Das Hinweisgeberschutzgesetz

Orientierungshilfe zur Einführung eines Hinweisgeberschutzsystems unter Berücksichtigung datenschutzrechtlicher Aspekte (DSGVO, DSG-EKD, KDG)

Version 1

Stand: 10.10.2022

ALTHAMMER & KILL

Das Hinweisgeberschutzgesetz

Informationen zum Hinweisgeberschutzgesetz (HinSchG) zur Umsetzung der Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (HinSch-RL) und deren Umsetzung.

Dieses Dokument soll Sie darüber informieren, welche Verpflichtungen aus dem demnächst verabschiedeten Hinweisgeberschutzgesetz für Ihre Organisation erwachsen und wie sie diesen nachkommen können. Primär ist es gedacht für Organisationen, die den Vorschriften der Datenschutz-Grundverordnung (DSGVO), dem Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) oder dem Gesetz über den Kirchlichen Datenschutz (KDG) unterliegen. Verweise auf das DSG-EKD bzw. KDG befinden sich in den Fußnoten oder in einer Hinweisbox.

Herausgeber/Autoren:

Althammer & Kill GmbH & Co. KG, Hannover (info@althammer-kill.de)
Frank Boje, Arne Wolf, Christian Klande, Simon Lang

Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern meist die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Inhalt

Kurz zusammengefasst

- Die Einführung eines Whistleblowing-Programms ist für praktisch alle größeren Organisationen von Vorteil und in naher Zukunft auch vorgeschrieben.
- Zentraler Punkt ist der Schutz von Hinweisgebenden.
- Ein wichtiger Baustein eines Whistleblowing-Programms ist ein digitales Hinweisgebersystem, das von den möglichen Meldekanälen am meisten Vorteile bietet.
- Grundsätzlich können (und sollten) alle Arten von Missständen gemeldet werden, nicht nur juristisch relevante.

Einführung

Mit einem neuen Gesetz zum Schutz hinweisgebender Personen soll ein Schutz dieser ausgebaut und verbessert werden. Das Gesetz verpflichtet deshalb Unternehmen und Organisationen ab 50 Mitarbeitenden, ein Meldesystem einzurichten, mit dem Mitarbeitende – aber auch Lieferanten, Kunden, Geschäftspartner oder andere Personen, die im Rahmen ihrer beruflichen Tätigkeiten mit einer solchen Organisation in Kontakt stehen – Kenntnisse über Korruption, Betrug oder sonstige gesetzwidrige Vorgänge melden können, ohne ihre Identität preisgeben zu müssen. Die Meldung erfolgt intern, es werden also nicht zwingend offizielle Stellen involviert.

Natürlich darf das Meldesystem in der Organisation auch für die Meldung von Verstößen gegen Compliance-Richtlinien oder ähnlichem genutzt werden – das ist in dem Entwurf des Gesetzes zwar nicht explizit vorgesehen, aber sehr sinnvoll, um den größtmöglichen Nutzen zu erzielen.

Hinweisgebersysteme sind keine neue Erfindung – sie sind in vielen Organisationen schon seit längerem erfolgreich im Einsatz. Wenn es gelebte Kultur ist, dass Mitarbeitende offen auch über sensible Themen sprechen können, ohne Repressalien fürchten zu müssen, können Probleme intern behoben werden, bevor sie öffentlich bekannt oder extern gemeldet werden. Und das sollte das vorrangige Ziel sein - externe Meldungen zu vermeiden oder gar eine Veröffentlichung von brisanten Interna zu verhindern. Beides wäre mit deutlich erhöhten Aufwänden und teils erheblichen Imageschäden verbunden. Darüber hinaus können Informationen von Hinweisgebenden dabei helfen, Risiken und Compliance-Verletzungen zu verhindern und so zu einer besseren Organisations-Performance beitragen.

Was ist Whistleblowing und was sind Hinweisgebende?

> Whistleblowing ist das Weitergeben einer Information über Fehlverhalten oder Missstände durch Mitarbeitende innerhalb einer Organisation bzw. eines Unternehmens.

> Ein Whistleblowing-Programm ist die Gesamtheit aller Maßnahmen, die eine Organisation bzw. ein Unternehmen ergreift, um die Meldung von Information über Fehlverhalten oder Missstände zu ermöglichen und zu unterstützen – vor allem die Einrichtung eines Hinweisgebersystems, aber auch andere Schritte, wie organisatorische Maßnahmen zum Umgang mit solchen Meldungen.

> Ein Hinweisgebersystem ist das technische System zur Meldung einer Information über Fehlverhalten oder Missstände.

Hinweisgebende (Whistleblower) sind in der Regel in der betroffenen Organisation tätig oder haben direkt mit dieser zu tun (z. B. als Kunde) und verfügen somit über Insiderwissen. Die Hinweisgeberin bzw. der Hinweisgeber informiert bisher zumeist die Medien oder direkt die Öffentlichkeit über Missstände in der Organisation.

Was ist ein Hinweisgebersystem?

Grundsätzlich sollen bei einem Hinweisgebersystem Mitarbeitende und andere hinweisgebende Personen über einen geschützten Kanal auf Missstände hinweisen können, ohne Repressalien fürchten zu müssen. Zu Missständen gehören insbesondere alle Vorgänge, die gegen ein Gesetz verstoßen. Darunter fallenbeispielsweise Betrug, Geldwäsche, Korruption, Diskriminierung oder auch sexuelle Belästigung am Arbeitsplatz. Wenn gewünscht, kann ein solches System auch Verstöße gegen organisationsinterne Richtlinien und Vorgaben erfassen.

Die Einrichtung eines Hinweisgebersystems ist nicht nur eine rechtliche Pflicht, sondern liefert Organisationen auch viele Vorteile. Die Organisation kann durch den Erhalt von Hinweisen

- schnell und zielgerichtet reagieren,
- Transparenz und Vertrauen schaffen und
- finanzielle Verluste, Strafen und Image-Schäden vermeiden.

Ein Hinweisgebersystem ermöglicht es, dass alle Fälle, die intern gemeldet werden, effektiv untersucht und bearbeitet werden – ohne öffentlichen Druck. Organisationen, die ein Hinweisgebersystem einrichten, demonstrieren ihre Bereitschaft, den eigenen Mitarbeitern zuzuhören und sie wertschätzend zu behandeln. Ein funktionierendes Hinweisgebersystem reduziert die Wahrscheinlichkeit, dass Missstände außerhalb der Organisation thematisiert werden, zum Beispiel in sozialen Medien oder in der Presse.

Was soll mit Hinweisgebersystemen gemeldet werden?

Grundsätzlich können alle Arten von Missständen berichtet werden – zum Beispiel:

- historischer oder aktueller Rassismus
- Betrugsfälle rund um Corona
- Diskriminierung oder Belästigung aufgrund des Geschlechts oder der sexuellen Identität
- Bestechung und Korruption

- der Einsatz von Zwangsarbeit oder unangemessene Arbeitsbedingungen bei Dritten
- Verletzungen des Datenschutzes und der Privatsphäre
- Angriffe auf das IT-System oder Cyber-Security-Verletzungen
- Geldwäsche
- Steuerflucht

Ist ein Hinweisgebersystem für meine Organisation rechtlich vorgeschrieben?

Das Hinweisgeberschutzgesetz verpflichtet Privatunternehmen ab 50 Mitarbeitende, sowie Behörden und öffentliche Einrichtungen zur Einrichtung einer internen Meldestelle. Außerdem sollen Hinweisgebende besseren Rechtsschutz erhalten.

Der Regierungsentwurf eines deutschen Hinweisgeberschutzgesetzes liegt vor und ist dem Bundestag zur Beratung zugeleitet (Stand 27.09.2022). Die Verabschiedung des Gesetzes in dieser Legislaturperiode ist Teil des Koalitionsvertrags – doch auch ohne gesetzliche Vorlagen ist es freigestellt, schon jetzt ein internes Hinweisgebersystem einzuführen.

Was sind die unternehmerischen Vorteile eines Hinweisgebersystems?

Die Mitarbeitenden einer Organisation sind die beste Quelle zur Erkennung eventueller Risiken – im Grunde genommen sind sie sogar ein sehr effizientes Frühwarnsystem. Deshalb machen viele Organisationen Whistleblowing-Programme und damit verbundene Hinweisgebersysteme zum Kern ihres Risikomanagements und ihrer Compliance-Maßnahmen. Immer mehr Untersuchungen zeigen eine klare Verbindung zwischen der Nutzung eines internen Hinweisgebersystems und einer positiven Organisationsentwicklung. Mitarbeitende anzuhalten, potenziell gefährliche Risiken in ihrem Arbeitsumfeld anzusprechen und zu thematisieren, befähigt Organisationen dazu, diese Risiken proaktiv anzugehen – so kann verhindert werden, dass sich die Missstände zu schwereren Problemen entwickeln, wenn sie unentdeckt bleiben. Werden Schadensfälle auf diese Weise verhindert, nimmt auch das Gesamtniveau finanzieller und Compliance-Risiken sowie von Rufschäden deutlich ab. So kann die Organisation nicht nur potenzielle finanzielle Verluste verhindern, sondern auch zukünftiges Wachstum schützen. Ein gutes Whistleblowing-Programm und eine gelebte „Speak-up-Kultur“ unterstreichen auch das Engagement einer Organisation für Ethik und Integrität und fördern so das Image sowie die Zufriedenheit der Mitarbeitenden.

Organisationskultur

Jede Organisation, die sich für ein digitales Hinweisgebersystem entscheidet, geht einen wichtigen Schritt in Richtung mehr Transparenz – ein Schlüsselwert innerhalb einer gesunden und modernen Organisationskultur. Mitarbeitende und externe Hinweisgeber schätzen vor allem die Möglichkeit des anonymen Meldens. Anonyme Meldewege erhöhen die Anzahl wertvoller Hinweise und tragen entscheidend dazu bei, frühestmöglich auf Missstände aufmerksam gemacht zu werden, Risiken zu minimieren, den eigenen Ruf zu schützen und das Vertrauen nach innen und außen zu sichern.

Bei der Kommunikation und der Etablierung eines Whistleblowing-Programms spielen Vorstände sowie Geschäftsführerinnen und Geschäftsführer eine zentrale Rolle. Ihr Ziel muss es sein, organisationsweit zu verdeutlichen, dass sie Hinweisgeber wirksam unterstützen und schützen. Mitarbeitende müssen sich sicher fühlen, wenn sie ihre Stimme erheben und sicher sein, dass sie als Hinweisgeber vor Vergeltungsmaßnahmen geschützt sind.

Bei der Einführung und Etablierung eines Hinweisgebersystems zur wirksamen Umsetzung eines Whistleblowing-Programms können Vorbehalte in der Belegschaft und bei Kunden und Lieferanten entstehen, denen es entgegenzuwirken gilt. Nicht selten ist von „*Verpetzer-Hotline*“ oder „*Beginn einer Denunziantenoffensive*“ bis hin zu „*alle stehen unter Generalverdacht*“ die Rede – viele Mitarbeitende, die das Konzept des Hinweisgebersystems noch nicht kennen, stehen der Einführung möglicherweise skeptisch gegenüber. Es muss deutlich gemacht werden, dass ein Meldesystem eine ethische Arbeitskultur fördert und Vertrauen – nach innen sowie nach außen – stärkt.

Unser Rat

Gehen Sie direkt auf die Mitarbeitenden zu, fördern Sie einen offenen Austausch und stellen Sie sich allen Fragen rund um die Einführung eines Hinweisgebersystems – insbesondere den kritischen Fragen. Dabei lohnt es sich, die Fragen vorab zu sammeln, entsprechende Antworten vorzubereiten und anschließend die Vorteile des Systems klar zu kommunizieren. Ihre Mitarbeitenden müssen verstehen, dass das Whistleblowing-Programm Teil der Ethik- und Integritäts-Kultur Ihrer Organisation ist. Ein Hinweisgebersystem, von dem niemand weiß oder bei dem Mitarbeitende Bedenken haben, es zu nutzen, ist nicht effizient.

Daher gehören zu den wichtigsten Best Practices:

- Auf alle Hinweise sollte angemessen und zeitnah reagiert bzw. kommuniziert werden. Dies fördert das Vertrauen in das gesamte System.
- Alle Mitarbeiter sollten eine Whistleblowing-Schulung bekommen, damit sie verstehen, wie sie auf einen Missstand aufmerksam machen können – sogar anonym. Die Mitarbeitenden sollten wissen was passiert, wenn sie die Meldekanäle dafür nutzen, um ein Problem zu thematisieren und wie der Prozess für die Untersuchung und die Lösung eines Problems aussieht.
- Organisationen sollten klar kommunizieren, welchen Schutz es für Hinweisgebende gibt. In einer entsprechenden Richtlinie sollte festgehalten werden, was im Falle von Vergeltungsmaßnahmen passiert und welche Gegenmaßnahmen ergriffen werden. Gemäß des Hinweisgeberschutzgesetzes sind Vergeltungsmaßnahmen gegen Mitarbeitende, die Hinweise abgeben, illegal.
- Das TOP-Management und der Vorstand bzw. die Geschäftsführung sollten den „Tone from the top" setzen, z. B. durch regelmäßige Kommunikation, die das Whistleblowing-Programm klar befürwortet und fördert. Ein Video der Organisationsleitung kann dabei helfen, eine entsprechende Gesprächskultur zu etablieren. Die entsprechenden Kommunikationsmaßnahmen sollten regelmäßig stattfinden.
- Whistleblowing-Kommunikation sollte strategisch wie ein internes Marketingprogramm verstanden werden. Für die Kommunikation eignen sich insbesondere E-Mail-Newsletter, Online-Events und Informationen im Organisations-Intranet. Mitarbeiter, die auf dem Firmengelände arbeiten, können auch mit Flyern, Postern und Bannern erreicht werden.

Geschützte Meldekanäle

Grundsätzlich bieten sich für ein Meldewesen verschiedene Kanäle an; alle bringen Vor- und Nachteile mit sich. Wichtig ist, dass der Kanal zu Ihrer Organisation passt. Viele Organisationen kombinieren auch unterschiedliche Kanäle miteinander, um die Zahl der eingehenden Meldungen zu erhöhen. Um herauszufinden, welcher Kanal zu Ihrer Organisation passt, hilft es, die folgenden Fragen zu beantworten:

- Zu welchen zentralen Themen erwarten sie die meisten Hinweise und in welchen Bereichen wollen Sie Risiken minimieren (z. B. Mobbing, Korruption, Betrug, Geldwäsche)?
- Wer soll Hinweise abgegeben können? Alle Mitarbeitenden oder zunächst nur ein Teil der Organisation?
- Sollen auch externe Stellen Hinweise abgeben können?
- In welchen Sprachen erwarten Sie Hinweise?
- Soll das Hinweisgebersystem auch außerhalb der Bürozeiten zur Verfügung stehen?
- Soll das Hinweisgebersystem auch von unterwegs/außerhalb der Organisation zugänglich sein?

Bedeutung der Anonymität

In vielen Ländern steckt der Hinweisgeberschutz noch in den Kinderschuhen. Die Angst vor Ächtung, Jobverlust oder anderen Konsequenzen schreckt viele potenzielle Hinweisgebende ab und führt möglicherweise dazu, dass wichtige Hinweise gar nicht eingehen.

Die Möglichkeit eine anonyme Meldung abzugeben, senkt die Hemmschwelle für Hinweisgebende. Viele Organisationen befürchten, dass dadurch die Zahl der missbräuchlichen Meldungen steigt – doch die aktuelle Studienlage spricht dagegen. Zudem entscheiden sich 60 Prozent der Hinweisgebenden für eine anonyme Erstmeldung. Erfahrungen zeigen außerdem, dass viele, zunächst anonyme Hinweisgebende, im Laufe des Dialogs doch ihre Identität preisgeben, wenn sie sich sicher und ernstgenommen fühlen.

Vor- und Nachteile gängiger Hinweisgeberkanäle

Die folgende Übersicht zeigt die gängigen Kanäle und deren Vor- und Nachteile.

Digitales Hinweisgebersystem

Das digitale Hinweisgebersystem hat sich mittlerweile als effizienteste Lösung durchgesetzt. Es liefert die meisten Vorteile und gewährleistet als einziger Kanal die vollständige Anonymität für Hinweisgebende. Es lässt sich beliebig skalieren und eignet sich so gleichermaßen für kleine und mittelständische Organisationen wie für DAX-Konzerne oder Global Player. Zusätzlich lässt sich ein digitales System durch E-Mail- oder Telefonkommunikation ergänzen.

Vorteile:

- Einziger Kanal, der vollständige Anonymität gewährleisten kann, auch beim anschließenden Dialog.
- Keine Einschränkungen bezüglich möglicher Sprachen sowie zeitlicher und örtlicher Verfügbarkeit.
- Geführter Meldeprozess zur Abfrage der wichtigsten Aspekte eines gemeldeten Missstands.
- Sichere Übermittlung von Dateien und Dokumenten über das Internet.
- Vollständiges Erfüllen aller relevanten Datenschutz-Anforderungen (wie DSGVO, DSG-EKD oder KDG).
- Sichere Dokumentation aller Hinweise und Nachrichten mit dem Hinweisgebenden.
- Dateien sowie Bearbeitungsschritte im System können transparent dargestellt werden.
- Hinweise in Fremdsprachen können direkt im System von zertifizierten Agenturen übersetzt werden.
- Einfaches Abbilden dezentraler Bearbeitung von Hinweisen durch Rollen- und Rechtekonzept sowie automatisches Routing von Hinweisen.

Nachteile:

- Hinweisgebende müssen sich Zugangsdaten zum System notieren, um den Dialog mit der Organisation aufrecht erhalten zu können.
- Bei sehr individualisierten und vielsprachigen Systemen (angepasste Texte, Fragen, etc.) kann das Aufsetzen des Systems eine gewisse Zeit in Anspruch nehmen.

Neben einem digitalen Hinweisgebersystem kann sich ein Hinweisgeber selbstverständlich auch direkt an den entsprechenden Ansprechpartner innerhalb der Organisation wenden. Diese Meldungen lassen sich nachträglich ebenfalls im System speichern, um den Überblick zu behalten.

Briefkasten

Ein Briefkasten auf dem Gelände der Organisation, in dem die Hinweisgebende ihre Meldung als Brief einwerfen.

Vorteile:

- Auch erreichbar, wenn Mitarbeiter nur schwer Zugriff auf andere Kommunikationskanäle der Organisation (Internet, Telefon, etc.) haben.
- Schnell einzurichten.

Nachteile:

- Hinweisgebende müssen den Zeitpunkt des Briefeinwurfs taktisch gut wählen, um unerkannt zu bleiben.
- Handschriftliche Einreichungen lassen Rückschlüsse auf den Hinweisgebenden zu.
- Keine Möglichkeit für Rückfragen bei anonymen Meldungen.
- Keine zentrale Lösung möglich; muss an jedem Standort separat eingerichtet und bearbeitet werden.

E-Mail-Konto

Ein zentrales E-Mail-Konto wie „*Hinweis@IhreOrganisation.de*“, an welches die Hinweisgebenden Ihre Meldung verschicken.

Vorteile:

- Einfach und kostengünstig einzurichten.
- Meldungen können rund um die Uhr, global sowie intern und extern abgegeben werden.
- Zwei-Wege-Kommunikation mit Hinweisgebenden ist möglich.

Nachteile:

- Keine Anonymität für Hinweisgebende - E-Mails können immer nachverfolgt werden.

- Keinerlei Formalität bezüglich gewünschter Informationen, möglicher Sprachen, etc.
- Personenbezogene Daten müssen mühsam manuell gemäß der Datenschutzbestimmungen (vgl. DSGVO, DSG-EKD, KDG) verwaltet werden.

Telefonnummer(n)

Eine zentrale oder mehrere lokale Telefonnummern, an die sich Hinweisgebende bei Bedarf wenden können. Das kann eine einfache Telefonnummer innerhalb der Organisation sein oder die Nummer eines externen Callcenters oder Anrufbeantwortersystems. Bei Letzterem sprechen Hinweisgebende ihre Meldung auf Band auf. Diese wird anschließend transkribiert und an die Organisation verschickt.

Vorteile:

- Persönlicher Dialog mit Hinweisgebenden kann helfen, Hemmschwellen abzubauen.
- Auch bei Lese- und Rechtschreibschwäche geeignet.
- Der Gesprächspartner kann Informationen strukturiert aufnehmen.

Nachteile:

- Keine Anonymität für Hinweisgebende – selbst bei unterdrückter Rufnummer lässt die Stimme Rückschlüsse zu.
- Keine Möglichkeit, Dokumente geschützt zu übermitteln.
- Callcenter in der Regel nicht rund um die Uhr verfügbar.
- Bei Anrufbeantworterlösungen können Verbindungs- oder Tonprobleme zu Übertragungs- oder Verständnisfehlern führen.
- Je nach Zahl der verfügbaren Länder oder Sprachen relativ teuer.
- Ein Telefonat kostet Überwindung.

Ombudsperson

Eine Ombudsperson, also eine externe und unabhängige Person (zum Beispiel ein Datenschutzbeauftragter oder ein Anwalt), die Meldungen von Hinweisgebenden persönlich entgegennimmt.

Vorteile:

- Juristisches Fachwissen erlaubt der Ombudsperson, gezielte Nachfragen zu stellen.
- Externe Stellen erhöhen das Vertrauen gegenüber potenziellen Hinweisgebenden.
- Bei mangelnden internen Ressourcen kann die externe Stelle auch die Einschätzung und Bearbeitung der Hinweise übernehmen.

- Besitzt eine „wahrgenommene“ Neutralität

Nachteile:

- Keine Anonymität für Hinweisgebende, wenn die Ombudsperson per Telefon oder E-Mail kontaktiert wird.
- Bei international tätigen Unternehmen reichen zeitliche Verfügbarkeit und Sprachfähigkeiten einer Ombudsperson in der Regel nicht aus.
- Entgegen der öffentlichen Wahrnehmung besteht für Ombudsstellen durch Rechtsanwälte kein besonderer Schutz vor Durchsuchung oder Sicherstellung von Unterlagen durch Behörden.

Was soll gemeldet werden?

Das Gesetz sieht vor, dass Verstöße gegen Unionsrecht, sowie verschiedene deutsche Gesetze gemeldet werden können. Ein Verstoß kann ein aktives Handeln sein, aber auch ein Unterlassen oder ein Verschleiern von Handlungen. Auch Hinweise oder Bedenken ohne einen eindeutigen Beweis können von einem Hinweisgebersystem erfasst werden, wenn es so gewollt ist – das System kann auch auf Verstöße gegen interne Richtlinien und Compliance-Verstöße ausgeweitet werden.

Welchen Weg Sie gehen, und wie umfangreich das anonyme Meldesystem ausgestaltet werden soll, ist eine Organisationsentscheidung, die klar und eindeutig formuliert werden muss.

Datenschutzrechtliche Anforderungen

Jedes Hinweisgebersystem enthält personenbezogene Daten und unterliegt damit den datenschutzrechtlichen Bestimmungen. Neben den Daten des Beschuldigten sind Daten über den Sachverhalt vorhanden, aber gegebenenfalls auch Daten von Kollegen, die z.B. als Zeugen fungieren. Zusätzlich können auch die Daten des Hinweisgebers enthalten sein, wenn er auf die Anonymität verzichtet. Welche Datenschutzanforderungen sind also für die Einführung und den Betrieb relevant?

Grundsätze für die Verarbeitung personenbezogener Daten

An erster Stelle steht der Nachweis der Einhaltung der Datenschutzprinzipien, die für jede Verarbeitung vorliegen sollte. Als Grundlage zur Überprüfung bietet sich Art. 5 Abs. 1 DSGVO[1] an. Anhand der dort aufgeführten Grundsätze lässt sich die Verarbeitung umfänglich beurteilen.

[1] § 5 Abs. 1 DSG-EKD; § 7 Abs. 1 KDG

- Rechtmäßigkeit der Verarbeitung – Art. 5 Abs. 1 lit. a) DSGVO[2]
- Festgelegter eindeutiger Zweck – Art. 5 Abs. 1 lit. b) DSGVO[3]

Für die Festlegung des eindeutigen Zweckes ist die interne Regelung unumgänglich, welche Meldungen zugelassen sein sollen. Nur so lässt sich einem Missbrauch des Systems vorbeugen. Dazu müssen die zugelassenen Meldungen dokumentiert sein.

- Datenminimierung – Art. 5 Abs. 1 lit. c) DSGVO[4]

Unter diesen Gesichtspunkt fällt auch die schnellstmögliche Pseudonymisierung der Daten, aber auch der Umstand das Falschmeldungen, oder Daten, die nicht unmittelbar für den gemeldeten Fall relevant sind, nicht mit erhoben werden, oder aber bei Bekanntwerden unverzüglich gelöscht werden.

- Datenrichtigkeit – Art. 5 Abs. 1 lit. d) DSGVO[5]
- Speicherbegrenzung und Dauer der Speicherung – Art. 5 Abs. 1 lit. e) DSGVO[6]
- Integrität der Daten durch geeignete technische und organisatorische Maßnahmen – Art. 5 Abs. 1 lit. f) DSGVO[7]

Rechtsgrundlagen für die Verarbeitung

Die Einwilligung des Meldenden kommt nur in Frage, sofern er bei einer anonymen Meldung die Identität offenlegen möchte. Ansonsten ist die Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten Art. 88 DSGVO in Verbindung mit § 26 Abs. 1 Satz 2 BDSG[8]. Dort ist aufgeführt, dass die Verarbeitung von personenbezogenen Daten von Beschäftigten zur Aufdeckung von Straftaten dann rechtmäßig ist, "*wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.*" Dies erfordert vom Verantwortlichen eine umfangreiche Dokumentation der gemeldeten Fälle.

[2] § 5 Abs. 1 Nr. 1 DSG-EKD; § 7 Abs. 1 lit. a) KDG

[3] § 5 Abs. 1 Nr. 2 DSG-EKD; § 7 Abs. 1 lit. b) KDG

[4] § 5 Abs. 1 Nr. 3 DSG-EKD; § 7 Abs. 1 lit. c) KDG

[5] § 5 Abs. 1 Nr. 4 DSG-EKD; § 7 Abs. 1 lit. d) KDG

[6] § 5 Abs. 1 Nr. 5 DSG-EKD; § 7 Abs. 1 lit. e) KDG

[7] § 5 Abs. 1 Nr. 6 DSG-EKD; § 7 Abs. 1 lit. f) KDG

[8] § 49 Abs. 2 DSG-EKD; § 53 Abs. 2 KDG

Wenn die Rechtsgrundlage nicht einschlägig ist, werden die Daten auf Basis einer Interessensabwägung gem. Art. 6 Abs. 1 lit. f) DSGVO[9] erhoben. Das berechtigte Interesse des Verantwortlichen liegt in der Aufdeckung und Aufklärung möglichen Fehlverhaltens von Stakeholdern, dem Schutz der Unternehmensinteressen durch Ad-hoc-Maßnahmen zur Verhinderung weiterer Schäden sowie der Geltendmachung von Schadensersatzansprüchen und anderweitigen Ahndungsmöglichkeiten.

§10 des HinSchG ermöglicht es der Meldestelle, notwendige und erforderliche personenbezogene Daten zur Erfüllung ihrer Aufgabe gem. HinSchG zu verarbeiten. Hier wäre Art. 6 Abs. 1 lit. c) DSGVO[10] in Verbindung mit §10 HinSchG relevant.

Mitteilungspflicht nach Art. 14 DSGVO

Nach Art. 14 DSGVO wären Sie verpflichtet, die beschuldigte Person spätestens innerhalb eines Monats nach Erhalt des Hinweises über die Verarbeitung (Vorwurf und Untersuchung) zu informieren. Der Hinweisgeber als Quelle darf nicht namentlich – sofern überhaupt bekannt – genannt werden, da dadurch die Ziele der Verarbeitung gem. Art. 14 Abs. 5 lit. b) DSGVO ernsthaft beeinträchtigt werden. Es empfiehlt sich hier als Quelle das "Hinweisgebersystem" zu nennen.

Die anderen Informationen nach Art. 14 Abs. 1 und 2 DSGVO sind im Regelfall der beschuldigten Person hingegen in geeigneter Form und fristgerecht zu liefern. Auch, wenn die Identität des Hinweisgebenden geheim halten werden muss, darf die Information nur so lange aufgeschoben werden, wie durch sie eine Klärung des Vorwurfs erschwert oder Beweise vernichtet werden können. Auch die beschuldigte Person hat Rechte.

Eine über die genannte Monatsfrist hinausgezögerte oder gar dauerhaft unterbliebene Information kann im Rahmen einer Interessensabwägung nach Art. 14 Abs. 5 lit. c) DSGVO i.V.m. §29 Abs. 1 S. 1 BDSG erfolgen, sofern der Ermittlungszweck im Einzelfall höher als die Informationspflicht gewichtet werden kann. Wenn diese Ausnahme gewählt wird, sollte ein passende Dokumentation der Prüfung absolute Pflicht sein. Es ist davon auszugehen, dass einer solchen im Rahmen einer späteren gerichtlichen Auseinandersetzung enorme Bedeutung zukommen wird.

Besonderheiten im DSG-EKD:

Sofern personenbezogene Daten eines Gemeldeten im Rahmen des Hinweisgebersystem verarbeitet werden, hat dieser gemäß § 18 DSG-EKD ein Recht darauf, dies zu erfahren. Die Informationspflicht besteht laut Gesetz

[9] § 6 Nr. 8 DSG-EKD; § 6 Abs. 1 lit. g) KDG

[10] § 6 Nr. 6 DSG-EKD; § 6 Abs. 1 lit. d) KDG

allerdings nur, wenn der Betroffene die Information verlangt. Dennoch empfehlen wir, den Betroffenen über die Verarbeitung seiner Daten pro aktiv zu informieren. Problematisch ist allerdings hierbei, dass der Beschuldigte Beweise vernichten könnte, wenn dieser sofort informiert werden würde. In einem solchen Szenario wäre der Ermittlungszweck ad absurdum geführt. Daher steht die Unterrichtungspflicht im Widerspruch zum Ermittlungsinteresse. Nach § 16 Abs. 3 S. 1 DSG-EKD ist es allerdings erlaubt, den Beschuldigten innerhalb von drei Monaten zu informieren. In Ausnahmefällen kann diese Frist um zwei weitere Monate verlängert werden. Folglich muss die Information des Verantwortlichen, der dem Anwendungsbereich DSG-EKD unterliegt, nicht wie in Art. 14 DSGVO grundsätzlich. innerhalb eines Monats erfolgen. Die Pflicht zur Information des Betroffenen kann aufgrund einer speziellen Rechtsvorschrift oder wegen überwiegender berechtigter Interessen Dritter nach § 18 Abs. 2 DSG-EKD entfallen. Eine dauerhafte Geheimhaltung bzw. Nichterfüllung der Informationspflicht nach § 16 DSG-EKD halten wir im Regelfall für nicht zulässig.

Besonderheiten im KDG:

Sofern personenbezogene Daten eines Gemeldeten im Rahmen des Hinweisgebersystem verarbeitet werden, hat dieser gemäß § 16 KDG ein Recht darauf, dies zu erfahren. Demnach hat der Verantwortliche dem Gemeldeten die in § 15 Abs. 1 und 2 KDG genannten Informationen und die zu ihm erhobenen Daten, sowie die Quelle aus der die Daten stammen und ob die Daten ggf. aus öffentlich zugänglichen Quellen erhoben wurden, mitzuteilen.

Problematisch ist hierbei, dass der Beschuldigte Beweise vernichten könnte, wenn dieser sofort informiert werden würde. In solch einem Szenario wäre der Ermittlungszweck ad absurdum geführt. Daher steht die Unterrichtungspflicht im Widerspruch zum Ermittlungsinteresse. Nach § 16 Abs. 2 KDG ist es allerdings erlaubt, den Beschuldigten innerhalb von einem Monat zu informieren. Folglich muss die Information nicht sofort erfolgen, sondern erst nach Sicherung der Beweise.

Sollten die personenbezogenen Daten zur Kommunikation mit dem Gemeldeten verwendet werden, so muss die Information spätestens zum Zeitpunkt der ersten Mitteilung an diesen erteilt werden. Gleiches gilt, wenn die Offenlegung an andere Empfänger beabsichtigt wird. Dann ist die Information spätestens zum Zeitpunkt der Offenlegung zu erteilen.

Eine Ausnahme zur Informationspflicht stellt § 16 Abs. 4 lit. b) KDG dar. Demgemäß muss die Information nicht erteilt werden, wenn die Erteilung dieser Informationen voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt. In diesem Fall ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit.

Außerdem ist die Information nicht zu erteilen, wenn gemäß § 16 Abs. 5 KDG, die Erteilung der Information im Falle einer kirchlichen Stelle im Sinne des § 3 Abs. 1 lit. a) die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben gefährden würde oder die Information dem kirchlichen Wohl Nachteile bereiten würde und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss.

Auskunftsrecht nach Art. 15 DSGVO

Gemäß Art. 15 DSGVO steht dem Gemeldeten das Recht zu, von dem Verantwortlichen eine Auskunft über seine verarbeiteten Daten zu erhalten. Grundsätzlich hätte der Betroffene somit die Möglichkeit, über das Auskunftsrecht die Identität des Hinweisgebers zu erfahren. Gemäß Art. 23 Abs. 1 DSGVO i.V.m. § 29 Abs. 1 S. 2 BDSG besteht kein Auskunftsrecht, wenn durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen geheim gehalten werden müssen, insbesondere wegen überwiegender berechtigter Interessen eines Dritten.

Vorliegend führen die überwiegenden berechtigten Interessen eines Dritten – dem Hinweisgebenden - zur Geheimhaltungspflicht. Da man sich künftig mit einer starken Argumentation im Anwendungsbereich des HinSchG auf die Ausnahmeregelung des § 29 Abs. 1 S. 2 BDSG berufen kann, wirken sich gesetzliche Privilegierung des Hinweisgeberschutzes auch hinsichtlich des Auskunftsanspruchs aus. Demzufolge kann die Auskunft ohne den Namen des Hinweisgebers erteilt werden, es sei denn, dieser willigt ausdrücklich in die Weitergabe seiner Daten an den Gemeldeten weiter, was eher die Ausnahme sein dürfte. Konkret wird der Name und sämtliche auf die Identität hinweisenden Merkmale und Umstände „geschwärzt". Ansonsten sind bei einer Auskunftsanfrage alle weiteren Informationen, mit Ausnahme von weiteren geheim zuhaltenden Informationen von Dritten oder Betriebsgeheimnissen, zu erteilen. Was zusätzlich zum Namen „geschwärzt" wird, sollte daher gut überlegt und abgewogen dokumentiert sein.

Besonderheiten im DSG-EKD:

Gemäß § 19 DSG-EKD steht dem Gemeldeten das Recht zu, von dem Verantwortlichen eine Auskunft über seine verarbeiteten Daten zu erhalten. Grundsätzlich hätte der Betroffene somit die Möglichkeit, über das Auskunftsrecht die Identität des Hinweisgebers zu erfahren. Gemäß § 19 Abs. 2 DSG-EKD besteht kein Auskunftsrecht, soweit die Daten oder die Tatsache ihrer Speicherung aufgrund einer speziellen Rechtsvorschrift oder wegen überwiegender berechtigter Interessen Dritter geheim gehalten werden müssen und das Interesse der betroffenen Person an der Auskunftserteilung zurücktreten muss, oder wenn durch die Auskunft die Wahrnehmung des Auftrags der Kirche gefährdet wird.

Vorliegend könnte die überwiegenden berechtigten Interessen eines Dritten zur Geheimhaltungspflicht führen. Demgemäß ist eine einzelfallbezogene Interessenabwägung durchzuführen. Dabei steht auf der einen Seite das Interesse des Beschuldigten daran, die Informationen zum Hinweisgeber zu erhalten; auf der anderen Seite das Interesse daran, die Vertraulichkeit des Hinweisgebers zu wahren.

Da man sich künftig mit einer starken Argumentation im Anwendungsbereich des HinSchG auf die Ausnahmeregelung des § 19 Abs. 2 DSG-EKD berufen kann, wirken sich die Vorgaben des EU-Gesetzgebers und die gesetzliche Privilegierung des Hinweisgeberschutzes auch hinsichtlich des Auskunftsanspruchs aus.

Ferner ist es für die Organisationen mit den gesetzlich geregelten Vertraulichkeitsgeboten des HinSchG vertretbar, aufgrund dieser gesetzlichen Regelungen die Ausnahme § 19 Abs. 2 DSG-EKD anzunehmen und einen Auskunftsanspruch hinsichtlich der Identität des Hinweisgebers zu verweigern, sofern dieser dem Verantwortlichen überhaupt bekannt ist und keine anonyme Meldung vorliegt. Demzufolge kann die Auskunft ohne den Namen des Hinweisgebers erteilt werden, es sei denn, dieser willigt ausdrücklich in die Weitergabe seiner Daten an den Gemeldeten weiter, was eher die Ausnahme sein dürfte. Konkret wird der Name und alle auf die Identität hinweisenden Merkmale „geschwärzt".

Besonderheiten im KDG:

Gemäß § 17 KDG steht dem Gemeldeten das Recht zu, von dem Verantwortlichen eine Auskunft über seine verarbeiteten Daten nach Art. 17 Abs. 1 KDG zu erhalten. Grundsätzlich hätte der Betroffene somit die Möglichkeit, über das Auskunftsrecht die Identität des Hinweisgebers zu erfahren.

Gemäß § 17 Abs. 6 KDG besteht keine Auskunftspflicht, wenn die betroffene Person nach § 15 Abs. 4 oder 5 KDG nicht zu informieren ist. Es ist jedoch zu beachten, dass diese Ausnahme irgendwann endet. Die Gründe der Auskunftsverweigerung sind nach § 17 Abs. 7 KDG zu dokumentieren. Die Ablehnung der Auskunftserteilung ist gegenüber der betroffenen Person zu begründen, soweit nicht durch die Mitteilung der tatsächlichen oder rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde.

Da man sich künftig zudem mit einer starken Argumentation im Anwendungsbereich des HinSchG auf die Ausnahmeregelung des § 17 Abs. 6 KDG berufen kann, wirken sich die Vorgaben des EU-Gesetzgebers und die gesetzliche Privilegierung des Hinweisgeberschutzes auch hinsichtlich des Auskunftsanspruchs aus. Ferner ist es für die Unternehmen mit den gesetzlich geregelten Vertraulichkeitsgeboten des HinSchG vertretbar, aufgrund dieser gesetzlichen Regelungen die Ausnahme § 17 Abs. 6 KDG anzunehmen und einen Auskunftsanspruch hinsichtlich der Identität des Hinweisgebers zu verweigern, sofern dieser dem Verantwortlichen überhaupt bekannt ist und keine anonyme Meldung vorliegt.
Demzufolge muss die Auskunft ohne den Namen des Hinweisgebers erteilt werden, es sei denn, dieser willigt ausdrücklich in die Weitergabe seiner Daten an den Gemeldeten ein, was eher die Ausnahme sein dürfte. Konkret wird der Name und alle auf die Identität hinweisenden Merkmale „geschwärzt".

Datenschutz-Folgenabschätzung

Sofern eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, ist gemäß Art. 35 DSGVO[11] vorab eine Datenschutz-Folgenabschätzung (DSFA) für den Schutz personenbezogener Daten durch den Verantwortlichen durchzuführen.

Es lässt sich festhalten, dass ein Hinweisgebersystem ein wahrscheinlich hohes Risiko mit sich bringt, denn es liegen sowohl vertrauliche, höchstpersönliche Daten als auch Daten zu schutzbedürftigen Betroffenen vor.

Die Sensibilität der Datenverarbeitung kommt als Kriterium zum Tragen, wenn gemäß Art. 9 DSGVO[12] die Verarbeitung besonderer Kategorien personenbezogener oder gemäß Art. 10 DSGVO[13] personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten geplant ist oder wenn sich aus dem Kontext der Verarbeitung eine besondere Sensibilität der Datenverarbeitung für die betroffenen Personen ergibt. Bei Nutzung eines Hinweisgebersystems ist mit hoher Wahrscheinlichkeit von derartiger Sensibilität der Daten auszugehen. Zudem handelt es sich bei Hinweisgebersystemen um die Daten von Beschäftigten. Diese werden als besonders schutzwürdig angesehen. Nach herrschender Meinung reichen in der Regel diese beiden Kriterien aus, um eine Pflicht zur Durchführung einer DSFA zu begründen.

Auch die DSK vertritt die Meinung, dass für ein Hinweisgebersystem in jedem Fall eine DSFA aufgrund des besonders hohen Risikos für Rechte und Freiheiten natürlicher Personen erforderlich ist.

[11] § 34 DSG-EKD; § 35 KDG

[12] § 13 DSG-EKD; § 11 KDG

[13] § 14 DSG-EKD; § 12 KDG

Anonymität

Die Anonymität der Hinweisgebenden ist das Grundprinzip eines jeden Hinweisgebersystems. Ein Großteil aller Hinweisgebenden kommt aus dem Kreis der Beschäftigten und wäre bei Verlust der Anonymität eventuellen Repressalien bis hin zum Verlust des Arbeitsplatzes ausgesetzt. Dies gilt es zu verhindern. Die Transparenz gegenüber den Hinweisgebenden gebietet es jedoch, dass sie darauf hingewiesen werden, das eine absolute Anonymität trotz aller Anstrengungen und rechtlichen Vorgaben nie gewährleistet werden kann – z. B. kann der Kreis der potenziellen Hinweisgebenden durch Detailinformationen eingeschränkt werden und es kommt schnell „ein Verdacht" auf. Auf solche Risiken sollte, z. B. durch die Ombudsperson, hingewiesen werden.

Benachteiligung ausschließen

Die genaue Bezeichnung des Gesetzes lautet „Gesetz für einen besseren Schutz hinweisgebender Personen". Damit ist bereits im Titel klargestellt, dass es um den Schutz der Hinweisgebenden geht. Insbesondere gilt es hinweisgebende Personen vor Benachteiligungen zu schützen. Um eine Benachteiligung handelt es sich, wenn ein unmittelbarer oder mittelbarer Zusammenhang zwischen einer Mitteilung und einer Repressalie besteht, die der Hinweisgeber erlitten hat. Um Benachteiligungen auszuschließen, kehrt sich im Falle einer Meldung auch die Beweislast um, und die Person, die die Benachteiligung vorgenommen hat, muss nachweisen, dass das Vorgehen nicht im Zusammenhang mit der Meldung steht.

Konsequenzen von Falschmeldungen

Mitarbeitende, die das System wissentlich und absichtlich für Falschmeldungen nutzen, sind durch das Gesetz nicht geschützt. In der internen Kommunikation und gegebenenfalls in Betriebs- bzw. Dienstvereinbarungen sollte diese Tatsache ausdrücklich herausgestellt werden. Personen, die durch wissentlich und absichtliche Falschmeldungen beschuldigt werden, steht Schadensersatz zu. Dies gilt jedoch nicht, wenn die Meldung ungenau war und sich auf einen begründeten Verdacht stützt.

Kommunikation an Mitarbeitende

Wie bereits in der Einleitung herausgestellt, ist eine rechtzeitige und offene Kommunikation der Einführung eines Hinweisgebersystems essenziell. Dabei ist das Einbeziehen der Mitarbeitervertretung so früh wie möglich nötig. Im Mittelpunkt der Kommunikation sollten die Ziele stehen, die mit dem System erreicht werden sollen. Es erscheint selbstverständlich, dass gerade diese offene Kommunikation von der Organisationsleitung getragen werden muss. Nur so ist ein Vertrauen in das Hinweisgebersystem zu erwarten.

Ziele definieren

Zum einen müssen bereits vor dem Einführen eines Hinweisgebersystems die Ziele definiert werden. Hierzu gehört neben dem Rahmen für die Art der Meldungen auch die Entscheidung darüber, für wen das Hinweisgebersystem offensteht.

Stellen Sie die Ziele in den Vordergrund und verhindern Sie durch offen geführte Diskussionen, dass das Image eines Generalverdachts oder von Denunziantentum von Beginn an unterbunden wird. Natürlich sollen kritische Stimmen nicht unterdrückt, sondern ernst genommen werden und Kritikpunkte in der Zieldefinition Berücksichtigung finden.

Kommunikationskanäle

Abhängig von Ihren definierten Zielen, also welche Meldungen und von wem sie diese erhalten wollen, müssen Sie alle zur Verfügung stehenden Kommunikationskanäle ansprechen, die Ihnen zur Verfügung stehen. Neben einer Kick-Off-Veranstaltung, bei der alle Beteiligten und Multiplikatoren eingebunden sein sollten, muss die Information über ein bestehendes Hinweisgebersystem immer (wieder) verbreitet werden. Dabei können E-Mail-Newsletter genutzt werden oder betriebsinterne Printmedien. Auch das Intranet muss zur Verbreitung der Informationen eingebunden werden. Auch in Mitarbeiter- oder Kundenzeitungen kann das Hinweisgebersystem „beworben" werden. Nichts wäre fataler als ein bestehendes Hinweisgebersystem, von dem niemand etwas weiß.

Schulung von Mitarbeitenden

Es sollten alle Mitarbeiter eine Schulung zum Thema Hinweisgebersystem erhalten. Dies ist notwendig, damit alle Mitarbeiter verstehen welche Möglichkeiten sie haben, um auf Unregelmäßigkeiten aufmerksam zu machen. Aus Gründen der Transparenz sollten Sie auch wissen, was nach einer Meldung passiert, und wer sich um Ihre Hinweise kümmert.

Onboarding-Prozess

Vergessen Sie nicht Ihre neuen und zukünftigen Mitarbeiter. Bereits beim Onboarding sollte auf die offene Kommunikation und die Möglichkeiten des Hinweisgebersystems hingewiesen werden. Eine Einweisung in das System sollte in die Checkliste zum Onboarding aufgenommen werden.

Beteiligte

An der Einführung und dem Betrieb eines Hinweisgebersystems ist die gesamte Organisation beteiligt. Die zentrale Rolle bei der Einführung fällt der Geschäftsleitung zu. Diese muss den Prozess tragen und vorantreiben. Aber auch andere Bereiche nehmen eine wichtige Position ein.

Geschäftsleitung

Die Organisationsleitung initiiert in der Regel die Einführung eines Hinweisgebersystems. Hintergrund ist, neben der rechtlichen Vorgabe, der Schutz des Images und der Akzeptanz. Durch die Schaffung einer ausgeprägten Compliance-Kultur wird die Angriffsfläche für Kritiker reduziert. Zeitgleich kann ein fehlendes Hinweisgebersystem auch in einer persönlichen Haftung der Geschäftsleitung münden.

Fachbereiche Personal, Compliance und Datenschutz

Für viele Unternehmen und Organisationen ist die Einführung interner Meldesysteme eine vielversprechende und kostengünstige Gelegenheit, einen Compliance-Diskurs im Unternehmen zu verankern. Etablierte Compliance-Strukturen können angepasst und verbessert werden. Zudem lassen sich diese mit der Identität der Organisation fest verbinden. Das fördert nicht nur ein sauberes, sondern zudem auch ein authentisches Organisationsimage und verbessert vielfältige Stakeholder-Beziehungen.

Whistleblowing durch die Auswahl von Mitarbeitern verhindern zu wollen, ist altes Denken. Katastrophal sind in der Regel Versuche, mit Verweis auf Geschäftsgeheimnisse und andere rechtliche Regelungen, Mitarbeiter zum Schweigen bringen zu wollen. Viele Stakeholder reagieren empfindlich, wenn der Anschein von Mobbing gegenüber Hinweisgebenden entsteht.

Der Whistleblower ist ein positiv besetzter Archetyp. Er kann geradezu als moderner Robin Hood gelten. Whistleblowing zu bekämpfen, ist darum wenig erfolgversprechend. Es muss vielmehr darum gehen, es zu kultivieren und einzuhegen. Darum befähigen zeitgemäße HR-Manager zu ethischen Abwägungen und moralischen Urteilen. Interne (anonyme) Meldesysteme können hierbei einen großen Beitrag leisten.

Mitarbeitervertretung

Für einen akzeptanzfördernden Umgang mit der Belegschaft versteht sich die Beteiligung der Mitarbeitervertretung von selbst. Womöglich ist diese auch aus rechtlichen Gründen einzubinden. Mitunter sind

auch Betriebs- bzw. Dienstvereinbarungen nötig. Auch die Umsetzungskompetenz der Mitarbeitervertretung sind unverzichtbar. Ängste, Sorgen, aber auch Potentiale und Chancen, die in der Belegschaft gesehen werden, gilt es über die Mitarbeitervertretung zu adressieren. Akzeptanz kommt aus integrierender und Partizipation ermöglichender Kommunikation. Die Mitarbeitervertretung ist darum die organisationsinterne Schlüsselinstitution.

Mitarbeitende

Die Mitarbeitenden sind die wesentliche Zielgruppe, an die sich das Hinweisgebersystem richtet. Es muss alles getan werden, damit sich die Mitarbeitenden sicher genug fühlen, um Missstände anzusprechen.

Abläufe bei Meldungen

Nachdem das Hinweisgebersystem in Betrieb genommen worden ist, ist mit Meldungen zu rechnen. Auf diese Situation müssen die Beteiligten vorbereitet sein. Ist ein externer Dritter mit der Entgegennahme der Meldung betraut, muss auch dieser in den Prozess eingebunden werden und die Weitergabe (insbesondere die Weitergabewege) müssen festgelegt sein.

Unparteiische Verantwortliche und Ansprechpartner

Im Idealfall gibt es mehrerer Meldewege, um Hinweisgebenden die Meldung zu erleichtern. Die Ansprechpartner an einer Hotline, die Betreuer eines Hinweisgebersystems, oder der persönliche Ansprechpartner müssen gesondert geschult werden. Neben der Verpflichtung auf die Verschwiegenheit muss eine vertragliche Regelung zum Schutz getroffen werden. Dabei ist ein wesentlicher Regelungspunkt das Weisungsrecht des Arbeitgebers. Eine Anonymität kann nie gewährleistet sein, wenn die (interne) Ombudsperson zur Herausgabe der erhaltenen Informationen durch den Arbeitgeber angewiesen werden kann.

Der Kreis der beteiligten Personen sollte so klein wie möglich gehalten werden. Neben der Ombudsperson sollte höchstens ein Vertreter involviert sein. Die Dokumentation der Fälle muss zentral und ohne Zugriffsmöglichkeiten durch Dritte erfolgen.

Prozess nach Eingang einer Meldung

Idealerweise ist der Prozess nach einer Meldung im Vorfeld abgestimmt. Alle beteiligten Mitarbeitenden und externe Dritte sind informiert und geschult.

Wie sieht der Prozess aus?

Der Prozess muss, abhängig von den Besonderheiten der Organisation, individuell festgelegt werden. Dieser sollte, wegen der nötigen Transparenz, schriftlich festgehalten werden. Es sollten einige wichtige Schritte in dem Prozess enthalten sein.

- Nach dem Eingang der Meldung ist diese auf Plausibilität zu prüfen. Ebenso ist zu prüfen, ob die Meldung in den vorher festgelegten Bereich der möglichen Meldungen fällt bzw. ob es sich um eine Compliance relevante Meldung handelt.
- Wenn möglich, sollte durch die Ombudsperson frühestmöglich ein persönlicher Termin mit dem Hinweisgeber abgestimmt werden, um Fakten zu besprechen und Fragen zu klären. Damit lässt sich eine konstruktive und vertrauensvolle Beziehung zu dem Hinweisgeber aufbauen.
- Ein Plan für die Untersuchung muss erstellt werden, der den weiteren Prozess bestimmt und für Transparenz sorgt.
- Auch der Umfang der Untersuchungen sollte im Voraus festgelegt werden.
- Soweit die Anonymität des Hinweisgebers dies zulässt, sollten nach Abschluss der Untersuchung die Ergebnisse präsentiert werden. Auch dies ist ein Mittel, um das Vertrauen in das Hinweisgebersystem zu stärken.

Wer ist involviert?

Involviert ist in jedem Fall die Ombudsperson. Dies kann eine Vertrauensperson aus den Bereichen Datenschutz oder Compliance sein. Aber auch Vertreter der Mitarbeitervertretung bzw. des Betriebsrats genießen bei den mitarbeitenden Personen häufig ein hohes Vertrauen.

Abhängig von dem Untersuchungsplan können weitere Personen in ein Untersuchungsteam bestimmt werden. Es ist darauf zu achten, dass in der Dokumentation eine Liste der „Eingeweihten" vorhanden ist. Der Kreis der „Eingeweihten" sollte sich auf ein Minimum beschränken, um zu verhindern, dass vertrauliche Informationen ungewollt das Hinweisgebersystem verlassen.

Wie wird dokumentiert?

Die Dokumentation sollte einheitlich erfolgen. Die Regeln für die Dokumentation müssen vorher festgelegt werden. Berücksichtigt werden sollte bei der Dokumentation, das Informationen aus der Dokumentation auch für das Abstellen von Risiken benötigt werden könnten.

Wenn die Dokumentation digital erfolgt, sind unbedingt die Zugriffsberechtigungen zu betrachten. Eventuell kann es notwendig sein, für die Dokumentation ein separates EDV-System zu benutzen.

Welche Fristen sind zu berücksichtigen?

Das HinSchG sieht eine Frist von sieben Tagen vor, bis zu der eine erste Rückmeldung (*„Ihre Meldung ist bei uns eingegangen und wird nun geprüft.“)* an Hinweisgebende erfolgen muss. Für einen Hinweisgeber, der vielleicht lange überlegt hat, bevor er sich zu seinem Schritt entschlossen hat, können sieben Tage eine lange Zeit sein – deshalb sollten Sie prüfen, ob eine erste Rückmeldung bereits früher erfolgen kann.

Die Frist für die Rückmeldung an den Hinweisgeber (*„Das Ergebnis unserer Untersuchung lautet wie folgt“* oder *„Wir ergreifen nun folgende Maßnahmen“)* ist auf drei Monate nach Bestätigung des Eingangs festgelegt.

Schulung der Verantwortlichen

Die am Verfahren beteiligten Personen müssen mit Schulungen besonders auf Ihre Aufgabe vorbereitet werden. Neben den Grundsätzen von Compliance und Datenschutz sind auch die besonderen internen Aspekte des Hinweisgebersystems zu vermitteln.

Meldewege

Auf die Bedeutung der unterschiedlichen Meldewege sind wir bereits im Kapitel über die rechtlichen Rahmenbedingungen eingegangen. Vom Gesetzgeber ist kein Meldeweg vorgeschrieben oder bevorzugt. Die Einrichtung interner Meldekanäle wird durch das Gesetz dahingehend vereinfacht, dass sich private Beschäftigungsgeber bis zu einer Größe von 249 Arbeitnehmern die Entgegennahme und durchzuführende Untersuchungen mit gemeinsamen Ressourcen teilen können.

Die Empfehlung geht dahin, so viele unterschiedliche Meldeweg wie mögliche anzubieten, um die Hemmschwelle zur Abgabe einer Meldung zu senken.

Welche Meldewege sollten genutzt werden?

Die Entscheidung darüber welche Kanäle tatsächlich von Ihnen genutzt werden, ist stark von den organisationsinternen Gegebenheiten abhängig. So bietet sich ein Online-Meldesystem bspw. besonders für Organisationen an, die verstärkt auf Home-Office Arbeitsplätze setzen. In einer kleineren Organisation mit einer offenen Kommunikationskultur kann jedoch eine Ombudsperson eventuell die ideale Lösung darstellen. Wie andere Prozesse auch, sollte auch die Wahl des Hinweisgebersystems regelmäßig überprüft werden. Wenn Überprüfungen ergeben, dass Missstände, die hätten gemeldet werden können, nicht gemeldet worden sind,

liegt dies vielleicht am falschen Meldekanal. Durch einen Systemwechsel lässt sich die Effizienz des Hinweisgebersystems gegebenenfalls steigern.

Sollen Dritte Zugriff haben, um Meldungen abzugeben?

Nicht nur Mitarbeitende sind wertvolle Informationsquellen, sondern auch ehemalige Mitarbeitende, Anteilseigner, Personen, die den Verwaltungs- oder Aufsichtsorganen angehören oder Auftragnehmerinnen und Auftragnehmer, Auftraggeberinnen und Auftraggeber sowie Lieferanten. Ob und in welcher Form das Hinweisgebersystem diesem Personenkreis zur Verfügung stehen soll, ist auch abhängig von den Meldungen, die von Ihnen erwartet werden, und davon, was von Ihnen festgelegt worden ist (*was soll gemeldet werden*).

Worauf sollten Sie bei der Systemauswahl achten?

Wenn Sie sich für ein Hinweisgebersystem eines Dritten interessieren, sollten neben Benutzergesichtspunkten und der Möglichkeit einer datenschutzfreundlichen Voreinstellung insbesondere die Schutzziele für personenbezogene Daten im Vordergrund stehen. Kann der Anbieter das von Ihnen gewünschte Schutzniveau für die Daten gewährleisten?

Beim Betreiben eines Hinweisgebersystems durch einen externen Dritten handelt es sich um eine Auftragsverarbeitung. Schließen Sie die entsprechenden Verträge ab und achten Sie besonders auf gegebenenfalls beauftragte Unterauftragnehmer und die vereinbarten technischen und organisatorischen Maßnahmen.

Bei dem Einsatz eines internen Hinweisgebersystems müssen die oben genannten Fragen gleichermaßen beantwortet werden. Für den Einsatz eines Hinweisgebersystems ist die Erstellung einer Datenschutz-Folgenabschätzung obligatorisch. Insbesondere Aspekte der Vertraulichkeit (innerhalb der Organisation) auf den eigenen Systemen sollten eingehend untersucht und sichergestellt werden. Wenn diese nicht gewährleistet werden können, müssen Sie gegebenenfalls auf ein separates System zurückgreifen.

Anonymität

Die Anonymität des Hinweisgebers steht an erster Stelle. Die Anonymität ist der wesentliche Garant für den Schutz vor Repressalien. Dieser Schutz muss jedoch auch gewährt werden, wenn ein Hinweisgeber anonym gemeldet hat, und anschließend (aufgrund der Meldung) identifiziert worden ist.

Vertraulichkeit

Die Wahrung der Vertraulichkeit der Identität des Hinweisgebers während des Meldeverfahrens und der durch die Meldung ausgelösten Untersuchungen ist eine wesentliche Vorsorgemaßnahme gegen Repressalien. Die Verletzung der Vertraulichkeit der Identität des Hinweisgebers kann unter Umständen empfindlich bestraft werden.

Checkliste zur Einführung eines Hinweisgebersystems

Empfehlungen für den operativen Ansprechpartner	
☐	Die Fachbereiche Personal, Recht, Compliance, Datenschutz und Kommunikation in den Prozess einbinden. Vor allem jedoch die Geschäftsleitung mit ihren hoheitlichen Aufgaben.
☐	Beim Einsatz eines externen Dienstleisters Auftragsverarbeitungsvertrag abschließen.
☐	Beim Einsatz eines technischen Systems Impressum und Datenschutzerklärung erstellen und veröffentlichen.
☐	Testmeldung durchführen.
☐	Datenschutz-Folgenabschätzung (inkl. systematischer Beschreibung, Datenflüssen und Risikoanalyse samt ergriffenen technischen und organisatorischen Maßnahmen wie z. B. ein enges dokumentiertes Berechtigungskonzept) durchführen.
☐	Informationen für den Gemeldeten vorbereiten und im Einzelfall dokumentiert begründen, sofern keine Meldung innerhalb gesetzlicher Fristen erfolgen soll bzw. kann (z. B., weil noch Beweise gesichert werden müssen bzw. eine zu frühe Information das Verfahren gefährden würde).
☐	Verzeichnis der Verarbeitungstätigkeiten ergänzen.

Empfehlungen für die Personalleitung	
☐	Informationen für Mitarbeitende bereitstellen, ggf. Schulungen planen.
☐	Den Onboarding-Unterlagen für neue Mitarbeitende Informationen zum Whistleblowing-Programm und zum Hinweisgebersystem hinzufügen.

Empfehlungen für die Geschäftsleitung	
☐	Als Geschäftsleitung die Einführung einer Whistleblower-Programmes aktiv gegenüber den eigenen Führungskräften und der Belegschaft unterstützen. Dazu kann es notwendig sein, die Vorteile einer internen Meldung gegenüber keiner Meldung bzw. den Folgen einer externen Meldung deutlich zu machen.
☐	Definieren, welche Verstöße gemeldet werden sollen. Klären, wie beim Eingang einer Meldung konkret vorgegangen, welcher Personenkreis involviert und wie die Dokumentation vorgenommen werden soll.
☐	Verantwortliche ohne Interessenskonflikt sowie Ansprechpersonen für die Bearbeitung von Meldungen benennen. Diese sollten in der Regel direkt an ein verantwortliches Mitglied der Geschäftsleitung berichten.
☐	Festlegen, über welche internen Kanäle den Beschäftigten das Hinweisgeberssystem kommuniziert werden soll. Ohne eine ausreichende Kommunikation wird das Hinweisgebersystem zu wenig genutzt werden.
☐	Eine Betriebs- / Dienstvereinbarung mit der Mitarbeitervertretung bzw. dem Betriebsrat schließen. Wenn keine Mitarbeitervertretung bzw. Betriebsrat vorhanden ist, sollte die Geschäftsleitung eine Selbstverpflichtung u.a. zur Wahrung der Anonymität veröffentlichen.
☐	Die handelnden Personen des Hinweisgebersystems sollten eine schriftliche Bestätigung der Geschäftsleitung erhalten, in der Ihnen garantiert wird, dass sie nicht angewiesen werden dürfen, Daten über eine bekannte Identität des Whistleblowers preiszugeben, es sei denn, die gesetzlichen Ausnahmetatbestände liegen vor oder der Whistleblower willigt ausdrücklich und nachweislich ein.
☐	Die Anonymität des Hinweisgebenden unter Berücksichtigung der Rechtslage gewährleisten, die Rechte des/der Gemeldeten wahren und jegliche Benachteiligung von Hinweisgebenden infolge einer Meldung ausschließen.
☐	Das Hinweisgebersystem in Datenschutz- und Organisationssprozesse einbinden.
☐	Hinweisgebende bei bewussten Falschmeldungen zur Verantwortung ziehen.

Anhang

Autoren

ALTHAMMER & KILL

Digitalisierung sicher gestalten – an der Schnittstelle von Recht und Technik

Kontakt: info@althammer-kill.de

Christian Klande

Dipl.-Kfm.
Berater für Datenschutz, IT-Sicherheit und Compliance

Erfahren in der Beratung als zertifizierter Compliance Officer & Datenschutzbeauftragter, verantwortlich für den Bereich Compliance

Arne Wolf

Dipl. -Inform. (TU)
Berater für Datenschutz und IT-Sicherheit

Erfahrung in der Beratung als zertifizierter Datenschutzbeauftragter, verantwortlich für den Bereich Wissensmanagement

Simon Lang

General Management (M.A.),
Produktmanager Althammer & Kill

Erfahrung in der Beratung als zertifizierter Datenschutzbeauftragter, verantwortlich für den Bereich Produkt & Marketing

Glossar

BDSG	Bundesdatenschutzgesetz
DSFA	Datenschutz-Folgenabschätzung
DSG-EKD	Kirchengesetz über den Dateschutz der Evangelischen Kirche Deutschland
DSGVO	Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz
HinSchG	Hinweisgeberschutzgesetz
KDG	Gesetz über den Kirchlichen Datenschutz