BVMed-Akademie

04.11.2026

Struktur und Aufbau einer Compliance-Organisation für MedTech Unternehmen

Referenten:

RAin Christiane Döring, Ahrensburg

RA Prof. Dr. Hendrik Schneider, Wiesbaden

Agenda

I. Compliance-Risikoanalyse (CRO)

II. Hinweisgebersystem

1. Gesetzliche Vorgaben
2. Inhouse vs. Outsourcing
3. Hinweiskanäle und digitale Lösungen
4. Schutz von Hinweisgeber und Beschuldigten
5. Anonyme und vertrauliche Hinweise
6. Einhaltung der gesetzlichen Vorgaben im Umgang mit Hinweisen

III. Grundelemente eines Compliance-Management-Systems (CMS)
IV. Compliance-Audit
V. Interne Untersuchung
VI. Rollenspiel
VII. Haftungsprävention

See something, say something

Das Hinweisgebersystem ist das Ohr Ihres Compliance-Management-Systems



Dazu muss aber der Gehörgang frei sein! Das bedeutet, das Hinweisgebersystem muss bekannt sein im Unternehmen, die Hinweisgeber müssen zur internen Meldestelle Vertrauen haben und es muss die Vertraulichkeit zu 100 % gewährleistet sein.

- Fakt ist: Hinweisgebersysteme werden kaum genutzt. Sie tragen daher nicht dazu bei, dass das Unternehmen vor der Staatsanwaltschaft von einer Verfehlung weiß.
- Unsere Empfehlung ist: Akzeptanzsicherung betreiben, Hinweisgebersystem populär machen, Ängsten vor dem Hinweisgebersystem abbauen. Schulungen anbieten, auch beim Onboarding.
- Gegenbeispiel: In einem Unternehmen, in dem wir die Interne Meldestelle betreiben, wusste der neue Compliance-Officer nichts von der Whistleblowing-Hotline.

Warum wenden sich Mitarbeitende an die Meldestelle?

„Bitte behandeln Sie mein Anliegen streng vertraulich, ich traue bei meinem Arbeitgeber niemanden mehr.“

„Ich hatte mit dem Kollegen was, aber jetzt stellt er mir nach. Ich weiß nicht, wie ich damit umgehen soll.“

„Bitte behandeln Sie mein Anliegen streng vertraulich, ich traue bei meinem Arbeitgeber niemanden mehr.“

… Aber auch

„Mein Ladekabel vom Handy ist weg.“

…. und

„Ich habe XYZ mitbekommen und wende mich an Sie, weil ich wissen will, ob das rechtmäßig ist.“

1. Gesetzliche Vorgaben

Überblick über das Hinweisgeberschutzgesetz

16.12.2019
EU-Hinweisgeber-richtlinie tritt in Kraft

Europäische Kommission

17.12.2021
Umsetzungsfrist

27.07.2022
Regierungsentwurf HinSchG-E

Die Bundesregierung

14.12.2022
Änderungsvorschläge des Rechtsausschusses des Bundestages

16.12.2022
Verabschiedung durch den Bundestag



02.07.2023
Inkrafttreten des HinSchG

Wer braucht ein Hinweisgebersystem?

Beachte: „**Beschäftigungsgeber**“ gem. § 3 Abs. 9 HinschG:

- Der Arbeitgeber des Beschäftigten als rechtlich selbstständige Einheit (z.B. GmbH, gGmbH, Einzelunternehmen),
- Maßgeblich ist die Beschäftigtenzahl des einzelnen Rechtsträgers, nicht die des gesamten Konzerns oder Unternehmensverbunds,
- Ab 50 Mitarbeiter benötigen Sie ein Hinweisgebersystem.

Beschäftigtenbegriff gem. § 3 Abs. 8 HinSchG

- Alle (auch ehemalige) Arbeitnehmer und Auszubildenden,
- unabhängig vom Umfang der Beschäftigung (d.h. auch geringfügig Beschäftigte).

Wer ist nach dem HinSchG Hinweisgeber?

Alle natürlichen Personen, die im beruflichen Zusammenhang Informationen über Verstöße erlangen:

- Aus Arbeits- und Dienstverhältnissen,
- Organmitglieder, z.B. Aufsichtsratsmitglieder,
- Bewerber,
- ehemals Beschäftigte,
- Lieferanten und Dienstleister,
- Vertreter von Arbeitnehmervertretungen.

Aber: Sie müssen Ihr Hinweisgebersystem nicht für außenstehende Personen, die nicht unter den Beschäftigungsbegriff fallen, öffnen.
Denn: „*Beschäftigungsgeber haben dafür zu sorgen, dass bei ihnen mindestens eine Stelle für interne Meldungen eingerichtet ist und betrieben wird, an die sich Beschäftigte wenden können (interne Meldestelle).“* § 12 Abs. 1 HinSchG

Was kann gemeldet werden? Sachlicher Anwendungsbereich

Rechtsgrundlage: § 2 HinSchG



Verstöße gegen Strafvorschriften (z.B. Betrug, Untreue, Korruption, Diebstahl),



Verstöße gegen bußgeldbewehrte Vorschriften, soweit die verletzte Vorschrift dem Schutz von Leben, Leib oder Gesundheit oder dem Schutz der Rechte von Beschäftigten oder ihrer Vertretungsorgane dient (z.B. Arbeitsschutzgesetz, Mindestlohngesetz oder Arbeitnehmerüberlassungsgesetz),



Verstöße gegen Rechtsvorschriften des Bundes und der Länder sowie unmittelbar geltende Rechtsakte der Europäischen Union, z.B. betreffend Datenschutz, Geldwäsche, Terrorismusfinanzierung, Produktsicherheit, etc.



Nicht erfasst vom Schutzbereich des § 2 HinSchG sind z.B.:

- Hinweise über privates Fehlverhalten
- Arbeits- oder tarifrechtliche Fragen

2. Inhouse vs. Outsourcing

Wer kann Meldestelle sein?

- Sowohl Einrichtung einer Stelle im Unternehmen (z.B. in Angliederung an Compliance-Abteilung oder Beauftragung einer Einzelperson) als auch Outsourcing möglich.

- Achtung: Bei Meldekanal, der zu Inhouse-Stelle führt, muss besonders darauf geachtet werden, dass **Vertraulichkeit** gewährleistet ist:

  Beispiel: E-Mail-Adresse muss unabhängig von sonstigem E-Mail-Verkehr des Unternehmens sein, damit IT-Abteilung keinen Zugriff nehmen kann.

Achtung: Der Mitarbeiter der internen Meldestelle kann im Strafverfahren Zeugenstatus haben und zur Aussage verpflichtet werden. Nichts ist sicher vor dem Zugriff der Staatsanwaltschaft.

Inhouse vs. Outsourcing

INHOUSE

VORTEILE	NACHTEILE
geringe Berührungs-ängste	Interessen-konflikte (Person muss intern ermitteln, soll Identität des HWG aber geheim halten)
interne Abläufe bekannt	Kein Zeugnisverweigerungs recht

OUTSOURCING

VORTEILE	NACHTEILE
gute Absicherung der Vertraulichkeit und der Unabhängigkeit	steht außerhalb der Organisation, weniger vertraut mit Unternehmen
Zeugnisver-weigerungsrecht bei Berufsgeheimnisträge rn	ggf. bestehen Berührungsängste seitens der MA

Kosten: Nach unserer Erfahrung kein Unterschied, sofern bei Outsourcing Stand-By nicht vergütet wird.

Inhouse vs. Outsourcing

Outsourcing ist mitbestimmungspflichtig: LAG Schleswig-Holstein, Beschluss vom 08.07.2025, Az.: 2 TaBV 16/24:

- Das Unternehmen hatte die Meldestelle bei einer Rechtsanwaltskanzlei eingerichtet und die Beschäftigten per Aushang darauf aufmerksam gemacht, dass dort Missstände wie Straftaten oder Verstöße gegen arbeitsrechtliche Vorschriften gemeldet werden können. Eine Beteiligung des Betriebsrates unterblieb.
- Das Arbeitsgericht hatte dem Arbeitgeber untersagt die Meldestelle zu betreiben. Die Beschwerde des Arbeitgebers blieb erfolglos.
- Nach LAG ergibt sich die Mitbestimmungspflicht aus § 87 Abs. 1 Nr. 1 BetrVG. Die Ordnung des Betriebes sei betroffen. Die Arbeitnehmer seien aufgefordert, sich Gedanken zu machen, ob ein meldepflichtiger Verstoß vorliege. Der vorgesehene Meldeweg betreffe das Verhalten der Arbeitnehmer untereinander und somit die Ordnung des Betriebes.
- Daran ändere sich nichts, wenn die Nutzung der internen Meldestelle lediglich ein unverbindliches Angebot sei. Das Mitbestimmungsrecht setze nicht voraus, das verbindliche Regeln geschaffen werden.

Inhouse vs. Outsourcing am Beispiel des digitalen Systems

- Alle Systeme arbeiten mit einem Zugangslink
- Es wird festgelegt, bei wem der Kanal endet, wer den Hinweis entgegennimmt und bearbeitet
- Gem. § 15 HinSchG muss der Beauftragte über die erforderliche Fachkunde verfügen

INHOUSE		**OUTSOURCING**
Einzelperson	**Abteilung**	**Dritter**
z.B. Compliance-Beauftragter, BR-Vorsitzender, DS-Beauftragter	z.B. Recht & Compliance	z.B. Ombudsperson, Anwaltskanzlei

Vorteil des digitalen Systems: Software wird von Dritten bereitgestellt und der Zugang nur der / dem Beauftragten ermöglicht. So ist Vertraulichkeit auch bei Inhouse-Lösung gewährleistet.

3. Hinweiskanäle und digitale Lösungen

Hinweiskanäle

Interne Hinweiskanäle müssen:



mündliche Hinweise, z.B.:

- Telefon,
- Sprachübermittlung,
- persönliche Zusammenkunft (selten),

oder



Hinweise in **Textform**,

- per E-Mail oder über digitales System,
- als Brief,
- als Fax.

ermöglichen.

→Möglichkeit der persönlichen Zusammenkunft (auf Anfrage des Hinweisgebers) muss immer gegeben sein.

Digitale Systeme

- Vielfältiges Angebot von digitalen Systemen am Markt: Hintbox, EQS Integrity Line, Vispato, Osapiens, etc.

- DIN ISO 37002:2022-03 Hinweismanagementsysteme – Leitlinien beziehen sich auf die digitalen Anwendungen als „gebräuchliche Methode für die Entgegennahme von Meldungen“.

- Vorteile des digitalen Systems sind:
  - die wechselseitige abgesicherte anonyme oder vertrauliche Kommunikation vereinfachen,
  - dem Hinweisgeber die Möglichkeit bieten, Anhänge hochzuladen,
  - in mehreren Sprachen verfügbar sein, falls relevant.

- Nachteile:
  - Im Vergleich zu direktem Kontakt zu einer Person (Gespräch, Telefonhotline) kann aber der Aufbau von Vertrauen seitens der hinweisgebenden Person schwieriger sein,
  - Es ist fraglich, ob sich der Hinweisgeber nochmal in das System einwählt, um eine Rückfrage zu beantworten. Die Hürde ist höher als bei der E-Mail oder dem Telefon, weil man sich ein komplexes Passwort auswählen muss, merken muss, eingeben muss… Viele Chancen des Bouncing-Out.
  - Der Betriebsrat muss einbezogen werden.

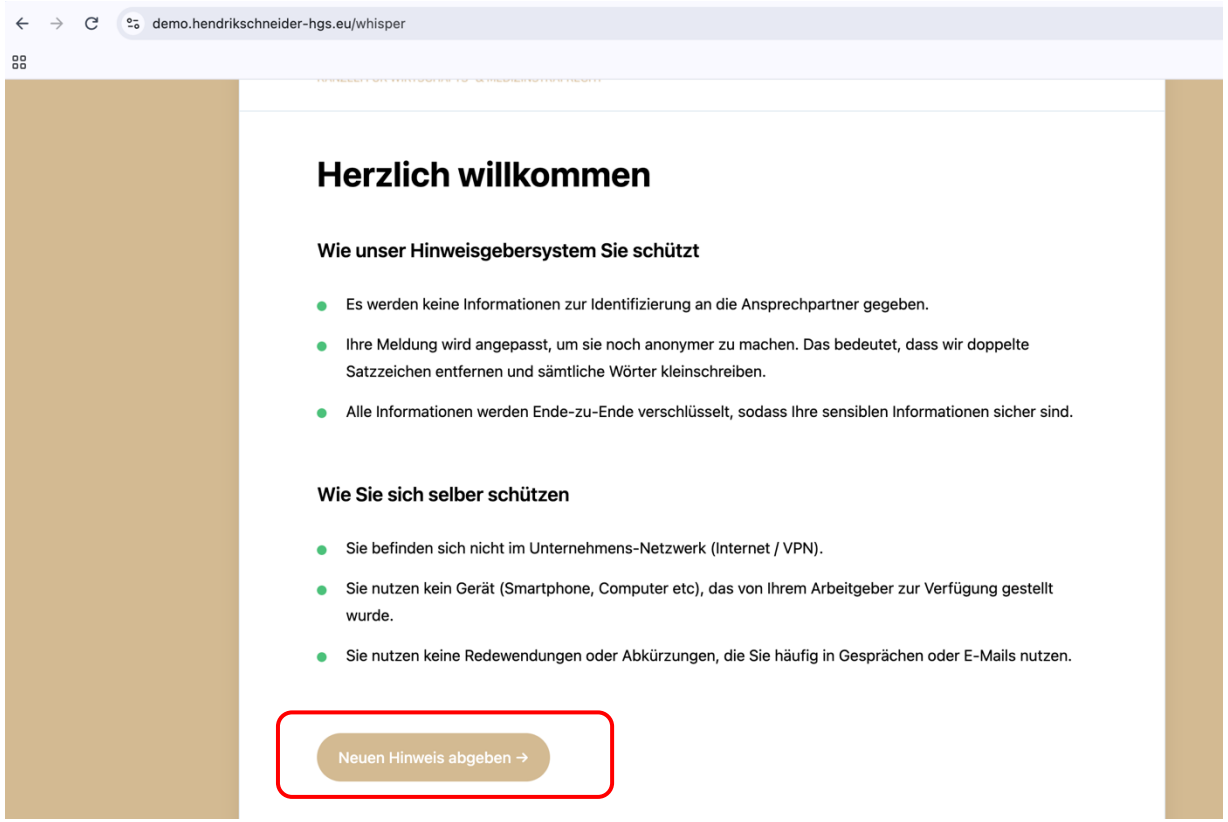
Unsere Erfahrungen aus der Praxis mit unserem System Vispato: Einige hinweisgebende Personen sehen das digitale Portal als erste Kontaktmöglichkeit, wollen aber im Anschluss gerne ein persönliches Gespräch, zumindest am Telefon führen.

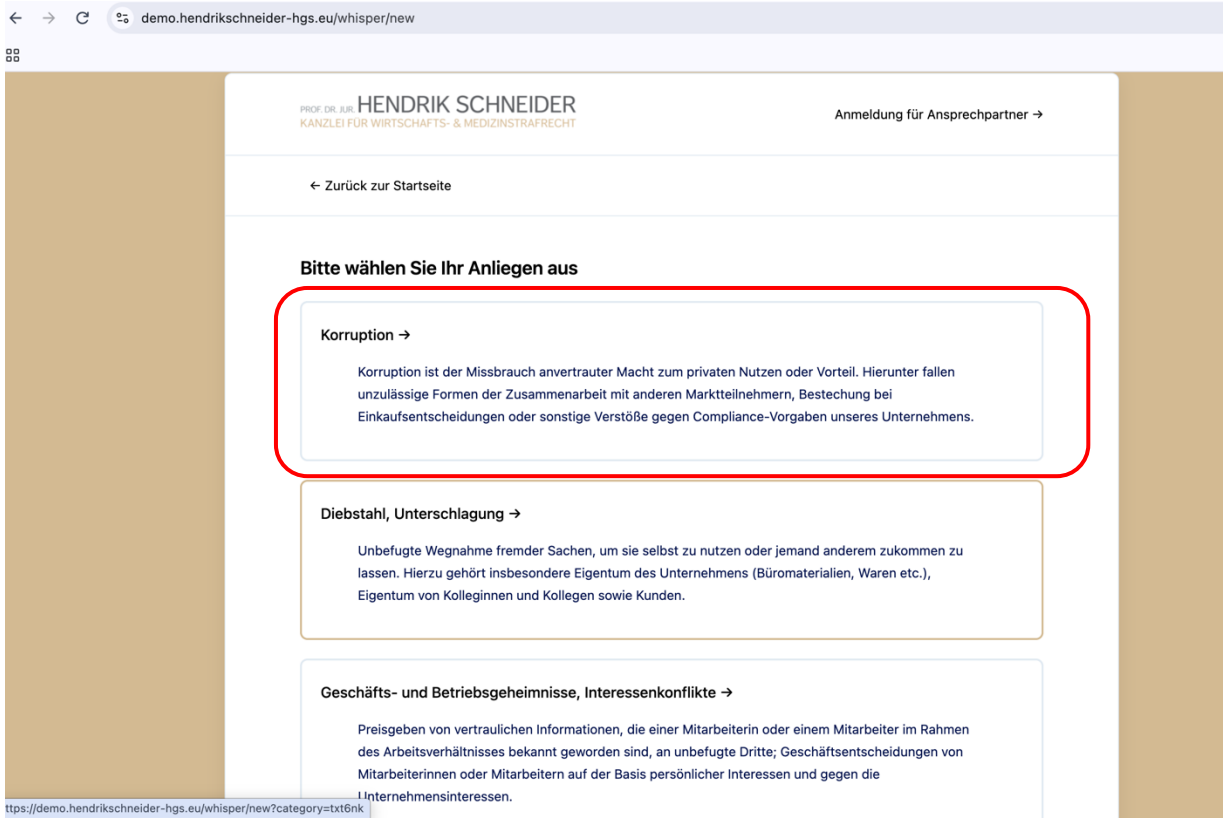
Wichtiger Faktor zur Vertrauensbildung: Antwortgeschwindigkeit wird geschätzt.

Vorteile des digitalen Systems

Aus Sicht der hinweisgebenden Person:

- Das System ist einfach, von überall und zu jederzeit erreichbar.
- Das System bietet adressatengerechte Erläuterungen, z.B. zu Straftatbeständen, zu denen Meldungen abgegeben werden können.
- Über den eingestellten Fragenkatalog kann der Hinweisgeber geführt werden und es wird sichergestellt, dass so viele relevanten Informationen wie möglich angegeben werden.
- Der Fragenkatalog kann auch auf die einzelnen „Kategorien“ angepasst werden.


demo.hendrikschneider-hgs.eu/whisper
Herzlich willkommen
Wie unser Hinweisgebersystem Sie schützt
Es werden keine Informationen zur Identifizierung an die Ansprechpartner gegeben.
Ihre Meldung wird angepasst, um sie noch anonymer zu machen. Das bedeutet, dass wir doppelte Satzzeichen entfernen und sämtliche Wörter kleinschreiben.
Alle Informationen werden Ende-zu-Ende verschlüsselt, sodass Ihre sensiblen Informationen sicher sind.
Wie Sie sich selber schützen
Sie befinden sich nicht im Unternehmens-Netzwerk (Internet / VPN).
Sie nutzen kein Gerät (Smartphone, Computer etc), das von Ihrem Arbeitgeber zur Verfügung gestellt wurde.
Sie nutzen keine Redewendungen oder Abkürzungen, die Sie häufig in Gesprächen oder E-Mails nutzen.
Neuen Hinweis abgeben →


demo.hendrikschneider-hgs.eu/whisper/new
PROF. DR. JUR. HENDRIK SCHNEIDER
KANZLEI FÜR WIRTSCHAFTS- & MEDIZINSTRAFRECHT
Anmeldung für Ansprechpartner →
← Zurück zur Startseite
Bitte wählen Sie Ihr Anliegen aus
Korruption →
Korruption ist der Missbrauch anvertrauter Macht zum privaten Nutzen oder Vorteil. Hierunter fallen unzulässige Formen der Zusammenarbeit mit anderen Marktteilnehmern, Bestechung bei Einkaufsentscheidungen oder sonstige Verstöße gegen Compliance-Vorgaben unseres Unternehmens.
Diebstahl, Unterschlagung →
Unbefugte Wegnahme fremder Sachen, um sie selbst zu nutzen oder jemand anderem zukommen zu lassen. Hierzu gehört insbesondere Eigentum des Unternehmens (Büromaterialien, Waren etc.), Eigentum von Kolleginnen und Kollegen sowie Kunden.
Geschäfts- und Betriebsgeheimnisse, Interessenkonflikte →
Preisgeben von vertraulichen Informationen, die einer Mitarbeiterin oder einem Mitarbeiter im Rahmen des Arbeitsverhältnisses bekannt geworden sind, an unbefugte Dritte; Geschäftsentscheidungen von Mitarbeiterinnen oder Mitarbeitern auf der Basis persönlicher Interessen und gegen die Unternehmensinteressen.
ttps://demo.hendrikschneider-hgs.eu/whisper/new?category=txt6nk

Vorteile des digitalen Systems

Aus Sicht der Internen Meldestelle und des Unternehmens:

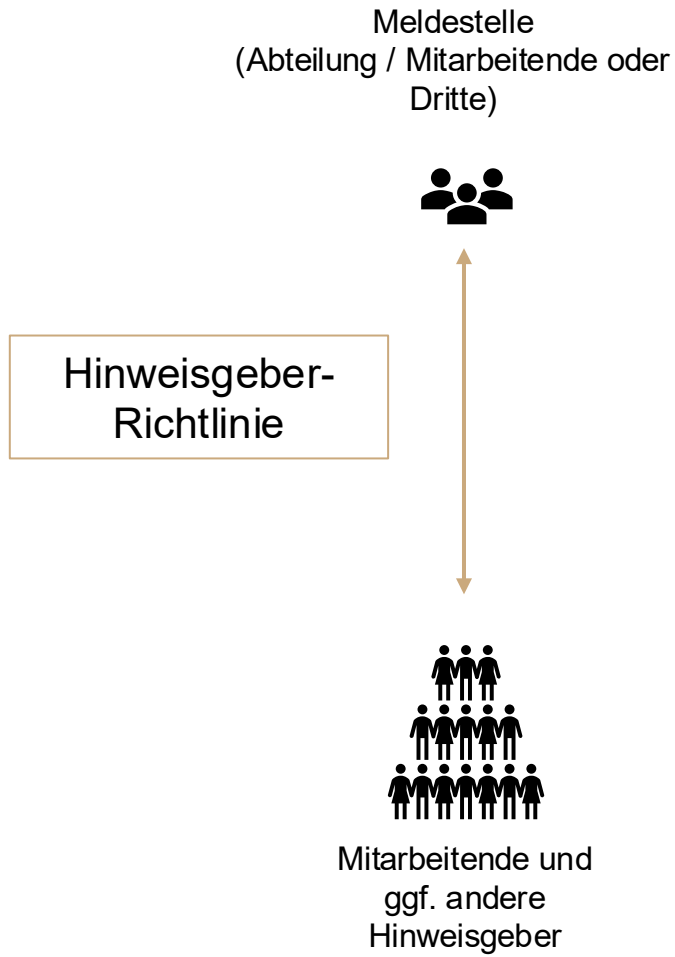
- Bestehen ausreichend Individualisierungsmöglichkeiten (Farben, Logo), kann das digitale System in den Internetauftritt des Unternehmens eingefügt werden.
- Das System erleichtert die Dokumentation.
- Die maßgeblichen Fristen können eingestellt werden. Hier können Erinnerungsfunktionen die Bearbeitung erleichtern.
- Es besteht die Möglichkeit, auch mit anonymen Hinweisgebern zu kommunizieren.

4. Schutz von Hinweisgebers und Beschuldigten

Hinweisgeber-Richtlinie

Hinweisgeber-Richtlinie erklärt und informiert:

- Wer und was die Hinweisstelle ist.
- Wofür die Hinweisstelle zuständig ist.
- Wie das Hinweisgebersystem funktioniert.
- Wie mit Hinweisen umgegangen wird.
- Welche Folgen Hinweise haben können.
- Welche Folgen ein Missbrauch haben kann.
- Welche externen Meldestellen dem Hinweisgeber ebenfalls zur Verfügung stehen (verpflichtend: § 13 Abs. 2 HinSchG).



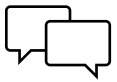
Es besteht keine Verpflichtung, eine Hinweisgeber-Richtlinie zu verabschieden. Sie sichert aber die Akzeptanz und baut Vorbehalte ab.

Erläuterungen zum Umgang mit Hinweisen

In der Hinweisgeber-Richtlinie soll dem potenziellen Hinweisgeber erläutert werden, wie mit seinem Hinweis umgegangen wird:



Bestätigung des Eingangs des Hinweises innerhalb von 7 Tagen.



Rückmeldung zu ergriffenen Folgemaßnahmen innerhalb von 3 Monaten.



Welche Folgemaßnahmen als Reaktion auf einen Hinweis ergriffen werden können, z.B. Durchführung einer Internen Untersuchung oder Weitergabe des Falls an die zuständige Stelle (intern oder Behörde).



Aber auch: Welche Folgen ihn treffen, wenn er vorsätzlich jemanden falsch beschuldigt.

Erläuterungen zum Schutz von Hinweisgebern

In der Hinweisgeber-Richtlinie soll dem Hinweisgeber erklärt werden, wie er …

… durch das Gesetz als Hinweisgeber geschützt ist.	**… durch das Hinweisgebersystem geschützt ist.**
• Schutz vor Repressalien sowie der Androhung von Repressalien im Zusammenhang mit der beruflichen Tätigkeit, z.B. Kündigung, Abmahnung oder sonstige Benachteiligung. • Schutz bleibt bestehen, auch wenn die Identität später bekannt wird. • Anspruch auf Schadenersatz bei Repressalien.	• Darlegung der Unabhängigkeit der Hinweisstelle. • Erläuterung der Gewährleistung der Vertraulichkeit und ggf. der Anonymität. • (Bei Nutzung eines digitalen Systems) Erläuterungen von automatisierten Schutzfunktionen.

5. Anonyme und vertrauliche Hinweise

Anonymität von Hinweisen

- Die Identität der hinweisgebenden Person ist der Meldestelle nicht bekannt.

- Keine Pflicht einen anonymen Meldekanal einzurichten gem. § 16 Abs. 1 HinSchG.

- **Empfehlung**: Anonyme Meldungen ermöglichen:



  - Erhöhte Missbrauchsgefahr bisher nicht empirisch erwiesen.

  - Wenn es keine Möglichkeit gibt, könnten aber Personen abgeschreckt werden, die einen relevanten Hinweis geben möchten (Angst, als Denunziant bekannt zu werden). Eine Untersuchung zu bereits aktiven Hinweisgebersystemen ergab zudem, dass in Deutschland besonders viele Hinweisgeber anonym melden.

  - Die Möglichkeit, einen anonymen Hinweis zu geben, kann die Attraktivität des internen Hinweisgebersystems erhöhen. Hierdurch könnte also z.B. von einer anonymen Meldung an die StA oder die Polizei abgesehen werden.

FH Graubünden / EQS Group, Whistleblowing Reports 2025.

Vertraulichkeit von Hinweisen

- Identität der hinweisgebenden Person ist der Meldestelle bekannt, wird aber geschützt und nur einem eng begrenzten Personenkreis zugänglich gemacht:
  - Zugang zur Identität nur für zuständige und unterstützende Personen (Need-to-Know-Prinzip).
  - Klare Rollen und Berechtigungen festlegen.
- § 8 HinschG verpflichtet Meldestelle, die Identität der hinweisgebenden Person vertraulich zu behandeln.
- Geschützt sind Personen, die Gegenstand der Meldung sind und sonstige darin genannte Personen.
- Offenlegung nur in gesetzlich geregelten Ausnahmefällen, z.B. in Ermittlungsverfahren oder mit Einwilligung (§ 9 HinSchG).

6. Einhaltung der gesetzlichen Vorgaben im Umgang mit Hinweisen

Umgang mit Hinweisen

Pflichtenkatalog aus § 17 HinSchG + Katalog der Folgemaßnahmen aus § 18 HinSchG:

- ☑ ***Bestätigung*** des Eingangs des Hinweises innerhalb von **7 Tagen**
- ☑ ***Prüfung*** der Meldung, ob Anwendungsbereich eröffnet und Stichhaltigkeitsprüfung

  → Ist der Schutzbereich des HinSchG nicht eröffnet, soll eine Meldung an den Hinweisgeber erfolgen. Diese kann den Zusatz enthalten, an welche zuständige Stelle sich die hinweisgebende Person mit seinem Anliegen wenden kann.
- ☑ ***Kontakt*** halten mit Hinweisgeber
- ☑ ***Rückfragen*** an Hinweisgeber
- ☑ ***Folgemaßnahmen*** auslösen
- ☑ Hinweis und Maßnahmen ***dokumentieren***
- ☑ ***Bericht*** über Folgemaßnahmen an Hinweisgeber innerhalb von **3 Monaten** (*soweit Folgemaßnahme nicht gefährdet oder Rechte der von der Meldung betroffenen Personen nicht verletzt werden*.)

Reaktion auf den Hinweis

§ 17 Abs. 2 S. 2 HinSchG:
„Die Rückmeldung umfasst die Mitteilung geplanter sowie bereits ergriffener Folgemaßnahmen sowie die Gründe für diese."

Zweck der Regelung nach dem gesetzgeberischen Willen:

„Durch die umfassende Rückmeldung und eine Begründung für das Ergreifen bestimmter Folgemaßnahmen soll das Vertrauen in die Wirksamkeit des Hinweisgeberschutzes insgesamt gestärkt und das Funktionieren des internen Meldekanals im Besonderen verbessert werden.
(…)
(Gilt) auch in Fällen, in denen einer Meldung nicht weiter nachgegangen und das Verfahren ohne weitere Maßnahmen abgeschlossen wird (…)."

Beim Bericht über ergriffene Maßnahmen ist die Dosis wichtig. Zu wenig stimuliert dazu, nach außen zu gehen. Zu viel verletzt ggf. Datenschutzinteressen der beteiligten Personen.

Reaktion auf den Hinweis

- Nicht umfassend rückmelden muss man nur, wenn:

  – die internen Nachforschungen

oder

  – die Rechte der Person, die Gegenstand der Meldung ist,

- beeinträchtigt werden können.

Tipp: Auch in Fällen, in denen das Prüfverfahren eingestellt wird, soll dies für den Hinweisgeber nachvollziehbar sein.

Denn: Hat der Hinweisgeber den Eindruck, auf den gemeldeten Verstoß werde nicht reagiert, soll er sich nach der internen Meldung nochmal an eine externe Stelle wenden können, § 7 Abs. 1 HinSchG.

Fallbeispiel 1

Die Velaqon Medizintechnik GmbH stellt Infusionspumpen her und beschäftigt 90 Mitarbeitende. Frau Weber arbeitet in der Qualitätssicherung. Bei der Auswertung mehrerer Kundenreklamationen stellt sie fest, dass bestimmte Infusionspumpen bei technischen Störungen möglicherweise keinen Alarm auslösen. Zudem entdeckt sie Unstimmigkeiten in den Prüfprotokollen. Sie vermutet einen Verstoß gegen geltende Sicherheitsanforderungen und meldet den Sachverhalt über das interne Hinweisgebersystem.

Die Meldestelle bestätigt den Eingang fristgerecht und leitet eine interne Prüfung ein. Knapp drei Monate später erhält Frau Weber folgende Rückmeldung:

> *„Wir haben Ihre Meldung sorgfältig geprüft. Es konnten keine relevanten Verstöße festgestellt werden. Der Vorgang ist damit abgeschlossen. Weitergehende Informationen können aus Vertraulichkeitsgründen nicht mitgeteilt werden.“*

Frau Weber ist unzufrieden. Sie kann nicht nachvollziehen, welche Untersuchungen durchgeführt wurden und weshalb ihre Bedenken als unbegründet angesehen werden. Sie verlangt daher eine konkretere Begründung.

Hat Frau Weber einen Anspruch auf diese?

Fallbeispiel 2

Die Bayerische Zentralstelle zur Bekämpfung von Betrug und Korruption im Gesundheitswesen (ZKG) unterhält auf ihren Seiten ein Hinweisgebersystem. Ein anonymer Hinweisgeber wendet sich an die ZKG und trägt vor, eine Apotheke quittiere Privatpatienten die Aushändigung von Medikamenten, die nie stattgefunden hat. Dies ermögliche den Patienten die Einreichung der Rezepte bei ihren Versicherungen.

Die Staatsanwaltschaft startet eine Durchsuchung der Apotheke und der privaten Räumlichkeiten der Apothekerin aufgrund eines richterlichen Durchsuchungsbeschlusses.

War der Durchsuchungsbeschluss rechtmäßig?

Fall nach Landgericht Nürnberg-Fürth, Beschluss vom 20.02.2024, Az.: 18 Qs 40/23.

Fallbeispiel 3

Fall nach Ettwig, CCZ 2025, S. 24 f., 26.

Arbeitnehmer A richtet einen offenen Hinweis an die interne Meldestelle. Der Arbeitgeber erstattet Strafanzeige und die Staatsanwaltschaft leitet ein Ermittlungsverfahren gegen Unbekannt ein. Später richtet sich das Verfahren auch gegen den Hinweisgeber selbst.

Ist A nach §§ 33, 35 HinSchG geschützt?

Gesetz für einen besseren Schutz hinweisgebender Personen (Hinweisgeberschutzgesetz - HinSchG)
§ 33 Voraussetzungen für den Schutz hinweisgebender Personen

(1) Die §§ 35 bis 37 sind auf hinweisgebende Personen anwendbar, sofern

1. diese intern gemäß § 17 oder extern gemäß § 28 Meldung erstattet haben oder eine Offenlegung gemäß § 32 vorgenommen haben,
2. die hinweisgebende Person zum Zeitpunkt der Meldung oder Offenlegung hinreichenden Grund zu der Annahme hatte, dass die von ihr gemeldeten oder offengelegten Informationen der Wahrheit entsprechen, und
3. die Informationen Verstöße betreffen, die in den Anwendungsbereich dieses Gesetzes fallen, oder die hinweisgebende Person zum Zeitpunkt der Meldung oder Offenlegung hinreichenden Grund zu der Annahme hatte, dass dies der Fall sei.

(2) Die §§ 35 bis 37 sind unter den Voraussetzungen des Absatzes 1 auch anwendbar auf Personen, die zuständigen Organen, Einrichtungen oder sonstigen Stellen der Europäischen Union in den Anwendungsbereich dieses Gesetzes fallende Verstöße gegen das Unionsrecht melden.

Gesetz für einen besseren Schutz hinweisgebender Personen (Hinweisgeberschutzgesetz - HinSchG)
§ 35 Ausschluss der Verantwortlichkeit

(1) Eine hinweisgebende Person kann nicht für die Beschaffung von oder den Zugriff auf Informationen, die sie gemeldet oder offengelegt hat, rechtlich verantwortlich gemacht werden, sofern die Beschaffung nicht als solche oder der Zugriff nicht als solcher eine eigenständige Straftat darstellt.

(2) Eine hinweisgebende Person verletzt keine Offenlegungsbeschränkungen und kann nicht für die bei einer Meldung oder Offenlegung erfolgte Weitergabe von Informationen rechtlich verantwortlich gemacht werden, sofern sie hinreichenden Grund zu der Annahme hatte, dass die Weitergabe der Informationen erforderlich war, um einen Verstoß aufzudecken.

Fallbeispiel 4

Fall nach ArbG Offenbach, Urteil vom 25.11.2025, Az: 1 Ca 136/25, CCZ 2026, S. 73.

A war General Counsel und gehörte dem konzernweiten Gruppen-Management. Er entwickelte Vorgaben für die Compliance-Abteilung und eine Verfahrensordnung zum Umgang mit Hinweisgebern. Einer Wirtschaftsprüfungsgesellschaft fiel auf, dass Whistleblower-Meldungen vorlagen, jedoch kein Abschlussbericht über entsprechende interne Untersuchungen. A wurde fristlos gekündigt.

Das Arbeitsgericht hielt die fristlose Kündigung für unwirksam. Die Defizite bei der Bearbeitung der Fälle seien bloße Schlechtleistungen. Die hilfsweise ausgesprochene Kündigung war jedoch wirksam, denn der General Counsel habe schuldhaft seine arbeitsvertraglichen Überwachungs-, Kontroll- und Schadensabwehrpflichten über einen längeren Zeitraum verletzt.

Exkurs

- Meldesysteme nach HinSchG und Beschwerdewege nach Lieferkettensorgfaltspflichtengesetz (LkSG) können miteinander kombiniert werden.
- Es ist zulässig im Konzernverbund mit einem gemeinsamen Hinweisgebersystem für die Tochterunternehmen zu arbeiten. In diesem Fall müssen aber Hinweismanagementverträge mit der Tochtergesellschaft abgeschlossen werden und es muss klar sein, wie das Reporting verläuft.
- Strafbarkeitsrisiken von Mitarbeitenden interner Meldestellen bei der Entgegennahme von Meldungen:

  § 201 StGB – Vertraulichkeit des gesprochenen Wortes:

  - Eine rechtswidrig erstellte Audio-Datei wird abgehört: Strafbarkeitsrisiken stehen und fallen mit dem rechtfertigenden Notstand oder einer Pflichtenkollision. Je gewichtiger der Vorwurf, um so eher ist eine Rechtfertigung gegeben.

  Teilnahme durch Unterlassen bei Untätigbleiben

  - Das Risiko besteht, sofern die gemeldete Tat noch nicht beendet ist.

Zur Vertiefung: Dilling, CCZ 2026, S. 117 ff.

Publikationen

- Andreoli, HinSchG - Informationspflichten gegenüber der beschuldigten Person nach Falschmeldung, Der Krankenhaus-Justitiar, 04/2024, S. 114.
- Andreoli/ Wermter/ Althaus, Rückmeldung an hinweisgebende Personen gem. § 17 HinSchG, Der Krankenhaus-Jus, 01/2024, S. 17.
- Schneider/ Wermter/ Althaus, Hinweisgebersysteme im Krankenhaus – Lösungen für die Unternehmensgruppe, Der Krankenhaus-Justitiar, 04/2023, S. 111.
- Schneider/ Albert/ Wermter, Hinweisgeberschutzsystem im Krankenhaus – im Konflikt zwischen Schweigepflicht und Offenbarungsrecht?, Der Krankenhaus-Justitiar, 03/2023, S. 83.

… Kaffee



… bevor es mit den Grundelementen des CMS weitergeht

Haftungsausschluss und Copyright:

Alle Informationen, die in dieser Präsentation enthalten sind, erheben keinen Anspruch auf Vollständigkeit.

Es wird keine ausdrückliche oder stillschweigende Zusicherung oder Gewährleistung für die Richtigkeit oder Vollständigkeit der in dieser Präsentation enthaltenen Informationen gegeben.

Alle Inhalte dieser Präsentation sind urheberrechtlich geschützt.

© RAin Christiane Döring, © RA Prof. Dr. Hendrik Schneider

Kontakt





Rechtsanwältin Christiane Döring

Hagener Allee 50
22926 Ahrensburg
Tel.: +49 173 2010175
c.doering@doering-rechtsanwalt.de

Prof. Dr. jur. Hendrik Schneider

Taunusstraße 5a
65183 Wiesbaden
Tel + 49 (0) 611 950 08110
schneider@hendrikschneider.eu
www.hendrikschneider.eu

KONTAKT SPEICHERN