Qualitativer Leitfaden für ein Hinweisgebersystem

Mitglied im:

Deutsche Gesellschaft für Kriminalistik

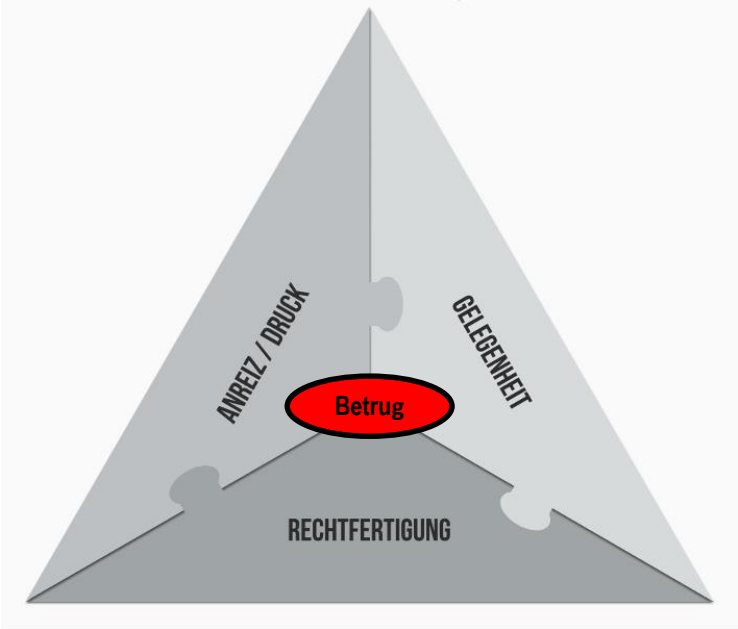
Gesellschaft für Datenschutz und Datensicherheit e.V.

Bayerischer Verband für Sicherheit in der Wirtschaft e.V.

Der Mittelstand. BVMW

…mit uns auf der sicheren Seite!

Einführung und Ziel



Faustregel: Die Betrugs-Eintrittswahrscheinlichkeit ist umso höher, je größer die Gelegenheit, die Motivation / der Anreiz sowie die eigene Rechtfertigung hierfür ist.

Security First geht Verdachtsmomenten und Verdächtigten mit kriminalistischem Spürsinn nach. Legitim, aber mit aller Konsequenz, in privaten wie geschäftlichen Bereichen.

Kriminalität ist vielschichtig und erfindungsreich. Wir steuern ihr entgegen, mit mindestens gleicher Finesse in der Sache und optionalem personellen wie technischen Einsatz.

Wir leisten effektive Aufklärungsarbeit und die Ergebnisse werden gerichtsverwertbar aufbereitet.

Unsere Arbeit bleibt in der Öffentlichkeit unbemerkt und nimmt keinen negativen Einfluss auf des Kunden. Alle eingesetzten Kräfte sind eigene Ermittler und keine Subunternehmer.

Durch die Spezialisierung im Bereich Fraud Management, Ermittlungen, Observationen und Internetrecherchen kann der Sachverhalt sowie eventuelle Wiedersprüche geklärt werden.

Security First arbeitet in Kooperation mit F.E.L.S Rechtsanwälte

…mit uns auf der sicheren Seite!

Hinweisgeberschutzgesetz

Das neue Hinweisgeberschutzgesetz wird in Unternehmen einen Kulturwandel auslösen: Künftig müssen interne Meldekanäle für Hinweisgeber („Whistleblower“) geschaffen werden, über die Missstände mitgeteilt werden können. Unternehmen und ihre Vertreter sind aufgrund ihrer Legalitätspflicht gehalten, die gemeldeten Missstände aufzuklären und notwendige Konsequenzen zu ziehen.

Am 12. Mai 2023 hat der Bundesrat das Gesetz verabschiedet.
Das Gesetz wurde am 2. Juni im Bundesgesetzblatt verkündet und tritt somit am 2. Juli 2023 in Kraft.

Unternehmen ab 250 Mitarbeitenden müssen ab 2. Juli sichere Hinweisgebersysteme einführen, Firmen mit 50-249 Mitarbeitenden haben eine Übergangszeit bis zum 17. Dezember 2023.

Beispiele der Meldefälle:

→ Korruption und Vetternwirtschaft
→ Geldwäsche
→ Untreue bei der Auftragsvergabe bzw. beim Einkauf von Produkten und Serviceleistungen
→ Diskriminierung oder Belästigung
→ Historischer oder aktueller Rassismus
→ Diebstahl
→ Angriffe auf das IT-System oder Cybersecurity-Verletzungen
→ Verletzungen der Datensicherheit und Privatsphäre
→ Betrug bei der Abrechnung von Reise- und Bewirtungsspesen
→ sonstige Rechtsverstöße, etc.

…mit uns auf der sicheren Seite!

Wer steht künftig unter dem besonderen Schutz?

Arbeitnehmende, Teilzeitbeschäftigte, befristet Beschäftigte, Freiberufler, Zulieferer, Dienstleister, Geschäftspartner, Beschäftigte im öffentlichen Dienst, wenn sie Verstöße gegen Unionsrecht oder nationales Recht, wie z. B. Korruption oder Steuerhinterziehung, melden. Dies umfasst auch ehemalige und künftige Arbeitnehmer.

Wie muss die Meldestelle aufgestellt sein?

- Es muss ein sicherer Meldekanal angeboten werden, über den vertrauliche Meldungen abgegeben werden können, so dass die Identität des Hinweisgebenden geschützt ist.
- Die Meldestelle muss organisatorisch unabhängig aufgestellt werden. Es muss sichergestellt sein, dass nur die Mitarbeitenden der Meldestelle Zugriff auf die Meldungsinhalte haben.
- Der interne Meldekanal muss umfassend kommuniziert werden und niedrigschwellig nutzbar sein.
- Ergänzend müssen potentiellen Hinweisgebenden externe Meldestellen im jeweiligen Mitgliedsstaat zur Verfügung stehen. Hinweisgebende können frei entscheiden, ob sie ihre Meldung an eine interne oder eine externe Meldestelle abgeben.
- Die interne Meldestelle eines Unternehmens kann beispielsweise an Anwaltskanzleien „outgesourct“ werden.
- Meldungen können entweder persönlich, schriftlich über ein Online-System (z. B. ein digitales Hinweisgebersystem), einen Briefkasten oder per Postweg abgegeben werden und/oder mündlich per Telefonhotline oder Anrufbeantwortersystem.
- Bei allen Meldekanälen muss die Vertraulichkeit der Identität des Whistleblowers gewahrt sein.
- Private und öffentliche Organisationen sind gut beraten, frühzeitig ein sicheres Hinweisgebersystem einzurichten, da die Implementierung je nach Größe und Komplexität der Organisationsstruktur einige Wochen bis Monate in Anspruch nehmen kann.

…mit uns auf der sicheren Seite!

Vorteile Hinweisgebersysteme

Warum ein Hinweisgebersystem?

- Bestandteil eines funktionierenden „risk managements“ sowie von „good corporate governance“
- Abschreckende Wirkung (Mitarbeiter beobachten Reaktion des Unternehmens)
- Schutz von Mitarbeitern, Kunden und anderen Geschäftspartnern
- Erwartungshaltung von Behörden erfüllen
- Reduzierung der Wahrscheinlichkeit, dass sich der Hinweisgeber an die Öffentlichkeit wendet

Weitere Gründe für ein Hinweisgebersystem:

- Frühzeitige Kenntniserlangung von Fehlverhalten

– Erforderliche Sorgfalt nach §§ 93 AktG u. § 43 GmbHG setzt voraus, „alle verfügbaren Erkenntnisquellen auszuschöpfen“
– Wesentliches Instrument zur Risikofrüherkennung („Frühwarnsystem“)
– Zusätzlicher Kommunikationskanal – hohe Effizienz

- Hinweise werden im Unternehmen „gehalten“

– Internes Hinweisgebersystem reduziert externes Whistleblowing
– Beschäftigte „müssen“ internes System nutzen, ehe externe Anzeige
– Arbeitsrecht fordert Loyalität auch bei Unregelmäßigkeiten - § 241 II BGB

- Erhöhung des Entdeckungsrisikos von Straftaten
- Möglichkeit positiver Außendarstellung

…mit uns auf der sicheren Seite!

Aufbau des Hinweisgebersystems

• **Externe Ombudsperson/Vertrauensanwalt**
→ Rechtsanwalt

• **IT-basierte Whistleblowing-Hotlines (Web-Portal Software)**
→ F.E.L.S Rechtsanwälte betrieben einen eigenen Server

• **S1st**
→ Spezialist im Bereich WiKri und doloser Handlungen

• **Kombination von drei Systemen**

-Unternehmen betreibt elektronisches System und mandatiert Anwalt sowie Ermittler S1st zur Entgegennahme, Erstbearbeitung u. Übermittlung der generierten Hinweise. Problem: Administrator im Unternehmen – hat de facto Zugriffsmöglichkeiten .

→ Deshalb: Auslagerung des Systems zu S1st

- S1st betreibt zusammen mit Anwälte das elektronische System IT-basiert incl. Hotline

…mit uns auf der sicheren Seite!

Kommunikationswege

Elektronische Systeme → Kommunikation über online Plattform

Ombudsmann → alle üblichen Kommunikationswege
(E-Mail, Post, Telefon, Fax, persönliches Gespräch)

Erreichbarkeit muss optimal sein
- Rund-um-die Uhr nur über Call-Center – idR Qualitätsprobleme
- Ombudsmann: Umfassende persönliche Erreichbarkeit

Persönliches Gespräch als Angebot und Regelfall
- baut Ängste ab, schafft Vertrauensverhältnis
- erfüllt bestehenden Beratungsbedarf
- ermöglicht Einschätzung zur Glaubwürdigkeit

Sprachbarrieren beachten; ggf. Angebot in Muttersprache zu kommunizieren (einzelfallabhängig)

…mit uns auf der sicheren Seite!

Mehrwert S1st zusammen mit Anwälten als Ombudsleute / Vertrauensanwälte

Rechtsanwalt als Ombudsmann

- ist unabhängig von der Geschäftsleitung
- kann Hinweisgeber in Compliance-Fällen zuverlässig schützen durch
• Verschwiegenheitspflicht
• Zeugnisverweigerungsrecht
• Beschlagnahmeverbot

- legt Identität von HWG nicht offen, garantiert Vertraulichkeit
- kann Ängste nehmen und Vertrauen aufbauen
-Aber: Ombudsmann sollte nur zusätzlicher Meldeweg sein

S1st als Vertrauensleute

- Haben entsprechendes wirtschaftskriminelles Know How
- können zur Verschwiegenheit verpflichtet werden
- Richtige Einschätzung zur Lage und Glaubwürdigkeit der Hinweise
- Maßnahmen können schnell eingeleitet werden

…mit uns auf der sicheren Seite!

Kreis möglicher Hinweisgeber

Einschränkung der Zugangsberechtigung erfolgt regelmäßig rein faktisch, z. B. Info zu Hinweisgebersystem nur über Intranet des Unternehmens

Gründe: Ausschluss von Kundenbeschwerden, Sorge vor „zu viel´Hinweisen“, befürchtete Missbrauchsgefahr

→ **Aber: Jede Einschränkung reduziert Möglichkeiten der Informationserlangung**

Empfehlung (und Gebot der Praxis): Alle potentiellen Hinweisgeber zulassen (auch „Dritte“)

…mit uns auf der sicheren Seite!

Umgang mit der Identität von Hinweisgebern

Hinweisentgegennahme von Offenlegung abhängig machen? Wahlmöglichkeit überlassen – offen oder anonym?

- Nachteile anonymer Meldungen

- Geringere Glaubwürdigkeit
- Keine erneute Kontaktaufnahme mit Hinweisgeber
- Erhöhte Missbrauchsgefahr - Denunzierungen

- Mehrzahl der Hinweisgeber möchte Identität nicht offenlegen, anonyme Mitteilungen sollten daher nicht ausgeschlossen werden. **Merke: Die Anonymität eines Hinweises ist kein Grund ihm nicht nachzugehen**

- Unternehmen sollten aber nicht zu **anonymen** Meldungen auffordern

- Wäre datenschutzrechtlich bedenklich – Art. 29-Datenschutzgruppe EU
- Sorge um Klima gegenseitigen Misstrauens
- Achtung: Ist typischer Fehler bei der Kommunikation/Implementierung

…mit uns auf der sicheren Seite!

Implementierung des Systems

Nach Abschluss aller Vorbereitungen:

Ausrollen des Systems national und ggf. international

→ Information aller potentiellen Hinweisgeber auf alleninternen Kommunikationskanälen („Tone from the top“)

→ Erläuterung des Systems, Innenwerbung

→ Info über Person und Erreichbarkeit des Ombudsmanns/des Systems

→ begleitende Schulungen/Info-Veranstaltungen

→ Vorstellung Ombudsmann z. B. in Mitarbeiterzeitung, bei Betriebsversammlung, Meetings leitender Mitarbeiter

→ Nachhaltigkeit – regelmäßiges Werben für das System – Rückmeldungen zu Nutzung, Hinweisaufkommen etc.

…mit uns auf der sicheren Seite!

Umgang mit Hinweisen im Unternehmen

- **Eingehende Hinweise bedürfen lückenloser Dokumentation**

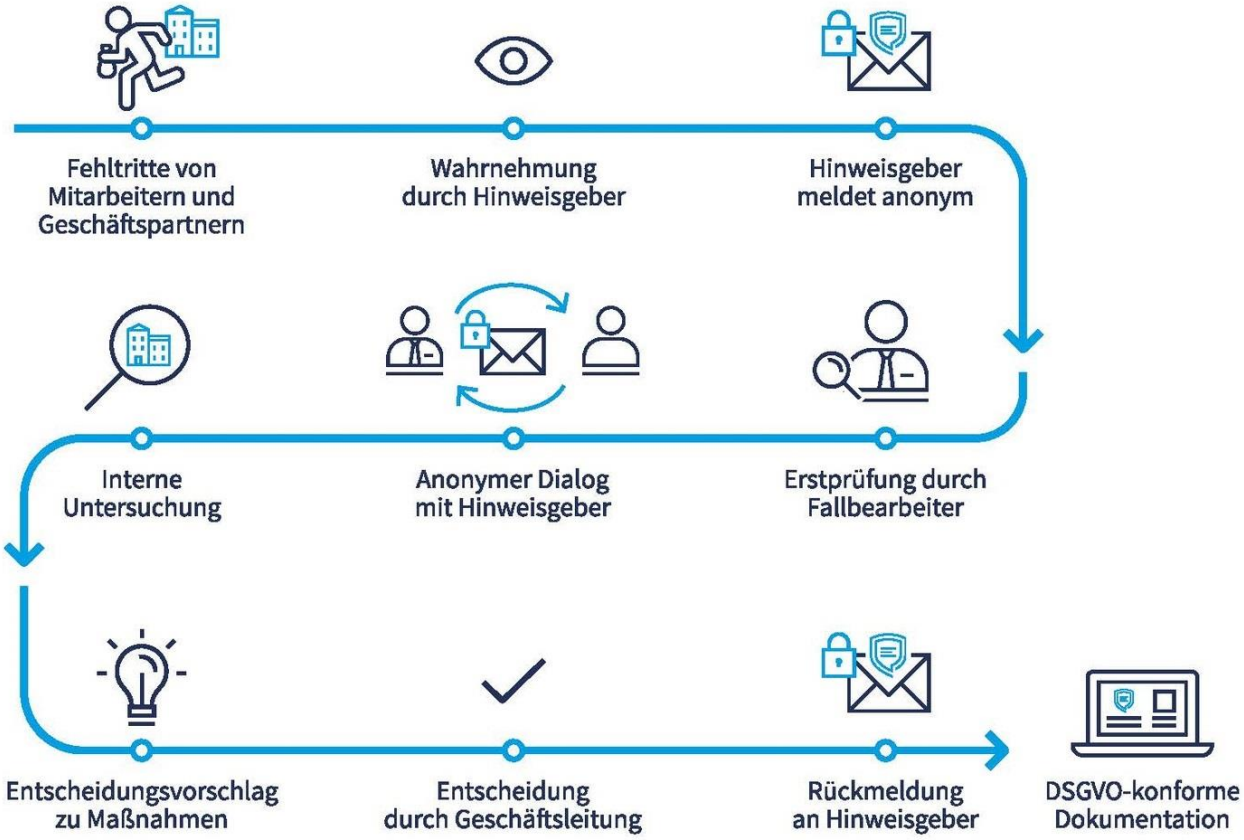
- **Entscheidung über Einleitung und Abschluss interner Ermittlungen durch Gremium, z. B. Arbeitskreis S1st und Unternehmen (AK WiKri)**
  - Erste Bewertung unter Berücksichtigung eines Anfangsverdachts und der Verhältnismäßigkeit
  - Beteiligung des Datenschutzbeauftragten bei besonderen internen Ermittlungen
  - Durchführung interner Ermittlungen/Prüfungshandlungen durch S1st

- **Ergebnisabhängig: Schließung des Falls ohne oder mit Einleitung von Sanktionen (Detaillierte Dokumentation, Festlegung Speicher-/Löschungsfrist)**

- **Prozess sollte in einer Geschäftsordnung verankert sein**
  - Festlegung der Mitglieder (z. B. Compliance, Revision, Recht, Sicherheit)
  - Beschreibung der Abläufe und ihrer Dokumentation
  - Entscheidungsträger für das Verhängen von Sanktionen

…mit uns auf der sicheren Seite!

Hinweisgebersysteme



Quelle Grafik:iWhistle

…mit uns auf der sicheren Seite!

Präventive Aspekte

• Täter/Teilnehmer von WiKri müssen verstärkt mit Aufdeckung durch Whistleblower rechnen, wenn professionelle Hinweisgebersysteme installiert sind (Generalprävention!)

• Hinweisgebersysteme führen zu deutlich erhöhtem Hinweisaufkommen und guten Erfolgen (präventiv u. repressiv)

Voraussetzungen:

- Hinweisgebersystem ist fachlich gut und professionell implementiert
- Korruption oder andere wirtschaftskriminelle Handlungen werden konsequent sanktioniert (arbeitsrechtlich, zivilrechtlich, strafrechtlich)
- Ergebnisse der Compliance-Arbeit werden nach innen und außen kommuniziert und publiziert
- Hinweisgebersystem wird nachhaltig kommuniziert und beworben

…mit uns auf der sicheren Seite!

Ansprechpartner

Unsere Zentrale:	**Fon: 0911 – 44 66 599** **Fax: 0911 – 44 68 760**	**info@security-first.de**
Geschäftsleitung:	**Herr Ingo Wenig**	**iw.info@security-first.de** **Mobil: 0175 – 36 12 929**
Operative Leitung	**Herr Sascha Dreyer**	**sd.info@security-first.de** **Mobil: 0175 – 36 12 62 123**
Rechtsanwalt	**Dr. iur. Tobias Liebau**	**ra.dr.liebau@fe-ls.de** **Telefon: 0921 7566-270**

…mit uns auf der sicheren Seite!