



Bundesverband

ASW - Leitfaden

Leitplanken – Interne Ermittlungen

Inhalt:

I.	Ziele, Gründe und Relevanz interner Ermittlungen.....	3
II.	Interne Governance-Struktur	4
III.	Durchführung von internen Ermittlungen	6
1.	Zielsetzung, Planung und Team-Setup der internen Ermittlung.....	6
2.	Ermittlungshandlungen	10
3.	Dokumentation und Konsequenzen	14
IV.	Kommunikation und Kooperation mit Externen	16

I. Ziele, Gründe und Relevanz interner Ermittlungen

Spätestens durch die großen Fälle von Wirtschaftskriminalität der letzten Jahre ist die Bedeutung unternehmensinterner Ermittlungen im Bewusstsein von Unternehmensorganen angekommen. Liegen im Unternehmen mögliche Hinweise für dolose Handlungen vor, können diese kaum mehr unbehandelt liegen bleiben. Materielle Verluste aufgrund von Schadensfällen durch wirtschaftskriminelles Handeln, Missmanagement oder Bearbeitungsfehler können im Einzelfall ein Ausmaß erreichen, das für ein Unternehmen eine ernsthafte Bedrohung darstellen kann. Neben den unmittelbaren wirtschaftlichen Auswirkungen erleiden die geschädigten Unternehmen zudem oftmals aufgrund der meist unvermeidlichen Publizität dieser Vorkommnisse einen Vertrauensverlust und eine Beeinträchtigung ihrer Reputation.

Aufdeckung, Aufklärung, Aufarbeitung von bekannt gewordenen Unregelmäßigkeiten sollten schon allein im ureigenen Interesse einer Geschäftsleitung eines Unternehmens sowie deren Anteilseigner liegen. Interne Ermittlungen sind eine wesentliche Säule eines umfassenden bzw. ganzheitlichen Managements zur Verhinderung, Prävention und Bearbeitung doloser Handlungen („Fraud Management“).

Das Erfordernis interner Ermittlungen – auch unabhängig von behördlichen Verfahren, z.B. der Strafverfolgungsbehörden – ergibt sich dabei bereits allein aus der Schadensminderungspflicht der Geschäftsleitung im Rahmen einer ordnungsgemäßen Geschäftsorganisation. Somit lässt sich eine Pflicht zur Aufklärung bereits aus den gesetzlichen Regelungen der bestehenden Sorgfaltspflichten und Verantwortlichkeiten der Geschäftsleitung ableiten, die in den jeweiligen Gesetzen für die einzelnen Unternehmensrechtsformen festgelegt sind.¹

Zudem ist eine Sachverhaltsaufarbeitung einschließlich der Ermittlung der Schadenshöhe für den eigenen Erkenntnisgewinn sowie für die Geltendmachung möglicher wirtschaftlicher Ansprüche gegenüber Versicherern bzw. von Schadenersatzansprüchen gegenüber den Tätern erforderlich. Und nicht zuletzt erwarten auch die Stakeholder sowie die Öffentlichkeit eine entsprechende Transparenz hinsichtlich Entstehung, Aufklärung und zukünftiger Verhinderung von Delikts- und Schadensfällen.

Aus der Aufarbeitung heraus gilt es, Erkenntnisse zu gewinnen und entsprechende Maßnahmen abzuleiten, so dass derartige Fälle in der Zukunft vermieden werden können sowie eine Optimierung des Risiko- und Sicherheitsmanagements und des internen Kontrollsystems (IKS) des Unternehmens erfolgt.

Zu den zu beachtenden rechtlichen Rahmenbedingungen gehören neben Datenschutzaspekten z.B. auch Inhalte der EU-Geldwäscherichtlinie oder der EU-Hinweisgeberrichtlinie mit ihrer Umsetzung in das jeweilige nationale Recht sowie Regelungen im Zusammenhang mit dem Unternehmensstrafrecht. Zudem sind immer auch die jeweiligen nationalen Gesetze und Rechtsprechungen zu beachten sowie auch internationale bzw. länderübergreifend geltende rechtliche Rahmenbedingungen, wie beispielsweise der UK Bribery Act aus Großbritannien oder der Foreign Corrupt Practises Act (FCPA) aus den USA.

Das vorliegende Dokument soll einen Überblick geben über grundsätzliche aufbau- und ablauforganisatorische Aspekte interner Ermittlungen: Organisationsstruktur, Vorgehensweisen, interne und externer Schnittstellen. Die Relevanz besteht unabhängig von der Unternehmensgröße.

¹ Vgl. insbesondere §§ 30, 130 Ordnungswidrigkeitengesetz (OWiG), § 91 Abs. 2 sowie § 93 Aktiengesetz (AktG), § 43 GmbHG-Gesetz (GmbHG) sowie § 34 Genossenschaftsgesetz (GenG).

Alle nachstehend dargestellten Leitplanken, Empfehlungen und Hinweise haben sich in vielen Fällen praktisch bewährt und stammen aus eigenen Erfahrungen zahlreicher Experten.

II. Interne Governance-Struktur

Aus der erläuterten Überwachungs- und Aufklärungspflicht bei Delikts-/Schadensfällen ergibt sich für die Unternehmensleitung die Notwendigkeit formale Vereinbarungen organisatorischer, prozessualer und regulatorischer Art zu etablieren, welche im Delikts-/Schadensfall den Rahmen für eine effektive interne Ermittlung bilden.

Hinweisgebersysteme

Hinweise sind, neben Zufallsfunden und Feststellungen im Rahmen von Prüfungen, häufige Auslöser einer internen Ermittlung. Die Implementierung eines Hinweisgebersystems im Unternehmen erlaubt Mitarbeitern eine unkomplizierte Meldung von möglichen Verstößen.

In der Praxis bewährte Hinweisgebersysteme sind für diesen Zweck eingerichtete E-Mail-Postfächer, eine Hotline oder ein Internet-Portal mit Kontaktformular. Letzteres ist für die Abgabe von anonymen Hinweisen geeignet, weil die systemische Umsetzung so gestaltet sein kann, dass eine Rückverfolgung auf den Melder nicht möglich ist und damit die Anonymität gewährleistet werden kann. Zudem bieten solche Portale eine Austauschmöglichkeit, sollten Rückfragen an den Melder bestehen. Bei der Konzeption eines passenden Hinweisgebersystems sind geltende Beteiligungsrechte der betriebsverfassungsrechtlichen Gremien ebenso zu beachten wie bestehende betriebliche Regelungen.

Tip: Die Effizienz eines Hinweisgebersystems im Unternehmen ist maßgeblich abhängig von seiner Bekanntheit bei allen Mitarbeitern. Es empfehlen sich deshalb regelmäßige Informationskampagnen über zu meldende Vorfälle sowie die sachgerechte Nutzung des Hinweisgebersystems zu initiieren.

Formale Vereinbarungen

Formale Vereinbarungen verweisen auf relevante unternehmenseigene Regelungen sowie den geltenden Rechtsrahmen. Grundsätzlich empfehlen sich für Unternehmen eine Arbeitsordnung und/oder ein Compliance-Programm, in deren Rahmen die wichtigen und allgemeingültigen Grundsätze dargestellt werden. Derartige Regelwerke erleichtern das Einleiten von internen Ermittlungen bei Verstößen gegen die darin aufgeführten Grundsätze.

Im Vorfeld abgeschlossene formale Vereinbarungen können langwierige Abstimmungsprozesse vermeiden und Risiken z.B. durch Verstöße gegen datenschutzrechtliche Bestimmungen vermindern.

Zu den Kerninhalten formaler Vereinbarungen zählt die Definition von Kompetenzen und Verantwortlichkeiten der für interne Ermittlungen zuständigen Organisationseinheit sowie ihrer Schnittstellen im Unternehmen. Folgende Stellen/Funktionen im Unternehmen können dabei involviert sein:

- Unternehmensführung bzw. beauftragte Stelle zur Genehmigung der Einleitung einer Ermittlung
- Arbeitnehmervertretung zur Wahrung der Arbeitnehmerrechte nach Betriebsverfassungsgesetz
- Konzernsicherheit oder Interne Revision zur Durchführung der Ermittlung und Beweissicherung
- Compliance-Ableitung zur Kontrolle der Angemessenheit und ggfs. Steuerung von Ermittlungen

- Rechtsabteilung zur Einordnung von Rechtsverstößen, Begleitung rechtlicher Schritte und gerichtlicher Verfahren
- Personalabteilung zur Bewertung und Durchführung arbeitsrechtlicher Maßnahmen und Sanktionen
- Datenschutzbeauftragter zur Überwachung der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten
- IT-Forensik zur Sicherung und Auswertung von IT-Systemen und Daten (inkl. E-Mail-Kommunikation)
- Steuerabteilung zur Prüfung möglicher steuerrechtlicher Handlungspflichten in Folge von Delikten
- Kommunikationsabteilung zur Steuerung interner und externer Kommunikation

Das Festlegen eines abstrakten Ablaufprozesses für interne Ermittlungen unterstützt effizientes Vorgehen der Ermittler und ihrer Schnittstellen und gewährleistet zudem Transparenz durch Schaffung einer Überprüfbarkeit von Ermittlungsvorgängen. In einer Verfahrensbeschreibung lässt sich bspw. regeln:

- Voraussetzungen für die Einleitung einer internen Ermittlung
- Anforderungen an die Dokumentation inkl. Aufbewahrungspflichten
- Erforderliche Eskalations- und Meldewege (Reporting)
- Belehrungspflichten und Verweigerungsrechte bei Befragungen
- Arbeitsrechtliche Vorschriften bei Sanktionierung
- Verhaltensprinzipien bei internen Ermittlungen (Verhaltenskodex/ Code of Conduct)

Organisationsstruktur

Um die Effizienz interner Ermittlungen sicherzustellen, sollte ein Unternehmen entweder über entsprechende interne Ressourcen verfügen oder im konkreten Bedarfsfall auf externe Hilfe zugreifen können. Auch im letzteren Fall bleibt die Verantwortung für die Steuerung der Ermittlung beim Unternehmen. Die Entscheidung zwischen internen oder externen Ermittlern ist zumeist abhängig von den zu erwartenden Kosten, der Fallkomplexität sowie dem individuellen Risikoprofil.

Für international präsente Unternehmen stellt sich die Frage, wie sich die Ermittlungseinheit zentral bzw. regional/lokal organisiert. Ab einer gewissen Unternehmensgröße kann die Kombination einer zentralen Ermittlungseinheit mit regionalen Einheiten sinnvoll sein, insbesondere wenn Steuerung und Kontrolle von Ermittlungen nach unternehmensweit vergleichbaren Standards gewünscht ist.

Bei der organisatorischen Verankerung der Ermittlungseinheit gibt es je nach Unternehmensgröße und -organisation unterschiedliche Optionen. Grundsätzlich empfiehlt sich die Unabhängigkeit der Ermittlungseinheit vom operativen Geschäft. Häufig sind Ermittlungseinheiten deshalb in Funktionen wie Compliance, Interne Revision oder Konzernsicherheit verankert. Die Alternative ist eine unabhängige Ermittlungseinheit durch direkte Anbindung an die Unternehmensleitung. Bei der Entscheidung fällt vor allem der Anspruch an Überprüfbarkeit, Objektivität und Unabhängigkeit von Ermittlungen ins Gewicht. Organisatorische Interessenskonflikte der Ermittler gilt es ebenso zu vermeiden wie persönliche.

Tipp: Es empfiehlt sich Repräsentanten von Ermittlungseinheit und relevanter Schnittstellen für ein sogenanntes „Investigation Case Committee“ zu nominieren. Eine solche Plattform erleichtert die notwendige Abstimmung bei organisatorischen und prozessualen Fragestellungen bzw. bei komplexen, schwerwiegenden Sachverhalten.

Datenschutz

Der Datenschutz hat bei internen Ermittlungen eine besondere Bedeutung. Verstöße gegen die einschlägigen Gesetze können zu individueller Strafbarkeit, erheblichen Bußgeldern, Gewinnabschöpfung und Reputationsschäden infolge negativer Berichterstattung führen. Seit dem Jahr 2018 unterliegt die Verarbeitung von personenbezogenen Daten insbesondere der Datenschutzgrundverordnung (DSGVO), was die Durchführung von internen Ermittlungen noch komplexer gemacht hat.

Die DSGVO enthält für die Verarbeitung von personenbezogenen Daten ein Verbot mit Erlaubnisvorbehalt, d.h. die Verarbeitung von personenbezogenen Daten ist nur rechtmäßig, wenn sie ausdrücklich gestattet ist. Daher ist zu prüfen, ob die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen (des Unternehmens) oder eines Dritten erforderlich ist und schutzwürdige Interessen der Betroffenen nicht überwiegen.

Dabei ist das Aufklärungsinteresse des Unternehmens sorgfältig gegen die schutzwürdigen Interessen der von der internen Ermittlung betroffenen Personen (i.d.R. die Mitarbeiter des Unternehmens) abzuwägen. Im Rahmen dieser Interessenabwägung sollten u. a. mögliche Alternativen zum Review der elektronischen Kommunikation (e-Discovery), die Eingrenzung des Untersuchungszeitraums, die automatisierte Durchsicht mittels einer sachbezogenen Suchwortliste und die Begrenzung der internen Untersuchung auf bestimmte Unternehmen, Abteilungen oder Personen berücksichtigt werden. Im Rahmen des e-Discovery-Prozesses sind auch Grundsätze zum Umgang mit privaten Daten, die natürlich auch bei einem Verbot seitens des Unternehmens vorhanden sein können, zu entwickeln.

Tip: Aufgrund der Vielzahl datenschutzrechtlicher Fallstricke sollte der betriebliche Datenschutzbeauftragte frühzeitig in die wesentlichen datenschutzrechtlichen Fragestellungen, die eine interne Ermittlung mit sich bringt, eingebunden werden. Weiter empfiehlt sich eine detaillierte Dokumentation der datenschutzrechtlichen Entscheidungen, um auf etwaige Beschwerden von Betroffenen oder Anfragen der Datenschutzbehörden schnell und angemessen reagieren zu können.

III. Durchführung von internen Ermittlungen

1. Zielsetzung, Planung und Team-Setup der internen Ermittlung

Mögliche Auslöser

Erste Anhaltspunkte für ein mögliches zu untersuchendes Fehlverhalten können sich durch verschiedene interne oder externe Faktoren ergeben.

- **Interne Auslöser**
 - Third Party Due Diligence
 - Whistleblower
 - Datenanalysen/IKS
 - Vorgesetzte/Leitende Angestellte
 - Interne Revision
 - Compliance Desk

- **Externe Auslöser**
 - Whistleblower
 - Staatsanwaltschaft
 - Steuerbehörde
 - Aufsichts- und Regulierungsbehörden (z.B. BaFin)
 - Presseberichterstattung/Investigativer Journalismus
 - Beschwerden Dritter
 - Jahresabschlussprüfung

Entscheidungsprozess hinsichtlich interner Ermittlungen

Grundsätzlich gilt es immer, den Gesamtkontext eines Anhaltspunktes für ein Fehlverhalten zu untersuchen. Nur so kann entschieden werden, ob aus ihm eine interne Ermittlung abgeleitet wird oder nicht und welche internen und externen Beteiligten eingebunden werden sollten. Die folgenden Fragen dienen als Hilfestellung zur Entscheidung, für oder gegen eine interne Ermittlung:

- **Komplexität**
 - Wie groß könnte der Umfang des Sachverhalts sein?
 - Sind verschiedene Standorte betroffen?
 - Ergeben sich komplexe Fragen zu Rechtsgebiet oder Rechtsordnung?
- **Schweregrad**
 - Sind, nach erstem Augenschein, hochrangige Mitarbeiter beteiligt?
 - Wie weitreichend sind die Vorwürfe?
 - Wie hoch ist die vermutliche kriminelle Energie?
 - Wie hoch ist der eingetretene Schaden?
- **Glaubwürdigkeit**
 - Ist die Quelle des Hinweises auf Fehlverhalten bekannt und als verlässlich einzustufen?
 - Gibt es leicht überprüfbare Fakten?
- **Dringlichkeit**
 - Ist die Sicherheit von Produkten, Mitarbeitern oder Zeugen gefährdet?
 - Bestehen unmittelbare Informationspflichten?
 - Welche unternehmensfremden Personen sind betroffen? Welche Drittparteien?
 - Wird das vermutliche Fehlverhalten bzw. der Sachverhalt bereits öffentlich diskutiert?

Für eine spätere Nachvollziehbarkeit kann es hilfreich sein, den Entscheidungsprozess z.B. entlang der o.g. Fragen zu dokumentieren.

Zielsetzung

Nachdem die auslösenden Faktoren zu der Entscheidung geführt haben, eine interne Ermittlung durchzuführen, bedarf es eines offiziellen Ermittlungsauftrags. Ein solches Mandat wird i. d. R. von autorisierten Stellen, wie der Unternehmensleitung, dem Aufsichtsrat oder Mehrheitsgesellschaftern schriftlich erstellt. Der Auftraggeber ist in der Ermittlung regelmäßig über den aktuellen Stand zu informieren, trifft ggf. wesentliche Entscheidungen während und am Ende der Ermittlung und ist Adressat des Abschlussberichts.

Leitplanken – Interne Ermittlungen

Der Auftrag beinhaltet u.a. auch die Zielsetzung der Ermittlung, welches ergebnisoffen formuliert werden sollte, um ein Ergebnis nicht schon von vornherein zu beeinflussen bzw. vorwegzunehmen. Die Zielsetzungen können z.B. reine Sachverhaltsaufklärungen, rechtliche Prüfungen, Prüfungen von Schadensersatzansprüchen und/oder die Unternehmensverteidigung im Rahmen eines möglichen OWiG-Verfahrens umfassen. Konkrete Zielvorgaben von Beginn an helfen u.a. dabei, mögliche Doppelarbeiten zu vermeiden und auch die Dokumentationen entsprechend zu erstellen. Dabei sollte bedacht werden, dass eine zu breite Zieldefinition die Gefahr von einer unverhältnismäßig hohen Komplexität (sowie Kosten) der Ermittlung und eine zu enge Definition (und das Festhalten an dieser während der Investigation) das Risiko von Nichtbeachtung relevanter Aspekte mit sich bringt. Die Zielsetzung beeinflusst schließlich auch den Ermittlungsgegenstand, d.h. z.B. welche Geschäftsvorgänge, in welchem Zeitraum und in welchen Bereichen (Abteilungen, Geschäftsteilen, Ländern) untersucht werden sollen.

Zusammengefasst weist die interne Ermittlung folgende Kernziele auf:

- Aufklärung (Erfüllung der Anforderungen §§ 43 GmbHG/91,93 AktG, 30/130 OWiG)
- Legalitätssicherung (Meldepflichten, Vermögenssicherung, Reputationsschutz, Unternehmensverteidigung)
- Sanktionierung (Signalwirkung, Selbstreinigung, Rückführung von Vermögen)

Welche Stellen im Unternehmen müssen/sollten eingebunden werden?

Bei internen Ermittlungen ist es wichtig, grundsätzlich eine verantwortliche Stelle im Unternehmen für die Durchführung und Kommunikation der Ermittlungshandlungen zu benennen. Zwar unterscheiden sich die einzubindenden Stellen und Funktionen je nach Sachverhalt und Unternehmensstruktur. In der Regel sind jedoch die folgenden Unternehmensfunktionen für interne Ermittlungen sachleitend:

- Compliance-Abteilung
- Interne Revision
- Rechtsabteilung/General Counsel
- Konzernsicherheit

Die Einbindung der folgenden Entscheidungsträger in der Unternehmenshierarchie sollte abgewogen werden:

- Geschäftsführung/Vorstand
- Aufsichtsrat
- Compliance-Officer und mögliche regionale Compliance-Verantwortliche
- Geschäftsführer von Tochtergesellschaften

Ergänzend dazu können und müssen lageangepasst weitere Stellen, insbesondere sachverhaltsrelevante Wissensträger, wie bspw. Mitarbeiter aus der betroffenen Abteilung, hinzugezogen werden. Es muss hierbei immer zwischen Erkenntnisgewinn und einer möglichen Preisgabe von Informationen abgewogen werden.

Bei der Einbindung der Personalabteilung, insbesondere im Hinblick auf arbeitsrechtliche Maßnahmen, müssen immer mögliche arbeitsrechtliche Fristen (Kenntnisnahme des Sachverhalts durch einen Kündigungsberechtigten, Auslösung der 14-Tages-Frist) betrachtet werden.

Grundsätzlich gilt: die Einbindung von Funktionen, Stellen und Einzelpersonen sollte nur nach dem „need-to-know“ Prinzip durchgeführt werden und durch entsprechende technische/organisatorische Sicherungsmaßnahmen (Zugangsberechtigungen zu Ermittlungsräumen, Datenzugriff, etc.) begleitet werden.

Eine interne Ermittlung beinhaltet in den allermeisten Fällen eine Verarbeitung personenbezogener Daten. Insbesondere bei einem Anfangsverdacht von Straftaten im Unternehmen verlangt der §26 BDSG die Dokumentation tatsächlicher Anhaltspunkte für ein mögliches strafbares Verhalten sowie eine Interessensabwägung – und zwar vor der Durchführung der Ermittlungshandlungen, bei denen personenbezogene Daten verarbeitet werden. Es ist daher empfehlenswert, den Datenschutzbeauftragten bzw. eine mögliche externe Rechtsberatung frühzeitig einzubinden.

Meldepflichten: Je nach Rechtscharakter des Tatvorwurfs, müssen externe Stellen eingebunden werden (bspw. die Ad-hoc-Meldung im Kapitalmarktrecht, der „Data Breach“ im Datenschutzrecht, etc.). Ein Ausbleiben der Meldung kann zu einem erneuten bzw. rechtlich selbstständigen Verstoß führen.

Je nach vorliegender Betriebsvereinbarung kann es erforderlich sein, den Betriebsrat über die Durchführung einer internen Ermittlung in Kenntnis zu setzen bzw. zu beteiligen.

Planung der Ermittlung

Eine strukturierte Planung ist aufgrund der oftmals komplexen internen Ermittlung unerlässlich, vor allem wenn die interne Ermittlung über verschiedene Themenbereiche und grenzüberschreitend geschehen soll. Es bieten sich daher folgende Planungsschritte nach der Analyse und Evaluation des Sachverhalts an:

1. Planung und Durchführung von Ad-hoc-Maßnahmen – es ist unerlässlich, Sofortmaßnahmen vor der eigentlichen internen Ermittlung zu treffen, um die Verdunkelung des Sachverhalts und einen möglichen anhaltenden Vermögensabfluss zu unterbinden. Diese sind lage- und sachverhaltsabhängig:
 - Identifizierung und Sicherung von möglichen Beweismitteln, welche von der Vernichtung bzw. Unterdrückung durch involvierte Personen bedroht sind (in Papierform und elektronisch) unter Einhaltung forensischer Gesichtspunkte
 - Unterbindung möglicher Vermögenstransfers
 - Entzug von Benutzungsrechten (ERP-Systeme, Cloud-Speicher, virtuellen Datenbeständen, Remote-Zugriff, Bankkonten, etc.)
 - Sperrung von Gebäudezugängen für involvierte Mitarbeiter
 - Festlegung einer krisengesteuerten Kommunikationsstrategie (siehe auch Kapitel IV)
2. Nach den erfolgten Sofortmaßnahmen sollte eine Planung der regulären internen Ermittlung erfolgen. Dies beginnt mit der Identifizierung von möglichen Strafbarkeiten nach StGB, HGB, UWG und weiteren Nebengesetzen- sowie, abgestuft, möglichen arbeitsrechtlichen Verstößen bzw. zivilrechtlichen Schadensfällen.
3. Bildung von Ermittlungskomplexen bzw. Ermittlungsabschnitten, Identifizierung der dafür relevanten Beweismittel und deren „Auffindewahrscheinlichkeit“.
4. Abwägung der Durchführung von Befragungen – wer wird zu welchem Zeitpunkt befragt? In welchem arbeitsrechtlichen Status befinden sich die jeweiligen involvierten Mitarbeiter? Befragungen führen auch immer zu einer graduellen Offenlegung der internen Ermittlung (siehe hierzu auch Kapitel III.2.b).

Team-Setup und Ressourcen

Interne Ermittlungen erfordern eine dem Sachverhalt angepasste Teamzusammenstellung. Je nach vorliegendem Tatvorwurf und der Art der zu erwartenden Beweismittel müssen entsprechende Spezialisten mit spezifischen Kenntnissen herangezogen werden. Dazu zählen neben Ermittlern mit kriminalistischen Kompetenzen auch IT-Forensiker, Juristen (bspw. für Steuerrecht, Exportrecht, Vertragsrecht, etc.) oder „Forensic Accountants“. Je nach Sachverhalt sind aber auch atypische Kenntnisse notwendig, wie Immobilienbewertungen, Finanzexpertise zu komplexen Finanzprodukten, Produktionsplanung, Werkstoffkunde, etc.

Im Zuge der Teamzusammenstellung muss ebenfalls eine Abwägung erfolgen, ob die interne Ermittlung mit unternehmenseigenen Ressourcen durchgeführt werden kann oder ob externe Unterstützung hinzugezogen werden muss. Hierbei gilt es die folgenden, beispielhaften Punkte abzufragen:

- Liegt ausreichend ermittlungstechnische Kompetenz und Fachwissen vor?
- Ist die Unabhängigkeit der internen Ermittlung durch unternehmenseigene Kräfte gewahrt?
- Wird die notwendige IT-Struktur (Hardware und Forensiksoftware) im Unternehmen vorgehalten?
- Können eigene Mitarbeiter die interne Ermittlung durchführen und auch im Nachgang dazu konfliktfrei und ohne persönliche Einschränkungen/Interessenskonflikte im Unternehmen weiterarbeiten (Stichwort: Bedrohungslage)?

2. Ermittlungshandlungen

Im Gegensatz zu behördlichen Ermittlungen stehen der internen Ermittlung deutlich weniger Werkzeuge zur Verfügung. Diese kategorisieren sich im Wesentlichen in drei Aspekten:

- Hintergrundrecherchen in öffentlich zugänglichen Quellen **a)**
- Befragungen/Interviews **b)**
- Unstrukturierte und strukturierte Datenanalyse, inkl. Digitale Forensik **c)**

a) Hintergrundrecherchen in öffentlich zugänglichen Quellen

Hintergrundrecherchen oder auch „Background Checks“ dienen der Aufdeckung privater und geschäftlicher Netzwerke und Aktivitäten von Personen. Sie sind eines der Hauptinstrumente, um verdeckte Interessen der beteiligten Akteure offenzulegen (Stichwort „Prinzipal-Agent-Theorie“).

Hintergrundrecherchen basieren auf Informationen aus verschiedenen, öffentlich zugänglichen, lokalen und internationalen Quellen, wobei die Recherchetiefe sowie die Informationsquellen an die Bedürfnisse und Ziele des spezifischen Sachverhalts angepasst werden. Mögliche Quellen sind hierbei:

- Internationale Unternehmensdatenbanken
- Lokale Unternehmensdatenbanken/Handelsregister
- Internationale Compliance-Datenbanken
- Internationale Pressearchive (z.B. Dow Jones Factiva, Nexis)
- Internetrecherchen
- Medienrecherchen

Hintergrundrecherchen dienen außerdem der Identifizierung von:

- rechtlichen und persönlichen Abhängigkeitsbeziehungen (Interessenskonflikte)
- Integritätsrisiken (Einträge in z.B. Compliance Datenbanken, „Sanktionen“, „Black-Lists“)

- negativer Berichterstattung über involvierte Personen, Unternehmenseigentümer oder Management
- Vernetzungen und Verbindungen zwischen ausgewählten Stakeholdern des Unternehmens
- öffentlicher Reputation des Unternehmens

b) Befragungen/Interviews

Die Befragung von Mitarbeitern stellt innerhalb des Werkzeugkastens der internen Ermittlungen eines der wesentlichsten Instrumentarien zur Informationsgewinnung bzw. zur Aufklärung von Sachverhalten dar. Sollten bereits Ermittlungsbehörden eingeschaltet worden sein, sollten sämtliche Befragungen mit diesen im Vorfeld abgestimmt werden.

▪ Rahmenbedingungen

Zunächst ist die Klärung der allgemeinen Rahmenbedingungen für eine Befragung vor dem Hintergrund des jeweiligen Sachverhaltes und der konkreten Zielsetzung erforderlich:

▪ Teilnahme und Pflicht an der Befragung

Nach herrschender Meinung kann ein Arbeitgeber seine Mitarbeiter aufgrund des Direktionsrechts an der Teilnahme von Befragungen arbeitsrechtlich verpflichten. Es besteht zudem nach allgemeiner Auffassung eine vollständige Auskunftspflicht über alle dienstlichen Kenntnisse, ein Aussageverweigerungsrecht gibt es bisher bei internen Ermittlungen nicht.

Zur Problemstellung „ehemalige Mitarbeiter“ greift lt. herrschender Meinung das Direktions- und Weisungsrecht nicht mehr. Eine Empfehlung könnte daher sein, Mitwirkungsklauseln in Aufhebungsverträge von jenen Mitarbeitern, die einen wichtigen Beitrag zur Aufklärung leisten könnten, aufzunehmen.

▪ Beistände für Mitarbeiter

Das Recht zur Hinzuziehung des Betriebsrates zu Gesprächen mit dem Arbeitgeber durch den Arbeitnehmer besteht nur in bestimmten, im BetrVG definierten, Fällen (z.B. Leistungsbeurteilung, berufliche Entwicklungsmöglichkeiten, Anhörung). In der Regel werden die zuvor genannten Themen bei Befragungen im Rahmen von internen Ermittlungen nicht berührt. Daher gilt:

- Der befragte Mitarbeiter hat rechtlich keinen Anspruch auf einen Beistand durch den Betriebsrat.
- Sollten relevante Regelungen in Betriebsvereinbarungen existieren, sind diese natürlich zu beachten.
- Grundsätzlich kann es hilfreich sein (je nach Hintergrund der Ermittlung), den Betriebsrat zumindest über Befragungen zu informieren, um eine Kooperation mit dem Befragten proaktiv zu fördern.

Für den Mitarbeiter besteht zudem ebenfalls zunächst kein rechtlicher Anspruch auf einen Rechtsbeistand. Sofern jedoch auf Unternehmensseite Rechtsanwälte der Befragung beiwohnen, kann es in Erwägung gezogen werden, dem Mitarbeiter aber das Recht auf einen Anwalt zuzugestehen, um eine „Waffengleichheit“ herzustellen.

▪ Belehrungspflichten

Grundsätzlich besteht bei einer Befragung keine rechtliche Pflicht hinsichtlich der Belehrung seitens interner Ermittler. Aus der allgemeinen Rechtsprechung im Arbeitsrecht empfiehlt es sich jedoch, den Mitarbeiter aus Fairness- und Transparenzgründen über Zweck, Dokumentation und Weitergabe der Informationen aufzuklären,

was grundsätzlich auch zum Abbau von etwaigem Misstrauen beitragen kann (auch im Hinblick auf mögliche Beweisverwertungsverbote). Rechtlich nicht eindeutig ist die Verwendbarkeit von Aussagen im Interview in einem späteren Strafverfahren. Daher kann es je nach Einzelfall angezeigt sein, den Mitarbeiter auf mögliche strafrechtliche Konsequenzen hinzuweisen.

- **Durchführung der Befragung**

Die Durchführung der Befragungen sollte sorgfältig vorbereitet sowie durchgeführt werden und richtet sich nach den jeweiligen Gegebenheiten und Hintergründen der Ermittlung. Neben dem Umgang mit den oben unter Punkt dem „Rahmenbedingungen“ genannten Aspekten, sollten u.a. folgende Fragestellungen bei der Durchführung berücksichtigt werden (die nachfolgende Aufstellung ist nicht abschließend und sollten auch nicht isoliert, sondern in Abhängigkeit voneinander behandelt werden):

Aspekt	Hinweis
Welche Mitarbeiter sollen – in/mit welcher Rolle – befragt werden?	Bei der Auswahl der Befragten lassen sich grundsätzlich Mitarbeiter unterscheiden, die voraussichtlich lediglich erhellende Informationen beitragen werden (Zeugen) und diejenigen, die wahrscheinlich selbst zusätzlich in die zu untersuchenden Handlungen involviert waren (Verdächtige/ Tatbeteiligte). Da sich zunächst eine möglichst umfassende Informationsgewinnung empfiehlt, sollte eine entsprechende Reihenfolge der Befragungen gewählt werden.
Wer führt die Befragung durch?	Eine Befragung sollte durch mindestens zwei Personen durchgeführt werden. Diese sollten über entsprechende Erfahrungen und alle notwendigen Informationen zu den konkreten Ermittlungen verfügen. Auch die Rollenverteilung innerhalb der Befragung (Gesprächsführer/Protokollant) sollten vorher festgelegt werden. Es empfiehlt sich zudem, zu klären, ob weitere Personen (z.B. Vertreter Personalabteilung, Rechtsanwalt) teilnehmen sollten.
Was ist das Ziel der Befragung?	Dient die Befragung der reinen Informationsgewinnung oder der Konfrontation von Verdächtigen mit entsprechenden Sachverhalten? Letzteres sollte auf Basis umfassender Erkenntnisse und somit möglichst am Ende einer Befragungsreihe stattfinden.
Wie ist die Gesprächstaktik?	Je nach Zielsetzung und Befragtem, sollte das Gespräch entsprechend gestaltet werden. Je mehr der reine Informationsgewinn im Vordergrund steht, empfehlen sich offene Fragestellungen. Je konkreter Verdachtsmomente sind, können auch geschlossene Fragen zielführend sein. Es sollte aber stets eine professionelle und faire Gesprächsatmosphäre seitens der Fragesteller erzeugt werden.
Wie wird dokumentiert?	Eine möglichst objektive und detaillierte Dokumentation sind für belastbare Ermittlungsergebnisse unerlässlich. Daher empfiehlt sich eine Protokollierung während des Gesprächs. Je nach Sachverhalt kann es sich empfehlen, das Protokoll auch vom Befragten gegenzeichnen zu lassen. Audio- und Videoaufzeichnungen gestalten sich erfahrungsgemäß aus datenschutzrechtlichen Gründen oftmals als problematisch.

c) Unstrukturierte und strukturierte Datenanalyse, inkl. Digitale Forensik

Dieser Abschnitt behandelt einerseits die sog. "Digitale Forensik", andererseits die Analyse von strukturierten und unstrukturierten Daten. Aufgrund der bereits sehr ausgeprägten Digitalisierung in Unternehmen (verschiedenste IT-Systeme und auch "neue" Applikationen, z.B. Messenger-Dienste), haben diese Themenkomplexe in der Regel eine wesentliche Bedeutung im Rahmen interner Ermittlungen.

Die digitale Forensik beschäftigt sich mit der systematischen Analyse von IT-Systemen und -Geräten, vor allem um Beweise gerichtsverwertbar zu finden und zu sichern. Ihre Methoden dienen der:

- Nachvollziehbarkeit und Dokumentation von sachverhaltsrelevanten Ereignissen im digitalen Umfeld
- Identifizierung möglicher Verantwortlicher und Zurechenbarkeit

Hierzu werden unterschiedliche Ermittlungs- und Analyseansätze verfolgt.

Die IT-Forensik unterteilt sich in die Gebiete „Datenforensik“ und „Computerforensik“:

- Die Datenforensik beschäftigt sich vor allem mit auf IT-Systemen gespeicherten Daten und Inhalten von Datenbanken
- Die Computerforensik kümmert sich vor allem um die Analyse von Geräten.

▪ Analyse von strukturierten Daten

Unter diesen Aspekt fällt die Auswertung der gesicherten Beweismittel, welche in strukturierter Datenform vorliegen. Dazu zählen klassischerweise Daten aus dem ERP-System (Enterprise Resource Planning System):

- Finanzbuchhaltungsdaten (Konten, Buchungen, Haupt- und Nebenbücher, etc.)
- Produktionsdaten
- Controlling
- Kostenstellendaten

Falls diese nicht im ERP, sondern als sogenannte „Insellösung“ vorhanden sind, müssen diese entsprechend gesichert und extrahiert werden. Viele Systeme mit verschiedenen Funktionen können hierbei Daten bieten, die für die Ermittlung von Relevanz sind (exemplarisch):

- Zugangsdaten zu Gebäuden über Betreten und Verlassen
- Standardisierte Personalakten
- Arbeitszeiterfassung
- Supply-Chain und Produktionssoftware
 - Materialverbräuche
 - Bestellungen und Lieferungen
 - Rechnungen
 - Freigaben
- Fuhrparksoftware über Fahrzeugnutzung
- Archivierungssoftware
- IT-Hardware-Verwaltungssoftware

Diese gilt es, unter Beachtung des Datenschutzes, am Sachverhalt entlang und unter Bezug auf die Tatvorwürfe zu analysieren und in einen Sachzusammenhang zu stellen. Hier können bereits wichtige Fakten zum Tathergang gewonnen werden, welche als Grundlage für Fragen im Interview dienen können.

▪ Analyse von unstrukturierten Daten

Dies betrifft die Auswertung der gesicherten Beweismittel, welche in unstrukturierter Datenform vorliegen. Bei internen Ermittlungen liegen diese sowohl in Papierform (und/oder Scan) als auch elektronisch vor und können verschiedener Natur sein, wie z.B.:

- Vertragsunterlagen
- Eingangsrechnungen
- Notizen und Kalendereinträge
- E-Mail-Accounts
- SMS
- Messenger-Chat-Dienste
- Kommunikationsplattformen

Dabei dürfte vor allem der Auswertung der E-Mail-Kommunikation (e-Discovery) eine wichtige Bedeutung zukommen, da hier Erkenntnisse zu subjektiven Tatbeständen wie Vorsatz, Motivation und Kenntnisnahme untersucht werden können. Hierbei gilt es besonders, die datenschutzrechtlichen Aspekte zu berücksichtigen, da sich hieraus oftmals folgende Problemstellungen ableiten lassen:

- Private Nutzung von Laptops oder Smartphones (Betriebsvereinbarung)
- Kernbereichsschutz (besondere Kategorien personenbezogener Daten, z.B. politische Meinung, Gesundheitsdaten)
- Löschfristen
- Auswertung unter forensischen Gesichtspunkten
- Kenntnisnahme und Fristen

Gerade in Ergänzung zu den Ergebnissen der strukturierten Datenanalyse sind die Ergebnisse aus der unstrukturierten Datenanalyse oft entscheidend für das Verstehen des zu Grunde liegenden Sachverhalts. Sie bietet wertvolle Informationen für die Vorbereitung der Interviews, insbesondere von tatbeteiligten Mitarbeitern.

3. Dokumentation und Konsequenzen

Dokumentation

Der mit Sicherheit zentrale Aspekt in der Dokumentation ist die Nachvollziehbarkeit der durchgeführten internen Ermittlung. Hierbei muss ersichtlich sein, welche Maßnahmen nach Bekanntwerden des Tatvorwurfs getroffen wurden, welche Ermittlungsschritte und -handlungen geplant und durchgeführt wurden (auch, welche nicht durchgeführt wurden; abhängig von dem Adressaten), welche Erkenntnisse sich daraus ziehen lassen und, bei Bedarf, eine Darlegung von Empfehlungen von zu treffenden weiteren Maßnahmen zu

- Geschäftsprozessen
- Arbeitsrecht
- Zivilrecht
- Reorganisation und Geschäftsverteilungsplan
- Zuständigkeiten und Verantwortlichkeiten

Es ist empfehlenswert, einen umfassenden Abschlussbericht zu verfassen, welcher die o.g. Aspekte beinhaltet. Der Bericht sollte folgende Eigenschaften aufweisen:

- Klare Struktur

- Eindeutige Darlegung der Fakten
- Deutliche Trennung von Fakten und Annahmen
- Verweis auf verwendete Beweismittel
- Der Bericht muss für sich allein stehen können

In der laufenden Ermittlung kann es nützlich sein, eine fortlaufende, vorläufige Berichterstattung zu fertigen. Dies dient den Entscheidungsträgern als Grundlage für Unternehmensentscheidungen und im Nachgang der Nachvollziehbarkeit des jeweiligen Wissensstandes zum jeweiligen Zeitpunkt. Dies ist vor allem von den fest gelegten Kommunikationswegen, welche bereits in der Planungsphase definiert werden, abhängig.

Oftmals dient der Abschlussbericht auch als Grundlage, um mit Behörden, sowohl Aufsichts- als auch Strafverfolgungsorganen, in den Austausch bzw. in Kontakt zu treten.

Der Bericht dient zudem als Wissensgrundlage für lange andauernde rechtliche Auseinandersetzungen. Erfahrungsgemäß können sich Zivil-, aber vor allem Strafverfahren, über Jahre hinziehen. Insbesondere bei einem möglichen Auftreten als Zeuge vor Gericht durch Unternehmensvertreter bzw. der beteiligten Ermittler kann ein Bericht die gemeinsame Basis der Aussage bilden, um vor allem um Widersprüche zu vermeiden und möglichst wahrheitsgetreue Angaben machen zu können.

Konsequenzen

In der Nachphase steht, neben der Dokumentation, die Bewältigung der Folgen aus der internen Ermittlung im Fokus, aber auch die Entwicklung und Optimierung der eigenen Organisation.

Dabei stehen folgende Punkte im Vordergrund:

- Durchführung arbeitsrechtlicher/disziplinarischer Maßnahmen (z.B. Kündigungen, Abmahnungen)
- Kontinuierliche Begleitung der laufenden Verfahren (zumeist im Straf-/Zivil-/Arbeitsrecht)
- Durchführung von Nachermittlungen (Behördenanfragen, offene Aspekte im zugrunde liegenden Sachverhalt, Unterstützung der Unternehmensverteidigung, etc.)
- Bewältigung der rechtlichen Folgen aus Sanktionen und Zivilverfahren (Begleichung verhängter Bußgelder, Prozesskosten, „Blacklisting“ im Vergaberecht)
- Begleitung des Schadensmanagementprozesses, v.a. im Hinblick auf Versicherer (D&O/Vertrauensschadensversicherung)
- Analyse und Bewertung der Reputationsschäden sowie ggfs. Aufbau einer Kommunikations- und Markenstrategie zum Zwecke der Öffentlichkeitsarbeit

Insbesondere Straf- und Zivilverfahren können sich hierbei über mehrere Jahre hinziehen, die oftmals eine enge Begleitung erfordern. Nicht selten fragen Behörden noch ergänzende Dokumentation an oder benötigen Unternehmensauskünfte zur Durchführung strafprozessualer Maßnahmen.

Neben den Konsequenzen bieten die Ergebnisse der internen Ermittlung aber auch eine Chance zur Verbesserung der eigenen Organisation. Nicht selten fördert die Ermittlung Schwächen in Prozessen und Kontrollabläufen zu Tage, die nun zur Vermeidung zukünftiger Verstöße verbessert und somit wirksamer gestaltet werden können:

- Stärkung von Prozessabläufen, welche mögliche Tatbegehungsweisen deutlich erschwert (bspw. Vier-/Mehr-Augen-Prinzipien, revisionssichere Dokumentation)
- Analyse des zugrunde liegenden Sachverhalts, um Organisations-/Kontrollschwächen zu identifizieren
- Optimierung bzw. Anpassung des Kontrollumfelds und der Compliance-Organisation

IV. Kommunikation und Kooperation mit Externen

Ein weiterer wesentlicher Gesichtspunkt in Ermittlungsfällen ist die geordnete und zielgerichtete Kommunikation im Unternehmen sowie mit relevanten Dritten. Dazu gehören neben den Strafverfolgungsbehörden u.a. weitere Behörden, Medienvertreter, Vertragspartner, externe Ermittler. Wie generell im Umgang mit Krisensituationen ist es daher wichtig, dass auch Kommunikationsabläufe für die Durchführung interner Ermittlungen im Vorfeld vorbereitet und eingeübt werden. Eine gute Vernetzung von Ermittlern innerhalb des Unternehmens, mit Geschäftsleitung, Kommunikationsbereich und operativen Einheiten, und eine klare Festlegung von Entscheidungswegen erleichtert den Informationsfluss und die schnelle Entscheidungsfindung.

Im Fall behördlicher Ermittlungen ist es wichtig, auch in der externen Kommunikation die volle Bereitschaft zur Zusammenarbeit zu betonen.

Es empfiehlt sich daher festzulegen, wer im Ermittlungsfall zu informieren ist, wenn Ermittlungen gegen z.B. Mitarbeiter, Geschäftsleitung oder Aufsichtsrat eingeleitet werden. Weitere Fragen betreffen z.B. interne und externe Kommunikationswege und Entscheidungskompetenzen hinsichtlich der Kommunikationsstrategie.

Was im Einzelfall die „richtige“ Kommunikation ist, richtet sich vor allem nach den Ermittlungszielen (vgl. Kapitel III.1), die erreicht werden sollen. Eine streng an den Ermittlungszielen orientierte Kommunikation und Kooperation stellt sicher, dass die Unternehmensinteressen im Fokus bleiben und auch im Umfeld hoheitlicher Strafverfolgungsmaßnahmen angemessene Berücksichtigung finden.

1. Umgang mit Polizei und Staatsanwaltschaft

Erhält das Unternehmen Kenntnis, dass eine Ermittlungsbehörde ein Ermittlungsverfahren eingeleitet hat, sollte das Unternehmen diese Ermittlungen nicht durch interne Ermittlungen behindern. Die Aufnahme oder Fortsetzung interner Ermittlungen sollte in diesen Fällen i.d.R. in enger Absprache mit der Polizei oder Staatsanwaltschaft erfolgen.

Haben die Strafverfolgungsbehörden (noch) keine Kenntnis von dem zu ermittelnden Sachverhalt, stellt sich für das Unternehmen die Frage, ob eine Strafanzeige (oder ggf. ein Strafantrag) gestellt werden soll. Bei der Entscheidung sollte berücksichtigt werden, dass die Ermittlungsbehörden aufgrund des Legalitätsprinzips der Strafprozessordnung bei Vorliegen eines Anfangsverdacht zur Durchführung von Ermittlungen verpflichtet sind. Eine allgemeine Pflicht zur Anzeige von Straftaten besteht in Deutschland nicht (Ausnahme § 138 StGB bei schweren Straftaten wie Raub und Mord). Im Einzelfall kann es nach Abwägung der zu erwartenden Vor- und Nachteile für das Unternehmen daher durchaus sinnvoll sein, einen Verdachtsfall nicht zur Anzeige zu bringen. Gründe dafür können z.B. sein:

- der voraussichtlicher Ermittlungs- /Unterstützungsaufwand steht außer Verhältnis zum voraussichtlichen Ergebnis
- eine geringe Aufklärungswahrscheinlichkeit
- der zu erwartende Reputationsschaden überwiegt das Aufklärungsinteresse
- eine Offenlegung von Betriebsgeheimnissen ist zu befürchten
- Fokussierung auf zügige Durchführung arbeitsrechtlicher Maßnahmen

2. Beantwortung behördlicher Auskunftersuchen

Unternehmen können im Rahmen von Auskunftersuchen der Staatsanwaltschaft oder der Polizei als Beauftragte der Staatsanwaltschaft gemäß §§ 161 a Abs.1, 163 Abs.3 StPO verpflichtet sein, Auskünfte jeglicher Art zu erteilen und Daten herauszugeben, z.B. zu Vertragsverhältnissen mit Kunden- oder Arbeitnehmern. Die Berechtigung der Herausgabe von personenbezogenen Daten ergibt sich in diesen Fällen aus § 24 BDSG und Art. 6 Abs.1 lit.c DSGVO.

Bei der Beantwortung ist auf einen sicheren Kommunikationsweg zu achten, damit die Daten unverfälscht und ausschließlich bei der Strafverfolgungsbehörde ankommen. Der Umfang der erteilten Auskünfte muss sich bei personenbezogenen Daten streng an der Anfrage orientieren.

3. Umgang mit Öffentlichkeit, Kunden und Partnern

Straftaten im Unternehmensumfeld können erhebliche Auswirkungen auf die Reputation des Unternehmens haben. Damit können unmittelbare Wirkungen auf Aktienkurs und Absatz verbunden sein. In börsennotierten Unternehmen können solche Taten im Einzelfall Insiderinformationen darstellen, die im Rahmen der Ad-hoc-Publizität nach der Marktmissbrauchsverordnung offenzulegen sind. Das Unternehmen sollte daher darauf vorbereitet sein, die Kommunikation mit der Öffentlichkeit so zu steuern, dass Schäden für das Unternehmen vermieden werden. Dies kann mithilfe eines professionellen Kommunikations-Teams geschehen oder – gerade in kleineren Unternehmen – durch Vorbereitung wichtiger Ablaufentscheidungen im Vorfeld eines Vorkommnisses. Eine schnelle und offene Kommunikation von Fehlverhalten im Unternehmen kann den Verlust von Vertrauen verhindern und verlorenes Vertrauen zurückgewinnen. Eine zielgerichtete Kommunikation mit Öffentlichkeit, Kunden und Vertragspartnern kann helfen, Missverständnisse und eine virale Ausbreitung von Fehlinterpretationen zu vermeiden.