FORUM



Krisenfest durch Compliance

Wie Unternehmen Compliance-Krisen früher erkennen, Pflichten erfüllen und handlungsfähig bleiben



Sehr geehrte*r Leser*in,

Compliance war lange ein Thema für Richtlinien, Schulungen und Kontrollen. Heute entscheidet sie zunehmend darüber, wie schnell ein Unternehmen aus einem einzelnen Vorfall in eine Krise gerät.

Ein Hinweis aus dem Hinweisgebersystem, ein Durchsuchungsbeschluss oder eine Presseanfrage zu einer Datenpanne können innerhalb weniger Stunden Melde-, Haftungs- und Kommunikationsfragen auslösen.

Geschäftsführung, Vorstand und Aufsichtsrat müssen in dieser Lage belastbar einschätzen, was bekannt ist, und Entscheidungen so treffen, dass sie später nachvollziehbar sind.

Dieses Whitepaper wurde mithilfe von KI erstellt.

Krisenfest durch Compliance

Wie Unternehmen Compliance-Krisen früher erkennen, Pflichten erfüllen und handlungsfähig bleiben

Compliance war lange ein Thema für Richtlinien, Schulungen und Kontrollen. Heute entscheidet sie zunehmend darüber, wie schnell ein Unternehmen aus einem einzelnen Vorfall in eine Krise gerät. Ein Hinweis aus dem Hinweisgebersystem, ein Durchsuchungsbeschluss oder eine Presseanfrage zu einer Datenpanne können innerhalb weniger Stunden Melde-, Haftungs- und Kommunikationsfragen auslösen. Geschäftsführung, Vorstand und Aufsichtsrat müssen in dieser Lage belastbar einschätzen, was bekannt ist, und Entscheidungen so treffen, dass sie später nachvollziehbar sind.

Dieses Whitepaper zeigt, warum Compliance-Krisen heute schneller entstehen, welche Haftungsrisiken für Unternehmen, Organe und Mitarbeitende bestehen und welche Maßnahmen in den ersten Stunden und Tagen den Ausschlag geben. Außerdem beschreibt es, wie sich Unternehmen schon im Normalbetrieb vorbereiten können.

1. Warum Compliance heute schneller in die Krise führt

Mehr Regulierung ist nur die sichtbare Oberfläche. Der eigentliche Treiber ist die Vernetzung der Themen. Ein einzelner Sachverhalt berührt heute oft mehrere Regelkreise gleichzeitig, etwa Datenschutz, IT-Sicherheit, Nachhaltigkeit, Kapitalmarktrecht und Arbeitsrecht. Fachbereiche besitzen dabei oft die entscheidenden Informationen, verfügen aber selten über Routine im Umgang mit einer Krise. Hinzu kommt, dass die Außenkommunikation häufig beginnt, bevor die interne Aufklärung abgeschlossen ist. Die regulatorische Unsicherheit erzeugt deshalb vor allem Entscheidungsdruck und weniger Entscheidungsfreiheit.

Gleichzeitig hat sich der Maßstab verschoben. Früher genügte der Satz „Wir halten uns an die Regeln“. Heute müssen Unternehmen belegen können, dass sie sich daranhalten. Regulatoren, Kunden und Investoren erwarten prüfbare Prozesse. Die Nachweise bestehen aus Daten, Protokollen, Freigaben und dokumentierten Entscheidungen. Damit wird Krisenvorbereitung zu einem festen Bestandteil des Compliance-Management-Systems (CMS). Krisenmanagement umfasst nach gängiger Lesart alle Maßnahmen zur Vermeidung, Vorbereitung, Erkennung, Bewältigung und Nachbereitung von Krisen.[1]

2. Neue Pflichten erzeugen neue Schnittstellen

Die neuen Regelwerke haben eine Gemeinsamkeit: Sie knüpfen an Risikoerkennung, Prozesse und Kontrollen an und nicht erst an den eingetretenen Schaden. Unternehmen müssen deshalb zeigen können, was sie wussten, wann sie entschieden haben und wie sie überwacht haben. Compliance wandert damit in Produktentwicklung, IT, Personalwesen, Einkauf, Vertrieb und Finanzen hinein. Eine Krise trifft daher selten nur die Rechtsabteilung.

Der **Data Act** gilt grundsätzlich seit dem 12. September 2025.[2] Im Krisenfall stellt sich dann die konkrete Frage, ob ein Unternehmen kurzfristig erklären kann, welche Daten vorhanden sind, wem sie zustehen und wie sie bereitgestellt werden können. Unfaire Datenzugangs- oder Datennutzungsklauseln in Verträgen können dabei ebenfalls angreifbar sein.

Der **AI Act** ist seit dem 2. August 2026 grundsätzlich anwendbar. Die Verbote und die Pflicht zur KI-Kompetenz gelten bereits seit 2025.[3] Die Fristen für Hochrisiko-Systeme werden derzeit im Zuge von Änderungsverfahren diskutiert. Unternehmen sollten die jeweils aktuellen Termine deshalb laufend prüfen. Unabhängig davon gilt: Wer ein KI-Inventar führt, kann im Ernstfall binnen Stunden sagen, welche KI eingesetzt wird, wer Anbieter oder Betreiber ist und welche Dokumentation vorliegt. Typische Auslöser für KI-bezogene Krisen sind Diskriminierungsvorwürfe bei algorithmischen Entscheidungen, nicht gekennzeichnete KI-Inhalte und sogenannte Schatten-KI, also Tools, die Fachbereiche ohne Freigabe oder Datenschutzprüfung nutzen.

Bei **ESG-Themen** hat die Verschlankung der Berichtspflichten die unmittelbare Betroffenheit vieler Unternehmen verringert. Die Wirkung bleibt trotzdem bestehen, denn Kunden, Banken, öffentliche Auftraggeber und Lieferketten verlangen weiterhin belastbare Nachweise. Krisen entstehen dabei selten im Nachhaltigkeitsbericht selbst. Häufig geht ein Umwelt- oder Sozialversprechen in der Werbung oder Kommunikation voraus, bevor Daten und Belege geprüft sind. Eine spätere Korrektur wird dann schnell als Schuldeingeständnis missverstanden. Deshalb sollten ESG-Daten in das interne Kontrollsystem eingebunden werden und nicht nur in Präsentationen erscheinen.

Auch das **Hinweisgeberschutzgesetz** wirkt im Krisenfall als Frühwarnsystem. Interne Meldestellen müssen den Eingang einer Meldung grundsätzlich innerhalb von sieben Tagen bestätigen. Die Rückmeldung an die hinweisgebende Person erfolgt in der Regel innerhalb von drei Monaten.[4] Eine Studie zu Hinweisgebersystemen ergab zudem, dass Unternehmen mit einem formalen Meldekanal im Schnitt einen niedrigeren Betrugsschaden verzeichneten als Unternehmen ohne solchen Kanal.[5] Hinweise sind damit nicht nur eine Pflicht, sondern auch ein Instrument zur frühen Erkennung von Risiken.

3. Typen der Compliance-Krise

Eine Compliance-Krise lässt sich grob in vier Typen einteilen. Der erste Typ sind Ermittlungen durch Staatsanwaltschaften, Kartellbehörden oder andere Ermittlungsbehörden. Der zweite Typ ist die Meldung eines angeblichen Regelverstoßes, die über das Hinweisgebersystem, direkt an das Unternehmen oder anonym eingeht. Der dritte Typ entsteht durch die interne Aufdeckung von Verstößen, etwa im Rahmen einer Revision. Der vierte Typ ist die Reputationskrise, die auch dann eintreten kann, wenn das Unternehmen regelkonform gehandelt hat.

Der Gegenstand einer Krise kann ganz unterschiedlich sein. Dazu zählen Korruptions- und Kartellfälle, Bilanz- und Finanzthemen, Datenschutz- und IT-Sicherheitsvorfälle, arbeitsrechtliche Fragen sowie Verstöße gegen Umwelt- oder Lieferkettenvorgaben. Entsprechend vielfältig sind die beteiligten Stellen. Dazu gehören Staatsanwaltschaften, Kartellbehörden, die EU-Kommission, Zollbehörden, Umweltbehörden und die Steuerfahndung. Schon ein unscheinbarer Anlass wie ein Revisionsbericht über unzureichend dokumentierte Einladungen oder ein anonymes Schreiben an den Aufsichtsrat kann den Prozess auslösen.

4. Haftungsrisiken für Unternehmen, Organe und Mitarbeitende

Unternehmen

Strafverfahren richten sich in erster Linie gegen natürliche Personen. Das Unternehmen kann aber Betroffener im Ordnungswidrigkeitenverfahren sein. Straftaten von Leitungspersonen werden dem Unternehmen zugerechnet. Bei Taten sonstiger Mitarbeitender kommt es darauf an, ob ein Organisationsverschulden vorliegt, also ob die gebotene Aufsicht verletzt wurde.[6] Das

mögliche Bußgeld liegt bei vorsätzlichen Straftaten bis zu zehn Millionen Euro und bei fahrlässigen bis zu fünf Millionen Euro.[6] Hinzu kommen Vermögensabschöpfung, der Ausschluss von Vergabeverfahren und in Einzelfällen sogar verwaltungsrechtliche Sanktionen.

Im Kartellrecht kann das Bußgeld bis zu zehn Prozent des Konzernumsatzes betragen. Zudem drohen Schadensersatzforderungen von Wettbewerbern und Kunden.[7] Gleichzeitig gilt: Bei der Bemessung des Bußgeldes sind vorab getroffene, angemessene und wirksame Vorkehrungen zur Vermeidung und Aufdeckung von Verstößen zu berücksichtigen. Ebenso zählt das Bemühen, die Zuwiderhandlung aufzudecken und den Schaden wiedergutzumachen, sowie die Weiterentwicklung des Systems nach der Tat.[8] Ein funktionierendes CMS wirkt also auch nach Aufdeckung eines Fehlverhaltens. Deshalb sollte die Weiterentwicklung des Systems ausdrücklich zum Maßnahmenpaket gehören.

Mitarbeitende
Mitarbeitende können sich strafbar machen, etwa durch Korruption, Bestechlichkeit im geschäftlichen Verkehr, Betrug, Untreue oder Kartellstraftaten. Eine besondere Verantwortung (Garantenstellung) kann für direkte Vorgesetzte mit Weisungsbefugnis gelten. Sie kann auch für Verantwortliche für Recht und Compliance gelten, wenn ihnen diese Pflichten übertragen wurden. Arbeitsrechtlich reichen die Maßnahmen von der Abmahnung bis zur Kündigung. Dabei gelten oft enge zeitliche Fristen, und die Null-Toleranz-Linie vieler Unternehmen ist ein wichtiger Maßstab. Schadensersatzansprüche des Arbeitgebers setzen in der Regel Vorsatz oder grobe Fahrlässigkeit voraus.

Geschäftsführung und Vorstand
Organmitglieder haben eine strafrechtliche Garantenstellung.[9] Sie müssen also gegen unternehmensbezogene Straftaten einschreiten. Wer trotz Kenntnis untätig bleibt, kann sich daraus als Täter oder Teilnehmer strafbar machen, auch wenn er selbst nicht aktiv mitwirkt. Die Kenntniserlangung markiert deshalb eine klare Zäsur. Sobald Verdachtsmomente vorliegen, sind unverzüglich alle erforderlichen Maßnahmen zu ergreifen, um fortgesetzte Handlungen zu unterbinden.

Mitglieder von Vorstand und Geschäftsführung haften bei schuldhafter Pflichtverletzung gegenüber der Gesellschaft auf Schadensersatz.[10] Die Business Judgment Rule schützt unternehmerische Entscheidungen, sofern sie auf sorgfältig ermittelten Grundlagen beruhen und am Unternehmenswohl orientiert sind. Sie gilt auch für Compliance-Risiken. Eine Pflichtverletzung liegt erst dann vor, wenn die Grenzen unternehmerischen Ermessens überschritten sind. Wichtig ist dabei: Interne Zuständigkeitsregeln heben die Gesamtverantwortung nicht auf. Sie beschränken lediglich die Verantwortlichkeit. Wer nicht zuständig ist, muss trotzdem eingreifen, sobald Anhaltspunkte bestehen, dass die Aufgaben nicht mehr zuverlässig erledigt werden. Deshalb sollten wichtige Entscheidungen und ihre Informationsgrundlagen möglichst vollständig dokumentiert werden.

Aufsichtsrat
Der Aufsichtsrat überwacht den Vorstand auch in einer Krise. Sind Mitglieder der Geschäftsführung betroffen, ist er für die Aufklärung und die weiteren Maßnahmen zuständig. Auch Aufsichtsratsmitglieder können eine Garantenstellung haben. Sie haben jedoch kein Weisungsrecht gegenüber dem Vorstand. Bei Kenntnis von Pflichtverletzungen sollte der Aufsichtsrat kurzfristig eine Sitzung einberufen, auf ein Einschreiten hinwirken und sein

Abstimmungsverhalten dokumentieren. Die Prüfung einer Strafanzeige gehört ebenfalls dazu. Erkennt ein Aufsichtsratsmitglied, dass das Gremium nicht handelt, kann auch die Niederlegung des Mandats in Betracht kommen.

5. Die ersten 72 Stunden

In einer Krise zählt zuerst nicht die vollständige Wahrheit, sondern die kontrollierte Handlungsfähigkeit. Krisenarbeit findet mit unvollständigen Informationen statt. Ziel ist es, den Schaden zu begrenzen, ohne die Aufklärung zu gefährden. Drei Stränge laufen dabei parallel: stabilisieren, kommunizieren und aufklären. Wer zu spät strukturiert, arbeitet später gegen Chaos, Datenverlust und Vertrauensverlust. Ein bewährter Orientierungsrahmen ist das 72-Stunden-Modell.

Zeitfenster	Schwerpunkt	Typische Maßnahmen
0 bis 2 Stunden	Aktivieren	Meldepflichten und Auslöser prüfen, Krisenstab einberufen, Rollen bestätigen
2 bis 8 Stunden	Sichern	Legal Hold auslösen, Daten, Zugriffe und Prozesse sichern, Datenlöschungen stoppen
8 bis 24 Stunden	Bewerten	Sofortmaßnahmen festlegen, Stakeholder einbinden, externe Berater hinzuziehen
24 bis 48 Stunden	Kommunizieren	Holding Statement, Q&A, Information von Aufsichtsgremium und Behörden, Mitarbeitende informieren
48 bis 72 Stunden	Aufklären	Investigation-Plan, Interviewfolge, Berichterstattung und Maßnahmen-Tracking

Zu Beginn ist es wichtig, die Krisenstufe festzulegen. Eine Angelegenheit gilt als „Case“, wenn sie lokal und begrenzt ist. Ein „High-Risk Case“ liegt vor, wenn mehrere Personen betroffen sind oder eine Meldepflicht möglich erscheint. Von einer Krise spricht man bei externer Sichtbarkeit, wahrscheinlichen Ermittlungen oder wesentlichem Betriebsimpact. Diese Einordnung entscheidet darüber, wer informiert werden muss und wie schnell.

Besonders kritisch sind die ersten Stunden, weil dort die meisten vermeidbaren Fehler passieren. Zu viele Personen wissen zu früh zu viel, was Leaks und Beweisgefährdung begünstigt. Die IT handelt technisch richtig, aber ohne rechtliche Beweissicherungslogik. Die Personalabteilung spricht Betroffene an, bevor eine Interviewstrategie steht. Die Kommunikation gibt ein Dementi ab, das sich später nicht halten lässt. Der größte Fehler in der Krise ist deshalb selten Untätigkeit, sondern unkoordinierte Aktivität.

Fristen im Blick behalten

Viele Krisen sind zugleich Fristenkrisen. Die wichtigsten Uhren sind dabei die folgenden:

- Im Datenschutz ist eine Verletzung des Schutzes personenbezogener Daten möglichst binnen 72 Stunden nach Kenntnis an die Aufsichtsbehörde zu melden, sofern ein Risiko besteht.[11]
- Nach der NIS2-Regulierung in Deutschland folgen auf erhebliche Sicherheitsvorfälle eine Frühwarnung innerhalb von 24 Stunden, eine Meldung innerhalb von 72 Stunden und ein Abschlussbericht nach einem Monat.[12]
- Für Meldungen nach dem Hinweisgeberschutzgesetz gelten die Fristen von sieben Tagen für die Eingangsbestätigung und drei Monaten für die Rückmeldung.[4]
- Bei Insiderinformationen im Kapitalmarktbereich ist die Veröffentlichung grundsätzlich unverzüglich vorzunehmen, sofern kein Aufschub zulässig ist.[13]

Entscheidend ist dabei, dass die Frist mit der Kenntniserlangung beginnt und nicht erst mit dem Abschluss der Analyse. Jede Meldeentscheidung sollte dokumentiert werden, einschließlich der Gründe für eine Meldung oder deren Unterlassung.

6. Kommunikation und Umgang mit Behörden

Für die Kommunikation gelten einige Grundregeln. Es sollte nur das gesagt werden, was belastbar ist. Betroffenheit darf man zeigen, ohne eine Schuld einzugestehen. Nach außen spricht nur eine Stelle, damit keine Fachbereichsstatements ohne Freigabe entstehen. Der Faktenkern muss für Leitung, Mitarbeitende, Kund*innen und Medien identisch sein. Jede Kommunikation sollte außerdem protokolliert werden, mit Anfrage, Antwort, Freigabe, Uhrzeit und Version.

Ein Holding Statement folgt meist einer klaren Logik: Das Unternehmen erkennt den Hinweis oder Vorwurf ernst an, ordnet den Stand der Prüfung ein, beschreibt die bereits eingeleiteten Schritte und nennt den nächsten Kommunikationsschritt. Zu vermeiden sind absolute Dementis, Schuldzuweisungen, Spekulationen und vertrauliche Details. Die kommunikative Grundspannung besteht darin, genug zu sagen, um Vertrauen zu erhalten, aber nicht so viel, dass Aufklärung, Rechte oder Personen gefährdet werden. Jede Aussage muss auch morgen noch tragfähig sein.

Wenn Ermittlungsbehörden mit einem Durchsuchungsbeschluss erscheinen, ist ein geordnetes Vorgehen entscheidend. Der Beschluss sollte sofort geprüft und kopiert werden. Dabei sind die Rechtsgrundlage, der Beschuldigte, das Ausstellungsdatum, die betroffenen Räumlichkeiten und die gesuchten Gegenstände zu klären. Die Durchsuchung sollte in einen Besprechungsraum verlagert werden, und der interne Durchsuchungsbeauftragte sowie externe Anwälte sind umgehend zu informieren. Mitarbeitende sollten keine Beweismittel vernichten oder verstecken, aber auch keine spontanen Aussagen machen. Zusagen während der Durchsuchung sind zu vermeiden. Gegen die Beschlagnahme ist am Ende des Verfahrens zu widersprechen, damit keine Rechtsmittel verloren gehen. Bei elektronischen Daten gilt: Löschen Sie nichts. Der Durchsuchungsbeschluss erlaubt in der Regel die Durchsicht der gesamten IT-Umgebung, der Umfang der Sicherstellung lässt sich jedoch häufig verhandeln. Zugriffe auf Daten im Ausland sollten die Beamten darauf hinweisen, dass diese grundsätzlich nicht erfasst sind.

Die Frage, ob ein Unternehmen mit den Behörden kooperiert oder eine Konfliktverteidigung wählt, ist eine strategische Entscheidung. Kooperation bedeutet nicht automatisch den Verzicht auf Rechte. Im Kartellrecht gibt es eine Bonusregelung, nach der der erste Antragsteller unter bestimmten Voraussetzungen einen vollständigen Bußgelderlass erhalten kann. Ein allgemeines Unternehmenskronzeugenprogramm für alle Delikte existiert in Deutschland dagegen nicht.[14]

Ein Amnestieprogramm für Mitarbeitende muss sorgfältig geprüft werden, denn das Unternehmen kann strafrechtliche Straffreiheit nicht versprechen. Auch Zivilansprüche gegen Beteiligte können dabei betroffen sein. Zeugen können sich von einem Zeugenbeistand begleiten lassen, und in komplexen Verfahren koordiniert ein Unternehmensverteidiger die Verteidigung des Unternehmens sowie die Abstimmung mit individuellen Verteidigern.

7. Aufklärung strukturiert führen

Ziel der internen Aufklärung ist ein belastbarer Sachverhalt, der Entscheidungen trägt. Eine möglichst große Datenmenge ist dafür nicht erforderlich. Das Untersuchungsteam muss von den Interessen des betroffenen Fachbereichs unabhängig sein. Datenzugriffe, Interviews und personelle Maßnahmen sollten verhältnismäßig und sauber begründet sein. Privilegien und Vertraulichkeit sind früh zu klären. Zwischenberichte sind Führungsinstrumente und keine endgültigen Wahrheiten.

Ein Investigation-Plan strukturiert den Prozess in fünf Schritten: Mandat und Berichtslinie festlegen, Datenquellen sichern, Hypothesen und Prüffragen formulieren, Interviews führen und abschließend berichten. Bei der Beweissicherung werden häufig Quellen übersehen. Dazu gehören informelle Chats in Teams, Slack oder vergleichbaren Diensten, Systemlogs mit Zugriffen und Änderungen, Transaktionsdaten aus ERP- oder CRM-Systemen sowie Versionen von Richtlinien und Präsentationen. Die Sicherung sollte nachvollziehbar erfolgen, etwa mit Zeitstempeln, Hashwerten und einer dokumentierten Beweiskette.

Bei Interviews hilft eine klare Reihenfolge. Zunächst werden die Dokumente gesichtet, dann folgen Kontextpersonen mit Prozesswissen. Randbeteiligte kommen vor den Schlüsselpersonen, und erst wenn der Beweisstand tragfähig ist, folgen Konfrontationen. Interviews ohne geklärtes Mandat oder ohne gesicherte Beweise sind zu vermeiden. Suggestivfragen und informelle Vorabgespräche schaden der Aufklärung. Zugleich müssen der Schutz hinweisgebender Personen und die Unschuldsvermutung gewahrt bleiben.

Parallel dazu entsteht der Krisenfile. Er beantwortet fünf Fragen: Was wurde wann bekannt, wer hat auf welcher Grundlage entschieden, welche Maßnahmen wurden mit welchem Verantwortlichen umgesetzt, welche Aussagen gingen in welcher Version an wen und welche Fristen wurden geprüft. Ein Decision Log in Minimalform enthält Zeitpunkt, Kenntnisstand, Entscheidung, Begründung und Verantwortlichkeit mit Frist. Dieses Protokoll schützt später sowohl das Unternehmen als auch die handelnden Personen.

8. Lehren aus bekannten Compliance-Krisen

Die großen Compliance-Krisen der vergangenen Jahre folgen wiederkehrenden Mustern. Fast immer gab es frühe Warnsignale, die nicht wirksam eskaliert wurden. Häufig spielten Dritte wie Berater, Lieferanten, Zahlungswege oder Prüfer eine zentrale Rolle. Kritische Daten waren unvollständig, widersprüchlich oder nicht prüfbar. Das öffentlich vermittelte Bild des Unternehmens passte nicht mehr zur internen Realität, und Leitungsgremien erhielten Informationen zu spät oder zu wenig kritisch. Die Krise endete daher selten mit der Sanktion. Sie endete erst mit dem Umbau von Kultur und Kontrollen.

Diese Muster lassen sich in Krisentypen übersetzen, die jedes Unternehmen für die eigene Situation prüfen kann.

Krisentyp	Frühwarnsignal	Kontrollfrage für das eigene Unternehmen
Kulturkrise	„So machen wir das hier“ setzt sich gegen das Regelwerk durch	Welche informellen Regeln bestimmen Entscheidungen tatsächlich?
Datenkrise	Daten sind nicht auffindbar, widersprüchlich oder nicht prüfbar	Welche kritischen Daten haben keinen verantwortlichen Owner?
Drittparteienkrise	Berater, Lieferanten oder Agenten bleiben eine Black Box	Welche Dritten könnten uns in eine Krise ziehen?
Produkt- oder Technikkrise	Technische Details erreichen die Leitung zu spät	Wie eskalieren technische Compliance-Risiken aus dem Engineering?
Kommunikationskrise	Öffentliche Aussagen passen nicht zum internen Wissen	Wer gleicht Werbeaussagen und Nachhaltigkeitsclaims mit den Fakten ab?

Aus diesen Erfahrungen folgt eine klare Konsequenz für die eigene Compliance-Praxis. Die Risikoanalyse muss Krisentrigger enthalten und nicht nur abstrakte Regelverstöße. Kontrollen sollten so gestaltet sein, dass sie Hinweise liefern, bevor die Öffentlichkeit davon erfährt. Fachbereiche müssen wissen, wann sie Recht oder Compliance einbinden müssen. Drittparteien-, Daten- und Produktcompliance gehören in ein gemeinsames Governance-Modell.[15]

9. Vorbereitung: Was Unternehmen heute tun können

Krisenfestigkeit ist keine Aufgabe einer einzelnen Abteilung. Sie ist eine geübte Organisationsfähigkeit. Die gute Nachricht ist, dass sich viele Voraussetzungen ohne großen Aufwand schaffen lassen. Ein Krisenteam mit benannten Stellvertretungen und erreichbaren 24/7-Kontakten bildet die Grundlage. Ebenso wichtig sind klare Entscheidungsrechte, die festlegen, wer über Stopp, Meldung und Kommunikation entscheidet. Eine Triggerliste beschreibt, wann eskaliert wird, und ein eingeübter Legal-Hold-Prozess zusammen mit der IT verhindert Beweisverluste. Eine Meldepflichten-Matrix mit Fristen aus Datenschutz, IT-Sicherheit, Kapitalmarktrecht und Branchenrecht gehört ebenso dazu wie vorformulierte Holding Statements für typische Szenarien.

Die Vorbereitung sollte auch Daten, KI-Systeme und Dritte umfassen. Ein Inventar dieser Bereiche zeigt, wo Risiken liegen und welche Prozesse kritisch sind. Darauf aufbauend lassen sich Rollen und Verantwortlichkeiten in einer RACI-Matrix festlegen. Für jede Funktion ist dann klar, was sie innerhalb von 24 Stunden liefern muss, etwa eine Rechtsbewertung durch Recht und Compliance, einen Systemstatus durch die IT oder ein Holding Statement durch die Kommunikation. In einer Befragung nordamerikanischer Unternehmen gaben 41 Prozent unklare Verantwortlichkeiten im Krisenmanagement als wesentliches Hindernis für eine bessere Vorbereitung an.[16]

Vorbereitung ist nur dann wirksam, wenn sie geübt wird. Tabletop-Übungen von 90 bis 180 Minuten erzeugen einen realistischen Druck, wenn das Szenario mehrdeutig ist und mehrere

Regelkreise berührt. Gute Übungen beobachten, wer entscheidet, wer dokumentiert, wer kommuniziert und wo Wartezeiten entstehen. Wichtig ist auch die Nachbereitung mit konkreten Maßnahmen, Verantwortlichen und Fristen. Eine Krise endet erst dann, wenn die Wirksamkeit der Maßnahmen überprüft wurde. Ein Remediation-Zyklus beginnt deshalb mit der Ursachenanalyse, führt über Maßnahmen und Verantwortliche zur Kontrolle und endet mit einem Board-Bericht, der auch offene Risiken benennt.

Ein realistischer Einstieg kann in 30 Tagen erfolgen. In der ersten Woche werden Krisentrigger, Rollen und Kontaktlisten aktualisiert, und die Inventare für Daten, KI und Drittparteien werden auf Krisenbezug geprüft. In der zweiten Woche testen Unternehmen Legal Hold, Meldefristen und Kommunikationsfreigaben und erstellen Holding Statements für die fünf wichtigsten Szenarien. In der dritten Woche findet eine Tabletop-Übung mit Leitung und Fachbereichen statt. In der vierten Woche werden Lessons Learned mit Verantwortlichen, Budget und Frist in einen Verbesserungsplan überführt.

Fazit

Compliance-Krisen kündigen sich häufig früher an, als Unternehmen es wahrhaben wollen. Wer Krisentrigger kennt, Zuständigkeiten klärt, Beweise frühzeitig sichert und Entscheidungen dokumentiert, gewinnt Zeit und Glaubwürdigkeit. Entscheidend ist dabei nicht, alles zu wissen, sondern unter Zeitdruck die richtigen Fragen zu stellen und entscheidungsfähig zu bleiben. Krisenvorbereitung ist damit kein Zusatz zum Compliance-Management, sondern dessen wirksamste Form.

Quellen

[1]: Wistev, Compliance-Krisenmanagement, Juni 2026: https://wistev.de/journal/2026/06/26/compliance-krisenmanagement/

[2]: Verordnung (EU) 2023/2854 (Data Act): https://eur-lex.europa.eu/eli/reg/2023/2854/oj

[3]: Verordnung (EU) 2024/1689 (KI-Verordnung, AI Act): https://eur-lex.europa.eu/eli/reg/2024/1689/oj

[4]: § 17 Hinweisgeberschutzgesetz (HinSchG): https://dejure.org/gesetze/HinSchG/17.html

[5]: ACFE Report to the Nations 2026, Auswertung: https://www.whispli.com/blog/occupational-fraud-2026-acfe-report-to-the-nations-whistleblowing

[6]: §§ 30, 130 Gesetz über Ordnungswidrigkeiten (OWiG): https://www.gesetze-im-internet.de/owig_1968/__30.html

[7]: § 81 Gesetz gegen Wettbewerbsbeschränkungen (GWB): https://dejure.org/gesetze/GWB/81.html

[8]: § 81d Gesetz gegen Wettbewerbsbeschränkungen (GWB): https://dejure.org/gesetze/GWB/81d.html

[9]: § 13 Strafgesetzbuch (StGB): https://www.gesetze-im-internet.de/stgb/__13.html

[10]: § 93 Aktiengesetz (AktG), Business Judgment Rule: https://dejure.org/gesetze/AktG/93.html

[11]: Art. 33 Datenschutz-Grundverordnung (DSGVO): https://dsgvo-gesetz.de/art-33-dsgvo/

[12]: Bundesamt für Sicherheit in der Informationstechnik (BSI), Meldepflichten nach NIS2 und BSIG: https://www.openkritis.de/betreiber/meldepflichten-bsig.html und https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Infopakete/NIS-2-Meldepflicht/NIS-2-Meldepflicht_node.html

[13]: Verordnung (EU) Nr. 596/2014 (Marktmissbrauchsverordnung, MAR), Art. 17: https://eur-lex.europa.eu/eli/reg/2014/596/oj

[14]: Bonusregelung des Bundeskartellamts, §§ 81h bis 81n GWB: https://dejure.org/gesetze/GWB/81h.html

[15]: Rechtskataster zu Hinweisgebersystemen und Verbandssanktionen, Stand August 2026

[16]: Der Bank-Blog, Befragung zur Krisenvorbereitung von Unternehmen: https://www.der-bank-blog.de/unternehmen-nur-unzureichend-auf-krisen-vorbereitet/studien/37719850/amp/

Zusätzlich zur Orientierung: Die Studie von FTI Consulting zeigt, dass sich Unternehmen häufig gerade auf die Krisen am wenigsten vorbereitet fühlen, die ihr Geschäft am stärksten gefährden: https://www.fticonsulting.com/de-de/germany/newsroom/press-releases/organisations-are-least-prepared-for-crises-that-pose-the-greatest-risk-according-to-fti. Eine Befragung von 1.224 Unternehmen in Deutschland weist ebenfalls auf Defizite bei der Krisenvorsorge hin: https://idw-online.de/de/news870442.

Passende Weiterbildungen finden Sie hier:

Weiterbildung zum Thema Recht

Finden Sie aus unserem erstklassigen Weiterbildungsangebot die für Ihre Bedürfnisse passende Fortbildung. Profitieren Sie von unseren maßgeschneiderten Seminaren und Lehrgängen mit erfahrenen, hochkarätigen Experten rund um das Thema Recht. Jetzt informieren.

e-Learning – Klicken und Lernen

Das FORUM Institut bietet mit hochwertigen e-Learning-Programmen eine flexible Weiterbildungsform. Entscheiden Sie selbst, wann und wo Sie lernen.
Jetzt unverbindlich testen.

Inhouse-Seminare – Maßgeschneiderte Lösungen

Alle unsere Seminare eignen sich auch hervorragend als Inhouse-Training.
Jetzt individuelles Angebot anfordern.

Wir garantieren fachlich hochwertige Weiterbildung für Ihren Erfolg – unsere ISO-Zertifizierungen nach 9001 und 21001 unterstreichen dies. Jetzt informieren

FORUM · Institut für Management GmbH · Postfach 10 50 60 · 69040 Heidelberg · Germany
Telefon: +49 6221 500-500 · Fax: +49 6221 500-555 · www.forum-institut.de