© depositphotos

Whistleblowing und Compliance in der Schweiz

Um das Risiko externen Whistleblowings und, auch persönliche, Haftungsrisiken zu reduzieren, setzen immer mehr Unternehmen und Verwaltungen auf interne Hinweisgebersysteme. Aber deren Einsatz ist kein Selbstläufer. Neben der Entscheidung für ein bestimmtes System kommt es vor allem darauf an, dieses in ein wertebasiertes Unternehmensumfeld zu integrieren und mithilfe einer glaubwürdigen Kommunikationsstrategie das Vertrauen der potenziellen Hinweisgeber zu gewinnen.

Von Kai Leisering

Hinweisgeber, auch Whistleblower genannt, sind Menschen, die auf tatsächliche oder gutgläubig angenommene Risiken, Missstände oder Rechtsverstösse aufmerksam machen, wenn sie befürchten, dass diese die Allgemeinheit gefährden oder schädigen. Eine Person, die andere wider besseres Wissen denunziert, ist – entgegen dem, insbesondere in europäischen Ländern, weitverbreiteten Vorurteil – per Definition kein Whistleblower.

Menschen werden zu Hinweisgebern, wenn sie den moralischen Konflikt zwischen einer beobachteten Unrechtmässigkeit und den eigenen Wertvorstellungen nicht länger ertragen. An diesem Punkt sind sie zumeist bereit, auch persönliche Nachteile wie beispielsweise den Verlust des Arbeitsplatzes in Kauf zu nehmen, um ihr Gewissen zu entlasten. Repressalien drohen Hinweisgebern insbesondere dann, wenn ihnen kein sicherer organisationsinterner Meldekanal zur Verfügung steht und sie das Insiderwissen in die Öffentlichkeit tragen.

Die interne Aufklärung von Vorfällen kommt Whistleblowern sowie auch Organisationen entgegen, indem sie dazu beiträgt, Risiken sowie potenzielle Rechtsverstösse frühzeitig und diskret aufzudecken und zu bearbeiten. Auch Missverständnisse können auf diese Weise vermieden werden. Gleichzeitig wird auf diese Weise das Risiko einer unkont-

ZEHN KRITERIEN

Nachfolgend werden zehn Kriterien für den erfolgreichen Einsatz eines elektronischen Hinweisgebersystems aufgelistet:

1. Höchste Anforderungen an Datenschutz und -sicherheit: In Hinweisgebersystemen werden regelmässig personenbezogene Daten verarbeitet. Aus diesem Grund müssen sie höchsten Anforderungen an den Schutz und die Sicherheit dieser Daten in allen Prozessschritten, von der Erfassung bis zur Löschung eines Hinweises, gerecht werden. Wird der Prozess ausgegliedert, sollte eine Vereinbarung zur Auftragsdatenverarbeitung geschlossen werden.

2. Spezielle Verschlüsselungstechniken und Dialogfähigkeit: Die Möglichkeit, bei Bedarf anonym zu melden, senkt die Hemmschwelle aufseiten des Hinweisgebers und erhöht somit die Akzeptanz und den Erfolg des Hinweisgebersystems. Gleichzeitig ist der Dialog zwischen Hinweisgeber und unternehmensseitigem Bearbeiter wichtig für die effiziente Aufklärung von Vorfällen. Mithilfe spezieller Verschlüsselungstechniken und einer davon unabhängig gesicherten Postkastenfunktion kann dieser vertrauliche Austausch gewährleistet sowie gleichzeitig die Identität des Hinweisgebers geschützt werden.

3. Datenhaltung und -zugriff: Eine Datenhaltung auf geschützten Servern in europäischen Ländern mit hohen Sicherheitsstandards, zum Beispiel Deutschland oder der Schweiz, ist in jedem Fall ratsam, nicht zuletzt als Konsequenz aus der NSA-Affäre. Zudem ist es wichtig, dass Externe, darunter auch der Anbieter des Hinweisgebersystems selbst, zu keinem Zeitpunkt interpretierbaren Zugriff auf die Daten haben.

4. Unabhängige Kontrollen der Sicherheit der Anwendung: Regelmässige Sicherheits- und Penetrationstests unabhängiger IT-Experten sind ein wichtiges Qualitätsmerkmal elektronischer Hinweisgebersysteme. Datenschutzzertifizierungen nach deutschem und/oder europäischem Datenschutzrecht dienen als weiteres Indiz für die Sicherheit einer Anwendung.

5. Erreichbarkeit rund um die Uhr: Ein grosser Vorteil von elektronischen Hinweisgebersystemen ist die permanente Erreichbarkeit weltweit, denn häufig werden Hinweise an Wochenenden oder ausserhalb der regulären Arbeitszeit abgegeben.

6. Sprachabdeckung: Abhängig von seiner Ausgestaltung ist ein webbasiertes Meldesystem in der Lage, Hinweise in einer Vielzahl von Sprachen entgegenzunehmen. Für international tätige Unternehmen ist dies ein wichtiges Kriterium, um Hinweisgebern die Meldungsabgabe in der eigenen Muttersprache zu ermöglichen und somit die Hemmschwelle so niedrig wie möglich zu halten. Mithilfe einer Übersetzungsfunktion können die eingegangenen Meldungen im zweiten Schritt in die Sprache des jeweiligen Meldungsbearbeiters übertragen werden.

7. Eingrenzung der Themen: Um wahlloses Melden sowie eine missbräuchliche Nutzung der Anwendung zu unterbinden, können in elektronischen Hinweisgebersystemen unternehmensindividuelle Themenschwerpunkte bestimmt werden. Mit der Definition der Themenschwerpunkte setzt das Unternehmen gleichzeitig ein deutliches Signal, welches Verhalten gewünscht und welches, im Falle eines Verstosses, sanktioniert wird.

8. Abbildung länderspezifischer Datenschutzanforderungen: Beim internationalen Einsatz eines Hinweisgebersystems müssen die landeseigenen Datenschutzanforderungen und Rechtsvorschriften berücksichtigt werden. So sind anonyme Hinweise oder Meldungen zu bestimmten Themen in einigen Ländern nicht zulässig. Webbasierte Applikationen können in der Lage sein, diese spezifischen Anforderungen flexibel abzubilden.

9. Fallbearbeitung und Dokumentation: Mit einem an das Hinweisgebersystem gekoppelten Case Management können Ergebnisse und Massnahmen des Bearbeitungsprozesses von Meldungen aus unterschiedlichen Quellen festgehalten und ausgewertet werden. Reports und Statistiken dienen gleichzeitig der rechts- und revisionssicheren Dokumentation der Fälle und vermitteln der Unternehmensleitung relevante Informationen.

10. Kombinationen unterschiedlicher Meldewege: Moderne webbasierte Hinweisgebersysteme sind modular aufgebaut und ermöglichen die Hinweiserfassung und -bearbeitung von Meldungen aus unterschiedlichen Quellen. Im Rahmen der Compliance Organisation eines Unternehmens können sie zum Beispiel in Kombination mit einer sprachbasierten Lösung und/oder einer Ombudsperson eingesetzt werden.

rollierten Veröffentlichung brisanter Informationen über Leak-Plattformen oder die Medien gesenkt.

Auch in der Schweiz sind Hinweisgeber mit der geplanten Teilrevision des Obligationenrechts (OR) angehalten, beobachtete Missstände zunächst gegenüber ihrem Arbeitgeber zu melden. Steht in der Organisation kein Hinweisgebersystem zur Verfügung, können Unregelmässigkeiten, bei denen es sich um Verstösse gegen das öffentliche Recht handelt, unter bestimmten Voraussetzungen im nächsten Schritt auch bei der zuständigen Behörde und, in letzter Konsequenz, in der Öffentlichkeit angezeigt werden. Um dieses Risiko externen Whistleblowings zu reduzieren, und um das Unternehmen proaktiv sowohl vor finanziellen als auch reputativen Schäden zu schützen, setzen immer mehr Unternehmen im Rahmen ihres Compliance Management Systems (CMS) auf Hinweisgebersysteme.

Entscheidet sich eine Organisation für den Einsatz eines Hinweisgebersystems, gilt es zunächst den jeweiligen Bedarf zu ermitteln. Wie setzt sich die Zielgruppe der Hinweisgeber zusammen, und wie gross ist sie? Gibt es mehrere Unternehmensstandorte oder Tochterunternehmen, die berücksichtigt werden müssen? Soll der Meldeprozess in mehreren Sprachen angeboten werden? Wie wird der Datenschutz gewährleistet, wie wird die Anonymität des Hinweisgebers in technischer Hinsicht sichergestellt?

Unterschiedliche Möglichkeiten der Hinweiserfassung

Vom Briefkasten im Haus über eine interne Vertrauensperson oder einen externen Ombudsmann bis hin zum elektronischen Hinweisgebersystem existieren unterschiedliche Möglichkeiten der Hinweiserfassung.

Ein Brief erfüllt zwar die Anforderung, jederzeit und von fast jedem Ort der Welt verschickt werden zu können, erreicht aber nicht immer den richtigen Ansprechpartner im Unternehmen. Wird er anonym verfasst, wird er zudem zu einer kommunikativen Einbahnstrasse. Hiermit sind bereits zwei wesentliche Anforderungen an Hinweisgebersysteme benannt: die Möglichkeit, eine Meldung (bei Bedarf) anonym tätigen zu können, und die Gewährleistung eines Dialogs für Rückfragen zum Vorfall. Eine anwaltliche Ombudsperson stellt in der Regel eine vertrauenswürdige Anlaufstelle für Hinweisgeber dar. Im Gespräch mit ihnen kann sie nicht nur das ungefilterte Melden zu unerwünschten Themen unterbinden, sondern, mithilfe gezielter Rückfragen, auch die Plausibilität und Glaubwürdigkeit des Hinweises prüfen. Allerdings kann sich die naturgemäss eingeschränkte zeitliche und örtliche Erreichbarkeit sowie eine für gewöhnlich limitierte Sprachabdeckung als Nachteil erweisen. Zudem muss auch berücksichtigt werden, dass Hinweisgeber die direkte Kontaktaufnahme mitunter scheuen.

Eine mögliche Alternative sind speziell für die Meldungsabgabe entwickelte autarke Webanwendungen, die in der Lage sind, all die genannten Anforderungen flexibel abzubilden und, bei Bedarf,

auch mit einer Ombudsperson kombiniert werden können.

Auch beim Einsatz elektronischer Hinweisgebersysteme empfiehlt sich eine Anwendung, die, optional, eine Hinweisabgabe ohne Angabe des Namens unterstützt, um die Hemmschwelle bei der Meldungsabgabe so niedrig wie möglich zu halten. Die besten Ergebnisse in der Hinweiserfassung werden erzielt, wenn die Plattform auch im Falle einer anonymen Meldung einen absolut sicheren Dialog zwischen Hinweisgeber und unternehmensseitigem Bearbeiter gewährleisten kann. Wie auch im persönlichen Gespräch mit einer Vertrauens- oder Ombudsperson ist es auf diese Weise möglich, Schritt für Schritt das Vertrauen der Hinweisgeber in die Bearbeitung des Vorfalls zu gewinnen, ihnen die Sorge vor persönlichen Nachteilen zu nehmen und gleichzeitig klärende Rückfragen zu stellen. Auch denunziatorisch motivierte Meldungen sowie Hinweise zu nicht meldungsrelevanten Themen können mithilfe gezielter Fragen herausgefiltert werden.

Eine passende Compliance-Lösung für jeden Bedarf

Mit Sicherheit gibt es kein «One fits all»-Patentrezept, aber für jede Unternehmensstruktur und -grösse eine adäquate Compliance-Lösung. Elektronische Hinweisgebersysteme sind, abhängig von ihrer jeweiligen Ausgestaltung, in der Lage, die individuellen Anforderungen einer Organisation flexibel abzubilden. Bei internationaler Geschäftstätigkeit können zudem auch landesspezifische Anforderungen, darunter rechtliche Vorgaben oder auch sprachliche Besonderheiten, berücksichtigt werden. Dient ihr Einsatz jedoch der blossen Regelbefolgung, werden sie schnell als Feigenblatt enttarnt. Um Hinweisgebersysteme im Interesse der Organisation einzusetzen, müssen sie in ein umfangreiches Werte- und Compliance-Management eingebettet werden. Dazu gehört auch, dass die Unternehmensführung den Einsatz befürwortet und ihr eigenes Verhalten am Code of Conduct ausrichtet.

Die Implementierung des Hinweisgebersystems sollte stets von entsprechenden Kommunikationsmassnahmen begleitet werden. Nur wenn die Mitarbeitenden und andere potenzielle Hinweisgeber verstehen, zu welchem Zweck das System eingesetzt wird und wie der Prozess der Hinweisbearbeitung und -beurteilung vonstattengeht, werden sie die Anwendung auch nutzen. Eine hohe Akzeptanz des Systems schliesslich ist ganz im Sinne der jeweiligen Organisation und reduziert nicht bloss das (persönliche) Haftungsrisiko der Geschäftsleitung. Mit der Nutzung sinkt darüber hinaus auch die Gefahr, dass sich Hinweisgeber einen öffentlichen Meldekanal suchen und Missstände bekannt werden. Auf diese Weise werden nachweislich sowohl finanzielle als auch reputative Schäden von der Institution abgewendet. ■

KAI LEISERING
ist Vorstand der Business Keeper AG mit Sitz in Berlin.