen festgelegt werden. Sollte eine Meldung anonym erfolgen und sollte die Identität des Hinweisgebers ohne sein Zutun bekannt werden, genießen die Hinweisgeber nach wie vor den Schutz der Vertraulichkeit.

Eine Richtlinie kann auch beinhalten, dass das Gesetz Hinweisgeber unter anderem vor Vergeltungsmaßnahmen schützt, wenn sie Sachverhalte melden, die ihnen im Zusammenhang mit ihrer Arbeit und dem Unternehmen bekannt werden.

Das Gesetz besagt, dass Hinweisgeber aufgrund ihrer Meldung keine Vergeltungsmaßnahmen wie z.B. Entlassung, Versetzung, Gehaltseinbußen, Belästigung usw. erleiden dürfen.

Hinweisgeber, die aufgrund einer Meldung Vergeltungsmaßnahmen ausgesetzt waren, haben Anspruch auf Ersatz des Vermögensschadens, eine Entschädigung für die erlittene persönliche Beeinträchtigung sowie die Wiederherstellung des rechtmäßigen Zustands.  Vergeltungsmaßnahmen, die reversibel sind (z.B. Kündigung, Entlassung, Suspendierung), sind darüber hinaus rechtsunwirksam.

Darüber hinaus sollte in einer Richtlinie festgelegt werden, wie und nach welchen Verfahren die Aufbewahrung und Löschung personenbezogener Daten erfolgt und wer der für die Datenverarbeitung verantwortliche Person in Bezug auf das Hinweisgebersystem ist.Die Bestimmungen des HSchG zu Aufbewahrungs- und Löschfristen sind zu beachten.

**7. Welche Verfahren werden in Bezug auf einen möglichen Hinweisgeber angewandt?**

Eine Richtlinie sollte eine Beschreibung der Verfahren enthalten, die bei Meldung eines Hinweisgebers gelten. Dazu gehören:

* Wie die technische Lösung aus der Sicht eines Hinweisgebers funktioniert
* Fristen für den Erhalt der Empfangsbestätigung des Hinweises
* Fristen für den Erhalt von Rückmeldung
* Fristen für eine persönliche Zusammenkunft zur Besprechung des Hinweises (sofern vom Hinweisgeber gewünscht)
* Anleitung für potenzielle Hinweisgeber über die Möglichkeit der Meldung über externe Hinweisgebersysteme

Für den unternehmensinternen Gebrauch sollte ein detailliertes Handbuch erstellt werden, in dem beschrieben wird, wie mit verschiedenen Hinweisen und Meldungen in der Zusammenarbeit zwischen der Unternehmensleitung, den zuständigen Mitarbeitern des Unternehmens und externen Sachverständigen umzugehen ist.

**8. Welche Rechte haben Personen, über die eine Meldung gemacht wurde?**

In der Regel sollten in einer Richtlinie die Rechte der gemeldeten Personen beschrieben und festgelegt werden, wie der Umgang mit diesen Mitarbeitern zu erfolgen hat.

Insbesondere ist zu beschreiben, wie die gemeldeten Personen gegen falsche Meldungen geschützt werden.

HSchG bestimmt, dass bestimmte Rechte der betroffenen Person nach DSGVO, insbesondere Recht auf Information (Art 13 und 14 DSGVO) und das Auskunftsrecht (Art 15 DSGVO) auf die von einem Hinweis betroffene natürliche Person nicht anwendbar sind. Das ist etwa dann der Fall, solange und insoweit dies zum Schutz der Identität des Whistleblowers oder um Versuche der Verhinderung, Unterlaufung oder Verschleppung von Hinweisen oder von Folgemaßnahmen aufgrund von Hinweisen zu unterbinden, erforderlich ist.

**9. Welche Rechte haben Mitarbeiter, die Untersuchungen durchführen oder daran mitwirken?**

In der Richtlinie sollten auch die Rechte von Mitarbeitern, die sich am Hinweisgebersystem beteiligen, in Bezug auf die Durchführung von Untersuchungen oder die Weitergabe von Informationen dargelegt werden, einschließlich des Schutzes vor nachteiligen Folgen für das Arbeitsverhältnis, die sich aus ihrer Beteiligung ergeben.

Für diese Mitarbeitern sind zweckentsprechende Vorkehrungen zu treffen, um ihnen eine weisungsfreie inhaltliche Erledigung der Hinweise zu ermöglichen.

**10. An wen kann man sich wenden, wenn man Zweifel am Hinweisgebersystem hat?**

In einer Richtlinie sollte eindeutig festgelegt werden, an wen man sich wenden kann, wenn man Zweifel am Hinweisgebersystem hat.

**Hinweisgeberrichtlinie für Mitarbeiter [anzupassen]**

***Zuletzt aktualisiert [Datum]***

**Hintergrund und Zweck**

[NAME DER ORGANISATION] (im Folgenden „die Organisation“) stellt seinen Mitarbeitern ein Hinweisgebersystem zur Verfügung.

Ein Hinweisgebersystem ist ein unabhängiger Kanal, über den Mitarbeiter Verdachtsfälle oder konkrete Kenntnisse über Verstöße gegen bestimmte Vorschriften, Vorschriften, deren Einhaltung im öffentlichen Interesse liegt, in der Organisation melden können.

Das Hinweisgebersystem sollte als Ergänzung zu Ihrer Möglichkeit als Mitarbeiter gesehen werden, sich an eine Führungskraft zu wenden, wenn Sie Missstände oder unbefriedigende Bedingungen feststellen, auf die Sie aufmerksam machen wollen.

In dieser Hinweisgeberrichtlinie wird genauer beschrieben, wann Sie als Mitarbeiter das Hinweisgebersystem nutzen können, was Sie melden können, wie eine Meldung behandelt wird, welche Rechte die Beteiligten haben usw.

Inhalt

[1. Wer kann über das Hinweisgebersystem Meldung erstatten? 9](#_Toc149647522)

[2. Wer kann gemeldet werden? 9](#_Toc149647523)

[3. Was kann gemeldet werden? 9](#_Toc149647524)

[4. Wie wird gemeldet? 11](#_Toc149647525)

[5. Wer erhält die Meldung? 11](#_Toc149647526)

[6. Verfahren bei Erhalt einer Meldung 12](#_Toc149647527)

[7. Prüfung einer Meldung 12](#_Toc149647528)

[8. Geheimhaltungspflicht und Weitergabe von Informationen 13](#_Toc149647529)

[9. Anonymität, Schutz vor Vergeltungsmaßnahmen und andere Rechte eines Hinweisgebers 13](#_Toc149647530)

[10. Laufende Kommunikation und Fristen 14](#_Toc149647531)

[11. Vertraulichkeit 14](#_Toc149647532)

[12. Registrierung von Meldungen 15](#_Toc149647533)

[13. Rechte der Betroffenen 15](#_Toc149647534)

[14. Externes Hinweisgebersystem 16](#_Toc149647535)

[15. Das Recht des Hinweisgebers auf Veröffentlichung 16](#_Toc149647536)

Zusätzlich zu diesen Informationen hat die Organisation eine Datenschutzerklärung entwickelt, die sich speziell mit der Verarbeitung personenbezogener Daten im Zusammenhang mit dem Hinweisgebersystem befasst. Sie ist hier zu finden: [Link einfügen].

# 1. Wer kann über das Hinweisgebersystem Meldung erstatten?

Das Hinweisgebersystem richtet sich an alle Mitarbeiter der Organisation. Dies gilt auch für Personen mit einem befristeten Arbeitsvertrag oder für Leiharbeitnehmer.

*Beispiele für weitere Zielgruppen, die Sie erweitern können: [* Aufsichtsratsmitglieder, Aktionäre, Verwaltungsratsmitglieder, Berater, Lieferanten, Auftragnehmer, Wirtschaftsprüfer usw.].

# 2. Wer kann gemeldet werden?

Das Hinweisgebersystem ist für die Meldung von Informationen und Fakten über Gesetzesverstöße und schwerwiegendes Fehlverhalten von Mitarbeitern oder anderen mit der Organisation verbundenen Personen gedacht. Andere Personen können z. B. Aufsichtsratsmitglieder, Aktionäre, Verwaltungsratsmitglieder, Berater, Lieferanten, Auftragnehmer, Wirtschaftsprüfer usw. sein.

# 3. Was kann gemeldet werden?

Der Anwendungsbereich des HSchG umfasst Meldungen über Verstöße gegen eine Reihe von Vorschriften, deren Einhaltung im öffentlichen Interesse liegt. Unter einer Rechtsverletzung ist nicht nur ein Rechtsverstoß gegen die unterstehenden Vorschriften bzw. Rechtsbereiche verstanden, sondern vielmehr ein Verstoß gegen deren Ziel oder Zweck, erhebliche Missstände und Unregelmäßigkeiten in den genannten Bereichen oder darauf bezogene Verschleierungs- und versuchte Verschleierungshandlungen. Auch bevorstehende Rechtsverletzungen (z.B. ein Versuch, Vorbereitungshandlungen) sind erfasst.

Erfasst sind Verletzungen von Vorschriften in einem der folgenden Bereiche:

* Öffentliches Auftragswesen,
* Finanzdienstleistungen, Finanzprodukte und Finanzmärkte sowie Verhinderung von Geldwäsche und Terrorismusfinanzierung,
* Produktsicherheit und -konformität,
* Verkehrssicherheit,
* Umweltschutz,
* Strahlenschutz und nukleare Sicherheit,
* Lebensmittel- und Futtermittelsicherheit, Tiergesundheit und Tierschutz,
* Öffentliche Gesundheit,
* Verbraucherschutz,
* Schutz der Privatsphäre und personenbezogener Daten sowie Sicherheit von Netz- und Informationssystemen,
* Verhinderung und Ahndung von Straftaten nach den §§ 302 bis 309 des Strafgesetzbuches (StGB) (verschiedene Korruptionsdelikte).

Weiters sind gemäß HSchG folgende Rechtsverletzungen erfasst:

* Rechtsverletzungen zum Nachteil der finanziellen Interessen der Union iSv Art 325 AEUV,
* Verletzungen von Binnenmarktvorschriften iSd Art 26 Abs 2 AEUV, sowie für Verletzungen von Unionsvorschriften über Wettbewerb und staatliche Beihilfen.
* Verletzungen von Binnenmarktvorschriften in Bezug auf Handlungen, die die Körperschaftsteuervorschriften verletzen oder in Bezug auf Vereinbarungen, die darauf abzielen, sich einen steuerlichen Vorteil zu verschaffen, der dem Ziel oder dem Zweck des Körperschaftsteuerrechts zuwiderläuft.

[OPTIONAL, NUR WENN DAS UNTERNEHMEN EINE AUSWEITUNG DES SACHLICHEN ANWENDUNGSBEREICHS WÜNSCHT: Neben den oben erwähnten Rechtsverletzungen, die zwingend vom Gesetz vorgeschrieben sind, kann unser Whistleblower-System ferner für Meldung folgender Verletzungen verwendet werden:

* [VOM UNTERNEHMEN ANZUPASSEN];
* [VOM UNTERNEHMEN ANZUPASSEN];
* [VOM UNTERNEHMEN ANZUPASSEN].

Das Hinweisgebersystem gilt nicht für Informationen, die beispielsweise Verstöße gegen interne Richtlinien über krankheitsbedingte Fehlzeiten, Rauchen, Alkohol, Kleidung, private Nutzung von Büromaterial oder Verstöße gegen Nebenbestimmungen wie die Nichteinhaltung von Dokumentationspflichten betreffen.

Das Hinweisgebersystem kann nicht genutzt werden, um Meldungen über Ihre eigene Arbeitssituation zu machen, einschließlich Konflikten zwischen Arbeitnehmern oder Problemen in den Arbeitsbeziehungen oder Angelegenheiten Probleme in den Arbeitsbeziehungen, die eine Gefahr die öffentliche Gesundheit oder Datenschutzverletzungen darstellen, sind jedoch abgedeckt).

Informationen über Verstöße oder Vorfälle, die vor der Einrichtung des Hinweisgebersystems durch die Organisation stattgefunden haben, können gemeldet werden.

# 4. Wie wird gemeldet?

Die Mitarbeiter der Organisation können sich schriftlich und anonym über eine digitale Lösung melden, die von einem externen Anbieter verwaltet wird.

Einen Link zum unserem Hinweisgebersystem finden Sie hier: [LINK EINFÜGEN].

Erfahren Sie mehr über das Meldeverfahren: [Link zur „Anleitung zur Nutzung des Hinweisgebersystems – Whistleblower“ einfügen welches im Speak Up Universe aufliegt].

# 5. Wer erhält die Meldung?

Informationen, die Gegenstand einer Meldung sind, gehen beim Whistleblower Partners Response Team ein, das Meldungen bearbeitet, die über das Hinweisgebersystem der Organisation eingehen. Das Whistleblower Partners Response Team (im Folgenden „der Empfänger“) ist ein externer und unabhängiger Berater. Wenn der Empfänger eine Meldung erhalten hat:

* prüft der Empfänger die Meldung, einschließlich dahingehend, über welche Ebene im Unternehmen eine Meldung gemacht wird,
* bestätigt der Empfänger dem Hinweisgeber den Erhalt der Meldung,

*Je nach der gewählten Organisation des Hinweisgebersystems anzupassen – den gesamten Abschnitt a. oder b. streichen, je nachdem, welcher Teil nicht relevant ist*

*(Von der Screening-Vereinbarung des Whistleblower Partners Response Teams abgedeckt):*

* a. [gibt der Empfänger den Fall an die zuständige Kontaktperson in der Organisation frei, je nachdem, über wen berichtet wird.

Bevor der Empfänger die Meldung an die zuständige Kontaktperson in der Organisation freigibt, muss er sich vergewissern, dass die Meldung die Kontaktperson nicht betrifft und dass die Kontaktperson nicht in einen Interessenkonflikt im Zusammenhang mit der Bearbeitung der Meldung gerät.

Ist dies der Fall, wird die Meldung an eine andere Kontaktperson der Organisation weitergeleitet, die der Empfänger für die betreffende Meldung für befähigt hält].

*(Nicht von der Screening-Vereinbarung des Whistleblower Partners Response Teams abgedeckt – erfordert eine separate Vereinbarung mit Whistleblower Partners. Bei Bedarf Kontakt aufnehmen:*

* *b.* [bearbeitet der Empfänger den Fall.]]

Wir haben uns für diese Lösung entschieden, weil wir die größtmögliche Sicherheit für die Mitarbeiter der Organisation im Zusammenhang mit einer Meldung schaffen wollen.

# 6. Verfahren bei Erhalt einer Meldung

Bei Eingang einer Meldung wird geprüft, ob die Meldung in den Bereich des Hinweisgebersystems fällt, vgl. Abschnitt 3 und ob die Meldung stichhaltig ist.

Wenn die Meldung nicht in den Anwendungsbereich des Hinweisgebersystems fällt oder wenn aus der Meldung dem keine Anhaltspunkte für ihre Stichhaltigkeit hervorgehen (insbesondere wenn sie offenkundig falsch ist), wird die Meldung zurückgewiesen und kann daher nicht im Rahmen des Hinweisgebersystems bearbeitet werden.

[OPTIONAL:] Fällt eine Meldung nicht in den Geltungsbereich des Hinweisgebersystems, erhält der Hinweisgeber eine Anleitung, an wen er sich stattdessen innerhalb der Organisation in der betreffenden Angelegenheit wenden kann.

# 7. Prüfung einer Meldung

*Wenn Lösung a. in Punkt 5 gewählt wurde, „die zuständige Kontaktperson in der Organisation“ einfügen. Wenn Lösung b. in Punkt 5 gewählt wurde, „Empfänger“ einfügen:*

Sobald [einfügen] die Meldung erhalten hat und diese nicht zurückzuweisen ist, muss [einfügen] eine gründliche Weiterverfolgung durchführen, die je nach den Umständen der Meldung Folgendes umfassen kann:

* Einleitung einer internen Untersuchung, um die Richtigkeit der Informationen in einer Meldung zu bestätigen oder zu widerlegen
* Unterrichtung der Geschäftsleitung oder des Aufsichtsrats der Organisation
* Anzeige an die Polizei oder die zuständige Behörde
* Entscheidung über Reaktionen, z. B. arbeitsrechtliche oder vertragliche
* Abschluss des Falls

Es liegt in der Verantwortung von [einfügen], zu verlangen, dass die Meldung gründlich untersucht wird, und in diesem Zusammenhang die erforderlichen Maßnahmen zu ergreifen.

Danach hat [einfügen] einen Bericht für die Geschäftsleitung zu erstellen, die über Reaktionen entscheidet – sei es eine Anzeige bei den Behörden oder andere arbeitsrechtliche oder vertragsrechtliche Maßnahmen.

Schließlich muss dem Hinweisgeber innerhalb der im Hinweisgebersystem festgelegten Frist von 3 Monaten eine Rückmeldung gegeben werden, vgl. weiter unten Abschnitt 10.

# 8. Geheimhaltungspflicht und Weitergabe von Informationen

Nur der Empfänger *Behalten, wenn Lösung a. unter Punkt 5 gewählt wurde:* [und die zuständige Kontaktperson in der Organisation] hat Zugang zu den Informationen in einer Meldung. Meldungen unterliegen einer besonderen Geheimhaltungspflicht, der Inhalt darf daher nicht mit anderen geteilt werden.

Die besondere Geheimhaltungspflicht gilt für die Identität des Hinweisgebers und der vom Hinweis betroffenen Person, einschließlich aller Informationen, aus denen deren Identitäten unmittelbar oder mittelbar abgeleitet werden können. Diese Informationen dürfen über den Kreis der mit der Meldung unmittelbar befassten Personen nicht offenbart werden – dies schließt auch die Personen ein, die mit allenfalls nachfolgenden unternehmensinternen Untersuchungen befasst sind. Erstatten Sie Ihre Meldung anonym und sollte Ihre Identität doch bekannt werden, wird sie ebenfalls geschützt.

Bitte beachten Sie aber, dass in bestimmten gesetzlich geregelten Fällen Ihre Identität ausnahmsweise offengelegt werden kann. Das kann passieren, wenn eine Verwaltungsbehörde, ein Gericht oder die Staatsanwaltschaft die Offenlegung Ihrer Identität im Rahmen des verwaltungsbehördlichen oder gerichtlichen Verfahrens oder eines Ermittlungsverfahrens für unerlässlich und im Hinblick auf Ihre Gefährdung im Hinblick auf die Stichhaltigkeit und Schwere der erhobenen Vorwürfe für verhältnismäßig hält. Sie werden in der Regel im Vorhinein davon informiert, es sei denn, es würde das Verfahren gefährden.

# 9. Anonymität, Schutz vor Vergeltungsmaßnahmen und andere Rechte eines Hinweisgebers

Die gewählte IT-Lösung bietet die Möglichkeit, anonym mit dem Empfänger der Meldungen zu kommunizieren.

Allerdings kann eine Meldung so beschaffen sein, dass es schwierig sein kann, eine Angelegenheit vollständig zu untersuchen, ohne dass sich der Hinweisgeber dazu entschließt, seine Identität in der Meldung preiszugeben. Es ist die eigene Entscheidung des Hinweisgebers, ob er dies tut.

Ob der Hinweisgeber die Meldung unter Bekanntgabe Ihrer Identität oder anonym erstattet, wird der Hinweisgeber vor Vergeltungsmaßnahmen, Drohungen oder Versuchen von Vergeltungsmaßnahmen geschützt, die aufgrund einer Meldung des Hinweisgebers erfolgen. Unter Vergeltungsmaßnahmen ist jede Art von nachteiliger Behandlung oder nachteiliger Folge zu verstehen, die als Reaktion auf eine Meldung erfolgt. Dazu können Suspendierung, Kündigung, Entlassung, Herabstufung oder Nichtbeförderung, Übertragung von Aufgaben, Versetzung, Gehaltskürzung, Disziplinarmaßnahmen, Nötigung, Einschüchterung, Belästigung, Diskriminierung usw. gehören.

Die Nennung von Namen in einer Hinweisgeber-Meldung kann schwerwiegende Folgen haben, weshalb der Hinweisgeber verpflichtet ist, den Inhalt seiner Meldung in gutem Glauben zu verfassen. Eine Kündigung falsche Meldung, beispielsweise aus Gründen der Belästigung, kann schwerwiegende Folgen für die Meldende haben, insbesondere beträchtliche Verwaltungsstrafen, arbeitsrechtliche Folgen bis hin zur Entlassung und Schadenersatzansprüche der genannten Person. Auch strafrechtliche Folgen sind möglich.

Im Gegensatz dazu kann ein Hinweisgeber nicht für die Weitergabe vertraulicher Informationen haftbar gemacht werden, wenn er *berechtigte* Gründe zu der Annahme hatte, dass die in Form einer Meldung weitergegebenen Informationen zum Zeitpunkt der Meldung korrekt waren und dass der Hinweis notwendig war, um eine von HSchG gedeckte Rechtsverletzung aufzudecken oder zu verhindern.

Vor diesem Hintergrund ist der Hinweisgeber auch nicht dafür verantwortlich, sich Zugang zu den gemeldeten Informationen verschafft zu haben. Dies setzt jedoch voraus, dass die Handlung selbst keinen Straftatbestand erfüllt, wie z. B. ein Einbruchsdiebstahl.

# 10. Laufende Kommunikation und Fristen

Der Empfänger wickelt die Kommunikation mit dem Hinweisgeber über das Hinweisgebersystem ab. Ein Hinweisgeber muss innerhalb von 7 Tagen nach Einreichung seiner Meldung eine Empfangsbestätigung für seine Meldung erhalten.

Darüber hinaus muss der Hinweisgeber so schnell wie möglich und innerhalb von drei Monaten nach der Empfangsbestätigung eine Rückmeldung erhalten, was bedeutet, dass er – soweit möglich – darüber informiert werden muss, welche Folgemaßnahmen die interne Stelle ergriffen hat oder zu ergreifen beabsichtigt oder aus welchen Gründen die interne Stelle den Hinweis nicht weiterverfolgt. Im Rahmen der Rückmeldung wird es Informationen geben, die nicht an den Hinweisgeber weitergegeben werden dürfen, z. B. aufgrund gesetzlicher Geheimhaltungspflichten, Bestimmungen zu personenbezogenen Daten usw.

Der Hinweisgeber hat die Möglichkeit, um eine Zusammenkunft zur Besprechung des Hinweises mit [einfügen] zu ersuchen, die binnen 14 Tagen stattfinden wird und über eine Videokonferenz abgehalten wird.

# 11. Vertraulichkeit

Das Hinweisgebersystem ist so konzipiert und wird so verwaltet, dass die Vertraulichkeit der Identität des Hinweisgebers und der vom Hinweis betroffenen Personengewährleistet ist.

Das zur Abwicklung des Hinweisgebersystems eingesetzte IT-System unterliegt einer Reihe strenger Sicherheitsanforderungen, die unter anderem Anonymität und Vertraulichkeit gewährleisten. Das bedeutet, dass die Person, die eine Meldung über das Hinweisgebersystem abgibt, auf Wunsch anonym ist und bleibt. Dies bedeutet auch, dass das System keine IP-Adressen protokolliert, dass Metadaten aus allen hochgeladenen Dateien entfernt werden und die gesamte Datenübertragung und Speicherung von Daten verschlüsselt ist.

Der Empfänger *Behalten, wenn Lösung a. in Punkt 5 gewählt wurde:* [und die zuständige Kontaktperson in der Organisation] unterliegt der Geheimhaltungspflicht und der Zugang zu allen Informationen im Zusammenhang mit einer Meldung ist eingeschränkt.

# 12. Registrierung von Meldungen

Erhaltene Meldungen, einschließlich der in einer Meldung enthaltenen Dokumente, müssen registriert (systematisch gespeichert) werden, um sicherzustellen, dass die Meldungen zugänglich sind und sie gegebenenfalls als Beweismittel in einem möglichen späteren Gerichtsverfahren verwendet werden können. Gleichzeitig bietet die Registrierung auch die Gewissheit, dass etwaige Meldungen über denselben Sachverhalt aufgedeckt werden und zu weiteren Ermittlungen in einer Angelegenheit führen können. Diese Registrierung erfolgt im Hinweisgebersystem.

Nach HSchG sind die Unternehmen verpflichtet, die Dokumentation der Whistleblowing-Meldung für einen Zeitraum von fünf Jahren ab der letztmaligen Verarbeitung oder Übermittlung und darüber hinaus so lange aufzubewahren, als es zur Durchführung bereits eingeleiteter verwaltungsbehördlicher oder gerichtlicher Verfahren oder eines Ermittlungsverfahrens nach der Strafprozessordnung erforderlich ist. Nach Entfall der Aufbewahrungspflicht sind personenbezogene Daten zu löschen. Tatsächlich durchgeführte Verarbeitungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen sind zu protokollieren. Protokolldaten über diese Vorgänge sind ab ihrer letztmaligen Verarbeitung oder Übermittlung bis drei Jahre nach Entfall der Aufbewahrungspflicht der Dokumentation der Whistleblowing-Meldung aufzubewahren.

Die Meldungen werden für einen Zeitraum von fünf Jahren ab der letztmaligen Verarbeitung oder Übermittlung und darüber hinaus so lange aufbewahrt, als es zur Durchführung bereits eingeleiteter verwaltungsbehördlicher oder gerichtlicher Verfahren oder eines Ermittlungsverfahrens nach der Strafprozessordnung erforderlich ist. Nach Entfall der Aufbewahrungspflicht werden sie gelöscht. Alle Abfragen, Übermittlungen und Änderungen der Meldungen werden protokolliert. Protokolldaten über diese Vorgänge werden ab ihrer letztmaligen Verarbeitung oder Übermittlung bis drei Jahre nach Entfall der Aufbewahrungspflicht der Dokumentation der Whistleblowing-Meldung aufbewahrt. Die Grundsätze der Aufbewahrung sind in der Datenschutzerklärung der Organisation für das Hinweisgebersystem aufgeführt.

# 13. Rechte der Betroffenen

Die Person oder Personen, die in einer Meldung erwähnt werden, haben das Recht, dass ihre Identität im Zusammenhang mit der Bearbeitung des Falles geschützt wird. Darüber hinaus müssen die betroffenen Personen Zugang zu einer wirksamen Verteidigung haben, was unter anderem durch die Registrierung einer Meldung erfolgt, die eine Dokumentation der genannten Fakten gewährleistet.

Betroffene Personen haben zudem eine Reihe von Rechten im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten. Die Geheimhaltungspflicht der Organisation und das Interesse an der Feststellung und Ahndung von Rechtsverletzungen bringt jedoch Einschränkungen in Bezug auf die Frage mit sich, wann betroffene Personen über die Verarbeitung von Daten informiert werden müssen und ob sie ein Recht auf Auskunft, Löschung usw. geltend machen können.

Hervorzuheben ist, dass Personen, die wissentlich falsche Meldungen erstatten, keinen Schutz des HSchG genießen. Derartige Handlungen sind mit einer Verwaltungsstrafe von bis zu EUR 20.000 (im Wiederholungsfall: EUR 40.000) bedroht. Allfällige Ansprüche des Betroffenen gegen solche Personen (wie z.B. Schadenersatzansprüche) bleiben unberührt.

# 14. Externes Hinweisgebersystem

Gemäß der Hinweisgeberrichtlinie ist die Organisation dafür verantwortlich, ihre Mitarbeiter über die folgenden externen Hinweisgebersysteme zu informieren, die als Alternative zum internen System der Organisation genutzt werden können:

Beim Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung wurde eine externe Meldestelle eingerichtet, die unter diesem Link zugänglich ist: [www.bkms-system.net/BAK](http://www.bkms-system.net/BAK). Diese Meldestelle ist für alle vom HSchG gedeckten Rechtsverletzungen zuständig, soweit nicht eine andere Behörde oder Stelle eine Spezialzuständigkeit hat (z.B. Finanzmarktaufsicht, Geldwäschemeldestelle). In solchen Fällen wird die Meldung an die zuständige Behörde oder Stelle weitergeleitet, wovon der Hinweisgeber verständigt wird.

Weitere Informationen darüber, wie Sie Meldungen an das Hinweisgebersystem machen können, finden Sie bei der entsprechenden Homepage des Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung hier: www.bkms-system.net/BAK.

Die Mitarbeiter der Organisation haben die Wahl, ob sie sich an das interne Hinweisgebersystem der Organisation oder an ein externes System wenden wollen. Die Organisation ermutigt jedoch ihre Mitarbeiter, das organisationseigene Hinweisgebersystem zu nutzen, wenn der Mitarbeiter der Ansicht ist, dass der mutmaßliche Verstoß intern wirksam behandelt werden kann und kein Risiko von Vergeltungsmaßnahmen besteht.

# 15. Das Recht des Hinweisgebers auf Veröffentlichung

Das HSchG und der Schutz, den es Hinweisgebern gewährt, gelten auch für die Veröffentlichung von Informationen, die in einer Meldung erwähnt werden.

Voraussetzung ist jedoch, dass der Hinweisgeber entweder:

* vor der Veröffentlichung eine Meldung an das interne Hinweisgebersystem der Organisation oder an ein externes Hinweisgebersystem gemacht hat, ohne dass daraufhin geeignete Folgemaßnahmen innerhalb vorgeschriebener Fristen ergriffen wurden, oder
* dass er hinreichende Gründe für die Annahme hat, dass der betreffende Verstoß eine unmittelbare oder offensichtliche Gefahr für das öffentliche Interesse darstellt; oder
* dass er berechtigte Gründe für die Annahme hat, dass eine Meldung an das externe Hinweisgebersystem das Risiko von Vergeltungsmaßnahmen mit sich bringen würde oder dass der Fall aufgrund der besonderen Umstände des Falles nicht wirksam bearbeitet werden würde.