

Compliance-Vorschriften in Deutschland

Ihr umfassender Leitfaden

2025



Inhalt

Einleitung	3
Was enthält dieser Leitfaden?	4
Aufbau einer starken Compliance-Kultur	5
Vertrauen – eine wertvolle Ressource für Ethik und Compliance	6
Whistleblowing in Deutschland: ein Thema mit Potenzial	10
Wie Chief Compliance Officers im Management mehr bewegen können	15
8 Schritte zu einem effektiven Compliance-Programm	19
Orientierung in den gesetzlichen und regulatorischen Anforderungen Deutschlands	37
Datenschutz in Deutschland und Europa	38
Arbeitsrecht in Deutschland	45
Berichtspflichten in Deutschland und der EU: LkSG, CSRD, CSDDD	50
Das Hinweisgeberschutzgesetz	58
EU AI Act: Was Unternehmen zum weltweit ersten KI-Gesetz wissen müssen	61
Wie NAVEX helfen kann	66

NAVEX® | Navigator Series

Die Navigator Series bietet fundierte Anleitungen zum Aufbau und zur Optimierung von Risiko- und Compliance-Programmen. Unsere Unterlagen stützen sich auf aktuelle Untersuchungen und bieten grundlegende Einblicke und vertiefende Analysen zu bestimmten Themen und Regionen. Sie sollen Ihnen als Grundlage für Ihre Planungen dienen, um die erfolgreiche Umsetzung Ihres Programms zu fördern.

Einleitung

Oliver Riehl

Regional Vice President, Sales, NAVEX

Unternehmen, die in der Europäischen Union und insbesondere in Deutschland tätig sind, stehen vor komplexen und immer größer werdenden Compliance-Verpflichtungen. Von Datenschutz und Lieferkettenanforderungen bis hin zu Arbeitsrecht und Whistleblowing – die Erwartungen an Unternehmen waren noch nie so hoch wie heute.

Mit den jüngsten Ergänzungen des deutschen Lieferkettensorgfaltspflichtengesetzes, der Corporate Sustainability Reporting Directive (CSRD), der Corporate Sustainability Due Diligence Directive (CSDDD) sowie dem EU-KI-Gesetz – alle entweder im Jahr 2024 eingeführt oder in Kraft getreten – steigt die Zahl der relevanten Gesetze und Vorschriften für Unternehmen in Deutschland kontinuierlich. Die Bewältigung dieser komplexen Compliance-Landschaft stellt daher für viele Unternehmen eine erhebliche Herausforderung dar.

„Dabei reicht es längst nicht mehr aus, lediglich über die neuesten Vorschriften informiert zu sein. Entscheidend ist, einen Schritt voraus zu sein: zukünftige regulatorische Entwicklungen zu verstehen, rechtzeitig zu antizipieren und so Risiken zu minimieren sowie die Resilienz des Unternehmens zu sichern.“

Dabei reicht es längst nicht mehr aus, lediglich über die neuesten Vorschriften informiert zu sein. Entscheidend ist, einen Schritt voraus zu sein: zukünftige regulatorische Entwicklungen zu verstehen, rechtzeitig zu antizipieren und so Risiken zu minimieren sowie die Resilienz des Unternehmens zu sichern. Gleichzeitig wächst auch der Druck, eine integre und nachhaltige Unternehmenskultur zu fördern.

Genau deshalb muss Compliance heute eine zentrale Rolle in der Unternehmensidentität spielen. Denn klar ist: gelebte Compliance bildet das Fundament für Vertrauen und eine starke, ethische Unternehmenskultur.

Um Unternehmen bei diesen Herausforderungen zu unterstützen, bietet dieser Leitfaden einen umfassenden Überblick über die wichtigsten Gesetze und Vorschriften in Deutschland, ergänzt um kulturelle Hintergründe und praxisnahe Handlungsempfehlungen. Er richtet sich an Compliance-Verantwortliche, Risikomanager und Führungskräfte. Darüber hinaus liefert der Leitfaden konkrete Werkzeuge – von Checklisten bis zu Ressourcen – für den Aufbau eines neuen oder die Optimierung eines bestehenden Compliance-Programms.

Wir bei NAVEX wissen: Compliance bedeutet weit mehr, als Sanktionen und rechtliche Konsequenzen zu vermeiden. Es geht darum, Vertrauen zu schaffen, Transparenz zu ermöglichen und die Zukunft Ihres Unternehmens nachhaltig zu sichern.

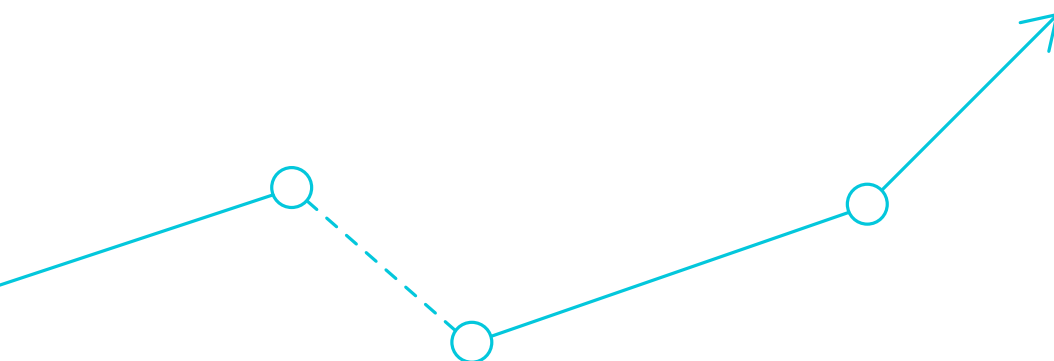
Was enthält dieser Leitfaden?

Dieser Leitfaden beginnt mit der **menschlichen** Seite der Compliance und beleuchtet die Rolle von Vertrauen, Kultur und Führung bei der Gestaltung effektiver Ethik- und Compliance-Programme in Deutschland. Themen sind unter anderem die Förderung einer offenen Speak-up-Kultur – und warum diese in Deutschland besondere Herausforderungen mit sich bringt – sowie die Stärkung der Stimme von Compliance in der Führungsetage. Dieser Abschnitt zeigt, wie Kultur und Strategie ineinandergreifen, um widerstandsfähige, wertorientierte Unternehmen zu formen.

Im Anschluss richtet sich der Blick auf den Aufbau und die Umsetzung von Compliance-Programmen. Was macht sie erfolgreich? Wie lassen sie sich sinnvoll in bestehende Unternehmensstrukturen integrieren? Ein praxisorientierter Leitfaden mit umsetzbaren Empfehlungen unterstützt bei der Einrichtung oder Verbesserung von Programmen.

Der zweite Teil des Leitfadens widmet sich der **rechtlichen und regulatorischen Landschaft**. Er gibt einen klaren Überblick über zentrale Gesetze und Rahmenbedingungen: vom **Datenschutz** und **Arbeitsrecht** über die aktuellen EU-Richtlinien wie **CSRD**, **CSDDD** und das **KI-Gesetz** bis hin zum **Hinweisgeberschutzgesetz**. Zudem erhalten Unternehmen praxisnahe Hinweise zu den Anforderungen für wirksame Hinweisgebersysteme – von internen Meldekanälen bis zu Schutzmechanismen gegen Repressalien.

Gemeinsam liefern diese Abschnitte eine solide Grundlage, um Compliance-Programme rechtlich fundiert und zugleich kulturell stark aufzustellen – damit Ihr Unternehmen Risiken immer einen Schritt voraus ist und mit Integrität führt.



Aufbau einer starken Compliance-Kultur

Zusammenfassung

Ein wirklich effektives Compliance-Programm beginnt bei den Menschen – ihrem Vertrauen in die Führungskräfte, ihrer Unternehmenskultur und den Systemen, die ethisches Verhalten fördern. Dieser Abschnitt untersucht die grundlegenden Elemente einer starken Compliance-Kultur, von der Förderung des Vertrauens innerhalb der Unternehmen und der Ermutigung zur Meldung von Missständen bis hin zur Stärkung der Rolle von Compliance-Führungskräften und der Gestaltung von Programmen für langfristigen Erfolg.

Vertrauen – eine wertvolle Ressource für Ethik und Compliance

Selbst wenn ein Unternehmen einen exzellenten Ruf hat, was ethische Geschäftspraktiken angeht, dürften die Feinheiten seines Compliance-Programms den allermeisten Kunden unbekannt sein. Kunden und andere Stakeholder messen effektiver Compliance zwar eine große Bedeutung bei, doch nur wenige von ihnen beschäftigen sich mit den konkreten Maßnahmen. Vielmehr achten Kunden auf die Reputation des Unternehmens und vertrauen darauf, dass es mit hohen ethischen Standards arbeitet.

Diese Vertrauensdynamik spielt für Compliance-Manager, die mit ihren Programmen einen geschäftlichen Mehrwert generieren wollen, eine entscheidende Rolle. Auch wenn Kunden, externe Partner und andere Beteiligte die genauen Abläufe des Compliance-Programms nicht kennen, kann das *Vertrauen* der Stakeholder, dass das Unternehmen Risiken kontrolliert und ethisches Verhalten fördert, den Weg zu stärkeren Geschäftsbeziehungen ebnen.

Compliance-Programme, die unterstreichen, wie wichtig es ist, inner- und außerhalb eines Unternehmens *Vertrauen aufzubauen*, werden tendenziell am stärksten mit positiven Geschäftsentwicklungen in Verbindung gebracht. Programmen dagegen, die sich lediglich auf Compliance im Hintergrund fokussieren, wird es eher schwerfallen, den wahren Wert ihrer Arbeit zu vermitteln und damit Kunden und andere Geschäftspartner zu erreichen. Compliance sollte nicht im Hintergrund stehen, sondern vielmehr ein fester Bestandteil der Marke sein.

„Compliance sollte nicht im Hintergrund stehen, sondern vielmehr ein fester Bestandteil der Marke sein.“

Die Zwänge des heutigen Risikoumfelds

„Rufschädigung“ stellt ein wesentliches Problem für Unternehmen dar, die unter den heutigen Risikobedingungen aktiv sind. Dieser Begriff steht für die potenziellen Auswirkungen von realen oder auch subjektiv empfundenen ethischen Fehlern auf Geschäftsbeziehungen. Diese führen oft, aber nicht immer, zu einer negativen Medienberichterstattung. Zudem können bei den Kunden erhebliche Zweifel daran entstehen, dass ein Unternehmen in der Lage ist, ein effektives Compliance-Programm umzusetzen.

Eine [kürzlich von NAVEX durchgeführte Umfrage](#) (in englischer Sprache) unter Compliance-Experten weltweit ergab, dass 14% der fast 1.000 Befragten angaben, ihr Unternehmen habe in den letzten drei Jahren aufgrund von Fehlverhalten von Führungskräften einen Reputationsschaden erlitten. Es ist durchaus möglich, dass der tatsächliche Anteil höher ist – neun Prozent gaben an, dass sie keine Compliance-Probleme offenlegen könnten.

Dies ist nur ein kleiner Einblick in die wichtige Rolle, die ein Compliance-Programm bei der Verhinderung von Rufschäden spielen kann. Wenn Kunden, externe Geschäftspartner, Aufsichtsbehörden und andere ein Unternehmen und dessen Einsatz für Ethik und Compliance als „nicht vertrauenswürdig“ wahrnehmen, zieht dies möglicherweise negative Konsequenzen nach sich. Fehlverhalten von Führungskräften ist nur ein Faktor, der den Ruf eines Unternehmens gefährden kann. Dabei müssen sich Compliance-Beauftragte stets vor Augen führen, dass eine Rufschädigung ganz reale Auswirkungen hat.

Compliance-Führungskräfte bewerten solche Unternehmenskulturen besser, in denen die oberste Managementebene hinter den Werten von Ethik und Compliance steht. Die bereits erwähnte NAVEX-Studie stellte einen engen Zusammenhang zwischen dem subjektiv wahrgenommenen Reifegrad des Compliance-Programms und dem Engagement der Unternehmensführung fest.

Drittparteien und die Bedeutung von Vertrauen

In den derzeitigen Geschäftsstrukturen sind bei fast allen Unternehmen die Leistungen von Drittanbietern fest in Betriebsabläufe eingebunden. Zahlungssoftware, Lieferketten und viele andere Bereiche sind eng mit einem Netzwerk von Dienstleistern verknüpft, die für den Kunden nicht vom Kerngeschäft zu trennen sind.

Durch diese Dynamik rückt die Bedeutung von Vertrauen als Geschäftsressource noch stärker in den Fokus. Hier können wir das [deutsche Lieferkettengesetz](#) als exemplarisches Beispiel für die zunehmende behördliche Kontrolle von Geschäftsbeziehungen mit Dritten betrachten. Die Dauerhaftigkeit, die ethischen Grundlagen und die Resilienz solcher Beziehungen sind wichtig. Wenn Kunden und Geschäftspartner darauf vertrauen, dass ein Unternehmen diese Beziehungen ernst nimmt, geht daraus ein produktiverer Austausch hervor, der wiederum Geschäftschancen eröffnet.

Auf diesem Feld bieten sich Unternehmen zahlreiche Gelegenheiten, sich weiterzuentwickeln und zu wachsen. Der gleichen NAVEX-Umfrage zufolge verwenden nur 33% der Organisationen bei der Überprüfung von Drittparteien einen risikogewichteten Bewertungsansatz. Demzufolge könnten viele Unternehmen ihre Ressourcen bei der Prüfung ihrer Lieferketten strategischer einsetzen. Zudem besteht eine Chance darin, den risikobasierten Ansatz bei der Lieferkettenprüfung gegenüber potenziellen Kunden zu kommunizieren.

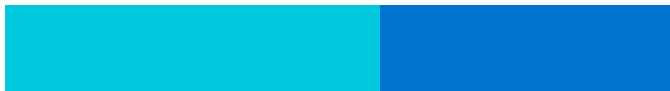


der Unternehmen verwenden bei der Überprüfung von Drittparteien einen risikogewichteten Bewertungsansatz.

Internes Whistleblowing als Ausdruck von „Vertrauenskultur“

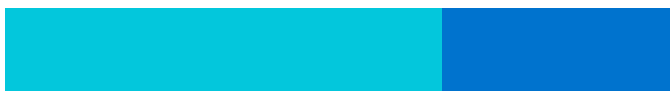
Viele Compliance-Experten betrachten internes Whistleblowing als Indikator für eine gesunde Ethik- und Compliance-Kultur. Wenn jemand ohne Angst vor negativen Konsequenzen eine Meldung machen und darauf zählen kann, dass das Unternehmen die Probleme ernst nimmt, zeigt dies ein grundlegendes Maß von internem Vertrauen. Eine solche interne Kultur geht höchstwahrscheinlich auch mit einer positiven Außenwirkung einher.

56%



Weltweit haben im Durchschnitt 56% der Hinweisgeber ihre Meldungen im Jahr 2024 anonym gemacht.

65%



Dies ist der letzte Stand eines seit 2009 anhaltenden Abwärtstrends bei anonymen Meldungen. 2009 betrug die anonyme Melderate noch 65%.

Bei der Betrachtung der entsprechenden Kennzahlen sollten Unternehmen die Anzahl der anonymen *Meldungen pro 100 Mitarbeiter* neben globalen und regionalen Trends auch mit dem eigenen historischen Durchschnitt vergleichen. Der jährlich von NAVEX veröffentlichte [Benchmark-Bericht zu Risiko und Compliance](#) (in englischer Sprache) liefert Hinweise zur Berechnung dieser und vieler anderer Kennzahlen.

Weltweit haben im Durchschnitt 56% der Hinweisgeber ihre Meldungen im Jahr 2024 anonym gemacht. Dies ist der letzte Stand eines seit 2009 anhaltenden Abwärtstrends bei anonymen Meldungen. 2009 betrug die anonyme Melderate noch 65%.

Die Möglichkeit einer anonymen Meldung ist zwar unverzichtbar für jedes Whistleblowing-Programm, allerdings kann eine niedrigere anonyme Melderate auch auf ein höheres Maß an Vertrauen hindeuten – nicht nur in das Programm, sondern in das Unternehmen.

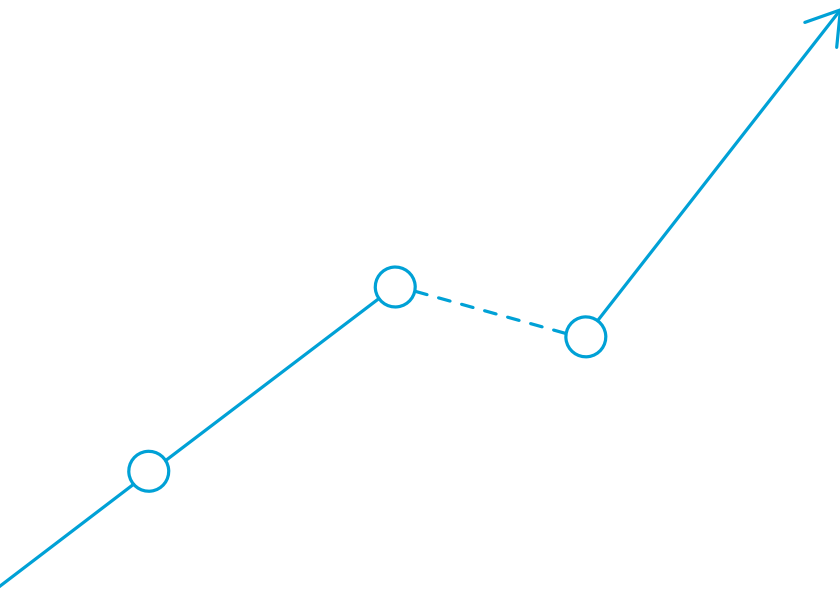
Interessant dabei ist auch, dass 2023 43% der externen Meldungen anonym erfolgten. Dem stehen 58% der internen Meldungen gegenüber. Daraus lässt sich die Überlegung ableiten, dass die Reputation eines Unternehmens am Markt Einfluss darauf hat, ob externe Whistleblower lieber anonym bleiben.

Schlussbemerkungen

„Vertrauen“ – und der ihm innewohnende Wert – kann in ergebnisorientierten Führungsetagen ein schwierig zu vermittelndes Thema sein. Dennoch ist es einfach, die Bedeutung von „Vertrauen“ auf eine Weise zu erzählen, die die meisten Führungskräfte erreicht. Bei welchen Marken haben Sie *Vertrauen*, dass diese über ethische Lieferketten verfügen? Können Sie diese Annahme mit Daten untermauern? Ist unterm Strich nicht *Vertrauen* die entscheidende Währung bei schnellen Geschäftsentscheidungen? Ist Vertrauen etwas, das unserem Unternehmen eine führende Position verschafft?

Neben den unumgänglichen regulatorischen Compliance-Verpflichtungen braucht „Compliance“ als Geschäftsressource ein entsprechendes Storytelling. Unternehmen, die ethische Entscheidungen treffen, können Verbrauchern mit nachhaltiger Wirkung vermitteln, dass sie diese wichtigen Fragen ernst nehmen.

Leider wird Compliance häufig nur als Hintergrundprozess betrachtet, doch die Realität sieht anders aus. Verbraucher, Geschäftspartner und viele andere legen Wert darauf, dass Unternehmen Vorschriften einhalten und ethisch arbeiten. „Vertrauen“ ist unbezahlbar. Gleichzeitig befindet sich die Compliance-Abteilung in der besten Position, Vertrauen aufzubauen und zu stärken und es als Wettbewerbsvorteil am Markt zu nutzen.



Whistleblowing in Deutschland: ein Thema mit Potenzial

Im März 2025 verurteilte der Europäische Gerichtshof in Luxemburg die Bundesrepublik Deutschland zu einer Strafzahlung von 34 Millionen Euro. Der Grund: Deutschland hatte sich 18 Monate Zeit gelassen, die EU-Richtlinie zum Whistleblowing vollständig umzusetzen und damit die Menschen, die Hinweise auf Missstände in Unternehmen geben, nach Auffassung des Gerichts nicht ausreichend geschützt.

Die EU-Whistleblower-Richtlinie ist am 16. Dezember 2019 in Kraft getreten. Die Mitgliedstaaten der EU hatten bis spätestens 17. Dezember 2021 Zeit, sie in nationales Recht umzusetzen. Das entsprechende deutsche Hinweisgeberschutzgesetz (HinSchG) wurde jedoch erst im Juli 2023 rechtsverbindlich. Diese Verspätung ist nur ein Indiz dafür, dass sich Deutschland schwertut mit dem Thema – dabei könnten deutsche Unternehmen vom Whistleblowing erheblich profitieren.

Was ist die EU-Whistleblowing-Richtlinie?

Ob Korruption, illegale Machenschaften oder ethisch fragwürdige Praktiken, ob geheime Absprachen, Umweltverstöße oder individuelles Fehlverhalten: Vielfach kommen Missstände in Unternehmen oder Behörden erst durch die Hinweise mutiger Menschen ans Licht der Öffentlichkeit.

Die EU-Whistleblower-Richtlinie von 2019 will Personen, die im beruflichen Kontext Informationen über Verstöße gegen EU-Recht erhalten und melden, vor Repressalien schützen. Sie soll verhindern, dass Hinweisgeber eingeschüchtert, degradiert oder gekündigt werden. Die Richtlinie sieht außerdem die Vertraulichkeit der Identität von Whistleblowern vor.

Und: Eine Meldung soll nicht einfach in der Versenkung verschwinden. Organisationen, denen Missstände gemeldet werden, müssen deren Eingang innerhalb von sieben Tagen bestätigen und binnen drei Monaten über ergriffene Maßnahmen berichten.

Die Richtlinie verpflichtet Unternehmen ab 50 Mitarbeitenden zur Einrichtung interner Meldestellen. Sie schreibt allerdings nicht vor, dass anonyme Meldungen entgegengenommen werden müssen; es bleibt nationalen Gesetzgebern überlassen, ob sie die Möglichkeit zur Anonymität verpflichtend vorschreiben oder nicht.

„Die Richtlinie verpflichtet Unternehmen ab 50 Mitarbeitenden zur Einrichtung interner Meldestellen.“

Wieso Whistleblowing so wertvoll ist

Whistleblowing ist im ureigenen Interesse eines Unternehmens, denn es bietet viele Vorteile – nicht nur mit Blick auf die Risikominimierung, sondern auch als Katalysator für Integrität, Innovation und Mitarbeiterbindung. Frühzeitige Hinweise auf Missstände helfen Unternehmen, gravierende rechtliche, finanzielle oder Image-Schäden abzuwenden. Interne Meldungen sind oft die erste und wichtigste Informationsquelle bei Compliance-Verstößen. Denn wer kennt das Unternehmen besser als die Menschen, die für oder mit ihm arbeiten?

Wer seine Beschäftigten dazu ermutigt, Probleme anzusprechen, statt sie zu vertuschen, kann Fehler im besten Fall beheben, bevor sie dem Unternehmen schaden. Valide [Studien](#) belegen, dass Organisationen mit funktionierenden Hinweisgebersystemen seltener von Behörden verfolgt oder sanktioniert werden und langfristig bessere Unternehmenskennzahlen aufweisen.

Ein professionelles Whistleblowing-System schafft Vertrauen und sorgt für Transparenz. Schulungen und eine gute, offene Kommunikation sorgen dafür, dass Ressentiments, Ängste und Unsicherheiten abgebaut werden und die Menschen sich trauen, Missstände zu benennen.

Warum Whistleblowing in Deutschland ein sensibles Thema ist

Die verspätete und politisch umstrittene Umsetzung der EU-Whistleblower-Richtlinie in Deutschland hängt sowohl mit politischen Differenzen als auch mit tief verankerten kulturellen Haltungen zusammen. Die Gegner einer strengen Auslegung fürchteten, dass Whistleblowing-Systeme für falsche Anschuldigungen oder persönliche Abrechnungen missbraucht werden könnten. Außerdem untergrabe ein anonymes Verfahren das gegenseitige Vertrauen innerhalb von Organisationen.

Diese Sorge speist sich aus historischen Erfahrungen: Sowohl in der NS-Zeit als auch in der DDR waren anonyme Anzeigen Teil staatlicher Unterdrückung. Das hinterlässt bis heute kulturelle Spuren und führt dazu, dass Whistleblowing in Deutschland häufig mit Denunziantentum gleichgesetzt wird. Hinweisgebern wird deshalb vielerorts erst einmal mit Misstrauen und Skepsis begegnet. So wundert es also nicht, dass sich Deutschland gegen ein anonymes Verfahren entschieden hat. Interessant ist, dass die deutsche Wirtschaft anders handelt als die Politik vorgibt: Obwohl keine Verpflichtung zur Entgegennahme anonymer Hinweise besteht, bietet die Mehrheit der Unternehmen in Deutschland entsprechende Lösungen und geht damit über die gesetzlichen Vorgaben hinaus.

„Interessant ist, dass die deutsche Wirtschaft anders handelt als die Politik vorgibt: Obwohl keine Verpflichtung zur Entgegennahme anonymer Hinweise besteht, bietet die Mehrheit der Unternehmen in Deutschland entsprechende Lösungen und geht damit über die gesetzlichen Vorgaben hinaus.“

Dennoch ist Whistleblowing in Deutschland nach wie vor nicht an der Tagesordnung: Viele Unternehmen in Deutschland sind hierarchisch organisiert; es mangelt an einer Fehler- und Feedbackkultur. Werte wie Ordnung, Pflichtbewusstsein und Loyalität zum Unternehmen prägen das Verhalten vieler Mitarbeitender. Kritik, insbesondere an Führungskräften, wird lieber intern und diskret geäußert – oder eben gar nicht. Der Wunsch nach einem reibungslosen Miteinander führt außerdem dazu, dass Konflikte nicht offen angesprochen werden. Der Schutz von Beziehungen im Team oder zu Vorgesetzten hat vielfach Vorrang vor dem Schutz der Organisation oder der Öffentlichkeit. Gerade in kleinen und mittleren Unternehmen wird die Veröffentlichung von Missständen im Unternehmen sogar als „Nestbeschmutzung“ oder Verrat betrachtet. Probleme werden intern und im Stillen geregelt. Wer Unregelmäßigkeiten aufzeigt, durchbricht diesen informellen Konsens und riskiert, selbst als Problem gesehen zu werden.

Noch eine weitere Entwicklung sorgt dafür, dass viele Mitarbeitende in Deutschland lieber den Mund halten, statt Missstände zu benennen: Sie sind unmotiviert. Laut dem Gallup Engagement Index 2024 ist die emotionale Bindung an den Arbeitgeber in Deutschland auf einem historischen Tiefstand angelangt. Das Vertrauen in Führungskräfte sinkt, und eine große Mehrheit der Beschäftigten macht laut Gallup lediglich „Dienst nach Vorschrift“. In diesem Klima fällt es schwer, eine offene Speak-up-Kultur zu etablieren.

Gegen den Trend

Die Einführung der gesetzlichen Vorgaben hat das Thema Whistleblowing in Deutschland stärker ins öffentliche und betriebliche Bewusstsein gerückt. Doch während die Anzahl interner Meldungen in vielen europäischen Ländern zwar leicht zunimmt, ist die Anzahl der Meldungen im Vergleich zu anderen Regionen weiterhin im unteren Bereich.

Laut dem [Regionalen Hinweisgeber- und Vorfallsmanagement-Bericht von NAVEX](#) aus dem Jahr 2025 ist die durchschnittliche Melderate im untersuchten Zeitraum unter den Melderaten in den Region Asien-Pazifik, Nordamerika und Südamerika.

Viele potenzielle Hinweisgeber fürchten berufliche Nachteile oder zweifeln daran, dass ihre Meldung ernst genommen wird. Sie haben Angst vor Repressalien, sind unsicher, an wen genau sie sich eigentlich mit einer Meldung wenden können oder kennen die vorhandenen Kommunikationskanäle nicht. Auch technische Hürden und unklare Prozesse schrecken ab. Hinzu kommt, dass Führungskräfte häufig nicht gut genug geschult sind, um Hinweise richtig aufzunehmen und zu bearbeiten.

„Doch während die Anzahl interner Meldungen in vielen europäischen Ländern zwar leicht zunimmt, ist die Anzahl der Meldungen im Vergleich zu anderen Regionen weiterhin im unteren Bereich.“

Damit lassen deutsche Unternehmen eine große Chance ungenutzt, besser zu werden, rechtskonform zu wirtschaften und ihre Wettbewerbsposition und Resilienz zu stärken.

Deutsche Besonderheiten als Chance für effektives Whistleblowing

Die deutsche Unternehmenskultur birgt zwar etliche Herausforderungen, aber auch viele Anknüpfungspunkte, um eine tragfähige Whistleblowing-Kultur zu etablieren. So verfügen die Menschen in Deutschland zum Beispiel über ein starkes Bewusstsein für Normen und Regeln – sowohl rechtlich als auch ethisch. Diese Grundhaltung sollten Unternehmen nutzen, um Whistleblowing als das zu positionieren, was es ist: ein Beitrag zur Sicherung von Qualität, Ordnung und unternehmerischer Integrität. Wer Missstände meldet, handelt schließlich regelkonform – nicht regelwidrig.

Deutsche Unternehmen sind außerdem oft gut darin, Verfahren zu dokumentieren und kontinuierlich zu verbessern, auch das ist ein idealer Ausgangspunkt für nachhaltige Hinweisgebersysteme.

Auch die starke Identifikation mit dem Unternehmen und dem Team kann als Motor für Whistleblowing dienen. Denn Hinweise auf Missstände sind kein Angriff auf das Unternehmen, sondern ein Beitrag, um es zu schützen. Wenn diese Botschaft in den Köpfen verankert wird, dann wird Whistleblowing als positiv wahrgenommen.

Letztlich hängt der Erfolg eines Whistleblowing-Systems eng mit der Kommunikation zusammen. Whistleblowing sollte als sachliches Verfahren zur Risikoprävention positioniert werden – nicht als moralische Anklage. Das fängt schon bei der Wortwahl an. Statt von „Whistleblowern“ oder „Meldung von Fehlverhalten“ zu sprechen, empfehlen sich Begriffe wie „Risikohinweis“, „Qualitätssicherung“ oder „Vertrauenskanal“, um kulturelle Hürden abzubauen.

„Wer Missstände meldet, handelt schließlich regelkonform – nicht regelwidrig.“

Unser Tipp

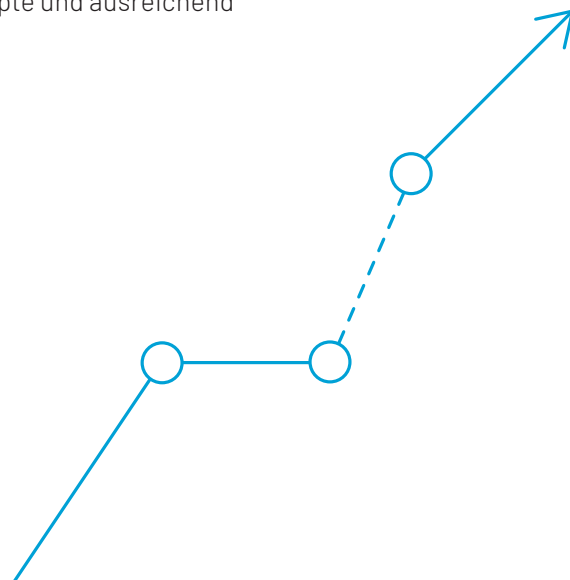
Es liegt auf der Hand: Auch für deutsche Unternehmen lohnt es sich, Whistleblowing nicht nur als regulatorische Pflicht, sondern als Chance zur Stärkung ihrer Unternehmenskultur und Resilienz zu verstehen. Wer mit klaren Strukturen, gelebten Werten und transparenter Kommunikation Vertrauen schafft, kann Whistleblowing als strategisches Instrument für Integrität und langfristigen Unternehmenserfolg nutzen.

Wir empfehlen, folgende Punkte zu beachten:

- **Schutz:** Hinweisgeber müssen darauf vertrauen können, dass ihre Identität geschützt wird.
- **Anonymität:** Anonyme Meldungen ermöglichen, auch wenn sie gesetzlich nicht gefordert sind.
- **Erreichbarkeit:** Unterschiedliche, klare und leicht zugängliche Meldewege: telefonisch, digital und über eine interne oder externe Vertrauensperson.
- **Information:** Regelmäßige Aufklärung der Mitarbeitenden über ihre Rechte und die Funktionsweise des Systems.
- **Saubere Prozesse:** Die Meldestellen brauchen klar definierte Zuständigkeiten, Datenschutzkonzepte und ausreichend Ressourcen.

- **Transparenz:** Eine transparente Bearbeitung der Hinweise und eine Rückmeldung an die Mitarbeitenden stärkt das Vertrauen zusätzlich.
- **Verpflichtung:** Die Führungsebene des Unternehmens muss hinter dem Whistleblowing stehen und es unterstützen, damit es von allen als legitimes Instrument wahrgenommen wird.
- **Mindset:** Positionierung des Whistleblowing-Systems als wichtiger strategischer Baustein, um ethisch korrekt zu wirtschaften, das Unternehmen vor Schäden zu bewahren und seine Resilienz nachhaltig zu stärken.
- **Integration:** Whistleblowing nicht isoliert, sondern als Teil eines umfassenden Compliance- und Integritätsmanagements etablieren.

Wenn Sie als Unternehmen in Deutschland tätig sind, lohnt es sich, jetzt zu handeln: Investieren Sie in die Weiterentwicklung Ihrer Whistleblowing-Systeme – nicht nur, um gesetzlichen Vorgaben gerecht zu werden, sondern um Vertrauen zu schaffen, Risiken frühzeitig zu erkennen und eine Kultur der Offenheit zu fördern.



Wie Chief Compliance Officers im Management mehr bewegen können

Die Rolle der Chief Compliance Officers (CCOs) umfasst inzwischen mehr als nur die reine Risikosteuerung – sie nehmen auch wichtige strategische Aufgaben wahr. Heute sind CCOs Verantwortungsträger für regulatorische Compliance und strategische Partner der Unternehmensführung. Sie prägen die Unternehmenskultur, treiben die Realisierung von Geschäftszielen voran und nutzen die Möglichkeiten der Technik, um ethische Prinzipien und Resilienz im Unternehmen zu stärken.

CCOs als strategische Berater – den Weg weisen mit Daten

CCOs tragen Sorge dafür, dass Compliance in die langfristigen Unternehmensziele einfließt. Sie liefern datengetriebene Erkenntnisse, die Entscheidungen stützen und ein nachhaltiges Wachstum ermöglichen. Durch ihren Fokus auf Compliance unterstützen CCOs die Führungsebene im Umgang mit Risiken wie Datenschutzbestimmungen, Fragen von Umwelt, Sozialem und Governance (ESG) oder Reputationsschäden für das Unternehmen.

„Immer mehr Unternehmen erkennen, dass sie Compliance in ihre grundlegenden Geschäftsstrategien einbinden müssen, um resilienter zu werden.“

Immer mehr Unternehmen erkennen, dass sie Compliance in ihre grundlegenden Geschäftsstrategien einbinden müssen, um resilienter zu werden. Compliance-Daten liefern CCOs Erkenntnisse, mit denen sie ein deutlicheres Bild von aufkommenden Bedrohungen für Stabilität und Wachstum zeichnen können. Indem CCOs solche Herausforderungen antizipieren, unterstützen sie ihr Unternehmen dabei, konkurrenzfähig zu bleiben und gleichzeitig Vorschriften und Vorgaben einzuhalten.

Compliance in die Geschäftsstrategie integrieren

Angesichts zunehmender regulatorischer Anforderungen und eines genaueren Blicks auf das Geschäftsgebaren von Unternehmen stellt Compliance einen unverzichtbaren Bestandteil der grundlegenden Geschäftsstrategie dar.

- CCOs sorgen dafür, dass das Risikomanagement den langfristigen Geschäftszielen entspricht, und setzen sich für einen proaktiven Umgang mit Compliance ein.
- Compliance-Daten liefern Führungskräften wesentliche Informationen, um informierte und risikobewusste Entscheidungen zu treffen, die die Compliance und den Erfolg des Unternehmens unterstützen.

Laut Erkenntnissen aus dem von [NAVEX herausgegebenen Leitfaden zur Risikoresilienz 2024](#) sehen sich Unternehmen mit einem höheren Ausmaß an regulatorischen Herausforderungen konfrontiert. Hinzu kommt eine starke Zunahme sozialer Fragestellungen, von ESG bis hin zu Arbeitnehmerrechten, die zu einem zentralen Faktor im Risikomanagement werden.

Durchblick in einem komplexen Geflecht von Richtlinien und Gesetzen

CCOs müssen neue Herausforderungen in Bereichen wie Datenschutz, ESG und Sanktionen stets im Blick behalten und dafür sorgen, dass ihr Unternehmen für diese Herausforderungen gerüstet ist. Indem sie zukünftige Problemstellungen erkennen und sich rechtzeitig darauf vorbereiten, können sie Risiken mindern und eine entsprechende Resilienz aufbauen.

Beispielsweise entwickeln sich Datenschutzvorschriften kontinuierlich weiter, während entsprechende Verstöße mit erheblichen Strafzahlungen und Rufschäden einhergehen können. Ein proaktiver CCO sorgt dafür, dass sich das Unternehmen auf diese Veränderungen einstellt, was wiederum den Ruf und die Geschäftsergebnisse absichert.

Eine Ethik- und Compliance-Kultur entwickeln

Ethische Führung bildet das Fundament einer starken Unternehmenskultur. Hier kommt dem CCO eine Schlüsselrolle zu, wenn es darum geht, Ethik und Compliance in den Alltagsbetrieb zu integrieren. Eine proaktive Compliance-Kultur ermutigt Mitarbeiter, ethische Entscheidungen zu treffen, und senkt gleichzeitig das Risiko von Compliance-Verstößen.

- **Schaffung einer proaktiven Compliance-Kultur:** Der Einsatz des CCO für eine Unternehmenskultur, in der Ethik eine zentrale Rolle spielt, stärkt die Compliance und fördert das Engagement und Vertrauen der Mitarbeiter.
- **Steuerung von externen Risiken:** Die Bedeutung des Drittparteien-Risikomanagements darf keinesfalls unterschätzt werden. CCOs achten darauf, dass Auftragnehmer und Partner die ethischen Standards des Unternehmens erfüllen, und schützen es so vor externen, potenziell geschäftsschädigenden Risiken.

Der [NAVEX 2025 Whistleblowing & Incident Management Benchmark Report](#) (in englischer Sprache) zeigt, dass Unternehmen mit überdurchschnittlich hohen Melderaten in der Regel einen größeren Anteil an Meldungen über Verhaltensweisen am Arbeitsplatz erhalten. Dies unterstreicht die Bedeutung der Förderung einer Compliance-Kultur, in der sich Mitarbeiter ermächtigt fühlen, sich zu äußern.

Technische Möglichkeiten für eine smartere Compliance nutzen

Während neue Technologien ganze Branchen verändern, sollten auch CCOs die Möglichkeiten von Tools wie KI und Automatisierung für den Ausbau ihrer Compliance-Arbeit nutzen. Mithilfe von KI können Teams Aufgaben effizienter bearbeiten, Daten effektiver analysieren und Risikopotenziale erkennen, bevor sie eskalieren.

- **KI und automatisierte Compliance:** Indem CCOs auf KI setzen, um manuelle Compliance-Bemühungen zu reduzieren, steigern sie die Effizienz und verbessern Risikovorhersagen. Hierbei müssen sie auch ethische Fragen bedenken und funktionsübergreifend arbeiten, um KI-Richtlinien zu entwickeln, mit denen die Einhaltung der im Wandel befindlichen Rechtsvorschriften gewährleistet ist.
- **IT- und Datensicherheit:** Gemeinsam mit den Chief Information Security Officers (CISOs) arbeiten CCOs daran, Cybersicherheitsrisiken zu reduzieren, die nach wie vor zu den Hauptproblemen für Unternehmen zählen. Sichere Verfahren bei der Daten-Governance schützen sensible Informationen, stärken die Compliance und schützen den Ruf des Unternehmens.

Compliance auch in der Führungsetage

CCOs werden zunehmend in die Entscheidungsfindung der Führungsebenen eingebunden, insbesondere da sie das Risikobewusstsein im Unternehmensvorstand stärken. Die Fähigkeit der CCOs, aus komplexen Compliance-Fragen handlungsorientierte Erkenntnisse abzuleiten, unterstützt Entscheidungsträger dabei, der Compliance bei der strategischen Planung eine hohe Priorität einzuräumen.

- **Risikobewusstsein der Führungsebene stärken:** CCOs unterstreichen gegenüber der Unternehmensführung die Bedeutung von Compliance für das gesamte Risikomanagement – sei es im Rahmen von ESG oder Datenschutzbestimmungen. Auf diese Weise prägen sie den Umgang ihres Unternehmens mit essenziellen Herausforderungen.
- **Compliance-Kennzahlen verständlich vermitteln:** Anhand von Compliance-Daten die konkrete Situation greifbar zu machen, auch Daten-Storytelling genannt, ist eine unverzichtbare Fähigkeit. CCOs müssen Daten auf eine Weise präsentieren, die auch Führungskräfte mit einem anderen fachlichen Hintergrund erreicht und Risiken und Chancen klar und handlungsorientiert aufzeigt.

Ein Erkenntnis des [Leitfadens zur Risikoresilienz](#) fördert eine Best Practice zutage: Daten-Storytelling ist heutzutage eine wesentliche Kompetenz für CCOs, um sicherzustellen, dass Probleme auf höchster Ebene verstanden und priorisiert werden.

Compliance und Unternehmensziele in Einklang bringen

Bei Compliance geht es nicht mehr nur darum, Vorschriften zu erfüllen, vielmehr handelt es sich um ein leistungsstarkes Werkzeug, um Geschäftschancen zu erschließen. CCOs zeigen, wie Compliance Innovationen vorantreiben, Wettbewerbsvorteile schaffen und nachhaltiges Wachstum ermöglichen kann.

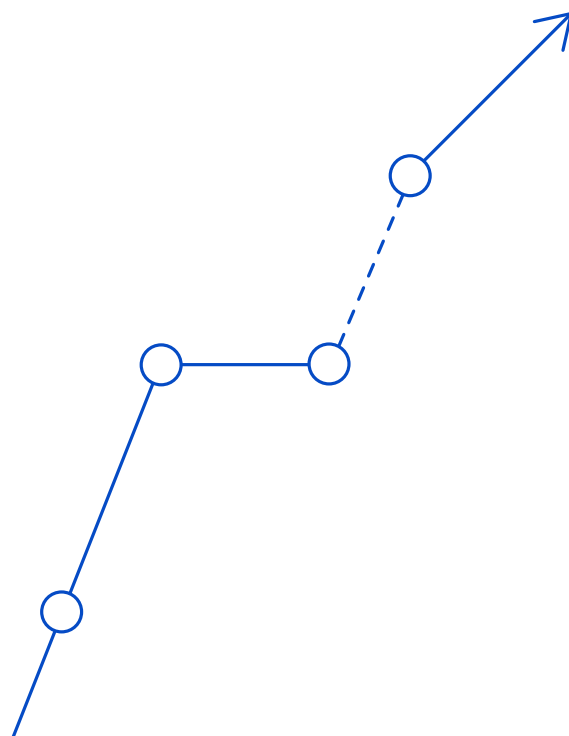
- **Compliance zu einer treibenden Kraft für Geschäftschancen machen:** Unternehmen, die Compliance als strategische Ressource betrachten, steigern ihre Innovationskraft und Wettbewerbsfähigkeit. CCOs übernehmen eine Schlüsselrolle dabei, Compliance in einen Wachstumsmotor zu verwandeln.
- **Risiken und Chancen abwägen:** CCOs helfen der Unternehmensführung, die Balance zwischen kalkuliertem Risiko und ethischer Governance zu finden. Indem sie Compliance und agile Geschäftsprozesse zusammenführen, unterstützen sie mit ihrem Risikomanagement unternehmerische Innovation ohne Abstriche bei ethischen Standards.

Diese strategische Rolle spielen CCOs für den Geschäftserfolg

Mit der neuen Rolle des CCO wandelt sich Compliance vom isolierten Aufgabenbereich zum strategischen Erfolgsfaktor für das gesamte Unternehmen. Indem CCOs wertvolle Erkenntnisse liefern, eine ethische Kultur stärken und technische Innovationen integrieren, leisten sie unternehmensweit einen entscheidenden Beitrag zu Resilienz und Wachstum.

Für Führungskräfte stellt Compliance nicht länger eine optionale Investition dar, sondern ist längst obligatorisch geworden. Unternehmen, die erkannt haben, welche strategische Bereicherung CCOs in der Führungsetage darstellen, bleiben konkurrenzfähig, resilient und ethischen Standards verpflichtet.

Compliance mindert Risiken **und** erschließt gleichzeitig Chancen für nachhaltigen Erfolg. Der CCO steht heute im Zentrum dieser Transformation und weist Unternehmen den Weg in eine Zukunft, in der Compliance zum Fundament für Fortschritt wird.



8 Schritte zu einem effektiven Compliance-Programm

Woche 1

Risikobewertung

Eine Risikobewertung ist eine entscheidende Voraussetzung, um ein Risikoprofil Ihres Unternehmens zu entwickeln und dieses vollständig zu verstehen – sie ist die Grundlage eines effektiven Programms. Ihr Risikoprofil ist eine Evaluation, bei der die speziellen Risiken Ihres Unternehmens vor dem Hintergrund seiner Branche, seines Standorts und seiner Belegschaft identifiziert werden. Eine regelmäßige umfassende Risikobewertung hilft Ihnen dabei, potenzielle strafrechtliche, ethische und Reputationsrisiken zu erkennen.

Die folgende Grafik bietet eine einfache Selbstbewertung, um zu bestimmen, wie Sie gegenwärtig Ihre Risiken evaluieren.

Grün: Wir haben bewährte Verfahren mit einem umfangreichen Risikobewertungsprozess

Gelb: Wir entwickeln gegenwärtig einen Prozess

Rot: Wir haben keinen Prozess und wissen nicht, wie wir einen einführen können

Wir bewerten regelmäßig Bereiche mit hohen Risiken und Bereiche, in denen strafrechtlich relevantes Verhalten auftreten kann	☐	☐	☐
Unsere Risikobewertungen umfassen ethische Risiken und Reputationsrisiken	☐	☐	☐
Das Ergebnis unserer Risikobewertungen und unsere Tätigkeitsberichte werden der Geschäftsleitung und/oder dem Vorstand vorgelegt	☐	☐	☐
Unsere Programmressourcen werden in einer risikoorientierten Weise eingesetzt	☐	☐	☐
Wir achten aufmerksam auf aufkommende Probleme und Entwicklungen, die unser Risikoprofil beeinflussen	☐	☐	☐

Wenn Ihre Antworten überwiegend in die grüne Spalte fallen, verfügen Sie über angemessene Prozesse, um ein genaues Bild von Ihren Risiken zu bekommen. Wenn die meisten Antworten in die gelbe oder rote Kategorie fallen, sollten Sie die in diesem Leitfaden enthaltenen Ressourcen genau prüfen, um eine bessere Vorstellung davon zu erhalten, wo bei Ihnen Risiken vorhanden sind.

Woche 2

Aufsicht, Aufbau und Leitung des Programms

Ein Compliance-Programm kann ohne Unterstützung der Geschäftsleitung und einer festgelegten Zuständigkeit für das Programm nicht effektiv sein. Ihr Programm braucht eine Aufsicht, um es gegen Risiken zu schützen, und die Unterstützung durch die Geschäftsleitung, damit sich das Verhalten der Mitarbeiter ändern und ein kultureller Wandel durchsetzen kann. Ebenso muss die oberste Aufsichtsebene einschließlich des Vorstands informiert und bei ihren Rollen innerhalb des Compliance-Programms geschult werden.

Stellen Sie sich die folgenden Fragen, um zu bewerten, ob sich Ihre Geschäftsleitung ausreichend für das Programm einsetzt.

Vorstand

- Kennt der Vorstand die Inhalte und Abläufe des Ethikprogramms?
- Übt der Vorstand eine angemessene Aufsicht über die Einführung und Effektivität des Programms und die Kultur des Unternehmens aus?
- Ist der Vorstand für Mitarbeiter mit Zuständigkeit für die tägliche Umsetzung des Compliance-Programms zugänglich, etwa durch Treffen bei Leitungssitzungen?

Leitung des Compliance-Programms

- Gibt es im Unternehmen eine hochrangige Person, der die Verwaltung des Compliance-Programms zugewiesen wurde, und eine Person mit der Zuständigkeit für die tägliche Umsetzung des Programms?
- Übt die Geschäftsleitung ihre Zuständigkeit bei der Gestaltung und Aufrechterhaltung einer Kultur aus, die die Einhaltung der Gesetze und ethischer Verhaltensweisen unterstützt, und hat sie ein Verständnis für diese Thematik?
- Gibt es ein Ethikkomitee oder einen Ethikrat, das/der Informationen von der hochrangigen Person oder der Person mit der Zuständigkeit für die tägliche Umsetzung erhält und zudem praktische Inputs zum Programm gibt?
- Sind der operativen Führungsebene Zuständigkeiten bei ethischen Fragen zugewiesen worden? Kennt sie die Inhalte und Abläufe des Ethikprogramms?

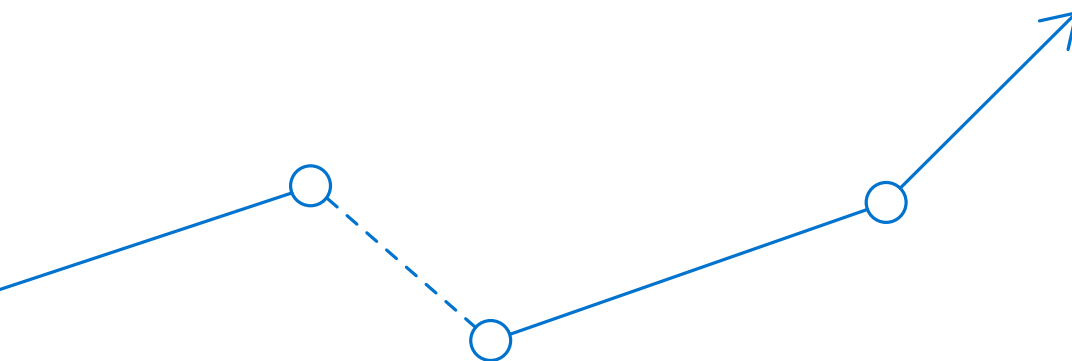
Wenn Sie viele dieser Fragen mit „Nein“ beantworten, erhalten Sie im Folgenden Tipps, wie Sie das Engagement für ethische Fragen seitens Ihres Vorstands und Ihrer Geschäftsleitung erhöhen können.

Zusätzliche Ressourcen für die Geschäftsleitung

Wenn Sie die Unterstützung des Vorstands erhalten haben, müssen Sie ihm auch effektiv Bericht erstatten. Erhalten Sie praktische Tipps und Ratschläge, wie Sie gegenüber dem Vorstand erfolgreich über die Compliance-Ergebnisse berichten können.

Um die Beteiligung des Vorstands zu erhöhen, empfiehlt sich ein engagiertes Storytelling, das ein Verständnis für die strategischen Ziele und Maßnahmen des Unternehmens und die integrale Rolle der Compliance bei der Anbahnung von Geschäften demonstriert. Weitere Tipps, wie Sie den Vorstand für ein vermeintlich langweiliges Thema begeistern können, erhalten Sie in diesem On-Demand-Webinar.

Webinar: [So motivieren Sie den Vorstand – Tipps für die Präsentation von Compliance-Maßnahmen \(in englischer Sprache\)](#)



Woche 3

Arbeitsplatzstandards: Richtlinien, Verfahren und Ihr Verhaltenskodex

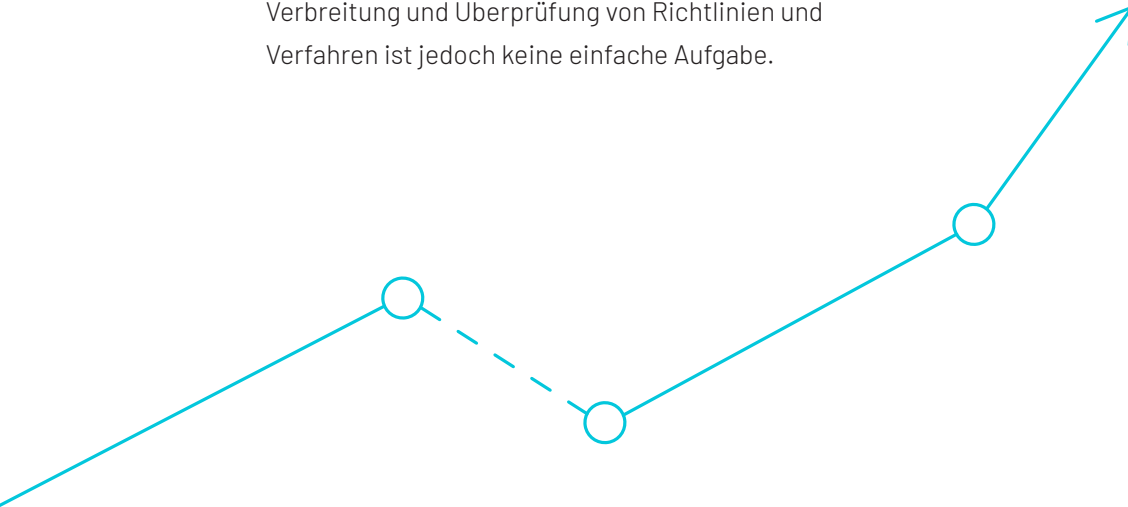
Bei der Schaffung der Grundlagen für ein effektives Compliance-Programm spielen Richtlinien und Verfahren eine große Rolle, ebenso wie Ihr Verhaltenskodex. Richtlinien und Verfahren sind ausschlaggebend, um die Kernwerte und Erwartungen Ihres Unternehmens (Richtlinien) und deren praktische Umsetzung (Verfahren) detailliert zu beschreiben. Ihr Verhaltenskodex ist der Eckpfeiler Ihres Unternehmensleitbilds. Darin wird das „Warum“ beschrieben und es werden geeignete Verhaltensweisen und Erwartungen an Ihre Mitarbeiter und an Dritte festgelegt.

Neben der Erstellung Ihrer Richtlinien und Verfahren müssen Sie auch darüber nachdenken, wie Sie die zunehmende Menge an Richtlinien bewältigen können, die Unternehmen zur Verwaltung des komplexen Compliance-Umfelds einführen müssen. Die Erstellung, Bearbeitung, Verbreitung und Überprüfung von Richtlinien und Verfahren ist jedoch keine einfache Aufgabe.

Zusätzliche Ressourcen:

[Warum eine „Richtlinie über Richtlinien“ so wichtig ist \(in englischer Sprache\)](#)

[Wie \(und warum\) gestalten Sie einen sinnvollen Verhaltenskodex zur Verbesserung der Kultur am Arbeitsplatz? \(in englischer Sprache\)](#)



Verwenden Sie die Grafik unten zur Selbstbewertung, um zu sehen, wie Ihre Richtlinien und Verfahren und die Inhalte Ihres Verhaltenskodex im Vergleich zu den Best Practices abschneiden.

- **Grün:** Wir haben einen Verhaltenskodex, der auf Best Practices beruht
- **Gelb:** Wir befinden uns in der Entwicklung unseres Verhaltenskodex
- **Rot:** Wir haben keinen Verhaltenskodex und wissen nicht, wie wir einen erstellen können

Standards			
Stellen der Verhaltenskodex und die Unternehmensrichtlinien Standards auf, die darauf abzielen, strafrechtlich relevantes Verhalten zu verhindern und zu erkennen?	☐	☐	☐
Verlangen die Richtlinien die Einhaltung der Unternehmenswerte und der geltenden Gesetze, Bestimmungen und Regulierungen?	☐	☐	☐
Werden in den Richtlinien mehrere Jurisdiktionen wie etwa die gesetzlichen Anforderungen auf föderaler, nationaler und internationaler Ebene berücksichtigt, wenn es um die Einhaltung der Compliance-Pflichten geht?	☐	☐	☐
Verlangt der Kodex unverzügliche interne Meldungen an eine im Kodex festgelegte Person, wenn es zu potenziellen Verstößen gegen den Kodex gekommen ist?	☐	☐	☐
Formuliert der Kodex eine Rechenschaftspflicht für die Einhaltung des Kodex und gilt diese für Geschäftsleitungsmitglieder, Führungskräfte und Mitarbeiter?	☐	☐	☐
Verfügt das Unternehmen über Richtlinien und Verfahren, die als Anleitung für Mitarbeiter dienen können, insbesondere für Mitarbeiter in Bereichen mit hohem Risiko?	☐	☐	☐
Werden der Kodex und die Unternehmensrichtlinien regelmäßig überprüft und aktualisiert, um die in Risikobewertungen definierten Bereiche mit spezifischen ethischen Risiken zu erfüllen?	☐	☐	☐

Wenn Ihre Antworten überwiegend in die grüne Spalte fallen, gibt es bei Ihnen eine gute Umsetzung Ihres Verhaltenskodex. Sehen Sie sich die Ressourcen unten an, um mehr über eine effektive Verwaltung von Richtlinien und Verfahren zu erfahren.

Wenn Ihre Antworten überwiegend in die gelbe oder rote Spalte fallen, stehen Sie noch vor einigen Aufgaben. Sehen Sie sich die Ressourcen unten an, um vertiefte Informationen über die Verwaltung von Richtlinien und Verfahren und die Entwicklung eines verbindlichen Verhaltenskodex zu erhalten.

Zusätzliche Ressourcen zum Richtlinienmanagement

[Umfassender Leitfaden für das Richtlinien- und Verfahrensmanagement](#)

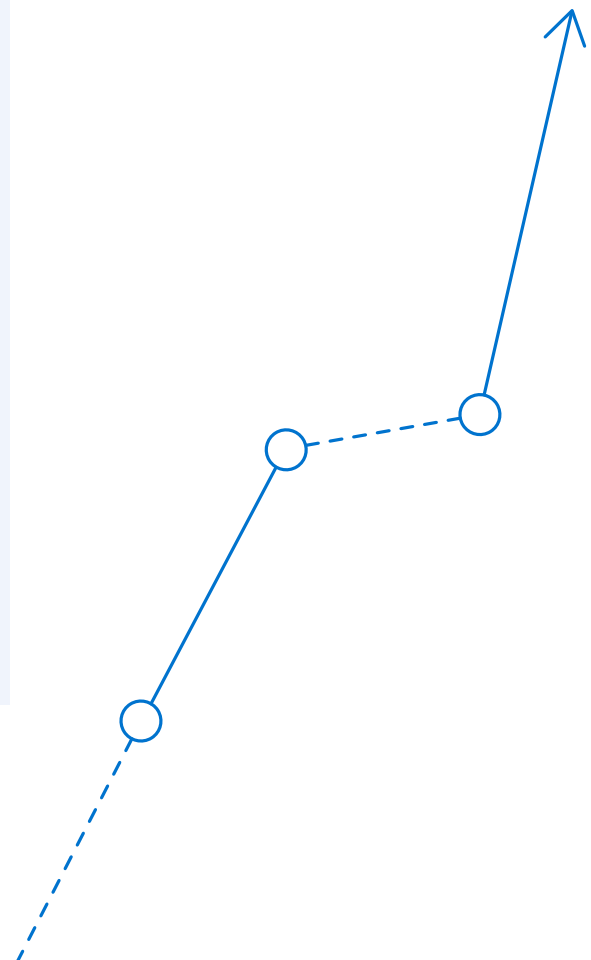
Dieser Leitfaden bietet Unternehmen aller Größenordnungen Einblicke in die Art und Weise, wie sie das Mitarbeiterhandbuch, den Verhaltenskodex, die Verfahren und andere wichtige Dokumente gestalten können, mit Beispielen aus der Praxis, hilfreichen Tipps und Forschungsergebnissen.

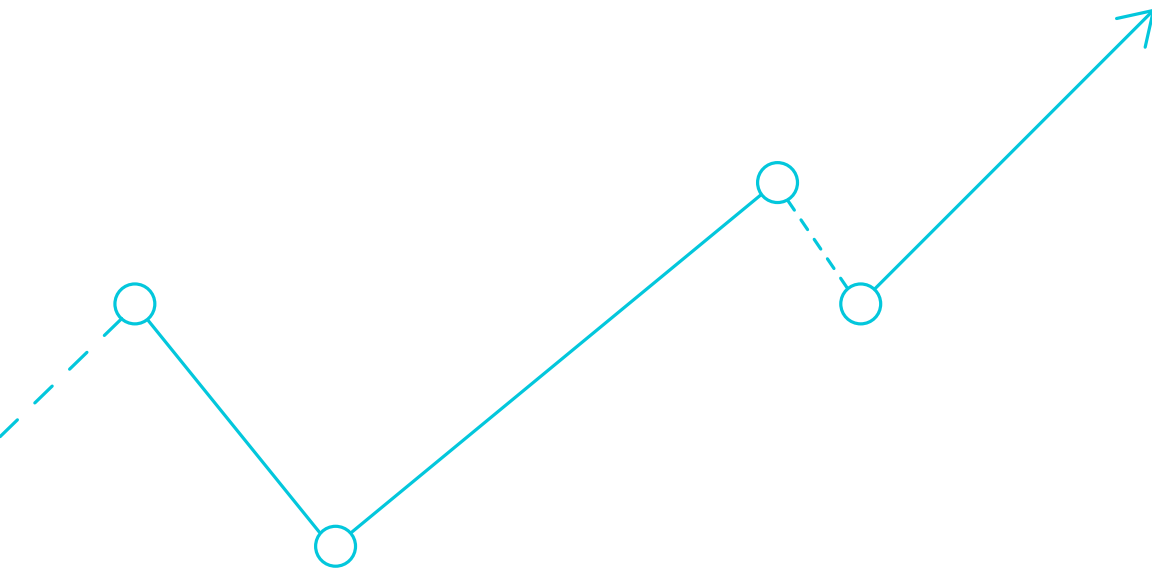
[Umfassender Leitfaden für Ihren Verhaltenskodex](#)

Ihr Verhaltenskodex ist das wichtigste Instrument zur Schaffung einer ethischen Kultur. Erfahren Sie alles, was Sie brauchen, um Ihren Verhaltenskodex von einem bloßen Dokument zu einer Ressource zu machen, mit deren Hilfe sich Ihre Mitarbeiter aktiv für die Ziele und Werte Ihres Unternehmens einsetzen.

[Musterrichtlinie über Geschenke und Bewirtungen \(in englischer Sprache\)](#)

Laden Sie diese Musterrichtlinie herunter, die Ihnen als Anleitung für Ihre eigene Richtlinie über Geschenke und Bewirtungen dienen kann. Mithilfe Ihrer Richtlinie können Mitarbeiter fundierte Entscheidungen treffen, wenn es darum geht, Geschenke oder Bewirtungen anzubieten oder anzunehmen.





Woche 4

Abstimmung mit der Personalabteilung

Wer in einem Unternehmen Personalentscheidungen trifft, sendet ein klares Signal darüber, welche Prioritäten das Unternehmen setzt. Ein Compliance-Programm kann nur in einem Unternehmen wirksam sein, in dem die Verfahren bei der Personalbeschaffung die geltenden Gesetze erfüllen und ethisches Verhalten fördern.

Bewertet Ihr Unternehmen Führungskräfte formell (in Leistungsbeurteilungen) darüber, ob sie ihre Verantwortlichkeiten in den Bereichen Ethik und Compliance erfüllen?

Die erfolgreichsten Unternehmen nutzen die Unterstützung der Personal- und Compliance-Abteilungen bei Richtlinien zu Themen wie Personalbeschaffung, Beförderungen und Leistungsbeurteilungen. Die Entwicklung von positiven Beziehungen zwischen der Ethik- und Compliance-Abteilung und der Personalabteilung bahnt den Weg hin zu einer ethischen Unternehmenskultur und sendet eine klare Botschaft, dass unethisches Verhalten nicht toleriert wird.

Nutzen Sie diesen Rahmen als Grundlage für die Abstimmung Ihres Compliance-Programms mit der Personalabteilung.

Elemente und Anforderungen des Programms	Leistungsmessungen und Fragen	Erforderliche zusätzliche Daten für die Prüfung
Verfahren beim Background-Screening: Neuanstellungen Beförderungen Strafrechtlich relevante Aktivitäten und Integritätsprobleme aussortieren	Werden potenziell neu angestellte Mitarbeiter überprüft, um die Anstellung von Mitarbeitern zu verhindern, die ein Verhalten gezeigt haben, das den Werten des Unternehmens widerspricht? Sind Mitarbeiter mit hohem Risiko oder erheblichen Befugnissen definiert worden? Ist ein hohes ethisches Verhalten ein Kriterium für interne Beförderungen – insbesondere bei Personen, die auf Stellen mit hohem Risiko oder erheblichen Befugnissen befördert werden? Bezieht das Unternehmen bei der Anstellung und Beförderung von Personen die Auswirkungen von illegalen Aktivitäten oder anderem Fehlverhalten der Person ein? Werden Background-Screening-Prozesse bei Dritten durchgeführt, die im Namen des Unternehmens auftreten?	Richtlinien und Verfahren für Background-Überprüfungen bei allen Neuanstellungen. Richtlinien und Verfahren für Background-Prüfungen – intern und extern für Mitarbeiter, die auf Stellen mit hohem Risiko oder Geschäftsleitungspositionen befördert werden (einschließlich ggf. frühere disziplinarische Maßnahmen, strafrechtliche Überprüfungen und Bonitätsprüfungen).
Anreize und Leistungsüberprüfungen: Ethics MR Angemessene Bonusziele Direkte Mitteilungen während der Zielsetzung und Überprüfung	Gibt es einen festgelegten Prozess, um dafür zu sorgen, dass alle Führungskräfte ihre Aufgaben bei der Sicherung eines effektiven Programms und einer effektiven Kultur erfüllen? Erfüllen alle Führungskräfte diese Aufgaben? Gibt es einen festgelegten Prozess, durch den alle Mitarbeiter evaluiert werden können, um zu gewährleisten, dass sie sich an den Unternehmenswerten orientieren und die Anforderungen des Verhaltenskodex erfüllen? Werden Mitarbeiter, insbesondere Führungskräfte und Geschäftsleitungsmitglieder, evaluiert, um zu gewährleisten, dass sie die Unternehmenswerte und die Anforderungen des Verhaltenskodex mit Leben erfüllen? Gibt es Bereiche, in denen Anreize oder andere Druckmittel Mitarbeiter zu Verhalten verführen können, das nicht im langfristig besten Interesse der Kunden, Kollegen oder des Unternehmens ist? Werden Austrittsgespräche mit allen austretenden Mitarbeitern geführt und wird darin das Thema Ethik angesprochen?	Alle Dokumente, die ethikbezogenen Zuständigkeiten bei den Zielen des Unternehmen und den Zielsetzungsprozessen für die Mitarbeiter einbeziehen. Formulare, Verfahren und Leitfäden zur Leistungsbewertung, in denen sich die Anwendung von ethischen Kriterien widerspiegelt. Berichte von Fokusgruppen und Gespräche mit der Geschäftsleitung. Dokumentation der Best Practices der Branche.

Woche 5

Kommunikation und Schulungen

Die Richtlinien und Verfahren in Ihrem Compliance-Programm müssen von einem strategischen Kommunikationsplan und Schulungsprogramm begleitet werden, um die Mitarbeiter über die Bestandteile des Programms zu informieren und ihren Kenntnisstand hinsichtlich der Richtlinien zu prüfen.

Vermittlung

Selbst die besten Richtlinien und Meldeprozesse für Mitarbeiter sind wertlos, wenn die Mitarbeiter nicht wissen, wo sie Richtlinien finden und wie sie Fehlverhalten melden können.

Kooperieren Sie mit Abteilungen im ganzen Unternehmen wie Marketing und HR, um einen Kommunikationsplan aufzustellen, damit Mitarbeiter, Führungskräfte und Dritte die Tools, die ihnen zur Verfügung stehen, und die an sie gestellten Erwartungen kennen.

Schulung

Die Mitarbeiter müssen nicht nur die Tools kennen, die ihnen zur Verfügung stehen, sondern auch wissen, was von ihnen erwartet wird. Compliance-Schulungen sorgen dafür, dass die Mitarbeiter bei den spezifischen rechtlichen Anforderungen und den Richtlinien Ihres Unternehmens auf dem Laufenden bleiben. Führen Sie Schulungen risikoorientiert durch, damit die Mitarbeiter mit der höchsten Risikoexponierung zuerst Schulungen erhalten.

Ein grundlegendes Ethik- und Compliance-Schulungsprogramm hat die folgenden Elemente:

- Mit einer Risikobewertung verknüpfte Schulung
- Führungskräfte kennen ihre Aufgaben und wissen, wie sie auf Probleme reagieren müssen
- Geschäftsleitung unterstützt laufend das Programm
- Ein mehrjähriger Weiterbildungsplan mit verschiedenen Formaten und Schulungsumfängen

Ein Best-Practice-Programm führt einen Schritt weiter und umfasst:

- Schulungen abgestimmt auf die Rolle eines Mitarbeiters
- Bewertung der Effektivität der Schulungen
- Schulung von Vorstand und Geschäftsleitung, nicht nur Briefing

Steigern Sie den messbaren Wert Ihres Schulungsprogramms mit den folgenden Ressourcen.

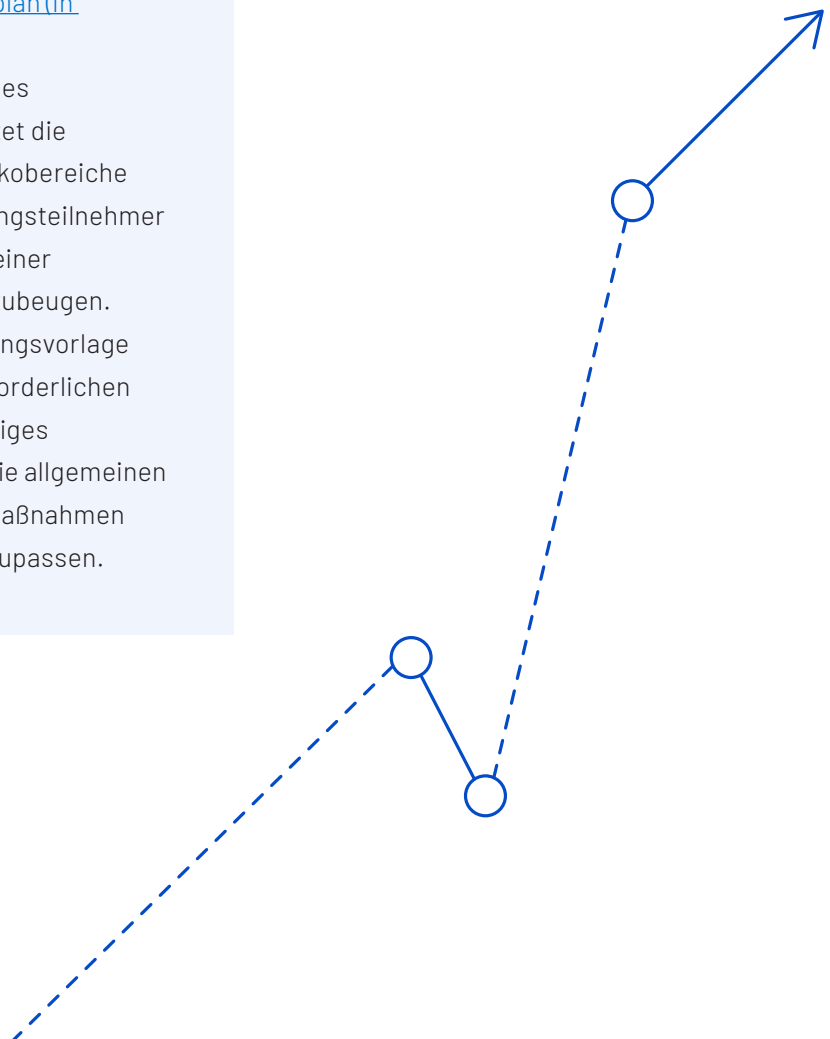
Zusätzliche Schulungsressourcen

[Maßgebliche Orientierungshilfe für Ethik- und Compliance-Schulungen](#)

In diesem Leitfaden finden Sie die Tools und Informationen, die Sie benötigen, um ein ansprechendes Compliance-Schulungsprogramm zu entwickeln, einen mehrjährigen Weiterbildungsplan zu implementieren, auf Ihre dringendsten Risiken einzugehen und die Effizienz Ihrer Compliance-Schulungen zu messen, zu bewerten und zu verbessern.

[Bearbeitbare Vorlage für einen mehrjährigen Schulungsplan \(in englischer Sprache\)](#)

Ein effektives mehrjähriges Schulungsprogramm bietet die Gewähr, dass Sie alle Risikobereiche abdecken und die Schulungsteilnehmer wirksam motivieren, um einer Schulungsmüdigkeit vorzubeugen. Diese bearbeitbare Planungsvorlage beschreibt die sieben erforderlichen Schritte, um Ihr mehrjähriges Schulungsprogramm in die allgemeinen Compliance-Schulungsmaßnahmen Ihres Unternehmens einzupassen.

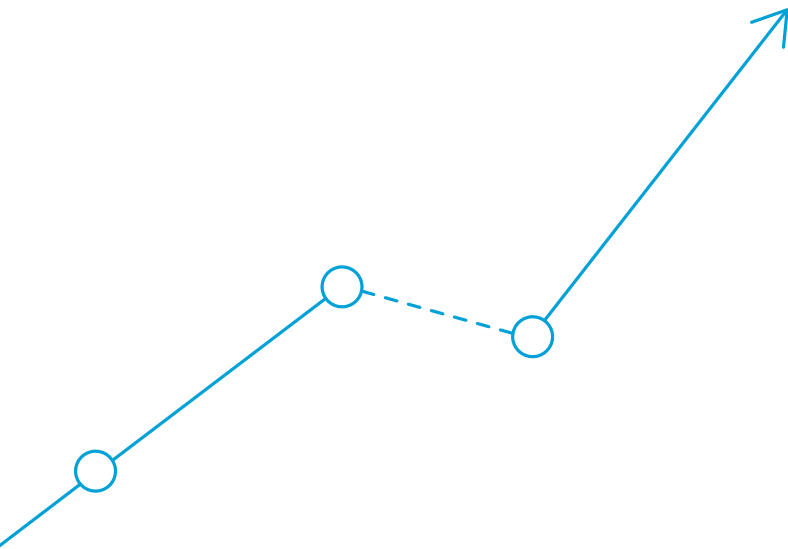


Woche 6

Meldewesen und Reaktionen

Jedes Compliance-Programm muss Mitarbeitern Wege bieten, wie sie einfach, sicher und ohne Angst vor Vergeltung Probleme melden können. Das Meldewesen und das Vorfallmanagement-Programm sind grundlegende Elemente eines effektiven Compliance-Programms. Es reicht aber nicht aus, einfach nur eine Whistleblower-Hotline einzurichten. Effektive Programme stellen mindestens drei Meldeoptionen bereit:

1. **Hotline.** Unabhängig davon, ob ein Hotline-Meldesystem für das Unternehmen vorgeschrieben ist oder nicht, ist es dennoch ein grundlegender und erwarteter Bestandteil jedes effektiven Compliance-Programms.
2. **Meldung über das Internet.** Manche Menschen fühlen sich nicht wohl dabei, mit einem Hotline-Mitarbeiter über ihr Problem zu sprechen, oder sie haben keinen privaten Ort, an dem sie anrufen können. Über ein Online-Formular können sie Informationen eingeben und sich Zeit nehmen, das Geschriebene zu überdenken und zu überprüfen, bevor sie es absenden.
3. **Gespräch mit einem Vorgesetzten.** Dies ist ein webbasiertes System, das es Vorgesetzten ermöglicht, gemeldete Probleme und getroffene Maßnahmen in ein zentrales Annahme- und Vorfallmanagementsystem einzugeben. Mit einem zentralen System können Untersuchungsteams und zuständige Personen konsistent auf Informationen zugreifen und die Vertraulichkeit der Hinweisgeber sichern, während sie ggf. Fortschrittsmeldungen beim betreffenden Fall hinzufügen können.



Verwenden Sie die folgende Grafik, um die Effektivität Ihres gegenwärtigen Programms zu bewerten. Wenn die meisten Ihrer Antworten in die rote oder gelbe Kategorie fallen, verwenden Sie die Ressourcen unten, um die Planung und Einführung eines Whistleblower-Hotline-Programms zu vertiefen.

Meldewesen und Reaktionen			
Ermutigt und unterstützt das Unternehmen Mitarbeiter und Außenstehende zur Meldung von Fehlverhalten?	☐	☐	☐
Erläutert das Unternehmen das Meldesystem und die entsprechenden Prozesse gegenüber allen Mitarbeitern?	☐	☐	☐
Hat das Unternehmen ein geeignetes Eskalationsverfahren?	☐	☐	☐
Glauben die Mitarbeiter, dass sie Probleme gegenüber der Geschäftsleitung oder über die interne Meldehotline ohne Angst vor Vergeltung melden können?	☐	☐	☐
Nutzt das Unternehmen ein Nachverfolgungssystem für alle eingegangenen Meldungen und Probleme? Überprüft das Unternehmen die Melde- und Ergebnisdaten, um potenzielle Problembereiche festzulegen? Werden diese Informationen an die Geschäftsleitung und den Vorstand weitergeleitet?	☐	☐	☐
Untersucht das Unternehmen Probleme zeitnah und schützt es dabei die Vertraulichkeit?	☐	☐	☐
Tragen die durchgeführten Untersuchungen dazu bei, die Ursachen von Fehlverhalten zu ermitteln und die Anforderung zu erfüllen, dass ein Unternehmen geeignete Schritte zu einer angemessenen Reaktion auf ein solches Fehlverhalten machen und weitere ähnliche (Verstöße) verhindern muss, etwa auch indem eventuelle erforderliche Änderungen am Ethikprogramm des Unternehmens vorgenommen werden?	☐	☐	☐
Werden disziplinarische Maßnahmen bei Verstößen gegen Kodex, Werte, Richtlinien und Gesetze angemessen und konsequent angewendet?	☐	☐	☐
Setzt das Unternehmen Richtlinien zum Verbot von Vergeltung gegen Personen durch, die vermutete oder tatsächliche Verstöße gegen die Unternehmensrichtlinien oder Gesetze melden?	☐	☐	☐

Zusätzliche Ressourcen zum Vorfallmanagement

[Leitfaden für das Incident-Management](#)

In unserem umfassenden Leitfaden erfahren Sie alles, was Sie wissen müssen, um ein effektives Fallmanagement aufzubauen – von der Planung über die Umsetzung bis hin zur Auswertung.

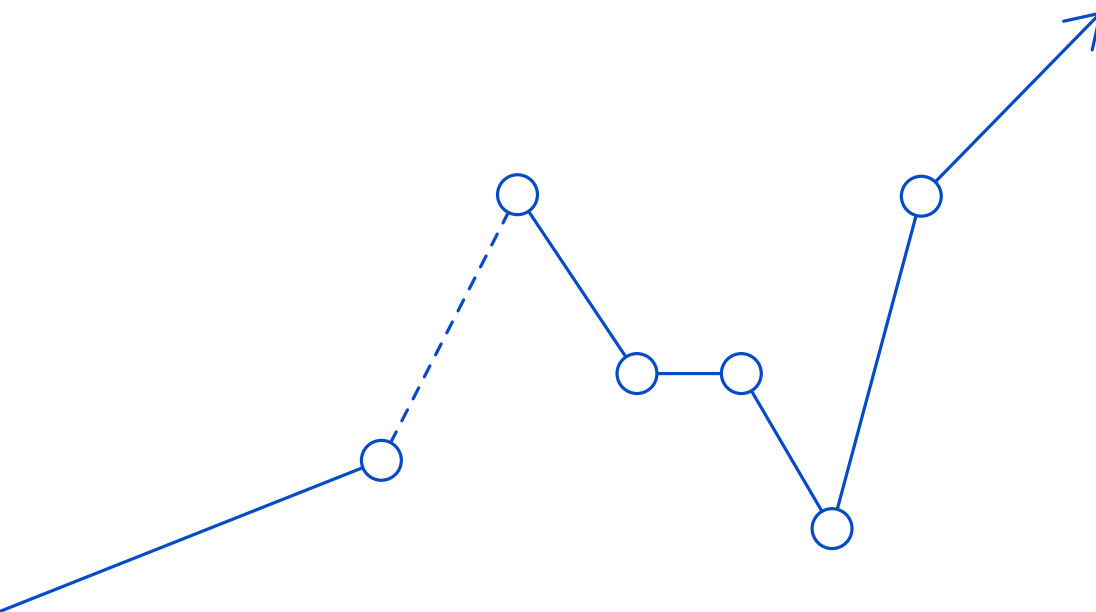
[Whistleblowing & Incident Management Benchmark Report \(in englischer Sprache\)](#)

Angesichts der zunehmenden Zahl von Mitarbeiteraussagen ist eine Bewertung Ihrer Hotline- und Vorfallmanagementdaten von entscheidender Bedeutung, um einen Überblick über Ihre Risiken zu bewahren und eine robuste, an Compliance ausgerichtete Arbeitsplatzkultur zu schaffen.

Blicken Sie mit Zuversicht in die Zukunft. Unser Whistleblowing & Incident Management Benchmark Report liefert Ihnen die neuesten Trends und Daten aus über 2,15 Millionen Vorfallmeldungen – der weltweit größten Datenbank zum Vorfallmanagement.

Infografik: [Whistleblowing am Arbeitsplatz: Was Ihr Vorstand wissen muss \(in englischer Sprache\)](#)

Remote-Arbeit und flexible Arbeitszeiten sind bleibende Trends. Da ist es wichtiger denn je, dass Geschäftsleitungs- und Vorstandsmitglieder verstehen, wie wichtig ein vertraulicher Whistleblowing-Prozess ist. Diese Infografik zeigt wichtige Kenngrößen über Whistleblowing am Arbeitsplatz und dessen Einfluss auf Kultur und Compliance in Ihrem Unternehmen, die an Ihren Vorstand und Ihre Geschäftsleitung weitergeleitet werden können.



Woche 7

Kultur

Wenn die Richtlinien und Verfahren, Belohnungen oder vielleicht sogar der Verhaltenskodex eines Unternehmens im Widerspruch zu seiner Kultur stehen, setzt sich die Kultur durch. Um ein effektives Ethik- und Compliance-Programm zu haben, muss ein Unternehmen daher auf die Kultur ebenso große Aufmerksamkeit richten wie auf Richtlinien, Schulungen, Prüfungen und andere Programmelemente.

Die Compliance-Abteilung unterstützt die strategischen Ziele und das Unternehmensleitbild ebenso stark wie alle anderen Abteilungen oder Funktionen. Zu einem effektiven Ethik- und Compliance-Programm gehört mehr als einfach das Zusammenstellen von Regeln und zusätzlichen Kontrollebenen. Erfolgreiche Programme sind integrierte Maßnahmen, die finanzielle Anforderungen und Compliance-Vorgaben am Leitbild und den Werten des Unternehmens ausrichten.

Vorausdenkende Unternehmen streben den Aufbau einer Kultur an, bei der alle Mitarbeiter wissen, welche ethischen Verhaltensweisen von ihnen erwartet werden. Sie müssen die Normen und Standards kennen, denen sie unterliegen, und sie müssen darauf vertrauen können, dass sich ihre Geschäftsleitung zu Integrität und ethischen Verhaltensweisen verpflichtet hat. Diese Mitarbeiter müssen sich dazu ermutigt fühlen, Bedenken wegen Fehlverhaltens ohne Angst vor Vergeltung zu melden, und sie müssen in ihrer Überzeugung bestärkt werden, dass ihre Meldungen bearbeitet werden.

Wenn ethisches Verhalten erwartet wird, sticht Verhalten, das unethisch ist oder auf andere Weise gegen die Unternehmensstandards verstößt, heraus und kann einfacher sanktioniert werden. Damit dies möglich wird, muss die Kultur des Unternehmens im Rahmen der Evaluation des Ethik- und Compliance-Programms bewertet werden.

Beantworten Sie die folgenden Fragen, um zu sehen, ob Ihre Kultur Ethik und Respekt fördert.

- Werden alle Mitarbeiter gleichermaßen für ihre Handlungen zur Rechenschaft gezogen?
- Wird ethisches Verhalten höher bewertet als Umsatz- und Unternehmensziele, wenn es hart auf hart kommt? Wird unethisches Verhalten klar als unakzeptabel gekennzeichnet?
- Glauben die Mitarbeiter, dass die Geschäftsleitung geeignete Maßnahmen ergreift, wenn ihr Fehlverhalten gemeldet wird?
- Glauben die Mitarbeiter, dass sie Probleme gegenüber der Geschäftsleitung oder über die interne Meldehotline ohne Angst vor Vergeltung melden können?
- Gilt das Programm als echte Selbstverpflichtung, die sich nicht nur in Worten, sondern auch in Taten äußert?

Zusätzliche Ressourcen zur Kultur

[Risiko- und Compliance-Benchmark-Bericht](#)

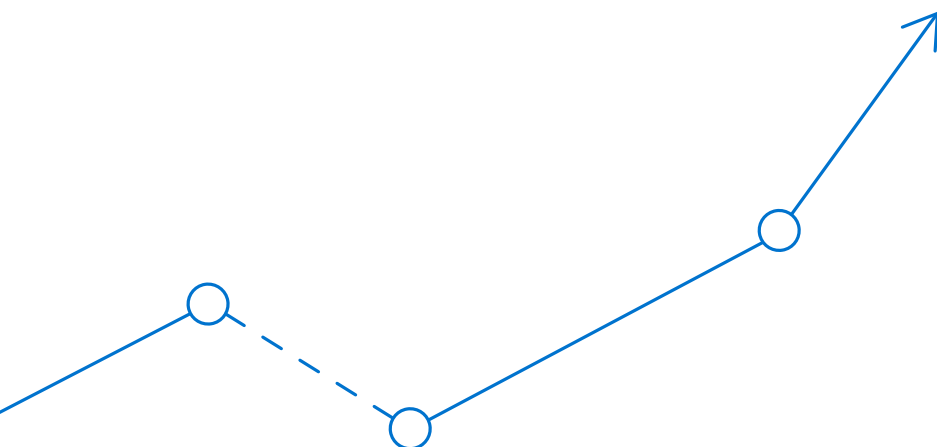
Neben- oder Hauptfigur? Ihr Risiko- und Compliance-Programm verdient eine Hauptrolle. Unser Risiko- und Compliance-Benchmark-Bericht führt die Erkenntnisse von über 1.000 Risiko- und Compliancebeauftragten aus aller Welt zusammen. Die Daten in diesem Bericht bieten Best Practices und Einblicke, die für genau Ihr Unternehmen von Bedeutung sind, ganz unabhängig von Größe, Standort und Branche.

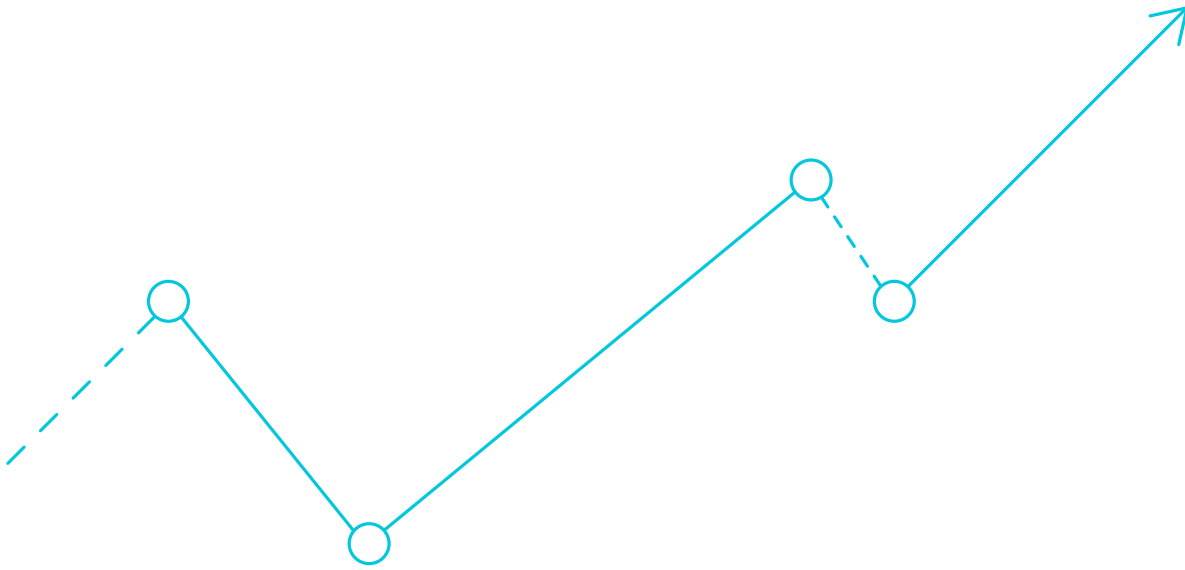
Fallstudie: [So skalieren Sie eine Kultur der Ethik \(in englischer Sprache\)](#)

Diese Kundenerfolgsgeschichte untersucht, wie ein führender Gesundheitsdienstleister in den USA nach der Fusion von zwei Gesundheitsunternehmen eine skalierbare Kultur der Ethik und Compliance aufgebaut hat. Der Dienstleister nutzte NAVEX One Whistleblowing & Incident Management und Policy & Procedure Management und konnte damit sein Hotline- und Richtlinienmanagement für alle Standorte integrieren und mehr als 150.000 Mitarbeiter unterstützen. Er konnte zudem die Daten aus diesen Systemen ausnutzen, um den Vorstand und andere Interessengruppen über die Compliance-Arbeit des Unternehmens zu informieren.

[Höhere Akzeptanz von Compliance-Standards durch ansprechende Aufgaben für Mitarbeiter \(in englischer Sprache\)](#)

Fördern Sie eine Kultur der Compliance, die bei allen Mitarbeitern ankommt. Erfahren Sie in diesem Whitepaper, wie Sie die Resonanz bei Fragen der Compliance in Ihrem Unternehmen steigern können. Es bietet Einblicke von Fachleuten und umsetzbare Strategien, mit denen Sie Ihre Compliance-Programme umgestalten können. Dies ist Ihre Roadmap für die Schaffung der personalisierten Erlebnisse, die Mitarbeiter heute verlangen, um die Unterstützung für Ethik und Compliance in Ihrem gesamten Unternehmen zu verstärken.





Woche 8

Laufende Überwachung und Messung

Die Überwachung und Messung Ihres Programms ist der einzige Weg, um zu erfahren, ob Ihr Programm wirklich effektiv ist. Wirksamkeitsmessungen können aus verschiedenen Quellen stammen. So viele Quellen wie möglich zu nutzen ist tatsächlich der genaueste Weg, um eine „Note“ für Ihr Programm zu erhalten. Verwenden Sie die folgende Grafik als Checkliste, um sich intern und extern nach Messungen und Benchmarks zur Verbesserung Ihres Programms umzusehen.

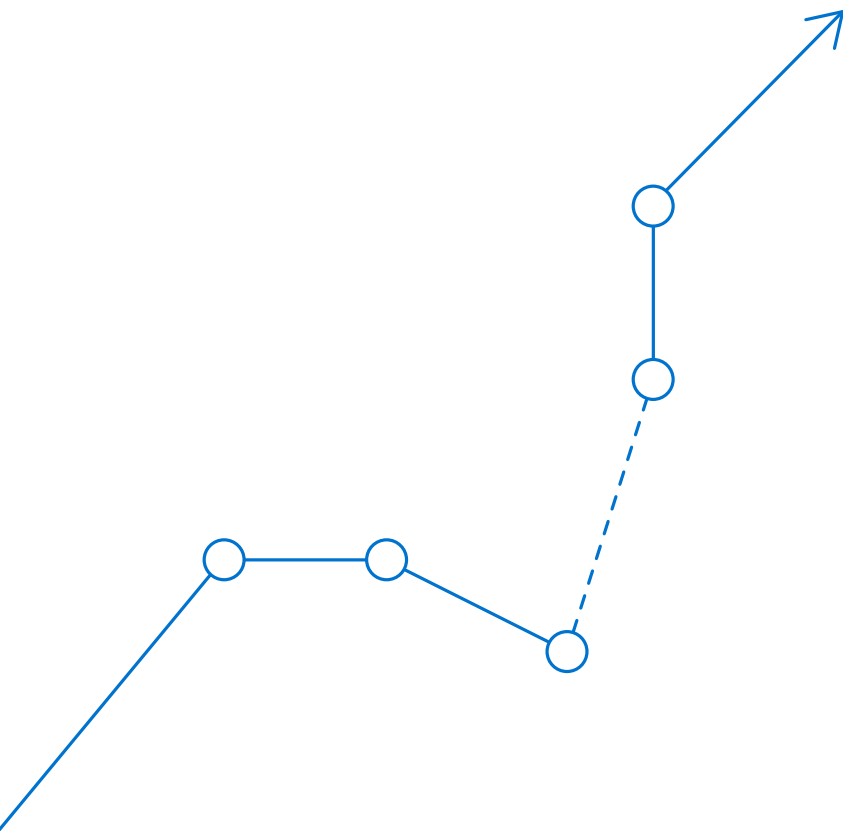


Fazit

Effektive Compliance-Programme entstehen nicht über Nacht. Ebenso wenig sind sie als abschließende Lösungen gedacht.

Ganz gleich, wie reif das Programm Ihres Unternehmens gegenwärtig ist, wie gut es ausgestattet ist (oder nicht) oder wie stark die Kultur der Ethik und Compliance verankert ist – es gibt immer wertvolle Erkenntnisse und Verfahrensweisen, die umgesetzt werden können, um sich schrittweise zu verbessern.

Unternehmen stehen zunehmend unter Beobachtung, unter anderem durch ihre Kunden, Mitarbeiter, Aktionäre und sonstige Stakeholder. Deshalb ist eine solide Grundlage aus Ethik und Compliance entscheidend für langfristigen Erfolg und anhaltende Resilienz. Ein effektives Compliance-Programm lässt sich nicht innerhalb von acht Wochen aus dem Nichts aufbauen. Mit einem strukturierten Ansatz und einheitlichen Botschaften über den Wert einer Kultur der Ethik und Compliance lassen sich aber beträchtliche Fortschritte erzielen. Wir hoffen, dass die Checklisten und Ressourcen in diesem Leitfaden Ihnen beim Aufbau Ihres Programms helfen – ganz gleich, ob Sie bei null anfangen oder Ihr vorhandenes Programm ausbauen möchten.



Orientierung in den gesetzlichen und regulatorischen Anforderungen Deutschlands

Zusammenfassung

Das regulatorische Umfeld in Deutschland ist komplex und unterliegt ständigen Veränderungen. In diesem Abschnitt bieten wir Ihnen einen klaren Überblick über die Gesetze und Richtlinien, die die Compliance-Verpflichtungen für Unternehmen mit Sitz in oder Verbindungen zu Deutschland bestimmen. Von Datenschutz und Arbeitsrecht über Sorgfaltspflichten in der Lieferkette bis hin zum Schutz von Whistleblowern und KI-Governance – dieser Abschnitt hilft Ihnen zu verstehen, was erforderlich ist und was als Nächstes kommt.

Datenschutz in Deutschland und Europa

Wer in Deutschland und der EU Geschäfte machen will, kommt an einem Thema nicht vorbei: dem Datenschutz. Seit dem Inkrafttreten der EU-Datenschutz-Grundverordnung (DSGVO) am 25. Mai 2018 gelten strenge Regeln, wie personenbezogene Daten verarbeitet, gespeichert und geschützt werden müssen.

In Deutschland sind die Menschen besonders sensibel, was die Nutzung ihrer Daten betrifft, hier wird Datenschutz traditionell sehr ernst genommen und streng gehandhabt. Da wundert es nicht, dass die deutsche Gesetzgebung das europäische Recht in einigen Punkten sogar noch ergänzt. Wer also den europäischen Markt inklusive Deutschland bedienen möchte, muss auch das deutsche Bundesdatenschutzgesetz (BDSG) im Blick haben.

Verstöße gegen die Datenschutzgesetze können sehr teuer werden, zum einen wegen der hohen Geldbußen und zum anderen, weil sie zu Imageschäden führen – die Menschen nehmen es Unternehmen übel, wenn nicht sorgfältig mit ihren Daten umgegangen wird. Und: Die EU-Datenschutzbehörden sind streng: Allein seit Inkrafttreten der DSGVO bis zur Vorlage des [„Zweiten Berichts zur Anwendung der Datenschutz-Grundverordnung“](#) im Juli 2024 verhängten sie über 6.680 Bußgelder in Höhe von insgesamt rund 4,2 Milliarden Euro.

Kurzum: Wirtschaftliche Aktivitäten in der EU und Deutschland erfordern eine genaue Kenntnis der Datenschutzgesetze sowie eine professionelle Strategie zum Schutz von Daten. Alles andere birgt unkalkulierbare Risiken.

Die europäische Datenschutz-Grundverordnung (DSGVO)

Die DSGVO ist der zentrale Rechtsrahmen für den Datenschutz in der gesamten EU. Sie regelt, wie Unternehmen personenbezogene Daten verarbeiten müssen und räumt dabei Betroffenen umfassende Rechte ein.

Wichtig: Die DSGVO gilt nicht nur für Unternehmen mit Sitz in der EU, sondern auch für alle, die EU-Bürgern ihre Waren oder Dienstleistungen anbieten.

Das deutsche Bundesdatenschutzgesetz (BDSG)

Das Bundesdatenschutzgesetz (BDSG) ergänzt die DSGVO dort, wo nationale Regelungen zulässig sind – etwa bei dem Beschäftigtendatenschutz, der Ernennung von Datenschutzbeauftragten oder bei besonderen Vorschriften für Datenübermittlungen an Sicherheitsbehörden.

„Wichtig: Die DSGVO gilt nicht nur für Unternehmen mit Sitz in der EU, sondern auch für alle, die EU-Bürgern ihre Waren oder Dienstleistungen anbieten.“

DSGVO vs. BDSG – Was gilt wo und was ist der Unterschied?

In Deutschland gilt nicht nur die EU-Datenschutz-Grundverordnung (DSGVO), sondern zusätzlich auch das Bundesdatenschutzgesetz (BDSG). Unternehmen, die in Deutschland aktiv sind, müssen also beide Regelwerke kennen und befolgen, dabei aber immer mit der DSGVO als oberstem Maßstab.

Die DSGVO ist das zentrale europäische Datenschutzgesetz – und gilt in allen EU-Ländern direkt.

Das BDSG ergänzt die DSGVO, wo sie nationale Regelungen erlaubt, zum Beispiel beim Datenschutz am Arbeitsplatz. So räumt die DSGVO in Artikel 88 ein, dass Mitgliedstaaten den Datenschutz im Beschäftigungskontext „genauer regeln“ dürfen. Deutschland hat diese Öffnung genutzt und im Paragraf 26 seines BDSG sehr spezifisch beschrieben, unter welchen Bedingungen Daten von Beschäftigten verarbeitet werden dürfen, etwa wenn es um Bewerbungsverfahren oder die Aufdeckung von Straftaten im Unternehmen geht.

Compliance-Anforderungen rund um den Datenschutz

Viele Datenschutzverstöße entstehen nicht aus bösem Willen, sondern weil Prozesse, Zuständigkeiten oder technische Details nicht auf ihre Gesetzeskonformität geprüft wurden. Wer sich vor dem Markteintritt in die EU um ein sauberes Datenschutzkonzept kümmert, ist auf der sicheren Seite – rechtlich und reputationsmäßig. Hier eine Auswahl an grundlegenden Anforderungen an den Datenschutz:

Weitere datenschutzrechtlich relevante Gesetze

Die **ePrivacy-Richtlinie** regelt insbesondere Tracking, Cookies und elektronische Kommunikation. Sie soll perspektivisch durch die **ePrivacy-Verordnung** ersetzt werden, deren Verabschiedung jedoch seit Jahren auf sich warten lässt.

Das **Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)** ist seit 2021 in Deutschland gültig. Es konkretisiert die ePrivacy-Regelungen für Websites und Apps. Unternehmen sollten die Entwicklungen genau verfolgen, da mit der ePrivacy-Verordnung zusätzliche Pflichten entstehen könnten – etwa strengere Anforderungen an Einwilligungen bei Online-Diensten.

„Privacy by Design“ und „Privacy by Default“

„Privacy by Design“ bedeutet, Systeme, Software und Prozesse so zu gestalten, dass der Schutz personenbezogener Daten von Beginn an berücksichtigt ist. Der Datenschutz muss bereits in der Entwicklung mitgedacht werden und nicht erst dann, wenn ein Produkt oder ein Prozess schon fertig ist.

„Privacy by Default“ heißt, dass die datenschutzfreundlichste Einstellung standardmäßig voreingestellt ist, etwa bei Apps, Websites oder Online-Diensten. So darf zum Beispiel eine neue App nicht automatisch Standortdaten erfassen, sondern muss die Nutzer aktiv fragen, ob sie damit einverstanden sind. Dabei muss es genauso einfach sein, mit „Nein“ zu antworten wie mit „Ja“.

Immens wichtig: Einwilligungen richtig einholen

Wenn Unternehmen personenbezogene Daten verarbeiten – zum Beispiel, weil sie Newsletter versenden oder personalisierte Werbung machen – brauchen sie in den meisten Fällen eine klare, freiwillige und informierte Einwilligung. Diese Zustimmung muss nachweisbar dokumentiert sein, zum Beispiel über ein Opt-in-Feld mit Zeitstempel. Ein bereits voreingestelltes abgehaktes Kästchen gilt nicht als gültige Zustimmung.

Kein Service, sondern Pflicht: Betroffenenrechte ernst nehmen

Jede Person hat laut DSGVO umfassende Rechte, wenn es um die Nutzung ihrer persönlichen Daten geht. Dazu zählen

- das Recht auf Auskunft, welche Daten gespeichert sind.
- das Recht auf Berichtigung falscher Angaben.
- das Recht auf Löschung (auch das „Recht auf Vergessenwerden“ genannt).
- das Recht auf Datenübertragbarkeit zu einem anderen Anbieter.

Unternehmen müssen solche Anfragen zügig und vollständig beantworten, meist innerhalb eines Monats.

Die Datenschutz-Folgenabschätzungen (DSFA)

Der Begriff ist bürokratisch, die Idee dahinter nachvollziehbar: die Datenschutz-Folgenabschätzung dient dazu, datenschutzrechtliche Risiken zu erkennen, bevor sie zu einem Problem werden. Wenn zum Beispiel neue Technologien oder Prozesse, wie etwa die Gesichtserkennung oder die Nutzung von Gesundheitsdaten, die Rechte und Freiheiten von Personen gefährden könnten, ist die DSFA Pflicht.

Sie prüft im Detail, wo Risiken liegen und wie sie sich reduzieren lassen.

Augen auf bei der Auswahl der Dienstleister

Unternehmen, die personenbezogene Daten von Dritten verarbeiten lassen – beispielsweise von einem Cloud-Anbieter, einem externen Callcenter oder einem Newsletter-Dienstleister – müssen sicherstellen, dass diese Dienstleister die Datenschutzregeln ebenfalls penibel einhalten.

Das heißt konkret, dass sie einen Auftragsverarbeitungsvertrag nach Art. 28 DSGVO brauchen. Die Unternehmen sind verpflichtet, ihre Dienstleister sorgfältig zu prüfen und im Zweifel zu wechseln. Es empfiehlt sich, die Prüfungen gut zu dokumentieren, um gegebenenfalls gegenüber Aufsichtsbehörden Rechenschaft ablegen zu können.

Achtung: Meldepflicht!

Wird ein Unternehmen auf eine Datenschutzpanne aufmerksam, ist es grundsätzlich verpflichtet, die zuständige Aufsichtsbehörde zu informieren – es sei denn, es ist absehbar, dass daraus kein Risiko für die Rechte und Freiheiten der Betroffenen entsteht. Die Meldung muss in der Regel innerhalb von 72 Stunden erfolgen.

Deutsche Sonderregelung: die Datenschutzbeauftragten

In Deutschland sind Unternehmen verpflichtet, eine Person als Datenschutzbeauftragte zu benennen, wenn mehr als 20 Mitarbeitende regelmäßig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind oder auch, wenn besonders sensible Daten verarbeitet werden. Die oder der Datenschutzbeauftragte kann intern oder extern arbeiten, gefordert sind Fachwissen, Unabhängigkeit und eine klare Zuständigkeit.

Was droht bei Verstößen?

Verstöße gegen europäische und deutsche Datenschutzvorgaben sind keine Kavaliersdelikte – sie können richtig teuer werden. Bei DSGVO-Verstößen drohen bis zu 20 Millionen Euro Strafe.

Die DSGVO sieht zwei Stufen von Bußgeldern vor: Verstößen Unternehmen gegen organisatorische Pflichten, sind Strafen bis zu 10 Millionen Euro oder 2 Prozent des weltweiten Jahresumsatzes vorgesehen.

Bei Verstößen gegen zentrale Grundprinzipien oder Betroffenenrechte sind es bis zu 20 Millionen Euro oder 4 Prozent des weltweiten Jahresumsatzes.

Noch nicht eingerechnet: eventuelle Schadensersatzforderungen betroffener Personen und Reputationsschäden, die mit Datenschutzverstößen einhergehen. Juristen sprechen mit Blick auf Schadenersatzforderungen von erheblichen Risiken, weil europäische Gerichte in der Vergangenheit immer wieder sehr verbraucherfreundliche Urteile gefällt haben. Da Verstöße gegen das DSGVO oft sehr viele Personen betreffen, können sie entsprechend viele Klagen gegen das Unternehmen nach sich ziehen.

„Bei DSGVO-Verstößen drohen bis zu 20 Millionen Euro Strafe.“

Wer zahlt bislang am meisten?

Bislang führen die großen US-Tech-Firmen nicht nur bei der Anzahl, sondern auch bei der Bußgeldhöhe die [Rangliste der DSGVO-Verstöße](#) an. Da wundert es nicht, dass im vergleichsweise kleinen Irland gut die Hälfte der gesamten Bußgeldsumme fällig wurde – dort unterhalten viele ausländische Tech-Unternehmen ihren EU-Hauptsitz. Unter den Top Ten der höchsten Bußgelder für Verstöße gegen das DSGVO findet sich tatsächlich nur ein europäisches Unternehmen: ein italienischer Energiekonzern, der 79 Millionen Euro Strafe wegen des Handels mit Kundendaten zahlen musste. Alle anderen sind – mit Ausnahme eines chinesischen Social Network-Betreibers – US-Firmen.

Teure Fehltritte

Es gibt eine große Bandbreite möglicher Verstöße: von technischen Mängeln über Cyber-Crime oder Virenattacken bis hin zu menschlichen Fehlern und individuellem kriminellen Verhalten. Hier eine kleine Auswahl von Verstößen, die bereits geahndet wurden:

Wenn ein Mitarbeiter Daten stiehlt

Im Mai 2023 wurde ein [erhebliches Datenleck im deutschen Werk eines US-Autobauers](#) bekannt. Ein ehemaliger Mitarbeiter soll etwa 100 Gigabyte vertraulicher Daten entwendet und weitergegeben haben. Diese Daten umfassten unter anderem persönliche Informationen von über 100.000 aktuellen und ehemaligen Mitarbeitern, darunter Gehälter, Adressen und Sozialversicherungsnummern, sowie sensible Kundendaten und interne Unternehmensinformationen. Außerdem steht der Verdacht im Raum, dass das Unternehmen den Verstoß nicht binnen 72 Stunden gemeldet hat.

Wenn, wie hier, ein möglicher Datenschutzverstoß Personen in gleich mehreren EU-Staaten betrifft, werden die Ermittlungen federführend von der Behörde des EU-Landes übernommen, in dem das Unternehmen seine Hauptniederlassung in der EU unterhält. Derzeit wird noch geprüft, ob und in welchem Ausmaß der Autohersteller gegen die DSGVO verstoßen hat. Je nachdem, was diese Prüfung ergibt, wird ein Bußgeldverfahren eingeleitet.

Wenn ein Unternehmen Mitarbeitende ausspäht

Im Jahr 2020 kassierte [ein großer schwedischer Modehändler einen Bußgeldbescheid](#) über rund 35 Millionen Euro. Der Händler hatte seine Mitarbeitenden nach den Corona-Lockdowns in sogenannten Welcome Back Talks über deren Privatleben und etwaige familiäre und gesundheitliche Probleme ausspionieren lassen. Diese Daten waren digital festgehalten und Führungskräften zugänglich gemacht worden. Das Unternehmen legte keine Berufung ein und entschuldigte sich.

Wenn Kundendaten ohne Einwilligung genutzt werden

Auch wenn Kundendaten ohne eine wirksame Einwilligung zu Werbezwecken genutzt werden, kann es teuer werden: [Eine Krankenkasse in Baden-Württemberg zahlte dafür ein Bußgeld von 1,24 Millionen Euro](#). Sie hatte personenbezogenen Daten von mehr als 500 Gewinnspielteilnehmern ohne deren Einwilligung zu Werbezwecken verwendet.

Wenn ein Streaming-Dienst Daten sammelt – und nicht sagt, wofür

Im Dezember 2024 verhängte die niederländische Datenschutzbehörde Dutch Data Protection Authority (Dutch DPA) [ein Bußgeld von 4,75 Millionen Euro gegen einen großen US-amerikanischen Streaming-Anbieter](#). Der hatte zwischen 2018 und 2020 massenhaft private Nutzerdaten gesammelt, allerdings in seinen Geschäftsbedingungen nicht klar genug darüber informiert, was genau mit diesen Daten geschieht – auch nicht, als diese nachfragten. Der Streaming-Anbieter hat Einspruch erhoben.

Wenn ein Fahrdienstleister Fahrerdaten nicht ausreichend schützt

Auch in diesem Fall ist ein US-Unternehmen ins Visier geraten: [Ein Fahrdienstleister soll zwischen August 2021 und November 2023 personenbezogene Daten von europäischen Kunden in seine Zentrale in den USA übermitteln und nicht ausreichend geschützt haben](#). Nach Angaben der Datenschutzbehörde in Den Haag gehörten zu den auf US-Servern gespeicherten Daten unter anderem Identitätsnachweise und Zahlungsdetails sowie teils sogar Standortdaten, Fotos oder strafrechtliche und medizinische Daten der Fahrer.

Die niederländische Datenschutzbehörde verhängte deshalb im August 2024 ein Bußgeld über 290 Millionen Euro. Auch dieses Unternehmen hat Widerspruch eingelegt. In dem beanstandeten Zeitraum war das Datenschutzabkommen zwischen der EU und den USA wegen europäischer Gerichtsentscheide außer Kraft gesetzt.

Auch die EU-Kommission musste schon eine Strafe zahlen

Die EU-Kommission muss einem Besucher einer von ihr betriebenen Website 400 Euro Schadensersatz zahlen: Der Kläger hatte sich über die Website zu einer Veranstaltung angemeldet und nutzte den Authentifizierungsdienst „EU Login“ der Kommission. Dabei entschied er sich für die Option „mit Facebook anmelden“. Später klagte er unter anderem deswegen, weil seine IP-Adresse an die Facebook-Mutter Meta übermittelt worden sei. Das Gericht der Europäischen Union in Luxemburg entschied im Januar 2025, der Betroffene habe durch die Übermittlung seiner IP-Adresse an Facebook einen immateriellen Schaden erlitten. Zu diesem Zeitpunkt sei nicht sicher gewesen, dass die USA personenbezogene Daten von EU-Bürgern angemessen schützt.

Künstliche Intelligenz und Datenschutz

Der Einsatz Künstlicher Intelligenz berührt viele Fragen des Datenschutzes. Unternehmen, die KI einsetzen – zum Beispiel für Chatbots oder automatisierte Analysen – betreten datenschutzrechtliches Neuland. Auf welcher Rechtsgrundlage erfolgt die Datenverarbeitung? Sind die Entscheidungsprozesse nachvollziehbar? Welche Rechte haben Betroffene bei automatisierten Entscheidungen? Diese Fragen werden in der EU derzeit intensiv diskutiert. Datenschutzbehörden warnen zunehmend vor „Black Box“-KI-Anwendungen, bei denen unklar ist, wie Entscheidungen zustande kommen.

Datenschutzbehörden in Deutschland

In Deutschland kümmern sich Datenschutzbehörden sowohl auf Bundesebene als auch auf Ebene der 16 Bundesländer um das Thema. Sie machen ihre Arbeit in alljährlichen Tätigkeitsberichten transparent. Im [Tätigkeitsbericht vom April 2025](#) meldete die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) einen neuen Beschwerde-Höchststand: Mit 8.670 Beschwerden sind im Jahr 2024 888 mehr bei der BfDI eingegangen als im Vorjahr.

[Schaut man auf die Bundesländer sind auch hier Rekorde zu verzeichnen](#): Allein der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit verzeichnete über 4.000 Beschwerden und Datenpannen sowie 20 rechtskräftig abgeschlossene Bußgeldverfahren mit einer Bußgeldhöhe von insgesamt über 1,2 Millionen Euro. Viele Fälle, so die Behörde in einer offiziellen Mitteilung, „waren Ausdruck eines schlechten Datenmanagements. Daten wurden vielfach deutlich länger gespeichert als notwendig, Datenlisten werden schlecht entsorgt, oft weniger aus bösem Willen als aus Unachtsamkeit oder fahrlässigem Unwissen. Gut strukturierte digitale Prozesse sind jedoch nicht nur für den Datenschutz unabdingbar, sondern auch für eine zukunftsfähige Unternehmensführung. Gerade für Unternehmen mit digitalen Geschäftsmodellen ist eine professionelle Datennutzung unumgänglich.“

Der EU AI Act

Am 1. August 2024 ist die europäische Verordnung über künstliche Intelligenz – die KI-Verordnung, auch bekannt als EU AI Act – in Kraft getreten. Die meisten Vorschriften gelten jedoch erst ab 2026. Der EU AI Act verpflichtet Unternehmen zum Beispiel beim Einsatz von „hochriskanten KI-Systemen“, wie etwa KI-basierter medizinischer Software oder KI-Systemen für die Personaleinstellung, zu strengen Prüfungen, Dokumentationen und einer menschlichen Kontrolle.

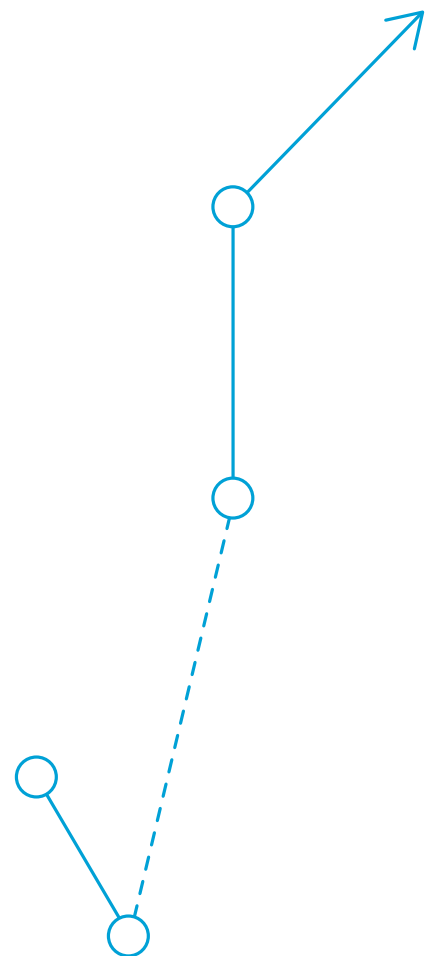
Die DSGVO wird Stand Frühjahr 2025 nicht geändert, aber in der Praxis durch die Regelungen des EU AI Act ergänzt – insbesondere dort, wo KI-Systeme personenbezogene Daten verarbeiten. Die DSGVO enthält bereits Regelungen, die KI-Anwendungen betreffen, etwa:

- **Artikel 5:** Grundsätze wie Datenminimierung und Transparenz
- **Artikel 22:** Verbot rein automatisierter Entscheidungen mit Rechtswirkung (mit Ausnahmen)
- **Artikel 13/14:** Informationspflichten – auch über die Logik automatisierter Verarbeitung
- **Artikel 35:** Datenschutz-Folgenabschätzung (DSFA) – verpflichtend bei risikoreichen KI-Systemen

EU-Kommission und Datenschutzaufsicht (EDPB) arbeiten an Leitlinien, wie DSGVO-Vorgaben auf KI anzuwenden sind. Deutschland prüft parallel dazu, ob auch das BDSG mit Blick auf KI-Anwendungen angepasst werden muss.

Übrigens: Schon seit Februar 2025 müssen Anbieter und Betreiber von KI-Systemen laut KI-Verordnung Maßnahmen ergreifen, die sicherstellen, dass „ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen“.

Wer KI im Unternehmen einsetzt, sollte die Gesetzeslage auf jeden Fall im Blick behalten und sehr sorgfältig prüfen, ob der KI-Einsatz rechtskonform geschieht.



Arbeitsrecht in Deutschland

Das deutsche Arbeitsrecht bildet den rechtlichen Rahmen für Arbeitsverhältnisse und betriebliche Abläufe. Es ist nicht in einem einzigen Gesetz festgehalten, sondern ergibt sich aus einer ganzen Vielzahl an Gesetzen, die vom Bürgerlichen Gesetzbuch über das Mutterschutzgesetz oder das Jugendarbeitsschutzgesetz bis hin zum Bundesurlaubsgesetz reicht. Die Liste der rechtlichen Regelungen ist lang.

Die Regelungen betreffen zum Beispiel den Abschluss von Arbeitsverträgen, die Arbeitsbedingungen, den Kündigungsschutz, die Rechte von Mitarbeitenden sowie die Mitbestimmung durch Betriebsräte. Unternehmen, die in Deutschland tätig sind oder den Markteintritt planen, müssen sich mit dem Arbeitsrecht sorgfältig auseinandersetzen – es ist essenziell, um rechtssicher zu agieren und arbeitsrechtliche Risiken zu minimieren.

Aspekte des deutschen Arbeitsrechts

Der deutsche Gesetzgeber unterscheidet im deutschen Arbeitsrecht grundsätzlich zwischen

- **Individualarbeitsrecht:** Dies regelt die Beziehung zwischen Arbeitgeber und einzelnen Mitarbeitenden, etwa wenn es um Arbeitsvertrag, Arbeitszeit, Vergütung und Kündigung geht.
- **Kollektivarbeitsrecht:** Dies betrifft die Rechte und Pflichten von Betriebsräten und Gewerkschaften, insbesondere Tarifverträge und Mitbestimmungsrechte.

Weil das deutsche Arbeitsrecht so detailreich, vielfältig und komplex ist, hier nur einige Kerninhalte, die für Unternehmen mit Aktivitäten in Deutschland besonders relevant sind:

Arbeitsverträge und Rechte von Mitarbeitenden

Arbeitsverhältnisse in Deutschland beruhen in der Regel auf schriftlichen Arbeitsverträgen. Zwar sind auch mündliche Absprachen rechtlich wirksam, allerdings verpflichtet das Nachweisgesetz (NachwG) Arbeitgeber dazu, wesentliche Vertragsbedingungen schriftlich festzuhalten.

Ein typischer Arbeitsvertrag enthält unter anderem

- die Bezeichnung der Tätigkeit und den Aufgabenbereich
- den Beginn und eventuell auch die Befristung des Arbeitsverhältnisses
- den Arbeitsort und die Arbeitszeit
- die Vergütung inklusive eventueller Bonus- und Überstundenregelungen
- den Urlaubsanspruch
- die Kündigungsfristen
- gegebenenfalls Hinweise auf geltende Tarifverträge

Die meisten Arbeitsverträge sehen eine Probezeit von maximal 6 Monaten vor. Während dieser Zeit können beide Parteien mit einer verkürzten Frist von zwei Wochen kündigen.

Kündigungsschutz

In Deutschland genießen Arbeitnehmende einen im internationalen Vergleich starken Kündigungsschutz. Kündigungen sind zwar nicht unmöglich, müssen aber gut begründet sein und rechtlich sauber umgesetzt werden.

Die wichtigsten Regelungen dazu finden sich im Kündigungsschutzgesetz (KSchG). Es gilt in der Regel für Betriebe mit mehr als zehn Mitarbeitenden und greift, sobald das Arbeitsverhältnis länger als sechs Monate besteht.

Wichtig zu wissen

Um mit dem deutschen Arbeitsrecht konform zu sein, muss ein Arbeitgeber einen triftigen Kündigungsgrund haben. Dafür gibt es drei Möglichkeiten:

- Die betriebsbedingte Kündigung bei wirtschaftlichen Schwierigkeiten oder Umstrukturierungen
- Die personenbedingte Kündigung, wenn Mitarbeitende dauerhaft nicht (mehr) geeignet sind, ihre Tätigkeit auszuüben
- Die verhaltensbedingte Kündigung, wenn sich jemand trotz Abmahnung wiederholt falsch verhält

Ein häufiger Stolperstein für rechtssichere Kündigungen ist die Missachtung von Fristen. In der Regel gelten gesetzliche Kündigungsfristen gemäß §622 BGB. Sie sind je nach Betriebszugehörigkeit gestaffelt, es sei denn, der Arbeits- oder Tarifvertrag regelt etwas anderes.

Besonderen Schutz genießen bestimmte Gruppen von Arbeitnehmerinnen und Arbeitnehmern, dazu zählen Schwangere, Menschen mit Schwerbehinderung oder Mitglieder des Betriebsrats. Sie sind nur in Ausnahmefällen und mit Zustimmung der zuständigen Behörden kündbar.

Wichtig zu wissen für Unternehmen mit Betriebsrat

Unternehmen müssen dem Betriebsrat vor jeder Kündigung die Gründe für die geplante Kündigung mitteilen und ihm Gelegenheit zur Stellungnahme geben. Ohne eine solche Anhörung ist die Kündigung automatisch unwirksam (§ 102 BetrVG).

Diskriminierungsverbot und Gleichbehandlung

Das Allgemeine Gleichbehandlungsgesetz (AGG) schützt Beschäftigte in Deutschland vor einer Benachteiligung am Arbeitsplatz. Das gilt schon im Bewerbungsverfahren. Das Gesetz will Diskriminierung aus Gründen der ethnischen Herkunft, des Geschlechts, der Religion oder Weltanschauung, einer Behinderung, des Alters oder der sexuellen Identität verhindern.

Arbeitgeber dürfen weder bei der Einstellung noch bei einer Beförderung oder Kündigung Entscheidungen treffen, die auf einem dieser Merkmale beruhen. Auch eine Belästigung am Arbeitsplatz fällt unter das AGG.

Achtung: Viele Unternehmen verstoßen schon in ihren Stellenausschreibungen gegen das AGG. Formulierungen wie zum Beispiel „junger, dynamischer Mitarbeiter gesucht“ können als Altersdiskriminierung ausgelegt werden. Es gilt also, sorgfältig zu formulieren.

Wer gegen das AGG verstößt, riskiert Schadensersatz- und Entschädigungsansprüche. Diese Ansprüche können sich auch dann ergeben, wenn die diskriminierte Person nicht eingestellt wurde.

Datenschutz im Arbeitsverhältnis

Auch im Arbeitsverhältnis gilt der umfassende Schutz personenbezogener Daten. Rechtsgrundlagen sind die Datenschutz-Grundverordnung (DSGVO) sowie das Bundesdatenschutzgesetz (BDSG). Arbeitgeber dürfen nur solche Daten verarbeiten, die für die Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses erforderlich sind (§ 26 BDSG).

Zulässig ist unter anderem

- die Speicherung von Personalstammdaten, also Name, Adresse und Steuer-ID
- das Führen von Arbeitszeitkonten
- die Lohn- und Gehaltsabrechnung
- das Dokumentieren von Gesundheitsdaten zur Lohnfortzahlung im Krankheitsfall (mit besonderem Schutz)

Generell sollten Unternehmen beim Thema Datenschutz sehr aufmerksam sein. Wenn zum Beispiel Fotos von Mitarbeitenden auf der Website veröffentlicht werden sollen, müssen diese vorher einwilligen. Die Einwilligung muss freiwillig, informiert und widerrufbar erfolgen.

Ein besonders sensibler Bereich ist die Überwachung am Arbeitsplatz. Ob Videoüberwachung, GPS-Tracking oder das Auswerten von E-Mails: All das ist in Deutschland nur sehr begrenzt erlaubt und muss transparent, verhältnismäßig und zweckgebunden erfolgen.

Mitbestimmung durch den Betriebsrat

In Unternehmen mit mindestens fünf dauerhaft beschäftigten Arbeitnehmerinnen und Arbeitnehmern kann ein Betriebsrat gewählt werden (§ 1 BetrVG). Der Betriebsrat vertritt die Interessen der Belegschaft gegenüber der Geschäftsführung und spielt eine zentrale Rolle im kollektiven Arbeitsrecht.

Das Betriebsverfassungsgesetz (BetrVG) regelt, in welchen Angelegenheiten der Betriebsrat mitbestimmen oder zumindest angehört werden muss. Dazu zählen unter anderem Kündigungen, Arbeitszeit- und Urlaubsregelungen oder die Einführung technischer Überwachungssysteme.

Wichtig zu wissen

Ohne Zustimmung des Betriebsrats sind bestimmte Maßnahmen unwirksam oder müssen per Einigungsstelle geklärt werden. Die Einigungsstelle ist ein innerbetriebliches Schlichtungsgremium, das aus Vertreterinnen und Vertretern beider Seiten sowie einem neutralen Vorsitz besteht.

Was Unternehmen im Blick behalten sollten

Das Arbeitsrecht in Deutschland entwickelt sich nicht zuletzt durch die Digitalisierung und New Work-Konzepte kontinuierlich weiter. Insbesondere drei Themen gewinnen an Bedeutung:

Remote Work & Homeoffice: Spätestens seit der Corona-Pandemie sind flexible Arbeitsmodelle auch in Deutschland nicht mehr wegzudenken. Noch gibt es kein umfassendes Homeoffice-Gesetz. Trotzdem sollten Unternehmen ihre Regelungen zur mobilen Arbeit arbeitsvertraglich klar festlegen und dabei Aspekte wie Arbeitszeit, Erreichbarkeit, Datenschutz und Kostenerstattung berücksichtigen.

Künstliche Intelligenz: Die rasante Verbreitung von KI-Tools wirft viele arbeitsrechtliche Fragen auf, zum Beispiel, wenn es darum geht, mit ihrer Hilfe Arbeitsleistungen zu überwachen, Entscheidungen zu treffen oder sie generell im HR-Bereich einzusetzen. Hier spielen auch wieder Mitbestimmungsrechte des Betriebsrats (§ 87 BetrVG) eine zentrale Rolle.

Hinweisgeberschutz: Unternehmen sollten auch das im Juli 2023 in Kraft getretene Hinweisgeberschutzgesetz (HinSchG) im Auge behalten. Ihm zufolge müssen Unternehmen ab 50 Mitarbeitenden interne Meldestellen für Whistleblower einrichten. Die Anforderungen betreffen nicht nur Compliance, sondern auch den Umgang mit Beschäftigten, die Missstände intern melden, also mit den Whistleblowern selbst. Unternehmen, die dem nicht nachkommen, drohen Bußgelder.

Strafen und Sanktionen bei Verstößen

Arbeitsrechtliche Verstöße können für Unternehmen nicht nur juristische und wirtschaftliche Folgen haben, sondern sich auch negativ aufs Image auswirken. Die Bandbreite reicht von internen Auseinandersetzungen über öffentliche Gerichtsverfahren bis hin zu empfindlichen Bußgeldern.

Typische Folgen arbeitsrechtlicher Verstöße sind zum Beispiel:

- **Arbeitsgerichtliche Verfahren:** Mitarbeitende können gegen Kündigungen, Abmahnungen oder Benachteiligungen klagen. Die Arbeitsgerichte entscheiden dann über Wiedereinstellung, Schadensersatz oder Abfindung.
- **Schadensersatzpflichten:** Verstöße gegen das AGG, das Mutterschutzgesetz oder das Arbeitszeitgesetz können zu Schadensersatz- oder Entschädigungsansprüchen führen.
- **Vertragsnichtigkeit oder -unwirksamkeit:** Unzulässige Klauseln in Arbeitsverträgen können im Streitfall als ungültig gewertet werden.

Beispiele aus der Praxis – und ihre Folgen

Missachtung von Arbeitszeitregelungen

Wer dauerhaft Überstunden ohne Ausgleich oder ohne gesetzliche Ruhezeiten anordnet, riskiert nicht nur Klagen von Mitarbeitenden, sondern auch Sanktionen durch die Arbeitsschutzbehörden.

Diskriminierung im Bewerbungsprozess

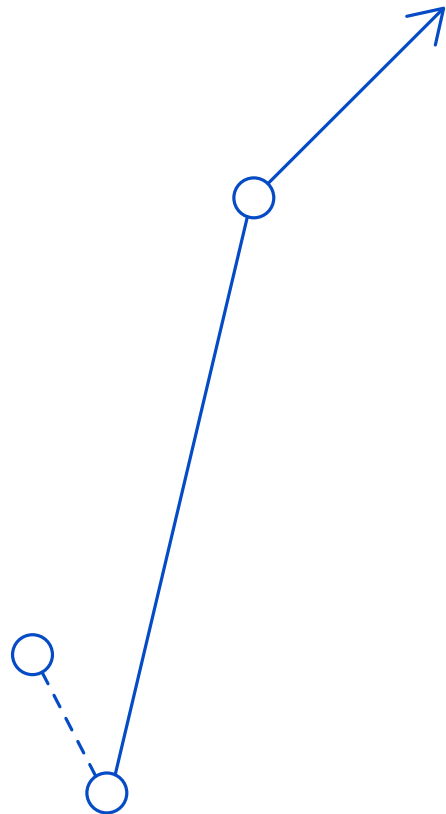
Wird eine Bewerber aufgrund des Geschlechts, Alters oder der Herkunft abgelehnt und kann dies nachgewiesen werden, droht eine Entschädigung gemäß § 15 AGG.

Unwirksame Kündigung

Wird ein Betriebsrat nicht ordnungsgemäß beteiligt oder liegt kein sozial gerechtfertigter Kündigungsgrund vor, ist die Kündigung anfechtbar, oft mit erfolgreichem Ausgang für die klagende Partei.

Datenschutzverletzungen

Unerlaubte Überwachung oder das Speichern sensibler Daten ohne Rechtsgrundlage oder Einwilligung führt zu Verfahren durch Datenschutzaufsichtsbehörden mit teils hohen Bußgeldern und Reputationsschäden.



Berichtspflichten in Deutschland und der EU: LkSG, CSRD, CSDDD

Alles im Fluss

Unternehmen, die in Deutschland und der EU tätig sind, sind mit anspruchsvollen Berichtspflichten konfrontiert. Das deutsche Lieferkettengesetz (LkSG) sowie die Corporate Sustainability Reporting Directive (CSRD) und die 2024 in Kraft getretene Corporate Sustainability Due Diligence Directive (CSDDD oder CS3D) verlangen den Unternehmen umfangreiche Informationen zu ihren Nachhaltigkeitsaktivitäten ab.

Seit Ende 2024 ist die Kritik an den Vorgaben immer lauter geworden. In Deutschland fordern Politiker eine Aussetzung des LkSG sowie eine erhebliche Abschwächung der genannten EU-Richtlinien. Wenn es nach ihnen geht, soll der Adressatenkreis verkleinert, die Fristen verschoben und die Umsatzschwellen angehoben werden. Ziel ist es, die bürokratische Belastung insbesondere von Kleinen und Mittleren Unternehmen zu minimieren. EU-Kommissionspräsidentin

Die „Global CSRD Survey 2024 – Ergebnisse für Deutschland“ zeigen, dass sich

62%

der befragten Firmen als sehr gut auf das CSRD-Reporting vorbereitet betrachten

Ursula von der Leyen stellte bei ihrer Rede beim Weltwirtschaftsforum in Davos im Januar 2025 in Aussicht, die „Vorschriften für nachhaltige Finanzierungsinstrumente und die Sorgfaltspflichten erheblich zu vereinfachen“. Schon mit der „Budapester Erklärung zur Wettbewerbsfähigkeit Europas“ vom 8. November 2024 kündigte Ursula von der Leyen an, die Mitteilungspflichten im Jahr 2025 bündeln und die Anzahl der zu meldenden Datenpunkte deutlich reduzieren zu wollen.

Experten wie Karl Würz, Geschäftsführer des auf die Einführung von Compliance Management Systemen (CMS) spezialisierten Unternehmens equeo CompCor, erwarten, dass eine neue Bundesregierung das jetzige LkSG nach der Bundestagswahl zeitnah ändern wird. Auch mit Blick auf die EU-Berichtspflichten prognostiziert CMS-Experte Würz Veränderungen. „Bestimmte bestehende und künftige ESG-Berichtspflichten der EU könnten in einer sogenannten Omnibus-Verordnung zusammengefasst werden. Das würde unter anderem Pflichten aus der Richtlinie zur Nachhaltigkeitsberichterstattung CSRD, der Taxonomie-Verordnung und der Lieferkettenrichtlinie CSDDD betreffen“

Es gibt aber nicht nur Kritik: Studien wie etwa die „Global CSRD Survey 2024 – Ergebnisse für Deutschland“ zeigen, dass Führungskräfte das CSRD-Reporting zunehmend als Chance betrachten und sich 62 Prozent der in Deutschland befragten Firmen als sehr gut auf das CSRD-

Reporting vorbereitet betrachten. Auch dass es sinnvoll ist, Menschenrechte und Umweltstandards in globalen Lieferketten zu schützen, ist in der Wirtschaft weitgehend Konsens. Unbestritten ist ebenfalls, dass Unternehmen resilienter werden, wenn sie Risiken in ihren Lieferketten kennen und durch eine Detailkenntnis ihrer Prozesse Ressourcen und somit Kosten sparen.

Dem Risiko ist es egal, ob es reguliert ist oder nicht. Mit anderen Worten: Unternehmen sollten auch bei einer möglichen Lockerung der Vorschriften eine Strategie beibehalten, mit der sie Risiken auf Grundlage bewährter Verfahren und Erfahrungen minimieren.

Grundsätzlich empfehlen wir, die Reputationsvorteile zu nutzen, die sich aus der Einhaltung dieser Vorschriften ergeben. Die Unternehmen sollten sich darüber im Klaren sein, dass „das Richtige tun“ immer noch eine Chance ist, bei Kunden, Geschäftspartnern, Mitarbeitern und der Öffentlichkeit langfristig Ansehen zu schaffen.

Das Lieferketten-sorgfaltspflichtengesetz (LkSG)

Das deutsche Lieferketten-sorgfaltspflichtengesetz, kurz: Lieferkettengesetz oder LkSG, ist aktuell noch in Kraft. Im Moment kann aber niemand so genau sagen, wie lange es in seiner derzeitigen Form noch existieren wird. Seit Anfang Dezember

2024 liegen dem deutschen Bundestag zwei Gesetzesentwürfe vor, die die sofortige Außerkraftsetzung des LkSG fordern. Die Kritik: Das LkSG sei zu bürokratisch, seine Umsetzung zu aufwändig und es schwäche insgesamt die Position deutscher Unternehmen im internationalen Wettbewerb. Selbst Befürworter des Lieferkettengesetzes fordern, dass es einfacher und unbürokratischer werden müsse, wollen aber nicht, dass es komplett ausgesetzt wird.

Das für die Überwachung des LkSG zuständige Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) hat die Pflicht zur Veröffentlichung und zur Bereitstellung eines Berichtes an das BAFA einstweilen auf den 31.12.2025 verschoben.

Wen betrifft das LkSG?

Das deutsche Lieferkettengesetz ist seit dem 1. Januar 2023 in Kraft und gilt aktuell unabhängig von Umsatz und Rechtsform für alle Unternehmen, die ihren Sitz oder eine Zweigniederlassung in Deutschland haben und mindestens 1.000 Mitarbeitende in Deutschland beschäftigen.

Das LkSG verpflichtet die Unternehmen, die Menschenrechts- und Umweltstandards in ihren Lieferketten zu überwachen und zu sichern. Dabei müssen sie in erster Linie ihre unmittelbaren Zulieferer auf Herz und Nieren prüfen, mittelbare Zulieferer geraten nur dann in den Fokus, wenn konkrete Verdachtsmomente für Verstöße gegen das LkSG vorliegen. Mit Inkrafttreten des LkSG sind zum Beispiel Finanzinstitute für Verstöße innerhalb der Lieferketten von Unternehmen verantwortlich, deren Geschäftstätigkeit sie finanzieren.

Auch beim LkSG gibt es – wie bei den EU-Richtlinien CSDDD und CSRD – eine Art Kettenreaktion, die dafür sorgt, dass indirekt auch kleinere Unternehmen betroffen sind: Da die größeren Unternehmen Transparenz in ihre

„Das LkSG verpflichtet die Unternehmen, die Menschenrechts- und Umweltstandards in ihren Lieferketten zu überwachen und zu sichern.“

Lieferkette bringen müssen, fordern sie von ihren Lieferanten entsprechende Informationen. Aus diesem Grund sind auch kleine und mittlere Unternehmen in der Lieferkette dazu gezwungen, die Daten zu erheben und aufzubereiten.

Das Ziel des LkSG?

Das LkSG will soziale und ökologische Missstände in globalen Lieferketten beheben und gleichzeitig Unternehmen in die Pflicht nehmen, ihre Macht und Ressourcen für positive Veränderungen einzusetzen. Menschenrechte und Umweltstandards sollen geschützt und gefördert werden, und zwar nicht nur bei den unmittelbaren Geschäftsaktivitäten eines Unternehmens, sondern auch bei deren Lieferanten und Partnern.

Was ist konkret zu tun?

- **Risiken analysieren :** Die Unternehmen müssen ihre Lieferketten genau analysieren, um die Risiken für Menschenrechtsverletzungen oder Umweltverstöße zu identifizieren, zu minimieren und zu verhindern – und um zu erkennen, welche Zulieferer oder Produktionsstufen besonders risikobehaftet sind.
- **Präventive Maßnahmen ergreifen:** Unternehmen sollen Probleme verhindern, bevor sie entstehen, das heißt im Klartext: Sie müssen vorbeugende Maßnahmen ergreifen, zum Beispiel indem sie in ihren Lieferantenverträgen klare Standards für Menschenrechte und Umweltschutz festlegen und ihre Mitarbeitenden und Geschäftspartner entsprechend schulen, damit sie die Regeln kennen und umsetzen.
- **Abhilfe schaffen:** Wenn etwas schief läuft, dann sind die Unternehmen verpflichtet, sofort Maßnahmen zu ergreifen, um die Schäden zu beheben – das erstreckt sich von der Verbesserung von Arbeitsbedingungen bei

einem Lieferanten bis hin zur Entschädigung von Betroffenen.

- **Beschwerdemechanismen einrichten:** Die Unternehmen müssen Menschen eine Möglichkeit geben, Probleme zu melden – und zwar, ohne dass diese Menschen Repressalien fürchten müssen. Ein internes Whistleblowing-System soll ermöglichen, dass Mitarbeitende, Zulieferer oder andere Personen Missstände anonym melden können.
- **Berichte erstellen und veröffentlichen:** Sämtliche Aktivitäten zur Einhaltung der Lieferpflichten müssen in jährlichen Berichten dokumentiert und dem Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) vorgelegt. Die Berichte sind öffentlich zugänglich zu machen.
- **Laufend überwachen:** Das LkSG ist keine Ad-hoc-Regelung, sondern eine Daueraufgabe. Unternehmen müssen sämtliche Maßnahmen regelmäßig überprüfen und gegebenenfalls anpassen; außerdem müssen sie auch eventuelle neue Risiken permanent im Blick haben.

Was droht bei Verstößen gegen das LkSG?

Im Gegensatz zu CS3D und CSRD enthält das Lieferkettengesetz keine eigenständige zivilrechtliche Haftungsregelung. Verstöße gegen das LkSG können allerdings mit empfindlichen Bußgeldern von bis zu 8 Millionen Euro oder bei Unternehmen mit einem Jahresumsatz von über 400 Millionen Euro von 2 % des Jahresumsatzes geahndet werden. Außerdem droht bei Verstößen der Ausschluss von Öffentlichen Aufträgen und ein Reputationsverlust bei Geschäftspartnern, Investoren und Konsumenten.

Die Corporate Sustainability Due Diligence Directive (CSDDD oder CS3D)

Die CS3D wird von den einen als bürokratisches Ungetüm und von den anderen als Meilenstein für nachhaltiges Wirtschaften betrachtet. Sicher ist, dass die Umsetzung der CS3D-Anforderungen Zeit, Geld und Ressourcen erfordert. Dieser Aufwand kann sich lohnen: für die Unternehmen, für die Shareholder und nicht zuletzt für Umwelt und Gesellschaft. Nachhaltiges Wirtschaften und die Einhaltung von Menschenrechts- sowie Umweltstandards stärken die Wettbewerbsposition von Unternehmen, minimieren Risiken und machen ihre Lieferketten insgesamt resilienter. Unternehmen profitieren also langfristig und leisten zugleich einen Beitrag zu einer verantwortungsvolleren Wirtschaft – mal ganz davon abgesehen, dass die Richtlinie für viele Unternehmen innerhalb und außerhalb der EU in naher Zukunft verpflichtend sein wird.

Wen betrifft die CS3D?

Die europäische Lieferkettenrichtlinie über die unternehmerische Sorgfaltspflicht im Bereich Nachhaltigkeit – die Corporate Sustainability Due Diligence Directive (CS3D) der EU – trat am 25. Juli 2024 in Kraft. Die Mitgliedstaaten sind nach aktuellem Stand dazu verpflichtet, die Richtlinie bis zum 26. Juli 2026 in nationales Recht umzusetzen.

Die CSDDD richtet sich zunächst an große Unternehmen innerhalb und außerhalb der EU, ihr Geltungsbereich soll aber schrittweise ausgeweitet werden:

Unternehmen innerhalb der EU:

- Ab Juli 2027: Unternehmen mit mehr als 5.000 Beschäftigten und einem weltweiten Nettoumsatz von über 1,5 Milliarden Euro.

- Ab Juli 2028: Unternehmen mit mehr als 3.000 Beschäftigten und einem weltweiten Nettoumsatz von über 900 Millionen Euro.
- Ab Juli 2029: Unternehmen mit mehr als 1.000 Beschäftigten und einem weltweiten Nettoumsatz von über 450 Millionen Euro.

Unternehmen außerhalb der EU: Die Richtlinie gilt auch für Unternehmen mit Sitz außerhalb der EU, sofern sie einen signifikanten Teil ihres Umsatzes innerhalb der EU generieren. Die oben genannten Umsatzschwellen beziehen sich dabei nur auf Umsätze innerhalb der EU.

Wichtig für kleine und mittlere Unternehmen:

Obwohl die CS3D primär große Unternehmen adressiert, betrifft sie indirekt auch kleinere und mittlere Unternehmen (KMU). Durch den sogenannten „Trickle-Down“-Effekt müssen KMU, die Teil der Lieferkette großer Unternehmen sind, ebenfalls valide Informationen bereitstellen, um den hohen Transparenzanforderungen zu genügen. KMU sind also gut beraten, sich mit den Anforderungen der CS3D auseinanderzusetzen und entsprechende Daten aufzubereiten. Damit stärken sie nicht nur ihre Wettbewerbsfähigkeit, sondern punkten auch bei Finanzinstituten, die ihre Kreditvergabe zunehmend an Nachhaltigkeitsdaten knüpfen.

Was ist konkret zu tun?

Um CS3D-konform zu agieren, müssen Unternehmen viele spezifische Maßnahmen entlang ihrer Wertschöpfungskette umsetzen. Dazu zählen:

- **Die Integration der Sorgfaltspflichten:** Die CS3D verpflichtet Unternehmen dazu, eine klare, transparente und umsetzbare Richtlinie zu entwickeln, die als verbindliche Grundlage der Unternehmenspolitik dient. In dieser Richtlinie sind die Ziele, Maßnahmen und Prozesse definiert, mit denen das

Unternehmen die Vorgaben der CS3D erfüllen will. Im Zuge dessen müssen auch Verantwortliche auf Leitungsebene und deren Aufgabe benannt werden. Mithilfe eines Risikomanagementsystems sollen die Unternehmen dafür sorgen, dass potenzielle und tatsächliche negative Auswirkungen ihrer Geschäftsaktivitäten auf Menschenrechte und Umwelt entlang der kompletten Lieferkette identifiziert, bewertet und priorisiert werden.

- **Die Risikoanalyse:**
Mithilfe regelmäßiger Risikoanalysen müssen Unternehmen sowohl direkte als auch indirekte Geschäftspartner einschließlich Subunternehmer unter die Lupe nehmen und dabei auch branchenspezifische und geografische Risiken einbeziehen. Sämtliche Risiken mit Blick auf Menschenrechtsverletzungen, wie etwa Zwangs- und Kinderarbeit, sowie auf Umweltverstöße, wie etwa illegale Abholzung, müssen klar erkannt, benannt und bewertet werden.
- **Maßnahmen zur Verhinderung und Abhilfe:**
Mithilfe präventiver Maßnahmen sollen Unternehmen die identifizierten Risiken von Vorneherein verhindern oder zumindest minimieren. Die Palette solcher Maßnahmen reicht von Anpassen der Lieferverträge bis zur Schulung von Mitarbeitenden und Lieferanten. Tritt ein Risiko ein, müssen sie Abhilfe schaffen und Maßnahmen ergreifen, um den Schaden zu begrenzen, zum Beispiel indem sie Betroffene entschädigen und im Zweifel sogar Geschäftsbeziehungen auflösen.
- **Das Etablieren eines Beschwerdesystems:**
Die CS3D verlangt von Unternehmen die Einführung von sicheren und vertraulichen Beschwerdekanälen für Mitarbeitende, Lieferanten und externe Betroffene. Dabei müssen sie sicherstellen, dass die Whistleblower vor Repressalien geschützt

sind. Alle gemeldeten Fälle müssen dokumentiert und verfolgt werden.

- **Überwachung und Berichtspflichten:**
Unternehmen müssen alle im Rahmen der CS3D eingeführten Maßnahmen und die erreichten Fortschritte regelmäßig – mindestens jährlich – überprüfen, bewerten und die Ergebnisse veröffentlichen; die entsprechenden Berichte müssen der Öffentlichkeit und relevanten Stakeholdern frei zugänglich sein.
- **Die Einhaltung von Klimazielen:** Im Zuge der CS3D müssen Unternehmen einen Plan entwickeln, wie sie im Einklang mit den Zielen des Pariser Klimaabkommens wirtschaften.

Was droht bei Verstößen?

- Bußgelder von bis zu 5 % des weltweiten Jahresumsatzes (festgelegt von den Mitgliedstaaten)
- Zivilklagen betroffener Einzelpersonen oder Gruppen
- Reputationsschäden, möglicher Ausschluss von öffentlichen Ausschreibungen, Verlust von Investoren oder Kunden
- Eingeschränkter Zugang zum EU-Markt für Unternehmen außerhalb der EU

Warum es sich lohnt, jetzt zu handeln

Betrachten Sie die CS3D als Chance! Mit der Einführung der CS3D entsteht Ihnen unweigerlich ein hoher Aufwand. Zugleich bietet sie aber auch große Chancen: Unternehmen, die umwelt- und menschenrechtskonform, nachhaltig und verantwortungsvoll handeln, dienen nicht nur unserem Planeten, sondern minimiere ihre Risiken, machen sich resilienter und steigern Image und Reputation ihres Unternehmens sowie ihre Attraktivität als Arbeitgeber und für Investoren.

Wie anfangen? Bei Prozessen, Datenmanagement & Mindset!

- **Prozesse:** Es empfiehlt sich in einem ersten Schritt, die komplette Wertschöpfungskette hinsichtlich ihrer möglichen Auswirkungen auf Menschenrechte und Umwelt zu überprüfen. Damit identifizieren Sie mögliche Risikobereiche. Integrieren Sie die potenziellen Umwelt- und Menschenrechtsrisiken in Ihr bestehendes Risikomanagement-System. Entwickeln Sie spezifische Kriterien und Kontrollen zur Bewertung und Steuerung dieser Risiken und führen Sie engmaschige Due-Diligence-Prüfungen durch, um sicherzugehen, dass Ihr Unternehmen die Compliance-Anforderungen tatsächlich erfüllt.
- **Datenmanagement:** Ohne ein professionelles IT-System sind die Berichtspflichten der CS3D nicht zu erfüllen. Führen Sie alle Datenquellen zusammen und werten Sie sie aus, um fundierte Entscheidungen treffen zu können. Nutzen Sie Technologien, um alle relevanten Informationen sammeln, aggregieren und analysieren zu können. Spezialisierte Compliance-Software-Lösungen helfen dabei, Due-Diligence-Prozesse zu automatisieren und zu verwalten. Diese Tools sammeln Daten, analysieren sie und generieren Berichte für interne und externe Audits.
- **Mindset:** Schaffen Sie eine starke Unternehmenskultur, die auf Integrität, ethischem Verhalten, Nachhaltigkeit und Verantwortung basiert. Organisieren Sie regelmäßige Schulungen für Mitarbeitende aller Ebenen, um das Bewusstsein und Verständnis für die Wichtigkeit von Nachhaltigkeit und Compliance zu stärken. Die Einhaltung der CS3D ist letztlich eine Gemeinschaftsaufgabe.

Corporate Sustainability Reporting Directive (CSRD)

Die 2022 vom Europäischen Parlament verabschiedete CSRD stellt einen Wendepunkt in der Unternehmensberichterstattung dar und verlangt von vielen Unternehmen eine deutlich transparentere und systematischere Darstellung ihrer Nachhaltigkeitspraktiken.

Die CSRD löst die NFRD (Non-Financial Reporting Directive) ab. Während die NFRD nur von großen Unternehmen einige nicht-finanzielle Informationen forderte, ist das von der CSRD geforderte Reporting deutlich anspruchsvoller. Die CSRD betrifft mehr Unternehmen und enthält detailliertere und standardisierte Berichtspflichten. Unternehmen müssen dokumentieren und veröffentlichen, wie sie nicht nur wirtschaftlich, sondern auch ökologisch, sozial und ethisch Verantwortung übernehmen. Auch nicht-europäische Unternehmen, die in der EU tätig sind und definierte Schwellenwerte überschreiten, fallen unter die Berichtspflicht.

Damit schlägt die CSRD hohe Wellen. Wie bei der CS3D und dem deutschen Lieferkettengesetz steht auch die CSRD wegen des hohen bürokratischen Aufwands in der Kritik. Befürworter wie NGOs und Gewerkschaften begrüßen die CSRD, weil sie Unternehmen dazu verpflichtet, Verantwortung zu übernehmen.

Zweck der CSRD

Die CSRD soll Stakeholdern – von Investoren und Kunden bis hin zu Mitarbeitern und Aufsichtsbehörden – ein klares, vergleichbares Bild der Nachhaltigkeitsleistung und -wirkung eines Unternehmens vermitteln. Ziel ist Transparenz und Rechenschaftspflicht in den Bereichen Umwelt, Soziales und Unternehmensführung.

Wen betrifft die CSRD?

Die CSRD wird schrittweise immer mehr Unternehmen betreffen:

Seit dem Geschäftsjahr 2024 (erster Bericht in 2025): Unternehmen, die bereits unter die NFRD fallen:

- Börsennotierte Unternehmen
- Banken
- Versicherungen

Ab dem Geschäftsjahr 2025 (erster Bericht in 2026): Große Unternehmen, die zwei der folgenden drei Kriterien erfüllen:

- sie beschäftigen mehr als 250 Mitarbeitende
- sie verzeichnen mehr als 40 Millionen Euro Umsatz pro Jahr
- sie verzeichnen mehr als 20 Millionen Euro Bilanzsumme

Ab dem Geschäftsjahr 2026 (erster Bericht in 2027):

- Kleine und mittlere Unternehmen (KMU), die börsennotiert sind
- Kleine Banken und Versicherungen

Ab dem Geschäftsjahr 2028 (Bericht in 2029):

Unternehmen aus Drittländern, wenn sie einen Umsatz von mehr als 150 Millionen Euro in der EU erzielen und eine Niederlassung oder Tochtergesellschaft in der EU unterhalten.

Wie bei dem Lieferkettengesetz und der CS3D gilt auch bei der CSRD der Trickle-down-Effekt:

Auch KMU, die nicht direkt betroffen sind, sollten sich möglichst frühzeitig mit der Nachhaltigkeitsberichterstattung auseinandersetzen, denn auch sie werden mittelbar entsprechende Aktivitäten nachweisen müssen: Größere Unternehmen werden von ihren Geschäftspartnern künftig Nachweise über deren Nachhaltigkeitsengagement

verlangen, um eine nachhaltige Lieferketten vorweisen zu können. Außerdem werden sich Banken bei der Kreditvergabe verstärkt an den Nachhaltigkeitskennziffern orientieren. Auch zunächst nicht unmittelbar von der CSRD betroffenen Unternehmen sind also gut beraten, sich mit den Anforderungen der CSRD auseinanderzusetzen.

Eine zentrale Voraussetzung in Deutschland – die finanzielle und nichtfinanzielle Integration

Ein zentraler Aspekt der Umsetzung der CSRD in Deutschland ist die Verknüpfung der Nachhaltigkeitsberichterstattung mit dem Jahresabschluss. Unternehmen sind verpflichtet, finanzielle und nicht-finanzielle Informationen eng miteinander zu verzahnen. Die Integration beider Berichtsfelder macht die Doppelberichterstattung zum neuen Standard.

Was wird benötigt?

Die CSRD-Berichterstattung ist umfassend und muss den Europäischen Standards für Nachhaltigkeitsberichterstattung (ESRS) entsprechen. Zu den wichtigsten Erwartungen gehören:

- **Standardisierte, prüffähige Berichte:** Unternehmen müssen detaillierte, überprüfbare Berichte über ihre ESG-Aktivitäten erstellen. Diese umfassen unter anderem Klimaauswirkungen, Biodiversität, Ressourcenverbrauch, Menschenrechte, Diversität, Korruptionsbekämpfung und mehr.
- **Vollständige Abdeckung der Wertschöpfungskette:** Die Berichterstattung muss interne Abläufe und die gesamte Liefer-/Wertschöpfungskette abdecken.
- **Externe Prüfung:** Nachhaltigkeitsberichte müssen von einem unabhängigen Prüfer validiert werden.

- **Doppelte Wesentlichkeitsbewertung für Unternehmen:**

- **Finanzielle Wesentlichkeit**

- (Outside-In):** Wie sich ESG-Themen auf die Unternehmensleistung auswirken (z. B. klimabedingte Lieferkettenunterbrechungen)

- **Impact-Wesentlichkeit (Inside-Out):**

- Wie sich die Geschäftstätigkeit des Unternehmens auf Menschen und Umwelt auswirkt (z. B. Emissionen, Arbeitspraktiken)

Dieser Ansatz stellt sicher, dass nur wesentliche Probleme ausführlich gemeldet werden, überträgt den Unternehmen aber auch eine größere Verantwortung für die Durchführung gründlicher Bewertungen.

Was droht bei Verstößen?

Verstöße gegen die CSRD können folgende Folgen haben:

- **Bußgelder** (die Höhe wird von den einzelnen EU-Mitgliedstaaten festgelegt)
- **Klagen** von Investoren oder NGOs wegen unvollständiger oder ungenauer Berichterstattung
- **Vertrauensverlust** bei Stakeholdern, wodurch es schwieriger wird, Investoren zu gewinnen oder Finanzierungen zu sichern
- **Reputationsschäden**, insbesondere wenn die Nichteinhaltung als vorsätzlich oder irreführend angesehen wird

Der Schaden für die Glaubwürdigkeit und den Markenwert kann über die rechtlichen Risiken hinaus erheblich sein.

Warum Unternehmen jetzt handeln sollten

Auch wenn Ihr Unternehmen zum jetzigen Zeitpunkt vielleicht noch nicht berichtspflichtig ist, ist es ratsam, sich auf die CSRD vorzubereiten und Prozesse entsprechend anzupassen:

- Sie haben ESG-Daten parat, wenn Investoren, Partner oder Aufsichtsbehörden danach fragen
- Sie können Möglichkeiten zur Kosteneinsparung, beispielsweise durch Ressourceneffizienz, identifizieren
- Sie sind besser aufgestellt, um Vertrauen bei Kunden und Mitarbeitern aufzubauen
- Sie gewinnen einen Vorsprung bei zukünftigen Berichtspflichten und Erhöhen Ihre langfristige Widerstandsfähigkeit

Die Einrichtung eines internen ESG-Teams, die Definition wichtiger Nachhaltigkeitskennzahlen und die Nutzung von Technologien zur Datenerfassung und -berichterstattung sind kluge Schritte, die jetzt unternommen werden sollten.

Das Hinweisgeberschutzgesetz

Übersicht

Die [EU-Whistleblower-Richtlinie \(EU-Richtlinie 2019/1937\)](#) ist 2019 in Kraft getreten, um Personen zu schützen die im beruflichen Kontext Verstöße gegen das EU-Recht melden. Sie verpflichtet Unternehmen zur Einrichtung sicherer Meldekanäle und untersagt jegliche Repressalien gegen Hinweisgebende. Die Mitgliedstaaten der EU sind verpflichtet, die EU-Whistleblower-Richtlinie in nationales Recht umzusetzen, um einen einheitlichen und effektiven Hinweisgeberschutz in ganz Europa sicherzustellen.

„Ziel ist es, Hinweisgebende wirksam vor Repressalien zu schützen und eine offene Unternehmenskultur zu fördern.“

Das [Hinweisgeberschutzgesetz \(HinSchG\)](#) – das am 02. Juli 2023 in Kraft getreten ist – ist die Umsetzung dieser Richtlinie in deutsches Recht. Das HinSchG verpflichtet Unternehmen mit mehr als 49 Angestellten zur Errichtung sicherer und vertraulicher Meldestellen, über die Mitarbeitende rechtssicher Missstände melden können. Hinweisgeber müssen klar und eindeutig über diese Meldestellen informiert werden. Zusätzlich muss sichergestellt sein, dass die Meldung schriftlich, mündlich oder persönlich vorgenommen werden kann. Der Hinweisgeber muss über den Eingang der Meldung sowie die weiteren Schritte informiert werden.

Ziel ist es, Hinweisgebende wirksam vor Repressalien zu schützen und eine offene Unternehmenskultur zu fördern. Das Recht auf Schutz umfasst überdies nicht nur direkte Angestellte. So sind z.B. auch Auszubildende, Beamte, freie Mitarbeiter und Personen, die den Hinweisgeber unterstützen mit inbegriffen.

Schlüsselbestimmungen des Hinweisgeberschutzgesetzes

1. Meldewürdige Verstöße

Nicht jeder Rechtsverstoß ist im Sinne des HinSchG meldewürdig. Der geltende Schutzbereich im Hinweisgeberschutzgesetz ist jedoch sehr weit gefasst. Es können unter anderem, aber nicht ausschließlich, Verstöße gegen

- Strafvorschriften nach deutschem Recht
- deutsches oder EU-Recht, wie z.B. Geldwäsche, Terrorismusfinanzierung, Steuerdelikte, Verletzung von Umweltschutzvorschriften, Missachtung arbeitsrechtlicher Vorschriften u.v.m.
- die DSGVO
- das Steuerrecht gemeldet werden.

2. Kreis der Hinweisgebenden

Als Hinweisgeber gilt nicht nur ein direkter Angestellter eines Unternehmens. Der Kreis der geschützten Personen umfasst alle Personen, die im Rahmen ihrer beruflichen Tätigkeit Informationen über Verstöße erlangt und diese gemeldet haben. Das sind unter anderem

- Arbeitnehmer, Auszubildende, Beamte
- ehemalige Mitarbeiter
- Selbstständige und freie Mitarbeiter
- Personen die den Hinweisgeber unterstützen

3. Meldestellen: intern und extern

Unternehmen mit mindestens 250 Mitarbeitern sind seit dem 2. Juli 2023 verpflichtet eine interne oder externe Meldestelle einzurichten. Für Unternehmen mit 50 bis 249 Mitarbeitern gilt diese Verpflichtung seit dem 17. Dezember 2023. Für bestimmte Einrichtungen und Unternehmen – wie z.B. Kreditinstitute, Versicherungsunternehmen etc. – gilt keine Mitarbeitergrenze. D.h. sie müssen bereits ab einem Mitarbeiter eine Meldestelle zur Verfügung stellen.

Mitarbeiter müssen klar und deutlich über die Meldestelle informiert werden. Zusätzlich muss die Meldung eines Verstoßes in schriftlicher, mündlicher und persönlicher Form ermöglicht werden. Unternehmen sind nicht verpflichtet, anonyme Meldungen zu ermöglichen. Sie werden jedoch darauf hingewiesen, dass auch anonyme Meldungen bearbeitet werden sollten.

Hinweisgeber haben zusätzlich die Möglichkeit sich an externe Meldestellen – wie z.B. die Bundesmeldestelle beim Bundesamt für Justiz – zu wenden. Dieser Schritt wird empfohlen, wenn nach einer internen Meldung keine Rückmeldung kommt, der Hinweisgeber Angst vor Repressalien hat oder interne Meldungen als zwecklos oder nicht vertrauenswürdig gehalten werden.

4. Wahrung der Vertraulichkeit

Ein zentraler Punkt des Hinweisgeberschutzgesetzes ist die Wahrung der Vertraulichkeit. Die Meldestellen müssen nach Eingang einer Meldung die Identität

- der hinweisgebenden Person
- der Personen, die Gegenstand der Meldung sind
- sowie sonstige in der Meldung genannten Personen wahren.

5. Schutz vor Repressalien

Dem Hinweisgeber darf durch die Meldung von Verstößen kein beruflicher Nachteil entstehen. Hierin inbegriffen sind auch die Androhung und der Versuch Repressalien auszuüben.

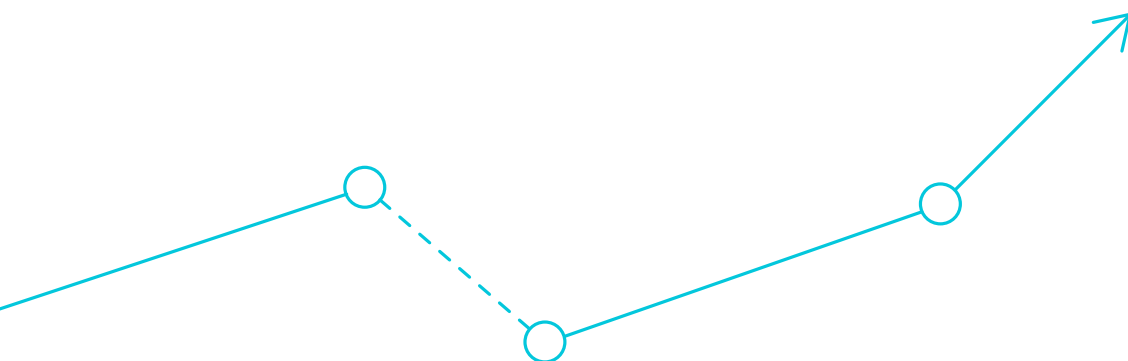
6. Bearbeitungspflicht

Die interne Meldestelle ist verpflichtet, den Hinweisgebern den Eingang der Meldung spätestens nach sieben Tagen zu bestätigen. Zusätzlich muss die Meldestelle der hinweisgebenden Person innerhalb von drei Monaten nach der Bestätigung des Eingangs Rückmeldung über bereits ergriffene sowie geplante Folgemaßnahmen geben.

Sanktionen

Verstöße gegen das Hinweisgeberschutzgesetz stellen Ordnungswidrigkeiten dar und können mit Bußgeldern sanktioniert werden. Die Höhe des Bußgeldes ist abhängig von der Art des Verstoßes.

- **bis zu 50.000€**
Behinderung einer Meldung oder Folgekommunikation, Ergreifung von Repressalien, Verletzung der Vertraulichkeitspflicht
- **bis zu 20.000€**
Keine oder unzureichende Einrichtung interner Meldestellen



EU AI Act

Was Unternehmen zum weltweit ersten KI-Gesetz wissen müssen

Der EU AI Act reguliert den Einsatz von Künstlicher Intelligenz. Das Gesetz ist der weltweit erste umfassende Rechtsrahmen dieser Art, es trat am 1. August 2024 in Kraft.

Der EU AI Act will die Innovation von KI-Systemen fördern und zugleich dafür sorgen, dass beim Einsatz von KI-Technologien Grundrechte, Sicherheit und demokratische Werte geschützt sind. Dabei gehen die Urheber der Verordnung von einem risikobasierten Ansatz aus: KI-Systeme werden nach dem Grad ihrer potenziellen Risiken für Einzelpersonen und für die Gesellschaft klassifiziert und reguliert.

Für das Europäische Parlament war oberste Priorität, „[dass die in der EU verwendeten KI-Systeme sicher, transparent, rückverfolgbar, diskriminierungsfrei und umweltfreundlich sind. KI-Systeme sollten von Menschen überwacht werden, anstatt durch Automatisierung, um schädliche Ergebnisse zu verhindern.](#)“

Seit dem Launch der generativen KI ChatGPT im November 2022 ist die Technologie einem breiten Publikum zugänglich und hat einen beispiellosen Siegeszug angetreten: Die Nutzerzahlen steigen in Rekordgeschwindigkeit und auch die KI-Anwendungen selbst entwickelten sich enorm schnell weiter. KI ist längst im Alltag vieler Menschen angekommen und wird in Unternehmen mittlerweile in zahlreichen sensiblen Bereichen eingesetzt.

Laut einer [Umfrage des ifo Instituts vom Juni 2025](#) verwenden 40,9 Prozent der Unternehmen in Deutschland KI in ihren Geschäftsprozessen, weitere 18,9 Prozent planen ihren KI-Start. Zugleich herrscht in Deutschland eine große Aufgeschlossenheit gegenüber KI-Technologien: Einer Erhebung des Branchenverbands Bitkom aus dem Jahr 2024 zufolge, halten 73 Prozent der Unternehmen und 63 Prozent der Bevölkerung Künstliche Intelligenz für die wichtigste Zukunftstechnologie.

In der EU wurde schon vor 2022 an einer einheitlichen KI-Strategie gearbeitet, 2018 veröffentlichte die EU-Kommission eine koordinierte „[Strategie für künstliche Intelligenz](#)“, gefolgt von einem [Whitepaper im Februar 2020](#), die den Grundstein für eine gezielte KI-Regulierung legten. Über die Ausgestaltung des EU AI Act wurde intensiv debattiert, heute ist er ein zentrales Element der europäischen Digitalstrategie: Er soll einen einheitlichen Rechtsrahmen für alle Mitgliedstaaten schaffen und Europa als globalen Vorreiter für vertrauenswürdige und menschenzentrierte KI positionieren.

Die wichtigsten Punkte des EU AI Act

Der EU AI Act klassifiziert KI-Systeme nach ihren Risiken und teilt sie in vier Kategorien ein:

KI mit unannehmbarem Risiko

Diese Systeme gelten als unannehmbar und sind verboten, weil sie mit europäischen Werten unvereinbar sind. Dazu zählen unter anderem

- soziale Bewertungssysteme (Social Scoring)
- biometrische Massenerkennung, zum Beispiel nach Ethnie, Religion oder sexueller Orientierung
- manipulative Systeme mit unterschwelligen Techniken
- biometrischen Echtzeit-Fernidentifizierungssysteme, wie etwa Echtzeit-Gesichtserkennung im öffentlichen Raum (nur mit wenigen, explizit geregelten Ausnahmen erlaubt)
- Emotionserkennung am Arbeitsplatz oder in Schulen

Hochrisiko-KI

Diese Systeme bergen erhebliche Risiken für Grundrechte, Gesundheit oder Sicherheit, darunter fallen zum Beispiel

- KI in der Personalrekrutierung oder Kreditvergabe
- KI in der medizinischen Diagnostik oder in kritischen Infrastrukturen.

Für die Hochrisiko-KI gelten strenge Anforderungen hinsichtlich

- der Risikobewertung und technischen Dokumentation
- der Transparenz über Funktionsweise und Entscheidungen
- dem Schutz personenbezogener Daten
- der Aufsicht durch natürliche Personen

KI mit begrenztem Risiko

Hierunter fallen KI-Systeme, bei denen Transparenzpflichten bestehen. Werden beispielsweise Chatbots eingesetzt, muss erkennbar sein, dass keine echte Person antwortet; bei KI-generierten Inhalten herrscht eine Kennzeichnungspflicht. Diese gelten verbindlich ab August 2025 für alle GPAI-Anbieter, und zwar nicht nur für Text- und Bild-, sondern auch für Audio-Content.

KI mit minimalem Risiko

In diese Kategorie fallen KI-Anwendungen wie Spamfilter, Übersetzungshilfen oder intelligente Textvervollständigung. Sie unterliegen keinen besonderen Auflagen, können aber freiwillig mit Gütesiegeln oder Selbstverpflichtungen arbeiten.

Wen betrifft der EU AI Act?

Der EU AI Act richtet sich an Unternehmen, Behörden und Organisationen, die KI einsetzen oder entwickeln. Er betrifft alle Akteure entlang der gesamten KI-Wertschöpfungskette. Unternehmen, die in irgendeiner Weise KI-Systeme entwickeln, vertreiben, einführen, bereitstellen, nutzen oder Drittanbieter-KI integrieren, müssen prüfen, ob sie unter die Regulierung fallen. Dabei ist nicht entscheidend, wo das Unternehmen seinen Sitz hat, sondern ob das KI-System auf dem EU-Markt verfügbar gemacht oder in der EU verwendet wird. Der EU AI Act betrifft also auch international tätige Unternehmen mit Bezug zur EU.

Im Kern richtet sich der EU AI Act an folgende Akteure:

Anbieter und Hersteller von KI-Systemen

Unternehmen, die KI-Anwendungen entwickeln und auf den Markt bringen, egal ob intern genutzt oder extern vertrieben.

Inverkehrbringer und Händler

Unternehmen, die KI-Systeme vertreiben oder weiterverkaufen, auch wenn sie von Dritten entwickelt wurden.

Nutzer von Hochrisiko-KI

Unternehmen, die ein fertiges Hochrisiko-KI-System zur Entscheidungsunterstützung oder Automatisierung einsetzen – zum Beispiel zur Bewertung von Bewerbungen, für Bonitätsprüfungen oder für die Diagnostik – müssen Pflichten beachten. Dazu zählen unter anderem die

Schulung von Mitarbeitenden, die Dokumentation oder die Überwachung der Nutzung.

Importeure

Wer KI-Systeme aus Drittstaaten in die EU einführt, ist dafür verantwortlich, dass diese rechtskonform sind.

Zulieferer in der KI-Entwicklung

Auch Teilanbieter, etwa für Trainingsdaten, Modellarchitekturen oder APIs, unterliegen bestimmten Pflichten.

Fristen

Der EU AI Act ist am 1. August 2024 in Kraft getreten. Die Regelungen gelten gestaffelt:

2. Februar 2025

Verbot von KI-Systemen mit unannehmbarem Risiko sowie die Pflicht zur KI-Kompetenzsicherung.

2. August 2025

Transparenz-, Kennzeichnungs- und Dokumentationspflichten für neue General Purpose AI (GPAI)-Modelle.

2. August 2026

Allgemein verpflichtende Vorgaben für Hochrisiko-KI-Systeme.

2. August 2027

Spezielle zusätzliche Anforderungen für (Hochrisiko-)Systemkomponenten, die als Teil von bestehenden Produkten wie etwa Medizinprodukten oder Maschinen eingesetzt werden.

Update November 2025:

Die Digital Omnibus-Initiative der Europäischen Kommission schlägt eine Verschiebung der strengeren Vorgaben des EU AI Acts vor. Besonders hervorzuheben ist, dass die Pflichten für Hochrisiko-KI auf Dezember 2027 verschoben werden sollen. Zudem sollen einige Compliance-Anforderungen reduziert werden – insbesondere für kleinere Unternehmen.

Damit diese vorgeschlagenen Änderungen in Kraft treten können, müssen sie sowohl von den EU-Mitgliedstaaten als auch vom Europäischen Parlament genehmigt werden.

Bis 2. August 2027 läuft die Übergangsfrist für bereits vor dem 2. August 2025 betriebene GPAI-Modelle; sie müssen dann ebenfalls konform sein.

Sanktionen

Die Strafen für Verstöße gegen den EU AI Act fallen je nach Schwere des Verstoßes unterschiedlich aus und können ziemlich teuer werden:

- Beim Einsatz verbotener KI-Systeme droht eine Geldstrafe in Höhe von bis zu 35 Millionen Euro oder 7 Prozent des weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist.
- Bei Verstößen gegen Vorschriften zur Anwendung von Hochrisiko-KI ist eine Strafe von bis zu 15 Millionen Euro oder 3 Prozent des Jahresumsatzes fällig.
- Falschangaben gegenüber Behörden werden mit bis zu 7,5 Millionen Euro Geldstrafe oder 1,5 Prozent des Jahresumsatzes geahndet.

Welche Behörden sind zuständig?

Zuständig für Überwachung und Durchsetzung des EU AI Act sind nationale Aufsichtsbehörden. In Deutschland könnten das je nach Anwendung zum Beispiel das Bundesamt für Sicherheit in der Informationstechnik (BSI), der Bundesbeauftragte für den Datenschutz (BfDI) oder Landesdatenschutzbehörden sein. Es wird aber auch diskutiert, ob eine neue zentrale KI-Aufsichtsbehörde diese Aufgaben übernehmen sollte.

Konkretes steht – Stand: Juli 2025 – noch nicht fest. Auf EU-Ebene soll ein neues „AI Office“ entstehen, das insbesondere den Einsatz von General Purpose AI wie ChatGPT, Gemini oder Claude kontrolliert.

Was Unternehmen tun müssen

Je nach Rolle und Risikoklasse müssen Unternehmen unterschiedliche Pflichten einhalten. Gerade Unternehmen aus den Bereichen HR-Tech, Medizintechnik, Banken und Versicherungen, kritische Infrastruktur oder öffentliche Verwaltung **müssen analysieren, ob regulatorischer Handlungsbedarf besteht**.

Dafür empfehlen sich folgende Schritte:

- **KI-Inventar erstellen:**
Welche KI setzt das Unternehmen intern oder extern ein?
- **Kategorisierung nach Risiko:**
Zu welcher Risikokategorie zählen die eingesetzten KI-Anwendungen?
- **Technische Dokumentation & Konformitätsbewertung:**
Liegen die für die Nutzung von Hochrisiko-KI erforderlichen umfangreichen technischen Unterlagen, Risikobewertungen und eventuell auch Audits vor?
- **Mitarbeitende schulen:**
Sind die Nutzerinnen und Nutzer von Hochrisiko-KI über die Funktionsweise, Risiken und Kontrollpflichten geschult? **Achtung:** Die Pflicht zur KI-Kompetenzsicherung gilt bereits seit Februar 2025!
- **Transparenz sicherstellen:**
Sind die Menschen, die mit KI wie etwa Chatbots oder KI-generierten Inhalten interagieren, darüber informiert, dass es sich um KI-Anwendungen handelt?
- **Meldesysteme einrichten:**
Ist dafür gesorgt, dass das Unternehmen bei schwerwiegenden Vorfällen („serious incidents“) während der Nutzung einer Hochrisiko-KI seiner Meldepflicht an die zuständige Behörde nachkommen kann?

Die Umsetzung in deutsches Recht

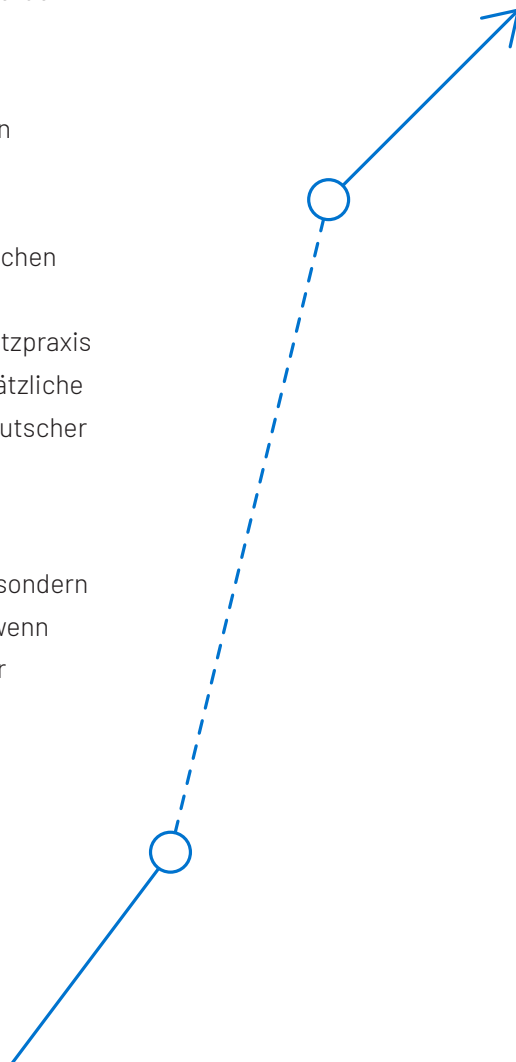
Der EU AI Act ist eine EU-Verordnung: Er gilt also grundsätzlich unmittelbar in allen EU-Mitgliedstaaten, sobald er in Kraft tritt. Im Gegensatz zu EU-Richtlinien ist keine umfassende nationale Umsetzung durch eigene Gesetze nötig. Dennoch ergeben sich wichtige Schnittstellen zum deutschen Recht, und in einigen Bereichen wird es voraussichtlich ergänzende nationale Regelungen geben.

Zum jetzigen Zeitpunkt (Stand: August 2025) liegt noch kein deutsches Umsetzungsgesetz zum EU AI Act vor. Experten erwarten, dass unter anderem nationale Datenschutzbestimmungen, das Arbeitsrecht und das Produktsicherheitsrecht mit den Anforderungen des EU AI Act verzahnt werden.

Tipp

Auch wenn der EU AI Act direkt gilt, sollten Unternehmen mit Deutschlandbezug die nationalen Entwicklungen aufmerksam verfolgen. Gerade im Bereich der behördlichen Zuständigkeiten, Kontrollverfahren, arbeitsrechtlichen Fragen und Datenschutzpraxis wird es mit hoher Wahrscheinlichkeit zusätzliche Regelungen oder Auslegungshilfen auf deutscher Ebene geben.

Unternehmen sollten also nicht nur die europäische Perspektive im Blick haben, sondern auch das nationale Recht, insbesondere wenn sie KI-Systeme im HR-, Gesundheits- oder Finanzbereich einsetzen.



Wie NAVEX helfen kann

NAVEX bietet branchenführende Lösungen, mit denen Sie ein umfassendes Risiko- und Compliance-Programm erstellen können, das Ihren spezifischen Anforderungen entspricht und gleichzeitig globale Compliance-Anforderungen erfüllt.

Unsere integrierte Plattform NAVEX One bietet einen ganzheitlichen Überblick über Ihr gesamtes Programm, unterstützt durch leistungsstarke Daten und Analysen, sodass Sie das Gesamtbild sehen und Risiken identifizieren können, um proaktive Compliance zu erreichen. Ebenfalls auf NAVEX One verfügbar ist der [Compliance Hub](#) – Ihre All-in-One-Lösung für das Management von Compliance-Aufgaben Ihrer Mitarbeiter. Der Compliance Hub bietet ein praktisches Portal für Compliance-Aufgaben wie Schulungen, Richtlinienbestätigungen und Offenlegungsmanagement sowie einen Ort, an dem Sie Berichte und Anfragen erstellen, auf Ihren Verhaltenskodex zugreifen und vieles mehr können.

Die folgenden Lösungen arbeiten auf der [NAVEX One-Plattform](#) Hand in Hand und bilden die Grundlage für ein umfassendes Risiko- und Compliance-Programm:

[Whistleblowing & Vorfalmanagement:](#)

Eine erstklassige Lösung, die es Mitarbeitern erleichtert, Bedenken zu melden, und Ihnen hilft, diese effizient zu verwalten und zu untersuchen. Dies trägt dazu bei, eine Kultur der Offenheit zu schaffen, in der sich Mitarbeiter sicher fühlen, Bedenken zu äußern, was für die frühzeitige Erkennung und Prävention von Verstößen unerlässlich ist. Eine umfassende Plattform zur Verwaltung von Untersuchungen und Ergebnissen ist für die Verwaltung von Meldungen und Anfragen unerlässlich – unabhängig von Ihrer Unternehmensgröße,

Branche oder geografischen Lage, NAVEX One Whistleblowing & Vorfalmanagement hilft Ihrem Unternehmen, die globalen Compliance-Anforderungen für Whistleblowing zu erfüllen.

[Ethik- und Compliance-Schulungen:](#) Wir bieten eine breite Palette interessanter, rechtlich geprüfter und interaktiver Kurse an, die ein breites Spektrum an Governance-, Risiko- und Compliance-Themen abdecken, einschließlich Standards und Leitlinien. Diese Kurse können auf bestimmte Rollen und Verantwortlichkeiten zugeschnitten werden, einschließlich adaptivem Lernen, das die Zeit der Lernenden optimiert, indem es ihnen ermöglicht, Kurse auf der Grundlage ihres Wissens zu absolvieren. Das Tool zur Kursanpassung ermöglicht Schulungen, die Ihre Marke widerspiegeln, und kann Inhalte an sich ändernde regulatorische Anforderungen anpassen. Verfolgen und verwalten Sie den Schulungsfortschritt Ihrer Mitarbeiter auf einer intuitiven und integrierten Plattform.

[Richtlinien- und Verfahrensmanagement:](#)

Erstellen, verwalten und verteilen Sie Richtlinien und Verfahren und stellen Sie sicher, dass diese aktuell und für Ihre Mitarbeiter und Drittparteien zugänglich sind. So können Sie sicherstellen, dass alle Ihre Compliance-Anforderungen kennen und verstehen. Dank des einfachen Zugriffs über Desktop und Mobilgeräte können Ihre Richtlinien sofort und problemlos zur Verfügung gestellt werden. Zusätzlich steht der [NAVEX One Compliance Assistant](#) zur Verfügung, mit dem Benutzer Fragen stellen und automatisierte, maßgeschneiderte Antworten erhalten können, die Ihre Richtlinien unter Angabe von Quellen erläutern und so wichtige Informationen zugänglicher und verständlicher machen.

Risikomanagement von Dritten: Das Management von Risiken durch Dritte, einschließlich (Lieferketten-)Due Diligence, Screening und laufender Überwachung, hat für Unternehmen jeder Größe Priorität. Das Ökosystem von Dritten ist aufgrund der zunehmenden Vernetzung und Abhängigkeit von Drittanbietern und Partnern sowie sich ändernder Vorschriften unglaublich komplex. Ein ordnungsgemäßes Risikomanagement von Dritten hilft Ihnen, Ihr Unternehmen vor den mit diesen Beziehungen verbundenen Risiken zu schützen und die globalen Due-Diligence-Anforderungen zu erfüllen.

Risiko und Governance: Identifizieren, bewerten und mindern Sie unternehmensweite Risiken auf einer einzigen Plattform. Die NAVEX One Risiko und Governance-Lösungen helfen Ihnen bei der Bewältigung von Compliance- und Richtlinienmanagement, Risiken durch Dritte, Audit-Bereitschaft, IT-Risiken, operationellen Risiken und vielem mehr. Durch proaktive Risikoidentifizierung erhalten Sie einen ganzheitlichen Überblick über Ihre Risikolandschaft und können einen proaktiven Ansatz für das Risikomanagement verfolgen, einschließlich Strategieänderungen, Schulungen in Bereichen mit hohem Risiko und Aktualisierung von Richtlinien. Diese Maßnahmen tragen dazu bei, die wichtigsten Risiken für Ihr Unternehmen zu priorisieren und zu mindern.

Verhaltenskodex: Erstellen Sie einen ansprechenden Verhaltenskodex, um sicherzustellen, dass Ihre kulturellen Werte allen Mitarbeitern effektiv vermittelt werden. Ihr Verhaltenskodex ist der kulturelle Leitstern Ihres Unternehmens und ein wichtiges Dokument zur Förderung einer Kultur der Integrität und des ethischen Verhaltens. Außerdem ist eine webbasierte Version verfügbar, mit der Sie die Interaktion mit Ihrem Kodex verfolgen können.

Offenlegungsmanagement: Interessenkonflikte, Geschenke und Bewirtungen sowie andere Offenlegungen stellen Risiken für Ihr Unternehmen dar, die es zu managen gilt. Stellen Sie sicher, dass Offenlegungen erfasst, geprüft und angemessen behandelt werden, indem Sie eine benutzerfreundliche Plattform einsetzen, die Ihnen hilft, die jährlichen Offenlegungspflichten und Ad-hoc-Offenlegungsanforderungen zu verwalten.

Compliance-Programm-Management: Vereinfachen Sie die Komplexität der Einhaltung gesetzlicher Vorschriften, indem Sie die Richtlinien des Justizministeriums (DOJ) in umsetzbare Schritte übersetzen und die Wirksamkeit anhand eines quantifizierbaren Compliance-Rahmens verfolgen. Identifizieren Sie schnell Programm-Lücken, zentralisieren Sie Compliance-Nachweise und optimieren Sie die Vorbereitung auf Audits. Pflegen Sie ein umfassendes Compliance-Programm, minimieren Sie Risiken und demonstrieren Sie Ihr Engagement für regulatorische Standards mit klaren Leitlinien zu den Erwartungen des DOJ und datengestützten Erkenntnissen.

Management regulatorischer Änderungen: Mit dem Management regulatorischer Änderungen für globales Whistleblowing können Unternehmen proaktiv Änderungen von Gesetzen und Vorschriften zu Whistleblowing und Meldepflichten weltweit verfolgen, ihren Fokus auf die für ihre globale Präsenz relevanten Regionen ausrichten und die Leistung ihres bestehenden Programms anhand der relevanten Gesetze bewerten. Reduzieren Sie Ratselraten, senken Sie Rechtskosten und beschleunigen Sie Ihre Compliance-Workflows.

Dieser Inhalt dient ausschließlich Informationszwecken. Er stellt keine Rechtsberatung dar und sollte auch nicht als solche herangezogen werden. Bitte konsultieren Sie Ihren Anwalt, um sich hinsichtlich Ihrer spezifischen Umstände beraten zu lassen.

NAVEX® | Navigator Series

Über 13.000 Unternehmen – darunter 70% der Fortune 100- und 500-Unternehmen – vertrauen auf NAVEX, dem weltweit führenden Anbieter von Risiko- und Compliance-Lösungen. Die NAVEX One-Plattform stärkt Risiko- und Compliance-Programme und unterstützt Unternehmen mit beispiellosen Benchmark-Daten und branchenspezifischen Erkenntnissen. NAVEX One bietet einen 360-Grad-Blick auf Risiken innerhalb des Unternehmens, bei Drittparteien und im gesamten Geschäftsumfeld – für eine bessere Einhaltung gesetzlicher Vorschriften und einem proaktiven Risikomanagement. Mit Niederlassungen in den USA, Europa und Asien und einem globalen Kundenstamm definiert NAVEX weiterhin die Zukunft von Governance, Risiko und Compliance.

Besuchen Sie unseren [Blog](#) oder folgen Sie uns auf [LinkedIn](#), [Facebook](#), und [YouTube](#).

NORD- UND SÜDAMERIKA

5885 Meadows Road, Suite 500
Lake Oswego, OR, 97035
USA

info@navex.com

www.navex.com

+1(866) 297 0224

EMEA + APAC

London
1 Queen Caroline St.
Londres W6 9YN
Großbritannien

info@navex.com

www.navex.com/en-gb/

+44 (0) 20 8939 1650