Deutsches Institut für Compliance

DICO LEITLINIE

L19 – COMPLIANCE IN NGOs

AUTOREN: ARBEITSKREIS
COMPLIANCE IN NGOs

STAND 10/2025

Stand: September 2025

Disclaimer

DICO Leitlinien richten sich an Compliance-Praktiker. Sie sollen einen Einstieg in das Thema erleichtern und einen Überblick verschaffen. Es wird daher bewusst darauf verzichtet, juristische Sonderfälle und Ausnahmeregelungen aufzuzeigen.

DICO Leitlinien bieten dem geneigten Leser praxistaugliche und umsetzbare Empfehlungen für ausgewählte Compliance-Themen. Mit Veröffentlichung einer Leitlinie soll zugleich eine Diskussion zum jeweiligen Themenkreis angestoßen werden mit dem Ziel, darauf aufbauend einen Standard zu entwickeln, der von Compliance-Praktikern anerkannt wird.

Senden Sie Ihre Anregungen und Beiträge an Leitlinien@dico-ev.de. Wir freuen uns auf eine lebhafte Diskussion und bedanken uns für Ihre konstruktive Unterstützung!

1. EINLEITUNG – WARUM IST DAS WICHTIG?

Compliance – das Rückgrat der Integrität einer Organisation – spielt bei NGOs (Non-Governmental-Organisations) eine tragende Rolle. Der sog. dritte Sektor, der auch als „Zivilgesellschaft" bezeichnet wird, in Abgrenzung vom staatlichen ersten Sektor und vom privat-wirtschaftlichen zweiten Sektor, umfasst Organisationen, die gemeinnützig tätig sind und oft humanitäre, karitative, soziale, wissenschaftliche oder ökologische Ziele verfolgen. Sie sind typischerweise nicht gewinnorientiert. Organisationsformen und Trägerschaften sind vielfältig.

NGOs sind häufig eingetragene Vereine, können aber auch in anderen Rechtsformen organisiert sein. Hinter ihnen stehen unterschiedliche Träger – von Kirchen und Wohlfahrtsverbänden über private Initiativen bis hin zu internationalen Netzwerken. Diese Vielfalt spiegelt sich auch in Größe, Struktur und Finanzierung wider: Manche NGOs arbeiten lokal und projektbezogen und basieren zum Teil stark auf ehrenamtlichem Engagement, andere international, z. B. in der humanitären Hilfe mit umfangreichen Verwaltungsstrukturen, hohen Mitarbeitendenzahlen und öffentlichen Fördermitteln. Entsprechend unterschiedlich sind auch die Anforderungen in der Compliance, da z. B. bei Standorten in verschiedenen Ländern auch die jeweiligen Rechtsordnungen berücksichtigt werden müssen.

Die Leitlinie mit spezifischen Hilfestellungen und Orientierung für eine sektorgerechte Compliance richtet sich demnach an alle Organisationen und Aktivitäten, die dem dritten Sektor zugerechnet werden können. Eingearbeitet sind auch Elemente aus den anderen beiden Sektoren, da die Arbeitsweise dieser Organisationen zum Teil übertragen werden kann. Oft sind bei Organisationen des dritten Sektors eine staatliche (Mit-) Trägerschaft, eine gewisse Gewinnerzielungsabsicht oder hohe Abhängigkeit von externem Mittelzufluss vorhanden, die eine wirtschaftliche Betrachtungsweise erfordern. Die Leitlinie ist durch den DICO-Arbeitskreis „NGO Compliance" erarbeitet worden und reflektiert die Erfahrungen und Expertise seiner Mitglieder.

NGOs haben im Vergleich zu wirtschaftlich tätigen Unternehmen einige besondere Compliance-Risiken, die sich aus ihrer Finanzierungsstruktur, ihrem gesellschaftlichen Auftrag und dem regulatorischen Umfeld ergeben. Zu den Herausforderungen gehören insbesondere:

- Große Abhängigkeit von Drittmitteln, wie Spendenmitteln durch private Geber*innen und öffentlichen Zuwendungen.
- Verstöße gegen Vorgaben bei der Verwendung von Spendengeldern und Fördermitteln. Verlust der Gemeinnützigkeit durch nicht zweckgebundene Mittelverwendung.
- Erhöhte Transparenz- und Rechenschaftspflichten gegenüber den öffentlichen Gebern und der Gesellschaft.
- Fehlverhalten bedroht das Vertrauen der Öffentlichkeit und Förderer, gefährdet die Reputation und kann die Existenz bedrohen.
- Umgang mit Dilemma-Situationen in nicht demokratischen Herrschaftsstrukturen (z. B. bei Zielkonflikten mit Gewinnorientierung sowie damit verbundenen Korruptionsrisiken).

- Bei länderübergreifender NGO-Tätigkeit, bei der finanzielle Mittel auch an andere Akteure weitergeleitet werden, gelten dieselben Anforderungen auch gegenüber Partnerorganisationen in diesen Ländern.
- Begrenzte finanzielle und personelle Ressourcen.
- Umgang mit Ehrenamtlichen, auf deren Engagement NGOs häufig angewiesen sind und die mit dem regulatorischen Umfeld und spezifischen Compliance-Risiken wenig vertraut sind.
- Der menschliche Faktor ist auch bei NGOs, wo hohe sinnstiftende Motivationen im Spiel sind, eine weitere zu beachtende Herausforderung. Wo sich Menschen engagieren, passieren Fehler (Fehlerkultur).

Die im folgenden aufgeführten Aspekte für Mindeststandards bei einem sektorspezifischen Compliance Management System (CMS) werden in den weiteren Kapiteln des Leitfadens detailliert behandelt:

- Insbesondere Mittelgeber aus der Wirtschaft und öffentlichen Stellen sind aufgrund interner Vorgaben, wie z. B. Richtlinien für Spenden sowie durch externe rechtliche Vorgaben verpflichtet, ihre Zuwendungen nur nach standardisierten Rahmenbedingungen an die jeweilige Durchführungsorganisation zur Verfügung zu stellen. Daher müssen NGOs (dokumentierte) Compliance-Mindeststandards zur Prävention vor besonders sensiblen Risiken aufsetzen. Machtmissbrauch, Korruption, mit oftmals vorgelagerten Interessenkonflikten, Unterschlagung und Betrug, Geldwäsche, aber auch der Umgang mit vertraulichen Daten und die IT Sicherheit sowie der Umgang mit KI sind wesentlich zu beachtende Risikothemen. Nicht weniger bedeutend sind hohe Standards bei der sog. „soft compliance“. Diese geben Orientierung zur erwarteten Einstellung, Haltung und den zentralen Werten der Organisation an Mitarbeitende (wie z. B. keine Duldung von Diskriminierung und Missbrauch, Förderung von Inklusion, nachhaltige Verfahren) sowie zum Umgang miteinander (wie z. B. Wertschätzung, Fehlerkultur, Speak-up-Kultur etc.). Diese Elemente prägen die Organisationskultur.
- Mit einem Code of Conduct (CoC) werden die Werte und der Umgang mit relevanten Compliance-Themen für die NGO kodifiziert und als Leitlinie nach innen verankert. So kann dieser eine gute Compliance nach innen sicherstellen und die gewünschte Außenwirkung erfüllen. Eine Checkliste „Bestandteile eines Verhaltenskodex für eine NGO“ steht in der Anlage als eigenes Hilfsmittel zur Verfügung.
- Um bestehende CMS-Rahmenwerke effektiv auf NGOs zuzuschneiden, bedarf es einer strategischen Ausrichtung auf sektorspezifische Herausforderungen und Vorsichtsmaßnahmen, welche die Integrität und Nachhaltigkeit von NGOs sicherstellen. CMS-Mindeststandards, die einem branchenweit akzeptierten Benchmarklevel entsprechen, sind durch spezifische Fokussierung auf bestimmte CMS-Elemente sicherzustellen. Einer spezifischen Risikoanalyse sollte ausreichend Gewicht beigemessen werden. Ferner gehören dazu die Entwicklung klarer Richtlinien, die Sorgfaltspflicht gegenüber Projekt- und Geschäftspartnern, angemessene Schulungen und proaktive Kommunikationsstrategien. Aufgrund oftmals sehr eingeschränkter personeller und finanzieller Mittel ist das CMS im höchsten Maße risikobasiert und proportional aufzusetzen. Dies kann mit einer strikten Fokussierung und klaren Priorisierung auf die relevanten Risiken und Ziele gelingen.

2. MINDESTANFORDERUNGEN AN EIN COMPLIANCE MANAGEMENT SYSTEM

Der Zweck eines Compliance Management Systems (CMS) ist primär ein Beitrag für die NGO und ihre Mitarbeitenden, im Einklang mit Recht, Gesetz und internen Regeln zu agieren.[1] Grundsätzlich ist jede*r Mitarbeitende verantwortlich für die Einhaltung dieser Regeln. Die Leitung der Organisation kommt ihrer Legalitätskontrollpflicht nach, indem sie Strukturen und Maßnahmen schafft, damit Fehlverhalten möglichst effektiv begrenzt werden kann. Das CMS der NGO soll die Geschäftsleitung bzw. den Vorstand dabei unterstützen durch seine Präventionswirkung Risiken zu mitigieren. Damit nicht jede Person in der Organisation verpflichtet werden muss, alle Regelungen und deren rechtliche Auslegung für das eigene Arbeitsgebiet selbst zu erarbeiten, ist eine angemessene und effektive Compliance-Struktur aufzubauen bzw. sind Compliance-Anforderungen in bestehende Strukturen angemessen und wirksam zu integrieren. Der sog. Prevent-Detect-Respond-Ansatz hat sich dabei bewährt, um präventive und kontrollierende Elemente zu kombinieren und das CMS kontinuierlich weiterzuentwickeln.

Den Ausgangspunkt für die Errichtung oder Weiterentwicklung eines CMS bildet eine Ist-Analyse bestehender Compliance-Elemente in der NGO. Nach dem IDW PS980 (Wirtschaftsprüfer-Standard für Compliance Managementsysteme) hat ein CMS sieben Elemente, um eine wirksame Compliance zu entfalten (bspw. Kultur, Kommunikation, Organisation, Risiken). Dieses Kapitel ist nach diesen Elementen aufgebaut und geht auf Schwerpunkte für NGOs ein.[2]

Wichtige Compliance-relevante Themen sind häufig schon adressiert (z. B. in einem Code of Conduct oder durch Schulungen zu einzelnen Richtlinien). Es bedarf daher zuerst eines Mappings, wo die Organisation in Bezug auf die folgenden Elemente steht. Daraus folgen die weitere Planung, Konzeption und Entwicklung des organisationsangepassten Managementsystems und der Implementierung seiner Elemente. Dieser Prozess lässt sich für jedes Compliance-Thema umsetzen, indem Maßnahmenbündel und themenbezogene Prozesse, evtl. auch eine eigene themenbezogene Organisation, bspw. im Datenschutz, entwickelt und etabliert werden kann.

Im Folgenden werden die Mindestanforderungen für ein Compliance Management System (CMS) für eine NGO skizziert, damit die jeweilige Organisation in die Lage versetzt wird, die für sie anwendbaren gesetzlichen Anforderungen, ethischen Standards und internen Richtlinien einzuhalten. Diese Vorgaben bauen auf den allgemein gültigen Normen des DICO für Compliance-Managementsysteme[3] auf.

2.1 Compliance-Kultur und -Ziele

Zunächst ist entscheidend, dass die Geschäftsleitung / der Vorstand ein klares Bekenntnis zur Compliance abgibt und Compliance vorlebt („Tone from the top“), den Begriff der „Compliance“ definiert sowie Compliance-Ziele vorgibt.

1 Vgl. DICO Standard CMS 2021.
2 Der IDW PS 980.2021 (Prüfungsstandard der Wirtschaftsprüfer für Compliance-Managementsysteme) versteht darunter ein Compliance-Programm, welches ein systematisches und zielgerichtetes Konzept ist, das zur Sicherstellung von gesetzlichen Vorgaben, internen Richtlinien, gesetzten Standards und ethischen Normen innerhalb einer Organisation eingesetzt wird. Es umfasst Maßnahmen zur Prävention, Aufdeckung und Reaktion auf Compliance-Verstöße.
3 Vgl. DICO-Standard CMS 2021.

Zur Analyse, ob und wie die gesetzten Ziele umgesetzt und Werte gelebt werden, können unterschiedliche Methoden angewendet werden, wie Beobachtung, Mitarbeitendenmeetings, Mitarbeitendenbefragung etc. Ist der Status quo erfasst, sollten Schritte geplant werden, die Compliance-Kultur und -Ziele zu verbessern und/oder stärker zu verankern.

Zentrale Fragen zu Compliance Kultur und Zielen einer NGO:

- Existiert ein Mission Statement und ein Code of Conduct, die der Tätigkeit und den selbst auferlegten Werten der Organisation entsprechen?
- Sind den Mitarbeitenden der NGO die oben genannten Dokumente und weitere Richtlinien bekannt? Werden sie als angemessen, verständlich und praktisch umsetzbar empfunden?
- Ist erkennbar, dass die Compliance-Ziele auf allen Ebenen der NGO verankert sind und gelebt werden?
- Welche Themen bzw. Gefahren oder Chancen sollen durch das CMS gesteuert und durch welche Maßnahmen nachgehalten werden?

Sektorspezifische Besonderheiten und Dilemmata:

- Selbstverständnis der NGO und Zielkonflikte: NGOs verfolgen gemeinnützige Ziele, können jedoch in Zielkonflikte geraten. Zur Zielerreichung dürfen keine Methoden eingesetzt werden, die gegen die Compliance-Standards der Organisation verstoßen. Eine Haltung nach dem Motto „der Zweck heiligt die Mittel“ ist zu vermeiden, um negative Folgen zu verhindern.
- Berücksichtigung dezentraler Strukturen: Bei der Entwicklung eines CMS ist es wichtig, sowohl die Zentrale als auch darunter liegende unselbständige Strukturen wie Orts- / Landesverbände (Deutschland) oder auch Regional- und Länderbüros (international) aktiv einzubeziehen. Lokale Gegebenheiten (insbesondere kultureller und rechtlicher Natur) sollten im Wirkbereich des CMS berücksichtigt und Maßnahmen (bspw. über Richtlinien) entsprechend angewandt werden, um ein einheitliches Verständnis sicherzustellen.
- Vertrauen zu Partnerorganisationen: NGOs arbeiten oft im Vertrauen mit Partnerorganisationen und leiten Mittel an diese weiter. Eine gründliche Due-Diligence-Prüfung der Partner ist unerlässlich. Um Compliance-Verstöße zu vermeiden, sollten auch während der Zusammenarbeit, regelmäßig überprüft werden, ob die ethischen und operativen Standards der Partner auch den eigenen entsprechen.

2.2 Compliance Risiken

Im nächsten Planungsschritt sind die Compliance Risiken festzustellen. Alle Risikofelder müssen in Bezug auf Tätigkeitsbereich, geografische Standorte und spezifische Projekte analysiert werden. Sofern bestimmte Compliance-Risiken bereits in einer allgemeinen Risikoanalyse der Organisation analysiert werden, ist diese auf Compliance-Relevanz zu überprüfen und ggfs. zu erweitern. Eine ausführlichere Betrachtung der Risikofelder ist in Kapitel 3 zu finden.

Grundsätzlich sollten folgende fünf Schritte für eine Compliance Risikoanalyse durchgeführt werden, um evtl. Lücken, Gefahren und Chancen zu identifizieren:

1. Identifikation des Compliance Risikos.
2. Priorisierung und Bewertung des Risikos.
3. Steuerung des Risikos.
4. Monitoring und systematische Überwachung.
5. Anpassung an aktuelle Entwicklungen.

Zentrale Fragen zu Compliance Risiken einer NGO:

- Gibt es eine regelmäßige Risikoanalyse, die den fünf oben genannten Schritten folgt?
- Sind die auf der Risikoanalyse basierenden Maßnahmen angemessen hinsichtlich der Art und des Umfangs der Tätigkeit der NGO? Sind sie angemessen hinsichtlich der zu erwartenden Schwere einer Verletzung und der Wahrscheinlichkeit des Eintritts einer Verletzung?
- Sind die getroffenen Präventionsmaßnahmen effektiv?

Sektorspezifische Besonderheiten und Dilemmata:

- Standardisierung und Ressourcen: Viele NGOs arbeiten mit begrenzten Ressourcen, was oft zu einem Mangel an Kapazitäten für umfassende und regelmäßige Risikoanalysen führt. Dies kann zu unvollständigen Analysen oder unzureichender Berücksichtigung zentraler Risiken führen.
- Finanzierung von Risikoanalysen: Es sollte stets geprüft werden, inwieweit die Kosten für Risikoanalysen auf Drittmittelgeber umgelegt werden können. Dies ist entscheidend, um ausreichende Ressourcen für effektive Risikoanalysen sicherzustellen.

Spezialfall: Spezifische Geschäftspartner-Compliance im Fall von Partnerorganisationen

Compliance-Risiken können organisationsintern entstehen, bspw. durch fehlende Zuständigkeiten oder Prozesse, aber auch von Dritten auf die NGO wirken. Das CMS muss in der Lage sein, den Überblick über die relevanten Compliance-Risiken der NGO zu gewährleisten und diese steuern zu können.

Der Umgang mit diesen Drittparteienrisiken kann in Form der „Geschäftspartner-Compliance“ strukturiert werden. Das Thema ist besonders für NGOs relevant, da ihr Geschäftserfolg zu großem Maß von dem in sie gesteckten Vertrauen abhängt, was auch durch Geschäftspartner beeinflusst wird. Denn eine Realisierung von Drittparteienrisiken kann das Vertrauen in die NGO wesentlich beeinträchtigen und zu nachhaltigen Schäden führen.

NGOs arbeiten im Rahmen von Lokalisierungsinitiativen zunehmend mit Partnerorganisationen vor Ort zusammen, die Projektaktivitäten oftmals besser umsetzen können, als internationale NGO selbst. In diesen Kooperationen können Risiken hinsichtlich der Rechtstreue des Projektpartners liegen, bspw. kann es im Verantwortungsbereich des Projektpartners zu Menschenrechtsverstößen (Erwachsenen- und Kinderrechte, sexuelle Gewalt) kommen, aber auch durch Versuche von Unterschlagung und Betrug.

Die Mindestanforderungen zur Drittparteien-Risikominimierung für NGOs stellen sich wie folgt dar:

- Bekenntnis des (zukünftigen) Partners zu den Grundprinzipien der NGO. Dabei sollten Minimalanforderungen der Prinzipien aus dem VENRO Verhaltenskodex bestätigt werden, insbesondere hinsichtlich Organisationsführung (soweit auf den Partner sinnvoll übertragbar), Kommunikation und Transparenz, Betriebsführung, Wirkungsorientierung und Verbindlichkeit.
- Standardklausel im Vertrag, durch die der NGO direkte Prüfungsrechte der Organisation des Projektpartners eingeräumt werden.
- Standardklausel im Vertrag, mit der der Partner verpflichtet wird, den (Whistleblower) Melde-Kanal der NGO auf seiner eigenen Website in Landessprache zu kommunizieren.
- Standardklausel im Vertrag, mit der Vereinbarungen im Fall von Unterbeauftragungen auch an Nachauftragnehmer weitergegeben werden müssen.
- Strukturierte und dokumentierte Prüfung, ob in der Vergangenheit Rechtsverstöße des (zukünftigen) Partners bekannt sind, einschl. Menschenrechtsverletzungen, die in seinem Einflussbereich verübt wurden. Dafür sollten alle öffentlich zugänglichen Informationen ausgewertet, sowie eine einheitliche Checkliste und eine durch die NGO vorgegebene Selbstauskunft des Partners angewendet werden.
- Verstetigung von Prüfungshandlungen auch in langfristigen Partnerschaften, in der Regel einmal jährlich. Die Prüfungshandlungen sollten möglichst immer wieder von anderen Beschäftigten der NGO vorgenommen werden.
- Trennung der ausführenden und überwachenden Funktionen in der Partnerorganisation („segregation of duties“ zur Vermeidung eines Governance Interessenkonfliktes): Soweit dies mit Hinblick auf die Größe des Partners realistisch ist, sollte der Betrieb eines Governance-Risk-Compliance (GRC-) Systems nach dem 3-Linien-Modell des Institute of Internal Auditors (IIA) sowie der Betrieb einer Revisionsfunktion durch den Partner vertraglich zugesichert werden.

2.3 Compliance Verantwortung und Organisation

Ein effektives und effizientes CMS erreicht seine Wirksamkeit über eine Compliance-Organisation dann, wenn klare Compliance-Aufgaben, -Verantwortungen und -Kompetenzen innerhalb der Organisation (Aufbauorganisation) allokiert, die notwendigen Ressourcen festgelegt und die Interaktion, also die Prozesse zwischen diesen Rollen (Ablauforganisation) geregelt sind. Um die Strukturen des CMS einer NGO effizient zu etablieren müssen ihre Organisationsform und ihre individuellen Besonderheiten berücksichtigt werden. Die individuelle Ausgestaltung der Compliance Organisation muss die Größe und Struktur der Organisation, wie die Anzahl der Mitarbeitenden, Anzahl der Ehrenamtlichen, Mittel der Organisation (Art und Vielfalt der Geldgeber) und das jeweilige Tätigkeitsfeld berücksichtigen. Gerade für kleinere und mittelgroße NGOs kann daher ein dezentraler Ansatz der Compliance-Organisation ressourcenschonender und sinnvoller sein als der zentrale Ansatz, der eher für große Organisationsformen geeignet ist.

Compliance Verantwortung

Im ersten Schritt benötigt es eine klare Compliance Verantwortung, die damit beauftragt wird, das CMS entsprechend der gesetzten Ziele auszugestalten oder zu errichten. Ihr wird der Compliance-Verantwortungsbereich „Betrieb des Compliance Management Systems“ mit entsprechenden Aufgaben zugewiesen und Kompetenzen zur Erfüllung der Aufgaben erteilt (vgl. Anhang).

Zentrale Fragen zur Compliance Verantwortung einer NGO:

- Sind Compliance Zuständigkeiten oder klare Rollen bzw. deren Funktionstrennung (zur Selbstkontrolle) in internen Regelwerken der NGO verankert?
- Wurden Compliance-Verantwortliche oder ein Compliance-Team mit einer Compliance-Verantwortung benannt, welche die Umsetzung und Überwachung des CMS verantwortet?
- Informiert die Geschäftsleitung / der Vorstand proaktiv über relevante Vorgänge und räumt der Compliance Funktion das Recht auf Einsicht in relevante Unterlagen ein?
- Gibt die Geschäftsleitung / der Vorstand regelmäßig und vor allem glaubwürdig ein Bekenntnis für Compliance und ethisches Verhalten ab? Je konkreter und praxisnäher der „Tone from the Top“ mit Beispielen unterlegt wird, desto überzeugender ist die Wirkung.

Sektorspezifische Besonderheiten und Dilemmata:

- Ressourcen für die Compliance Verantwortung: Die Kosten für eine dezidierte Compliance Funktion können (zu) hoch sein, insbesondere bei Bestrebungen, Verwaltungskosten niedrig zu halten. Ein dezentraler Ansatz, bei dem Verantwortlichkeiten auf verschiedene Stellen verteilt werden, kann hilfreich sein, um diese Herausforderung zu meistern. Um bei einer dezentralen Struktur Dilemmatasituationen zu verhindern, können die lokalen Compliance-Verantwortlichen durch eine „Compliance prevails“ Arbeitsanweisung gestärkt werden. Darin wird ihnen – ggf. unter bestimmten Voraussetzungen – die Befugnis eingeräumt, Vorgänge (in die Zentrale) zu eskalieren oder zu stoppen, um ein compliancewidriges Verhalten zu verhindern.
- Fachliche Voraussetzungen: Im NGO Sektor mangelt es an Expert*innen mit der notwendigen Expertise, die Compliance-Funktionen übernehmen und umsetzen können. Dies kann die Erreichung der Compliance-Ziele gefährden. Eine enge Abstimmung der Compliance-Ziele mit den finanziellen und personellen Ressourcen ist entscheidend für deren nachhaltigen Einsatz.
- Gewichtung von Werten und Qualifikationen: Bei der Besetzung von Compliance-Funktionen sollte ein Gleichgewicht zwischen der Identifikation mit den Grundwerten der NGO und der fachlichen Qualifikation gewahrt bleiben. Eine übermäßige Gewichtung der Werte kann die Compliance-Bemühungen der Organisation untergraben. Es ist wichtig, dass die Compliance-Funktion die Mission der NGO unterstützt, ohne die fachlichen Anforderungen aus den Augen zu verlieren.

Compliance-Organisation

Im nächsten Schritt wird die Compliance-Organisation ausgestaltet. Themenbezogene Zuständigkeiten und von den Zielen abgeleitete Leitplanken, Maßnahmen und Prozesse bilden das präventive und reaktive Compliance-Rahmenwerk in Form eines CMS.

Das CMS der NGO sollte daher immer dieser fortlaufenden Verbesserung im Sinne des PDCA-Zyklus[4] unterliegen, um systematisch Schwachstellen aufzudecken und Optimierungen verbindlich zu etablieren.

Zu den weiteren Aufgaben der Compliance-Organisation gehört es, Meldungen und Hinweise zu Compliance-Verstößen zu ermöglichen und mit angemessenen Folgemaßnahmen zu reagieren.

Zentrale Fragen zur Compliance-Organisation einer NGO:

- Sind die Informations- und Berichtswege zur Zielerreichung oder zu reaktiven Maßnahmen zwischen Geschäftsleitung/Vorstand, Mitarbeitenden, Externen und Compliance-Verantwortlichen geregelt?
- Ist geklärt, wie mit Compliance Meldungen umgegangen wird (es bewährt sich, diese nach Themenbereichen bzw. Art der Meldung zu regulieren)?
- Ist geregelt, wie mit potenziellen Verfehlungen der Führungskräfte oder von Mitgliedern der Geschäftsleitung umgegangen wird? Sind Berichtslinien entsprechend fixiert (bspw. dotted lines)? Hilfreich ist die Corporate Governance der NGO mit klaren Zuständigkeiten bzw. Verantwortungen der Organe zu regeln, die Funktionen zu trennen (bspw. Aufsichtsrat = Kontrollorgan, Geschäftsleitung = Exekutivorgan) und Berichtslinien daran auszurichten.
- Sind Kontrollprozesse beschrieben und ist klar wie und durch wen mit den Ergebnissen umgegangen wird?

Sektorspezifische Besonderheiten und Dilemmata:

- Ressourcenschwierigkeiten: Begrenzte finanzielle und personelle Ressourcen können die Umsetzung umfassender Compliance-Maßnahmen herausfordernd gestalten.
- Klare Definitionen: Es ist entscheidend, dass Abläufe / Prozesse, Zuständigkeiten und Aufgaben klar definiert sind, um die Effektivität der Compliance-Maßnahmen zu gewährleisten.
- Vielfalt der Mitarbeitenden: In NGOs arbeiten Menschen oftmals ehrenamtlich oder freiwillig mit begrenztem Zeiteinsatz. Auch diese Mitarbeitenden unterliegen den Compliance-Anforderungen und müssen hierzu geschult werden. Dies zu organisieren und nachzuhalten kann eine Herausforderung sein, die zusätzliche Ressourcen benötigt.

2.4 Compliance Kommunikation und Schulung

Im Bereich der Umsetzung und Implementierung der Compliance-Maßnahmen spielt eine gute Information und Sensibilisierung eine wichtige Rolle. Entscheidend im Bereich Schulung ist die zielgruppenorientierte Kommunikation und Verwendung geeigneter Instrumente, um Schlüsselbotschaften zu verankern. Entsprechende DICO-Standards enthalten hierzu wertvolle Informationen zur effektiven Gestaltung und Umsetzung von Kommunikations- und Schulungsmaßnahmen.

4 Der PDCA-Zyklus besteht aus vier Schritten: Plan (Planen): In diesem Schritt überlegt man sich, was erreicht werden soll und wie man das umsetzen kann. Do (Umsetzen): Hier werden die geplanten Schritte ausgeführt. Check (Überprüfen): Nachdem man den Plan umgesetzt hat, prüft man, ob es so funktioniert, wie man es geplant hat und ob das gewünschte Ergebnis damit erreicht wird. Man überprüft also die Ergebnisse und vergleicht sie mit dem ursprünglichen Ziel. Act (Handeln): Wenn das ursprüngliche Ziel erreicht wurde, kann die Praxis so in den laufenden Arbeitsprozess aufgenommen werden. Wenn es noch Verbesserungsbedarf gibt, passt man den Plan an und durchläuft den Zyklus erneut.

Zentrale Fragen zur Compliance-Kommunikation und Schulung einer NGO:

- Sind die Kommunikationswege zur Erreichung der Compliance-Ziele und der Integrität der Mitarbeiter*innen aufeinander abgestimmt und in einem Kommunikationskonzept erfasst?
- Gibt es einen Schulungsplan und berücksichtigt dieser die unterschiedlichen Zielgruppen?
- Wurde eine Zielvorgabe erstellt, die Aufschluss gibt, wer geschult werden soll mit welchem messbaren Ergebnis?
- Wurden angemessene, praktikable Tools zur Schulung identifiziert?
- Ist sichergestellt, dass die Schulungsteilnehmer*innen erfasst werden, um sich im Falle eines späteren Verstoßes entlasten zu können?

Sektorspezifische Besonderheiten und Dilemmata:

- Priorisierung von Compliance-Schulungen: Mitarbeitende sind oft stark in ihre Kernaufgaben eingebunden, was die Zeit für umfassende Compliance-Schulungen einschränkt. Um sicherzustellen, dass diese Schulungen die nötige Aufmerksamkeit erhalten, sollten folgende Maßnahmen ergriffen werden:
  1. Auswahl passender und leicht zugänglicher Formate einschließlich NGO-bezogener Beispiele und Anwendungsfälle.
  2. Verbindlichkeit der Schulungen zur Sicherstellung der Teilnahme.
  3. Kommunikation der Bedeutung von Compliance innerhalb der gesamten Organisation.
  4. Kluges Timing der Schulungen, um Überlastung zu vermeiden.
- Nutzung neuer Schulungstools: Am Markt sind verschiedene Software-Tools verfügbar, die Inhalte prägnant und ansprechend vermitteln. Obwohl diese zusätzlichen Kosten verursachen und Einarbeitung erfordern, sollten NGOs diese mit langfristiger Perspektive prüfen und einführen. Dies kann insbesondere ressourcenschwache Organisationen unterstützen, um eine nachhaltige Compliance-Schu lung zu gewährleisten.
- Wirksamkeit in Einsatzkontexten: In zeitkritischen Situationen z. B. der humanitären Hilfe, insbesondere bei plötzlichen Katastrophen, besteht die Gefahr ungewollter Regelverstöße. Kurze, kontinuierlich sichtbare Compliance-Botschaften (z. B. Aufkleber an Ausrüstung und in Büroräumen) können Mitarbeitende an wichtige Compliance-Prinzipien erinnern, ohne den Arbeitsablauf zu stören.
- Wissensvermittlung in kulturell diversifizierten und internationalen Teams: Unterschiedliche kulturelle Wahrnehmungen und Sprachbarrieren können das einheitliche Verständnis und die Umsetzung von Compliance-Themen erschweren. Im Deutschen klar definierte Begrifflichkeiten und Zusammenhänge können nicht immer 1:1 übersetzt, sondern müssen umschrieben werden. Beim Gestalten von Schulungsveranstaltungen sollten die verschiedenen kulturellen Kontexte, sowie das unterschiedliche Bildungs- und Sprachniveau der Mitarbeitenden berücksichtigt werden.

2.5 Compliance Überwachung und Verbesserung (Monitoring)

Das CMS kann die Compliance in der Organisation nur zuverlässig sicherstellen, wenn die Angemessenheit und Wirksamkeit der etablierten Maßnahmen regelmäßig überwacht, Schwachstellen identifiziert und Verbesserungsmaßnahmen zuverlässig etabliert werden. Monitoringmechanismen sollen also primär die Funktionsfähigkeit des CMS bewerten können.

Die Gestaltung des Monitorings orientiert sich an der Vermeidung und Aufdeckung von Compliance Vorfällen, was von den spezifischen Risiken der NGO abhängt.

Im NGO-Sektor bietet es sich an, über Interviews oder Befragung mittels Fragebogen die Mitarbeitenden die umgesetzten Maßnahmen in den verschiedenen Compliance Bereichen auf ihre Funktionsfähigkeit bewerten und mögliche Lücken identifizieren zu lassen. Ein weiteres wichtiges Element für die Wirksamkeit ist der Betrieb einer internen Meldestelle bei der Compliance-Verantwortung. Diese ermöglicht einen strukturierten Feedback-Prozess für das CMS, bei dem Hinweise zu Fehlverhalten oder Verstößen direkt in präventive Folgemaßnahmen übertragen werden können. Neben der vorbeugenden Funktion ist auch die reaktive Funktion der Meldestelle sehr bedeutend für die Wirksamkeit der Compliance in der NGO, da mit sofortigen Abhilfemaßnahmen reagiert werden kann und Signale in die Belegschaft gesendet werden können, dass Verstöße nicht geduldet werden (was wiederum auf die Compliance-Kultur einwirkt). Um Synergien zu nutzen, kann in der internen Meldestelle das Hinweisgebermanagement betrieben und zugeordnet werden, das nach dem HinSchG[5] für die NGO in der Regel Anwendung findet.

Zentrale Fragen zur Compliance Überwachung in einer NGO:

- Wurden die zentralen Fragen der anderen CMS Elemente und die sich daraus ergebenden Mindestanforderungen umgesetzt?
- Wurden vereinbarte Ziele der Compliance Arbeit erreicht (z.B: Mitarbeitendenschulungen)?
- Wurden Standards und Handlungsempfehlungen, die typische Risikobereiche der NGO betreffen, umgesetzt? (vgl. Kapitel 3)
- Kommen Mechanismen zum Einsatz, die die Funktionsfähigkeit des CMS beurteilen?
- Bewertet die Geschäftsleitung/Vorstand regelmäßig das bestehende CMS anhand von Berichten, die sie von Compliance Verantwortlichen erhalten?
- Sind neue regulatorische Anforderungen entstanden, die angepasste oder neue Compliance-Maßnahmen erfordern (z. B.: neuen Standort im Ausland eröffnet, Änderungen in der Gesetzgebung)?
- Gibt es eine Ebene außerhalb der Compliance-Funktion, die die Wirksamkeit des CMS überwacht, wie z. B. eine Interne Revision und werden hier regelmäßige Bewertungen des CMS erstellt und die Empfehlungen in das CMS integriert?

Sektorspezifische Besonderheiten und Dilemmata:

- Ressourcenschwäche und Kontrollmechanismen: Die Einführung effizienter EDV-Systeme und die Schulung der Mitarbeitenden sind anfangs kostenintensiv, sollten jedoch als langfristige Investition betrachtet werden, die sich auszahlt. Es ist ratsam, Unternehmen zu gewinnen, die die NGO pro bono bei der Implementierung neuer Systeme und Tools unterstützen.
- Betriebsblindheit: Aufgrund von Personal- oder Zeitknappheit neigen NGOs dazu, bestehende Situationen und Arbeitsweisen nicht kritisch zu hinterfragen. Eine Neubewertung und Anpassung von Routinen kann zunächst zeitaufwändig sein, ist jedoch essentiell, um geänderten Rahmenbedingungen Rechnung zu tragen.

5 Hinweisgeberschutzgesetz (HinSchG), vgl. DICO-Standard S11 Hinweisgebersysteme.

- Zertifizierungen im gemeinnützigen Sektor: Es gibt zahlreiche Zertifizierungsstellen für NGOs, die extern das CMS einer NGO prüfen und deren Prozesse oft langwierig und kostenintensiv sind. NGOs sollten sorgfältig abwägen, welche Zertifizierungen a) für ihr Kerngeschäft relevant sind und somit zur Reputation beitragen, und b) sie in eine bessere Position bei der Mittelbeantragung wichtiger Geber bringen.

3. RISIKOMANAGEMENT

3.1 Sektorspezifische Risikoanalyse

Vor dem Hintergrund der stetig steigenden regulatorischen Komplexität gewinnt die Risikoanalyse als Instrument des strategischen Risikomanagements und als Grundlage für ein vorausschauendes Compliance-Management zunehmend an Bedeutung. Eine Compliance-Risikoanalyse ist die systematische Identifizierung, Bewertung und Dokumentation potenzieller Risiken, die sich auf die Reputation einer Organisation auswirken und rechtliche Konsequenzen nach sich ziehen können.

Ziel der Risikoanalyse ist es,

- mögliche Schwachstellen in der Organisation zu identifizieren. Damit schafft die Risikoanalyse die Grundlage für ein präventives Risikomanagement durch geeignete und wirksame Maßnahmen.
- Ressourcen möglichst effizient und sinnvoll einzusetzen. Sie bildet die Ausgangsbasis für Entscheidungen über notwendige Ressourcen und die Festlegung von Verantwortlichkeiten und deren Verankerung in den relevanten Organisationsprozessen.

Die Risikoanalyse erfolgt auf Basis einer Relevanzanalyse bzw. eines Scopings: Die Relevanzanalyse ist eine erste Einschätzung auf Basis allgemeiner und leicht zugänglicher Informationen, in welchen Themenfeldern Compliance-Vorfälle auftreten können. Grundlage einer solchen Analyse können Unterlagen relevanter Organisationsfunktionen (z. B. Interne Revision, Rechtsabteilung, Risikomanagement, Internes Kontrollsystem, Hinweisgebersystem) über bereits eingetretene Compliance-Vorfälle oder Schwachstellen sein.

Folgende Fragen können helfen, Risikobereiche zu identifizieren:

- Welche Gesetze und Vorschriften sind für die Organisation relevant?
- Welche Produkte und Dienstleistungen werden angeboten?
- In welchen Ländern ist die Organisation direkt oder indirekt tätig?
- Über welche Mittelquellen verfügt die Organisation? (Zuschüsse, Subventionen / Fördermittel, Spenden, etc.)
- Welche Größe (Mitarbeitende, Umsatz) hat die NGO?

Sektorspezifische Besonderheiten im Rahmen der Arbeit von NGOs sind u.a.:

- Bedeutung des Länderrisikos: In der Compliance-Risikoanalyse spielt das Risikoprofil des jeweiligen Einsatzlandes eine entscheidende Rolle. Risiken wie politische Instabilität, zunehmende Einschränkung der Handlungsspielräume (Shrinking Space), Korruption oder schwache staatliche Institutionen können die Compliance-Risiken deutlich erhöhen und erfordern besondere Maßnahmen. Hinzu kommt die unterschiedliche Gesetzgebung in anderen Ländern, die nicht immer der deutschen Rechtslage entspricht, z.B Vorgaben zum Datenschutz, Regelungen zum Hinweisgeberschutz.
- Dynamische Risikolage in instabilen Kontexten: International tätige NGOs arbeiten oft in instabilen Regionen, in denen sich die Compliance-Risiken, etwa durch plötzliche politische Veränderungen, veränderte Sicherheitslage, besondere Naturereignisse, Shrinking Space oder wirtschaftliche Unsicherheit, rasch ändern können. Dies bedingt die Notwendigkeit, situationsbezogene Risikoanalysen durchzuführen. Da im Einsatz jedoch oft die zeitlichen und personellen Kapazitäten knapp sind, sollten NGOs diesen Bedarf frühzeitig und strategisch einplanen, um flexibel und schnell auf sich ändernde Risiken reagieren zu können.
- Abhängigkeit von Drittmitteln, Rechenschaftspflicht und Gemeinnützigkeit: Können alle regulatorischen Anforderungen eingehalten werden? Werden lokale rechtliche Sachverhalte und Gegebenheiten außer Acht gelassen, um die Zielvorgaben eines genehmigten Projektes (Zeitplan der Implementierung und weitere Indikatoren) zu erreichen? Werden Mittel, die aus dem Bereich der Gemeinnützigkeit stammen, nicht zweckgebunden, sondern außerhalb der gemeinnützigen Sphären eingesetzt? Dies kann zu steuerrechtlichen Konsequenzen und zum Verlust der Gemeinnützigkeit führen.
- Arbeit mit Ehrenamtlichen und Freiwilligen: Ehrenamtliche bzw. freiwillige Mitarbeitende werden häufig nicht systematisch in Regelwerke, Schulungen oder Prozesse eingebunden. Es fehlen zum Teil klare Zuständigkeiten, und die Sensibilisierung für Compliance-Themen ist dadurch begrenzt. Durch hohe Fluktuation und kurze Einsatzzeiten entstehen zusätzliche Risiken, etwa durch unzureichende Einarbeitung oder fehlenden Wissenstransfer.
- Dezentrale Strukturen: Beim Arbeiten in dezentralen Strukturen mit Mitarbeitenden, die womöglich weit entfernt von der dezidierten Compliance-Funktion tätig sind, kann die Wirksamkeit des CMS durch den fehlenden regulären Kontakt und das Monitoring abnehmen und Richtlinien und Vorgaben zunehmend ignoriert werden.

3.2 Risikogebiete und Risikominimierung

Im Folgenden werden die wichtigsten Risiken kurz erläutert und mögliche Schutzmaßnahmen beschrieben. Zu den meisten Risiken existiert ausführliche Literatur, die für ein vertieftes Verständnis des Themas genutzt werden kann.

3.2.1 Korruption

Korruption – der Missbrauch anvertrauter Macht zum privaten Vorteil oder Nutzen[6] – ist weltweit ein großes Problem. Für NGOs birgt sie besondere Risiken, insbesondere in Ländern mit schwachen staatli

6 Definition nach Transparency International.

chen Strukturen oder instabilen politischen Verhältnissen. Dort laufen sie Gefahr, entweder ungewollt in Korruptionssysteme verstrickt zu werden oder durch interne Schwachstellen selbst Korruptionsfälle zu verursachen.

NGOs verwalten oft erhebliche Spenden- und Fördermittel, die für konkrete Projekte oder Hilfsmaßnahmen bestimmt sind. Ihre Aufgabe ist es sicherzustellen, dass diese Gelder ausschließlich dem vorgesehenen Zweck dienen. Schon der bloße Verdacht auf Korruption kann das Vertrauen von Spender*innen, Partnern und der Öffentlichkeit massiv beschädigen und schwerwiegende Konsequenzen für die Organisation nach sich ziehen.

Korruption zeigt sich in vielen Formen. Grundsätzlich wird unterschieden zwischen aktiver und passiver Korruption. Aktive Korruption liegt vor, wenn Mitarbeitende Dritten einen Vorteil anbieten oder gewähren, um Einfluss auf deren Entscheidungen zu nehmen. Passiv korrupt handelt, wer Vorteile einfordert, annimmt oder sich versprechen lässt, um im Gegenzug seine berufliche Stellung zum Vorteil anderer einzusetzen. Solche Vorteile können materiell sein – wie Geld, Geschenke oder private Fahrzeugnutzung – oder immateriell, etwa durch berufliche Gefälligkeiten oder persönlichen Einfluss.

Besonders risikobehaftet ist in diesem Zusammenhang der Umgang mit Amtsträgern. Nach dem Strafgesetzbuch sind bereits Vorteile strafbar, die als Gegenleistung für die „allgemeine“ Dienstausübung des Amtsträgers erfolgen, als Handlungen, durch die ein Amtsträger die ihm übertragenen Aufgaben im Rahmen seiner Zuständigkeit wahrnimmt. Nicht erforderlich ist der Bezug zu einer konkreten Diensthandlung. Daher ist bereits die Pflege der Geschäftsbeziehung nur um dem Projektziel zu dienen, gut gemeinte Geschenke an Beamte, um Abläufe zu beschleunigen oder Entscheidungen zu beeinflussen, z. B. durch Einladungen zu Veranstaltungen, unzulässig und können strafrechtliche Folgen haben (Vorteilsannahme / Vorteilsgewährung). Das bedeutet für die NGO, dass Situationen, die den Anschein einer Vorteilsannahme oder Vorteilsgewährung bzw. Bestechung und Bestechlichkeit erwecken, zu identifizieren sind. Dies kann über die Risikosteuerung von Interessenkonflikten sinnvoll gelingen, vor allem weil diese ein häufig unterschätztes Risiko im Vorfeld von potenziellen Korruptionssachverhalten darstellen.

Ein Interessenkonflikt liegt vor, wenn persönliche Interessen, private Belange oder anderweitige Aktivitäten eines Mitarbeitenden mit den Interessen der NGO, auch im internationalen Organisationskontext, in Konflikt geraten. Bei einem Interessenkonflikt überlagern subjektive Erwägungen die für Weichenstellungen und Entscheidungen zur Verfolgung des NGO Auftrags notwendige Objektivität.

Private Interessen und persönliche Vorteile dürfen niemals Entscheidungen im Rahmen der NGO-Tätigkeiten beeinflussen. Das heißt: Entscheidungen sind stets objektiv und unabhängig von eigenen unmittelbaren oder mittelbaren Vorteilen zu treffen. Sie sollen ausschließlich im Interesse der NGO – auf Basis ihrer Werte, Integrität und Verhaltensweisen, häufig kodifiziert in einem für alle MitarbeiterInnen geltenden Verhaltenskodex (CoC),[7] erfolgen.

7 Eine Stuktur für einen Muster Code of Conduct für NGOs findet sich im Anhang.

Klassische Konstellationen einer NGO, bei der ein potenzieller Interessenkonflikt gegeben sein kann:

- Annahme finanzieller Mittel öffentlicher und privater Geber.
- Vergabe finanzieller Mittel, von Sachmitteln, von Services und Hilfe in Erfüllung des NGO-Auftrags und Vergabeprozesses.
- Aufnahme und Unterhaltung von Beziehungen mit Partnerorganisationen und Kooperationspartnern weltweit.
- Annahme oder Vergabe von Sachzuwendungen (wie Geschenke und Einladungen).
- Umgang mit Mandats- und Amtsträgern.
- Aufnahme von Nebentätigkeiten.
- Organmitgliedschaft und gleichzeitige Spender- oder Beratungstätigkeit.
- Umgang mit Familienangehörigen und Freunden von Mitarbeitenden.

Bewährte Praktiken im Umgang mit Interessenkonflikten:

- Transparentes Handeln und Einhalten von Verhaltenskodizes, bspw. organisationseigener Code of Conduct oder Verhaltenskodex aus dem Lobbyregister.
- Trennung von beruflichen und privaten Rollen, aber auch von politischen Rollen, sofern vorhanden.
- Etablieren von Richtlinien, Schulungen und Sensibilisierungsmaßnahmen für betroffene Zielgruppen in der NGO. Konsequente Dokumentation rechenschaftspflichtiger Transaktionen.

Treten potenzielle Interessenkonflikte dennoch auf, weil sie unvermeidbar sind, ist Transparenz oberstes Gebot: Eine unaufgeforderte Offenlegung gegenüber der Führungskraft oder dem betreffenden Organ oder Gremium ist erforderlich. Um spätere Unklarheiten zu vermeiden, sollte die Offenlegung schriftlich dokumentiert werden. Alternativ kann in der Regel auch die Compliance-Funktion[8] einen professionellen und fairen Umgang unter Beachtung der internen Regelungen sowie von Gesetz und Recht unterstützen.

In der Praxis zeigt sich, dass gerade NGOs in bestimmten Situationen besonders anfällig für Korruption sind. Dazu gehören Hilfslieferungen in Krisengebiete, bei denen Behörden oder lokale Gruppen Zahlungen verlangen, um Transporte durchzulassen. Auch schwache interne Kontrollen bergen Gefahren: Fehlende Transparenz, unzureichende Buchhaltung oder ausbleibende Audits begünstigen, dass Gelder über Jahre hinweg zweckentfremdet werden. Besonders heikel wird es, wenn Spendengelder ohne klare Nachverfolgbarkeit eingesetzt werden und so indirekt sogar Korruptionszahlungen ermöglicht werden – etwa an Politiker*innen oder Entscheidungsträge*innen vor Ort.

Auch international gelten strenge Vorschriften: Der US-amerikanische „Foreign Corrupt Practices Act“ (FCPA) etwa verbietet Bestechungen gegenüber ausländischen Amtsträgern und verpflichtet Unternehmen – und auch NGOs mit US-Bezug – zur genauen Buchführung.

Ähnlich weitreichend ist der britische „UK Bribery Act“, der weltweit greift, wenn Organisationen in irgendeiner Form im Vereinigten Königreich aktiv sind. Auch in den Einsatzländern international tätiger NGOs gibt es häufig weitreichende Gesetze gegen Korruption.

8 Siehe dazu im Anhang auch eine Profil-Beschreibung für einen Compliance-Beauftragten oder -Manager.

Für NGOs bedeutet das: Ein wirksames Antikorruptionsprogramm ist heute Pflicht – nicht nur aus juristischen Gründen, sondern auch, um die eigene Glaubwürdigkeit zu schützen und Vertrauen bei Förderern und Partnern aufzubauen. Ein solches Programm umfasst klare Regeln, systematische Risikoanalysen, transparente Abläufe und regelmäßige Schulungen. Internationale Standards, wie die ISO 37301, bieten dabei eine gute Orientierung.

Ein zentrales Instrument jeder Organisation sollte eine verbindliche Antikorruptionsrichtlinie sein. Eine Vorlage zu Erstellung einer solchen Richtlinie findet sich im Anhang. Sie schafft klare Verhaltensregeln für alle Mitarbeitenden, definiert den Umgang mit Zuwendungen, Geschenken und Einladungen und regelt, wie meist vorausgehende Interessenkonflikte erkannt und gemeldet werden. Auch der sorgfältige Umgang mit Geschäftspartnern und regelmäßige Due-Diligence-Prüfungen sollten fester Bestandteil dieser Richtlinie sein.

Sollten trotz aller Vorsichtsmaßnahmen dennoch Verdachtsfälle auftreten, ist es wichtig, professionell und konsequent zu reagieren. Aus jedem Vorfall sollten klare Lehren gezogen und interne Prozesse gegebenenfalls angepasst werden.

Viele Geldgeber – von der Europäischen Union über nationale Ministerien bis zur Weltbank – verlangen heute längst den Nachweis wirksamer Antikorruptionsmechanismen. Sie fordern transparente Dokumentationen, funktionierende Kontrollsysteme und Hinweisgebersysteme (Whistleblowing), damit Verstöße frühzeitig erkannt und gemeldet werden können.

Spezialfall „Interessenkonflikte und Lobbyarbeit“
NGOs und die Politik sind auf einen guten und vertrauensvollen Informationsaustausch angewiesen. NGOs benötigen vom Staat vor allem verlässliche rechtliche, operative und datenbasierte Informationen, um wirksam und compliant zu arbeiten. Daher kann Lobbyarbeit ein wichtiges Instrument für NGOs sein, um Gelder zu generieren. Bspw. können Großspender politische Ziele verfolgen und entsprechend Einfluss auf Positionen oder Programme der NGO nehmen wollen. Auch Kooperationen mit Akteuren der Privatwirtschaft können Abhängigkeiten schaffen oder politisch motiviert sein. Die hieraus entstehenden Risiken sind eng mit Korruptionsrisiken für die NGO verbunden, weil sie ebenfalls aus potenziellen Interessenkonflikten entstehen.

Die Lobbylandschaft in Deutschland umfasst inzwischen verschiedene Spezialregelungen, indem die unzulässige Interessenwahrnehmung strafbewehrt gestellt wurde (§ 108 f StGB) oder eine fehlende oder mangelhafte Eintragung im Lobbyregister des Bundes bußgeldbewehrt ist. Lobbyaktivitäten müssen bspw. öffentlich gemacht werden und Stellungnahmen von Verbänden zu Gesetzesentwürfen mit diesen gemeinsam veröffentlicht werden. Politiker und Beamte (oft Amtsträger) unterliegen strengen Regeln hinsichtlich ihrer Beteiligung in der Privatwirtschaft oder in gemeinnützigen Organisationen, um ihre Unabhängigkeit zu sichern. Diese Vorgaben und entsprechende Praktiken zur Vermeidung bzw. zum Umgang mit diesen Konstellationen sind im Compliance-Programm der NGO zur Lobbyarbeit zu identifizieren und aufzunehmen. Sofern die NGO im Lobbyregister eintragungspflichtig ist, ist ein regelmäßiger Aktualisierungsprozess zu etablieren und der Verhaltenskodex des Lobbyregisters verbindlich zu verankern.

Spezialfall „Interessenkonflikte Compliance-Beauftragter“
Compliance-Beauftragte übernehmen in NGOs oft mehrere Funktionen und Aufgaben oder sie sind in Themen involviert, in denen sie teils widersprüchlichen Interessenlagen ausgesetzt sind. Die Compliance-Arbeit kann diese Personen dadurch schnell in einen Interessenkonflikt bringen oder ein Dilemma erzeugen. Diesem Thema widmet sich das DICO-Arbeitspapier "A23 – What keeps you up at night? Hilfsmittel für Compliance Officers im Umgang mit Ihren Interessenkonflikten und Dilemmata". Darin sind Lösungsansätze zu finden, wie Compliance-Beauftragte mit diesen Situationen umgehen können.

3.2.2 Geldwäsche und Terrorismusfinanzierung

Geldwäsche und Terrorismusfinanzierung gehören weltweit zu den größten Herausforderungen für Sicherheit, Gesellschaft und Wirtschaft. Kriminelle Netzwerke und terroristische Gruppen nutzen Geldströme, um ihre Aktivitäten zu finanzieren, sich Zugang zu Ressourcen zu verschaffen und ihre Organisationen weiter auszubauen. Dabei fließen die Gelder häufig durch scheinbar legale Kanäle – und genau hier geraten auch internationale Nichtregierungsorganisationen ins Visier.

NGOs arbeiten oft in Krisen- und Konfliktgebieten und leisten dort lebenswichtige Hilfe. Genau diese Nähe zu betroffenen und schwer kontrollierbaren Regionen birgt Risiken: Es kann passieren, dass Organisationen – ob bewusst oder unbewusst – in Geldwäsche- oder Terrorismusfinanzierung verstrickt werden. Kriminelle Gruppen versuchen beispielsweise, lokale Partner-NGOs als Tarnung zu nutzen oder über Spendenkanäle illegale Gelder zu schleusen.

Besonders gefährlich wird es, wenn Hilfsgelder in Regionen gelangen, die unter der Kontrolle terroristischer Organisationen stehen. Dort ist es oft kaum möglich, vollständig auszuschließen, dass Projekte oder Ressourcen am Ende von diesen Gruppen missbraucht werden. Selbst bei bester Absicht besteht das Risiko, dass Gelder für illegale Zwecke zweckentfremdet werden – mit schwerwiegenden Folgen für die Organisation und die betroffenen Menschen.

Die Konsequenzen solcher Vorfälle können dramatisch sein: Reputationsschäden, rechtliche Verfahren, der Verlust von Fördermitteln oder der Ausschluss von Finanzdienstleistungen.

Die Gefahr der Terrorismusfinanzierung in diesem Sektor stellt zudem nicht nur eine erhebliche Bedrohung für die wirksame Hilfeleistung dar, sondern gefährdet auch die Sicherheit der Mitarbeitenden vor Ort, wenn diese mit den terroristischen oder kriminellen Aktivitäten in Verbindung gebracht werden können.

Deshalb sind NGOs verpflichtet, nationale und internationale Gesetze zur Verhinderung von Geldwäsche und Terrorismusfinanzierung einzuhalten – darunter das deutsche Geldwäschegesetz, EU-Verordnungen, UN-Resolutionen sowie Vorgaben aus allen Ländern, in denen sie aktiv oder Geldgeber ansässig sind oder aus denen Mitarbeitende stammen.

Um diese Risiken effektiv zu minimieren, müssen NGOs klare Strukturen schaffen und vorbeugende Maßnahmen umsetzen. Grundlage ist eine umfassende Risikoanalyse: Wo arbeitet die Organisation? Gibt es Länder oder Regionen mit erhöhtem Risiko? Gibt es auffällige Zahlungen, große Bargeldtransfers oder anonyme Spender? Werden alle Partner und Lieferanten ausreichend geprüft?

Wichtig ist auch ein konsequenter „Know Your Customer" (KYC)-Prozess. Das bedeutet: Alle Mitarbeitenden, Geldgeber, Partnerorganisationen und deren zentrale Mitarbeitende und Dienstleister müssen identifiziert, geprüft und mit internationalen Sanktionslisten abgeglichen werden. Je nach Risiko und Umfang der Zusammenarbeit können zusätzliche Hintergrundrecherchen notwendig sein.

Ein weiterer Schwerpunkt liegt auf der Transparenz und Nachvollziehbarkeit aller Finanzströme. Bargeld sollte – wo immer möglich – vermieden werden. Stattdessen braucht es klare Regeln, Kontrollmechanismen und ein Monitoring, damit jederzeit nachvollzogen werden kann, wo Gelder hingehen und wofür sie verwendet werden. Besonders bei Projekten in Risikogebieten sollten regelmäßige Vor-Ort-Kontrollen und strikte Rechenschaftspflichten eingeplant werden.

Zentral ist außerdem die regelmäßige Schulung aller Mitarbeitenden – besonders derer, die in Risikogebieten arbeiten oder mit der Abwicklung von Finanztransaktionen befasst sind. Nur wer die Gefahren kennt, kann Risiken erkennen und entsprechend handeln. Ergänzt wird das durch ein funktionierendes Hinweisgebersystem, über das verdächtige Aktivitäten vertraulich gemeldet werden können.

Alle diese Maßnahmen sollten fest im Compliance-Management der Organisation verankert sein. Dazu gehören klare Richtlinien, regelmäßige Risikoanalysen und – wo möglich – der Einsatz von IT-Tools, die Transaktionen überwachen und automatisierte Prüfungen gegen Sanktionslisten ermöglichen. Auch die regelmäßige Veröffentlichung von Finanzberichten sowie externe Prüfungen stärken Transparenz und Vertrauen.

Schließlich sollte jede NGO vorbereitet sein, wenn ein Verdachtsfall auftritt. Ein Notfallplan regelt, wie die Organisation reagiert, wen sie informiert und wie sie mit Behörden zusammenarbeitet.

Der Schutz vor Geldwäsche und Terrorismusfinanzierung ist für NGOs eine zentrale Aufgabe. Nur wer Risiken frühzeitig erkennt, professionell vorbeugt und im Ernstfall konsequent handelt, schützt die eigene Organisation, sichert die Hilfe für betroffene Menschen und wahrt das Vertrauen von Spendern und Partnern.

3.2.3 Menschenrechte und Diskriminierung jeder Art

Menschenrechte und Diskriminierung sind eng miteinander verknüpft. Menschenrechte sind Grundrechte, die jedem Menschen unabhängig von Herkunft, Geschlecht, Religion, Alter, Behinderung, sexueller Orientierung oder anderen Merkmalen zustehen. Sie sind in internationalen Dokumenten wie der Allgemeinen Erklärung der Menschenrechte (AEMR) verankert. Diskriminierung hingegen bedeutet, dass eine Person oder eine Gruppe von Personen aufgrund bestimmter Merkmale benachteiligt oder ungerecht behandelt wird.

Diskriminierung kann sich in viele Formen äußern, darunter:

- ***Direkte Diskriminierung:*** Wenn eine Person aufgrund eines bestimmten Merkmals schlechter behandelt wird als eine andere Person in einer vergleichbaren Situation.
- ***Indirekte Diskriminierung:*** Wenn eine scheinbar neutrale Regelung oder Praxis Personen mit bestimmten Merkmalen benachteiligt.
- ***Belästigung:*** Unerwünschte Verhaltensweisen, die ein von Einschüchterungen, Anfeindungen oder Erniedrigungen gekennzeichnetes Umfeld schaffen.
- ***Mobbing:*** Wiederholtes, schikanierendes Verhalten, das darauf abzielt, eine Person zu verletzen oder zu demütigen.

Die Förderung der Verbesserung der Menschenrechtssituation in der Welt ist oft ein inhärentes Ziel einer NGO. Gerade deshalb stehen die Glaubwürdigkeit und die Reputation einer NGO bei diesem Thema im Vordergrund. Es geht also nicht nur um die Förderung der Menschenrechte im Rahmen der Aufgabenerfüllung, sondern um die Sicherstellung der Einhaltung der Menschenrechte in allen direkten und indirekten Geschäftstätigkeiten.

NGOs sollten daher folgende risikominimierende Maßnahmen umsetzen, um Menschenrechtsverletzungen und Diskriminierungen im Rahmen ihrer Geschäftstätigkeit vorzubeugen:

- Ein klares und öffentlich kommuniziertes Bekenntnis zur Achtung der Menschenrechte, das im Leitbild und in der Mission der Organisation verankert ist.
- Regelmäßige Durchführung von Risikoanalysen und Implementierung von Sorgfaltspflichtprozessen, um potenzielle Menschenrechtsverletzungen und Diskriminierungen sowohl im Rahmen der eigenen Geschäftstätigkeit als auch bei Partnerorganisationen zu identifizieren und zu bewerten.
- Regelmäßige Sensibilisierung und Schulung der Mitarbeitenden, um das Bewusstsein für Menschenrechte zu schärfen und sicherzustellen, dass alle Beteiligten die Richtlinien und Verfahren verstehen und einhalten.
- Einrichtung sicherer und leicht zugänglicher Beschwerdemechanismen, die es Betroffenen ermöglichen, Menschenrechtsverletzungen und Diskriminierungen zu melden. Diese Mechanismen sollten transparent und vertrauenswürdig sein.
- Regelmäßige Berichterstattung über die Maßnahmen und Fortschritte im Bereich der Menschenrechte, um Transparenz zu gewährleisten und das Vertrauen der Stakeholder zu stärken.

3.2.4 Safeguarding: Gewalt gegen Kinder und Jugendliche

In jedem Land und jeder Gesellschaft sind Kinder von Gewalt betroffen, unabhängig von Alter, Geschlecht, Herkunft, Hautfarbe, Religion, kulturellem und sozialem Hintergrund, Behinderung oder sexueller Orientierung. Laut Angaben der Weltgesundheitsorganisation werden beispielsweise rund 20 % aller Mädchen und etwa 8 % aller Jungen weltweit Opfer von sexueller Gewalt. Manche Kinder sind aufgrund von bestimmten Charakteristiken und Kontexten einem besonderen Risiko ausgesetzt. So sind bspw. Kinder mit

Behinderungen zweimal so häufig betroffen wie Kinder ohne Behinderungen. Die Dunkelziffer ist dabei um ein Vielfaches höher. Diskriminierung und Vorurteile können dazu führen, dass besonders schutzbedürftige Kinder nicht den notwendigen Schutz erfahren. Viele Fälle von Gewalt werden gar nicht oder erst sehr spät bekannt. Zudem unterliegen Kinder, die in Institutionen gefördert oder anderweitig in einer Einrichtung betreut werden, einem erhöhten Risiko, Opfer von Gewalt zu werden. Unabhängig von den unterschiedlichen Risikofaktoren steht allen Kindern das gleiche Recht auf Schutz zu. Im Kontext einer zunehmenden Digitalisierung ist es insbesondere von Bedeutung, die Risiken für den Kinderschutz in der Kommunikation stets in seiner gesamten Dimension abzuwägen und zu bedenken.

Organisationen der internationalen Zusammenarbeit und der Humanitären Hilfe sowie deren lokale Partnerorganisationen sind dabei in besonderer Weise herausgefordert. Sie arbeiten oftmals in Kontexten – etwa in oder nach Katastrophen – in denen der Schutz von Kindern schwierig ist und in den Hintergrund zu geraten droht. Daher kommt es auch vor, dass potenzielle Täter*innen über diese Organisationen Zugang zu Kindern suchen. Die Organisationen tragen entsprechend eine besondere Verantwortung dafür, dass alle Kinder (einschließlich der besonders vulnerablen Gruppen), mit denen sie direkt arbeiten, mit denen sie Kontakt haben oder die von ihrer Arbeit berührt werden, sicher und geschützt sind. Sollten trotz aller präventiver Maßnahmen Fälle von Gewalt auftreten, liegt es an ihnen, Sorge zu tragen für die Unterstützung, die das betroffene Kind braucht. Darüber hinaus müssen sie geeignete Schritte ergreifen, um die Verursacher:innen einer angemessenen Sanktion beziehungsweise strafrechtlichen Verfolgung zuzuführen.

Alle Mitarbeitenden müssen zu einer Kultur der Sicherheit der Kinder beitragen, über die sie im Rahmen ihrer Arbeit Kontakt haben. Zu den präventiven Maßnahmen gehören Verhaltensrichtlinien für verschiedene Personengruppen, Standards im Rahmen der Personalpolitik sowie Standards für die unterschiedlichen Kommunikationsformen. Alle präventiven Maßnahmen sollen das Risiko der Gefährdung von Kindern minimieren und den entsprechenden Personengruppen im Zusammenhang ihrer Arbeit einen sicheren Umgang mit Kindern aufzeigen. Kommt es zu einem Verstoß gegen die Vorgaben, müssen entsprechende Beschwerdemechanismen in Gang gesetzt werden, um den Verdachtsfällen nachzugehen und alle notwendigen Maßnahmen einzuleiten. Dazu bedarf es klar definierte Verantwortlichkeiten und eine absolute Transparenz über die einzelnen Schritte des Fallmanagements.

3.2.5 Safeguarding: Gewalt gegen Erwachsene / Machtmissbrauch

Dasselbe was für Gewalt an Kindern und Jugendlichen gilt, ist in gleicher Form für die Gewalt zwischen Erwachsenen gültig. Jeder Mensch lebt in bestimmten Machtstrukturen, die zu Machtmissbrauch und zu Gewalt führen können. Diese Art von Machtungleichgewichten kann nicht direkt durch eine einfache Organisationsvorgabe angegangen werden. Es ist wichtig, dass diese Ungleichgewichte kontinuierlich reflektiert werden müssen. Gewalt ist als jede Handlung, die anderen körperlichen, emotionalen oder psychologischen Schaden zufügt zu definieren.

Es ist hervorzuheben, dass bestimmte Situationen und Beziehungsformen gewalttätiges Verhalten begünstigen können, die daher in den Risikoanalysen zu berücksichtigen sind. Gewalt kann sich auf unterschiedliche Art und Weise äußern, z. B. durch die Verletzung von Grenzen und individuellen Rechten einer Person,

durch Übergriffe oder kriminelles Verhalten. Daher ist es wichtig die persönlichen Grenzen und individuellen Rechte zu respektieren und Situationen, in denen Grenzen und Rechte verletzt wurden, anzusprechen. Mit der Verletzung von Grenzen und Rechten sind einmalige Vorfälle oder gelegentliches unangemessenes Verhalten oder unangemessene Äußerungen gemeint, selbst wenn diese unbeabsichtigt sind. In den meisten Fällen sind solche Handlungen auf einen Mangel an persönlicher oder beruflicher Reflexion zurückzuführen. Wenn Grenzen oder Rechte wiederholt verletzt werden, handelt es sich um einen Übergriff der im Rahmen sexualisierter Gewalt schnell in strafrechtlich relevantes Verhalten übergehen kann.

Deshalb gilt es, Organisationsstrukturen und Prozesse zu überprüfen, damit ethische und professionelle Grundsätze überall angemessen umgesetzt werden. An erster Stelle steht der Schutz. Hierbei kommt der Prävention eine wichtige Rolle zu. Vorbeugend tätig zu werden heißt, Wissen über sexualisierte Gewalt zu vermitteln, die ohnehin schon gelebte Kultur der Achtsamkeit weiter zu vertiefen und einen respektvollen, grenzachtenden Umgang miteinander weiter zu entwickeln. Gleichzeitig gilt es, wirksame Mechanismen einzurichten, um Hinweise entgegenzunehmen, Fälle zu verfolgen sowie Überlebende und Betroffene sexualisierter Gewalt zu unterstützen.

Die Inhalte eines Safeguarding-Konzepts, das neben allen Formen von Gewalt insbesondere auf den Schutz vor sexualisierter Gewalt abzielt, entsprechen den oben aufgezeigten Mindestvoraussetzungen wie eine umfassende Risikoanalyse, Präventivmaßnahmen und eines klar definierten Fallmanagement-Systems.

3.2.6 Umwelt-, Menschenrechts- und Governance-Risiken (ESG)

In der Compliance werden die Risiken, die sich aus der Nichteinhaltung von Nachhaltigkeits-Anforderungen ergeben, auch als ESG-Risiken bezeichnet. ESG steht für Environment (Umwelt), Social (Soziales) und Governance (Unternehmensführung), worauf sich die gesetzlichen Verpflichtungen fokussieren. Sie umfassen in der Regel eine entsprechende Transparenz zu Umwelt- und Menschenrechtsthemen sowie die Gewährleistung bestimmter unternehmerischer Pflichten durch die Organisation. Damit stehen auch NGOs vor der Herausforderung Nachhaltigkeitsziele in diesen drei Säulen zu definieren und zu erreichen. Ziel für die NGO sollte damit sein, eine werthaltige und langfristig stabile Organisation, inkl. ihrer Wertschöpfungskette zu erreichen.

In einem ersten Schritt ist wichtig, dass jede Organisation die für sie anwendbaren gesetzlichen Anforderungen kennt. So könnten bspw. die Normen der „Corporate Sustainability Reporting Directive“ (CSRD) oder des „Lieferkettensorgfaltspflichtengesetz“ (LkSG) in Frage kommen. Unter bestimmten Voraussetzungen sind Organisationen zur Nachhaltigkeitsberichterstattung (nach der CSRD) oder zur Sicherstellung menschenrechtsbezogener und umweltbezogener Sorgfaltspflichten (nach dem LkSG) angehalten, auch wenn diese für sie nicht direkt anwendbar sind. Dies ist bspw. der Fall, wenn Erwartungen spezieller Interessengruppen wie insbes. Spenderorganisationen zur Transparenz oder zu Pflichten in Bezug auf das unternehmerische Handeln bestehen.

Aber auch weitere Vorschriften wie die EU-Verordnungen zu nachhaltigen Investitionen (Offenlegungsverordnung und EU-Taxonomie-Verordnung), die EU-Verordnung über entwaldungsfreie Produkte (EUDR), die EU-Verordnung über ein CO_2-Grenzausgleichssystem (CBAM) oder die europäische Lieferkettenricht-

linie (CSDDD) zählen zu den Vorgaben, aus denen sich ESG-Risiken ergeben können, wenn sie anwendbar sind. Nach den sog. OMNIBUS-Regelungen von 2025 werden Berichtspflichten für große und mittelgroße Unternehmen erst ab 2027 und die unternehmerische Sorgfaltspflicht für Lieferketten in großen Unternehmen ab 2029 notwendig. Für die weiteren Vorschriften, wie CO_2-Grenzausgleich etc., werden Entlastungen der Unternehmen durch vereinfachte und klarere Vorgaben zum Bürokratieabbau angestrebt. Aufgrund der oft branchenspezifischen Anwendbarkeit von gesetzlichen Nachhaltigkeits-Anforderungen wird nachfolgend auf die ESG-Risiken, die nach der CSRD transparent gemacht werden müssen, konkreter eingegangen.

Compliance-Risiken aus der CSRD (Berichterstattung zu ESG-Risiken)
Die CSRD erweitert die Berichtspflicht von Unternehmen und Organisationen in der EU und führt verbindliche Standards für die Berichterstattung zu Nachhaltigkeitsthemen ein. Ein Aufschub der Umsetzung dieser Richtlinie in nationales Recht wurde zuletzt vom Europäischen Rat vom 14.04.2025 um zwei Jahre genehmigt.

Bei der Ermittlung der Berichtspflichten erfordert die CSRD eine Wesentlichkeitsanalyse zu den folgenden drei ESG-Themen und deren Umfang:

1. Umweltthemen (Klimawandel, Umweltverschmutzung, Wasser- und Meeresressourcen, biologische Vielfalt und Ökosysteme, Ressourcennutzung und Kreislaufsysteme).
2. Soziale Informationen (Eigene Belegschaft, Arbeitskräfte in der Wertschöpfungskette, betroffene Gemeinschaften, Verbraucher und Endnutzer in Bezug auf Menschenrechte).
3. Informationen zur Unternehmensführung (Unternehmenspolitik in Bezug auf Hinweisgeberschutz, Anti-Korruption, Tierschutz, Umgang mit Lieferanten, Lobbyarbeit).

Die Wesentlichkeitsbetrachtung von Auswirkungen des geschäftlichen Handelns setzt zwei Perspektiven voraus. D.h. einerseits sind die Auswirkungen durch die Geschäftsprozesse auf die Umwelt bzw. Dritte (Inside-Out-Perspektive) zu betrachten und andererseits sind die Auswirkungen von Dritten in Bezug auf das Handeln der Organisation von Relevanz (Outside-In-Perspektive). Die Berichtspflicht erstreckt sich dann auf die als wesentlich betrachteten Themen.

Neben der Angabe zu den Nachhaltigkeitsrisiken in den oben genannten drei Bereichen, denen die Organisation ausgesetzt ist, sind darüber hinaus allgemeine Informationen transparent zu machen, worin sich ebenfalls Risiken verbergen.

Denn der Nachhaltigkeitsbericht muss ermöglichen, dass sich eine dritte Person über folgende Themen informieren kann:

1. Geschäftsmodell und Strategien, Widerstandsfähigkeit des Geschäftsmodells und Chancen.
2. Vereinbarkeit von Geschäftsmodell und Strategie mit dem Erderwärmungsziel 1,5 Grad Celsius.
3. Rollen des Vorstands- und Überwachungsorgans sowie deren Qualifikation in Bezug auf nachhaltiges Handeln.
4. Unternehmenspolitik und Anreizsysteme zu Nachhaltigkeit der Organisation.
5. Angaben zur Wertschöpfungskette und damit verbundenen Auswirkungen.

Die ESG-Risiken umfassen für die Organisation daher sowohl die Implementierung von Verfahren im Umgang mit den Nachhaltigkeitsthemen „Umwelt“, „Soziales“ und „Governance“ als auch die unternehmerische Auseinandersetzung mit den Auswirkungen ihres Handelns in diesen drei Bereichen (doppelte Wesentlichkeitsanalyse).

Da die CSRD keine Sonderregelungen für gemeinnützige Organisationen oder NGOs enthält, ist es wichtig, den Anwendungsbereich der CSRD für die jeweilige Organisation zu klären oder eine Entscheidung über eine freiwillige Nachhaltigkeitsberichterstattung zu treffen, wenn sie aufgrund ihrer Rechtsform nicht betroffen ist. Dadurch kann sichergestellt werden, dass die Risiken für die Organisation rechtzeitig identifiziert, bewertet und priorisiert behandelt werden.

Für die NGO ergeben sich damit ggfs. neue Anforderungen für die Unternehmensstrategie und für den Einsatz von Managementsystemen, die eine resiliente Organisationsstruktur schaffen. Eine frühzeitige Planung und rechtzeitige organisationsadäquate Umsetzung ist daher ratsam.

3.2.7 Data- und KI-Compliance sowie Cyber Security

Die fortschreitende Digitalisierung macht den verantwortungsvollen und gesetzeskonformen Umgang mit Daten und Künstlicher Intelligenz (KI) für Organisationen aller Art – gerade auch für NGOs – immer wichtiger. Moderne Datenanalysen und KI-basierte Verfahren bieten große Chancen, sind aber auch mit neuen Risiken und Haftungsfragen verbunden. Die Sicherstellung von Data- und KI-Compliance ist daher ein essenzieller Bestandteil guter Organisationsführung. Gerade in NGOs und sozialen Unternehmen können Daten und KI-Lösungen zur Bewältigung gesellschaftlicher Herausforderungen beitragen:[9] So helfen etwa KI-gestützte Spendenanalysen bei der Prognose von Spendenverhalten und Optimierung von Fundraising-Strategien,[10] KI-basierte Assistenzsysteme unterstützen Menschen mit Behinderungen und kommen in der Altenpflege zum Einsatz.

Alle Organisationen und Unternehmen, die in Europa Daten verarbeiten und/oder KI-Systeme nutzen, müssen umfangreiche Data- und KI-Compliance-Anforderungen erfüllen. Das umfasst insbesondere die Verpflichtung, dass alle Datenverarbeitungsverfahren und KI-Systeme verantwortungsvoll, transparent und im Einklang mit gesetzlich definierten Standards und Vorschriften betrieben werden.

EU-Digitalstrategie 2030 und in dessen Rahmen relevante Rechtsakte
(EU-DSGVO, AI Act, Data-Act, NIS2)

Die Datenschutzgrundverordnung der Europäischen Union (EU-DSGVO), die seit 2018 verbindlich ist, sowie der im Juli 2024 in Kraft getretene EU Artificial Intelligence Act (AI Act)[11] sind zentrale rechtliche Rahmenwerke für Europa, die den verantwortungsvollen Umgang mit Daten und neuen Technologien konkret

regeln. Beide EU-Verordnungen verpflichten Unternehmen und Organisationen zu einem „risikobasierten Ansatz“, sodass diese ihre Schutzmaßnahmen an den Risiken ausrichten müssen, die von der Verarbeitung personenbezogener Daten bzw. dem Einsatz von KI-Systemen ausgehen.

9 Zu Anwendungsmöglichkeiten im sozialen Bereich siehe z. B. Der Paritätische, KI-Textsammlung Künstliche Intelligenz in der sozialen Arbeit, Version 2.0, S. 4-8; Johanniter, Blog KI in der Altenpflege.
10 Rechtsanwältin Dr. Isabella Löw, Blog, Künstliche Intelligenz und Spenderdaten – was NPOs jetzt beachten müssen!
11 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 (EU AI Act).

Je höher das Risiko, desto höher sind die damit verbundenen Anforderungen und Pflichten. Für NGOs und soziale Unternehmen ist der AI Act besonders dann relevant, wenn sie KI-Systeme in besonders sensiblen Anwendungsbereichen, wie etwa in der Gesundheitsversorgung, in der Bildung oder im Rahmen von Sozialleistungen einsetzen.[12]

Je nach Art und Anwendung der KI sind sie dazu verpflichtet, bestimmte Transparenz- und Sicherheitsstandards zu erfüllen, wie bspw. die Gewährleistung der Fairness, Nichtdiskriminierung und Nachvollziehbarkeit von KI-Entscheidungen.

Ergänzend dazu ist die NIS2-Richtlinie (EU 2022/2555) für NGOs bedeutsam, da sie Mindeststandards für Cybersicherheit in der EU festlegt. Kleinere NGOs fallen meist nicht unter die gesetzlichen Pflichten, die NIS2 bietet aber eine wertvolle Orientierung, da sie ein systematisches Management von Cyberrisiken, klare Meldepflichten bei Sicherheitsvorfällen und eine Stärkung organisatorischer und technischer Schutzmechanismen einfordert. Diese Pflichten können unmittelbar für größere NGOS ab 50 Mitarbeitenden greifen, die kritische Infrastrukturen betreiben oder besonders sensible Daten verarbeiten. Cybersicherheit wird zusammen mit dem Datenschutz und KI-Compliance zu einem zentralen Baustein digitaler Verantwortung.

Diese EU-Verordnungen verpflichten Organisationen, interne Governance-Strukturen zu implementieren, die sicherstellen, dass Datenverarbeitung und KI-Nutzung jederzeit im Einklang mit den gesetzlichen Vorgaben stehen. Ein Compliance-Managementsystem muss daher Risiken identifizieren, geeignete Maßnahmen zur Risikominimierung treffen, klare Verantwortlichkeiten definieren und die Einhaltung laufend überprüfen.

Der Digital Plan 2030 der EU spielt also für NGOs eine wichtige Rolle, da er ethische Standards für KI, Datenschutz und eine digitale Verantwortung fordert: Dazu gehören Programme zur Steigerung der digitalen Kompetenzen, der Ausbau digitaler Infrastrukturen, die Unterstützung der Digitalisierung von Unternehmen und öffentlicher Dienste sowie die Schaffung einer nachhaltigen und sicheren Digitalisierung, um sich den neuen digitalen Herausforderungen zu stellen. Eine eigene Digitalstrategie entlang dieser entsprechenden Maßnahmen und Prozesse auszurichten ist empfehlenswert, um Vertrauen bei Spender*innen, Partner*innen und Zielgruppen zu stärken.

Best Practices für Data- und KI-Compliance in NGOs:

- ***Klärung zentraler Verantwortlichkeiten für KI-Governance:*** Es sollte ein klar definiertes Verantwortlichkeitsmodell etabliert werden, das die relevanten Schnittstellen und fachlichen Perspektiven – etwa Datenschutz, Compliance, Recht, IT-Sicherheit, Innovation und Fachbereiche – berücksichtigt. Dies kann durch benannte zentrale Personen oder auch durch ein interdisziplinäres Gremium wie ein KI-Governance Board erfolgen. Ziel ist die koordinierte Steuerung KI-bezogener Aktivitäten, die Entwicklung einer KI-Strategie, die Begleitung von Projekten sowie die Verabschiedung und Umsetzung von Richtlinien.[13]

12 Siehe auch Tobias Kutschka, EU-Gesetz zu Künstlicher Intelligenz, Neue Caritas, Heft 2 (2024).
13 Siehe auch Felix Kraft und Sven Eimertenbrink, So setzen Unternehmen den EU AI Act um - Ideen zum Aufbau eines KI-Compliance-Management-Systems, in: Compliance Business, Ausgabe 3/2025.

- ***Klare Richtlinien:*** NGOs sollten interne Leitlinien zur Nutzung von Daten und KI entwickeln, die technische, rechtliche und ethische Aspekte berücksichtigen. Eine regelmäßige Überprüfung der Einhaltung ist zentral. Beispiele aus bestehenden KI-Orientierungshilfen und KI-Leitlinien von NGOs – etwa vom Paritätischen Gesamtverband,[14] dem Deutschen Rote Kreuz Wohlfahrt,[15] dem Evangelische Werk für Diakonie und Entwicklung e.V.,[16] der Bundesverband der Arbeiterwohlfahrt (AWO)[17] sowie dem Arbeiter-Samariter-Bund NRW e.V.[18] – können als Orientierung für einen sicheren, transparenten und ethisch vertretbaren KI-Einsatz in NGOs dienen.
- ***Implementierung transparenter Entscheidungsprozesse:*** Um Vertrauen bei Stakeholdern aufzubauen, sollten NGOs sicherstellen, dass ihre Data- und KI-Entscheidungsprozesse nachvollziehbar sind. Dies kann durch Offenlegung des Zwecks und der Methoden der Datenverarbeitung und der verwendeten statistischen Verfahren sowie durch einen Dialog über die Bewertung und Schlussfolgerungen geschehen.[19]
- ***Schulungen und Sensibilisierung:*** Mitarbeitende der NGOs sollten regelmäßig zu Datenschutz, Datensicherheit und KI-Compliance geschult und über aktuelle gesetzliche Anforderungen informiert werden. Wenn sich NGOs dazu entschließen, fremdentwickelte KI-Systeme in eigener Verantwortung zu verwenden, so ist zu beachten, dass sie Betreiber im Sinne des AI Act sind und als solche verpflichtet sind, die KI-Kompetenz ihrer Beschäftigten gemäß Artikel 4 AI Act sicherzustellen.
- ***Bias-Prüfung:*** NGOs und soziale Unternehmen sollten ihre Trainingsdaten und Algorithmen systematisch auf potenzielle Vorurteile analysieren und bereinigen, um diskriminierende und benachteiligende Ergebnisse zu vermeiden.[20] Zudem sollten bei der Auswahl und der Nutzung von KI-Systemen darauf geachtet werden, dass diese möglichst frei von Vorurteilen konzipiert sind.[21]
- ***„Human-in-the-Loop" und ethische Prüfung:*** Ergebnisse und Entscheidungen von KI-Systemen sollten stets durch menschliche Expertise überprüft werden,[22] um Fehlentscheidungen, diskriminierende Muster oder automatisierungsbedingte Verzerrungen (Biases) frühzeitig zu erkennen und zu korrigieren – insbesondere dann, wenn diese Auswirkungen auf Menschen haben[23] oder ethisch sensible Themen betreffen.[24]
- ***Umgang mit Urheberrechtsfragen:*** NGOs und soziale Unternehmen sollten sicherstellen, dass KI-Tools keine urheberrechtlich geschützten Inhalte ohne Genehmigung der Rechteinhaber verwenden.[25] Um Urheberrechtsverletzungen vorzubeugen, sollten NGOs die Lizenzbedingungen von KI-Tools sorgfältig prüfen, Mitarbeitende bezüglich der urheberrechtlichen Risiken sensibilisieren und schulen, sowie bei Bedarf juristischen Rat einholen. Dies gilt insbesondere auch für durch KI generierte Inhalte (bspw. Bilder), deren urheberrechtlicher Status unklar und deren Nutzung rechtliche Risiken bergen kann.

14 Der Paritätische, KI-Textsammlung Künstliche Intelligenz in der sozialen Arbeit, Version 2.0, S. 22-35;.
15 DRK Wohlfahrt, Blogbeitrag KI-Guidelines – Warum klare Regeln im Umgang mit Künstlicher Intelligenz so wichtig sind.
16 Evangelische Werk für Diakonie und Entwicklung e.V., Leitlinien zur Nutzung von Künstlicher Intelligenz (im Folgenden „EWDE KI-Leitlinien").
17 Bundesverband der Arbeiterwohlfahrt, Leitlinien für den verantwortungsvollen KI-Einsatz (in der AWO).
18 Arbeiter-Samariter-Bund NRW e.V., Grundsätze für den Einsatz von KI-Technologie beim ASB in ganz Nordrhein-Westfalen.
19 Siehe z. B. EWDE KI-Leitlinien, Abschnitt D, Ziffer 23.
20 Siehe z. B. Entwurf der KI-Leitlinien der AWO, S. 1.
21 Grundsatz „Fairness und Nicht-Boshaftigkeit" der KI-Grundsätze des ASB NRW.
22 Zinnbauer, D. (2025), Artificial intelligence in anti-corruption – a timely update on AI technology. Bergen: U4 Anti-Corruption Resource Centre, Chr. Michelsen Institute (U4 Brief 2025:1) (im Folgenden „Zinnbauer D. (2025)"), S. 9-10.
23 DRK Wohlfahrt, Blogbeitrag Künstliche Intelligenz in der Wohlfahrtsarbeit vom 31.08.2023.
24 Vgl. Grundsatz „Autonomie und Kontrolle" der KI-Grundsätze des ASB NRW sowie EWDE KI-Leitlinien, Abschnitt D, Ziffer 22.
25 Vgl. EWDE KI-Leitlinien, Abschnitt D, Ziffern 16 und 20.

- ***Umgang mit Daten in KI-Systemen:*** Personenbezogene und betriebsinterne Daten sollten (möglichst) anonymisiert in KI-Tools eingespeist werden. Dabei ist zu berücksichtigen, dass KI auch indirekt Rückschlüsse auf Personen ziehen kann. Sofern personenbezogene Daten verarbeitet werden, sind die DSGVO-Vorgaben (bspw. Zweckbindung, Transparenz, Datenminimierung, Rechtsgrundlagen) einzuhalten. Die Nutzung personenbezogener Daten zum Training von KI-Modellen kann beispielsweise eine Zweckänderung darstellen und unzulässig sein. Bei Bedarf sollte der Datenschutzbeauftragte zwecks datenschutzrechtlicher Bewertung der eingesetzten KI-Systeme und Identifizierung geeigneter Schutzmaßnahmen eingebunden werden. Liegt ein hohes Risiko für die Rechte und Freiheiten der Betroffenen vor, ist zudem eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen.

3.2.8 Gemeinnützigkeit – Steuer-Compliance

Für NGOs hat steuerliche Compliance einen hohen Stellenwert:

- Gravierende Verstöße gegen steuerliche Regelungen können hohe finanzielle Risiken (bis hin zum Verlust der Gemeinnützigkeit und eventueller Existenzbedrohung), aber auch Reputationsrisiken bergen.
- NGOs arbeiten mit treuhänderisch anvertrauten Mitteln, von denen ein erheblicher Teil aus öffentlichen Mitteln und freigiebigen Zuwendungen (Spenden) stammt.

Ziel ist deshalb, Verstöße gegen steuerrechtliche Vorschriften zu vermeiden und eine Haftung der Vorstände und Geschäftsführer zu verhindern, die persönlich und unbeschränkt für Steuerschulden ihrer gemeinnützigen Organisation aufgrund von Mittelfehlverwendungen haften. Letztere können auch im Zusammenhang mit einer Mittelweiterleitungen an nachfolgende Zuwendungsempfänger eintreten. Denn NGOs sind nicht nur darauf beschränkt, ihre satzungsmäßigen Zwecke selbst zu erfüllen und selbst operativ tätig zu werden. Das Gemeinnützigkeitsrecht lässt es auch zu, dass NGOs fördernd tätig werden und Mittel an Dritte weiterleiten.

Hieraus ergeben sich folgende Sorgfaltspflichten im Umgang mit der Steuer-Compliance:

- Einhaltung aller relevanten steuerrechtlichen Regelungen.
- Proaktive Festlegung von Prozessen, die geeignet sind, die Einhaltung zu gewährleisten und die Gefahr von Fehlern und Verstößen zu minimieren.
- Regelmäßige Kontrolle der steuerlichen Tätigkeiten, der steuerlichen Prozesse und der hierbei ermittelten steuerlichen Werte.
- Korrektur entdeckter steuerrechtlicher Fehler und Verstöße.
- Dokumentation der Behandlung steuerlicher Themen und der zugehörigen Prozesse als Leitfaden für ausführende Mitarbeiter*innen und zum Nachweis für Steuererklärungen und bei Steuerprüfungen.
- Regelmäßige Kommunikation steuerrechtlicher Festlegungen und Änderungen an Mitarbeitende, die steuerlich relevante Sachverhalte entscheiden oder ausführen.
- Gute Zusammenarbeit und Kommunikation mit den Finanzbehörden.

Um die Gemeinnützigkeit nicht zu gefährden, sollten bei der steuerlichen Behandlung der Fokus auf die Einhaltung der steuerlichen Begünstigung und die Zweckbindung der Mittel gerichtet sein. Hierin integriert ist die unterjährige Handhabung der Spendenverwaltung und der Nachweis der Mittelverwendung im Ausland. Hierzu gehören im Wesentlichen: die Prüfung der Satzung auf Gemeinnützigkeitsvoraussetzungen, Durchführung der Mittelverwendungsrechnung, Abstimmung und Kontrolle mit und von den Verantwortlichen intern und extern (Steuerberater), Einreichung der Steuererklärung bei der Finanzbehörde, Prüfung der Steuerbescheide intern und extern (Steuerberater) und Beachtung der gesetzlichen Aufbewahrungsfrist.

ANHANG ZUM LEITFADEN COMPLIANCE IN NGOS
VERWEISE AUF DICO-STANDARDS
CHECKLISTEN
LITERATURLISTE

INHALT

ANHÄNGE

A. AUFGABENBESCHREIBUNG EINER CMS-VERANTWORTUNG

Einrichtung einer Funktion mit Zuständigkeit für das Compliance Management System

Funktionsbezeichnung: bspw. Compliance-Beauftragte:r, Compliance Manager, Compliance Officer

Typische Aufgaben dieser Funktion sind:

- CMS-Einrichtung und -Systemverantwortung.
- Organisation betreffender Gremien, soweit diese existieren (z. B. Compliance-Board).
- Abstimmung mit anderen Funktionen mit Überschneidungspotenzial (z. B. Recht, Datenschutz, Einkauf, Kommunikation, Controlling, HR, …).
- Überprüfung wesentlicher Geschäftsprozesse unter Compliance-Gesichtspunkten.
- Initiativrolle bei konkreten Regelungen, speziell Verhaltenskodex und Antikorruptionsrichtlinie.
- Herstellung interner Transparenz von Gesetzen und Richtlinien, Überwachung der Funktionsfähigkeit des Rechtsmonitorings.
- Treiberfunktion für die Ermittlung und Bewertung der Compliance-Risiken.
- Treiberfunktion für die Bestimmung und Beauftragung notwendiger Compliance-Risikomaßnahmen.
- Aktive Compliance-Kommunikation, insbesondere Konzeption, Planung und Durchführung von Compliance-Schulungen in Abstimmung mit der Personalentwicklung.
- Ansprechpartner und Berater für Geschäftsführung, Mitarbeiter und Dritte in Compliance-Zweifelsfällen.
- Stichproben-Kontrollen zu Regelkonformität und Funktionsfähigkeit von Präventionsmaßnahmen.
- Compliance-Reporting.
- Aufklärung von Verdachtsfällen auf Compliance-Verstöße, Initiativ- oder Unterstützerrolle bei der Ahndung von bestätigten Verdachtsfällen.
- Überwachung und Verbesserung des CMS sowie Pflege der CMS-Beschreibung.

B. CHECKLISTE: BESTANDTEILE EINES VERHALTENSKODEX FÜR EINE NGO

1. Vorwort

- Vorstand / Geschäftsführung.
- „Tone from the top" / Vorbildfunktion.

2. Präambel & Geltungsbereich

- Zweck des Kodex (z. B. Förderung von Integrität, Transparenz, Rechenschaftspflicht).
- Mission und Werte der NGO (z. B. Solidarität, Menschenrechte, Nachhaltigkeit).
- Personenkreis (Mitarbeitende, Ehrenamtliche, Vorstand, externe Partner, Lieferanten, Dienstleister).
- Ggf. Verweis auf Grundsatzerklärung / Menschenrechtserklärung (LkSG).
- Räumlicher Geltungsbereich (national / international).

3. Allgemeine Verhaltensgrundsätze

- Ehrlichkeit, Integrität und Fairness im Handeln.
- Respektvoller und wertschätzender Umgang miteinander.
- Offene, respektvolle und transparente Kommunikation.
- Verantwortung für das eigene Handeln.
- Respekt und Sensibilität ggü. anderen Bräuchen und Kulturen.
- Ggf. keine religiösen und politischen Aktivitäten im Namen der NGO.

4. Ethische und rechtliche Verpflichtungen

- Einhaltung aller geltenden Gesetze, Vorschriften und internen Richtlinien.
- Bezugnahme auf anerkannte, internationale Standards zur Qualität, Antikorruption, Kinderschutz u,ä. (z. B. UN-Menschenrechtsdeklaration, Kinderrechtskonvention, Core Humanitarian Standard, ICRC Code of Conduct).
- Ggf. Verbot von Alkohol, Drogen und Waffen.
- Keine Beteiligung an illegalen Aktivitäten (z. B. Geldwäsche, Terrorismusfinanzierung).
- Verpflichtung zur Meldung von Verstößen (Whistleblower-Schutz) / Speak-Up-Policy.

5. Umgang mit Interessenkonflikten

- Policy gegen Interessenkonflikte mit Offenlegungs- und Handlungsregeln bei potenziellen Interessenkonflikten.
- Keine Bevorzugung privater oder externer Interessen gegenüber NGO-Interessen.
- Unzulässigkeit von Vorteilsannahmen (Geschenke, Einladungen), ggf. Geschenkeregister.

6. Anti-Korruption & Transparenz

- Striktes Verbot von Bestechung und Korruption.
- Klare Regeln für Zuwendungen, Spenden und Sponsoring.
- Dokumentationspflichten bei relevanten Transaktionen.

7. Gleichbehandlung & Anti-Diskriminierung

- Keine Diskriminierung aufgrund von Geschlecht, Herkunft, Religion, Alter, Behinderung, sexueller Orientierung oder politischer Einstellung.
- Keine religiösen oder politischen Aktivitäten im Namen der NGO.
- Förderung von Diversität und Inklusion sowie einer diskriminierungssensiblen und respektvollen Sprache.

8. Gesundheit, Sicherheit & Gewaltprävention

- Verantwortung für Gesundheit und Sicherheit am Arbeitsplatz und bei NGO-Einsätzen.
- Striktes Verbot von Gewalt, sexualisierter Gewalt und Belästigung.
- Schutz vor Überlastung, Mobbing und psychischer Belastung.
- Einführung von Präventions- und Interventionsverfahren.

9. Nachhaltiger Umgang mit Ressourcen und verantwortungsvolle Beschaffung.

- Nachhaltiger Einsatz von Finanz-, Sach- und Umweltressourcen.
- Vermeidung von Verschwendung.
- Verantwortungsvolle Beschaffung unter der Berücksichtigung sozialer und ökologischer Standards.

10. Datenschutz, Vertraulichkeit & Digitale Verantwortung

- Einhaltung von Datenschutzgesetzen (z. B. DSGVO).
- Sicherer Umgang mit sensiblen Informationen.
- Schutz geistigen Eigentums und vertraulicher Informationen.
- Vertraulichkeitsvereinbarungen für besonders schützenswerte Daten.
- Verantwortungsbewusster Einsatz digitaler Technologien und KI.
- Förderung digitaler Kompetenz und Sensibilität für digitale Risiken.

11. Melde- und Beschwerdeverfahren

- Klare interne Meldekanäle (auch anonym möglich).
- Schutz vor Repressalien für Hinweisgebende.
- Verfahren zur Untersuchung und Sanktionierung von Verstößen.

OPTIONAL: 12. Verstöße & Konsequenzen

- Mögliche arbeitsrechtliche, zivilrechtliche oder strafrechtliche Folgen.
- Disziplinarmaßnahmen und deren transparente Kommunikation.
- Möglichkeit der Rehabilitation / Wiedereingliederung.

OPTIONAL: 13. Implementierung & Überprüfung

- Verpflichtung zur Unterzeichnung durch alle relevanten Personen.
- Regelmäßige Schulungen zum Kodex.
- Periodische Überprüfung und Anpassung des Kodex an neue rechtliche Rahmenbedingungen.

C. CHECKLISTE ZUR ERSTELLUNG EINER ANTI-KORRUPTIONSRICHTLINIE

1. Einleitung und Zielsetzung:

a) Beschreibung des Zwecks der Richtlinie (z. B. Prävention oder Bekämpfung von Korruption im Rahmen des Compliance Managements).
b) Bedeutung der Antikorruption für die Mission der NGO.
c) Verweis auf internationale und nationale Standards und rechtliche Rahmenbedingungen, an denen sich die Antikorruptionsarbeit der NGO orientiert (z. B. ISO 37001).

2. Geltungsbereich:

a) Klare Definition, für wen die Richtlinie gilt: Mitarbeitende, Führungskräfte, ehrenamtliche Helfer, Partnerorganisationen und Förderer.
b) Mögliche Abstufung von Maßnahmen für Organisationsbereiche mit hohem Korruptionsrisiko (z. B. strengere Vorschriften für Organisationseinheiten in Hochrisikoländern).

3. Definitionen:

a) Korruption: Allgemeine Definition.
b) Aktive und passive Korruption: Unterschiedliche Formen und Beispiele.
c) Zuwendungen / Vorteile: Materielle (z. B. Geschenke, Geld) und immaterielle Vorteile (z. B. Ehrungen, Beförderungen).
d) Öffentliche Amtsträger: Vor allem Amtsträger, mit denen die NGO regelmäßig interagiert oder interagieren könnte.
e) Interessenkonflikte: Typische Szenarien und Konsequenzen.

4. Verbotene Handlungen:

a) Klare Auflistung und Beschreibung von Handlungen, die nicht toleriert werden, z. B.:
   i. Bestechung, Schmiergeldzahlungen.
   ii. Zweckentfremdung von Hilfsgeldern.
   iii. Vergabe von Vorteilen ohne rechtmäßige Grundlage.
   iv. Übergabe oder Annahme von Bargeld.
   v. Zahlungen auf das private Bankkonto eines Geschäftspartners oder Dritten.

5. Erlaubte Handlungen:

a) Klare Auflistung und Beschreibung von Handlungen, die erlaubt sind, z. B.:
   i. Festlegung maximal zulässiger Werte für Geschenke und Einladungen.
   ii. Transparenzvorgaben / Freigabeworkflows für Entscheidungen in Grenzbereichen, wichtig: Immer unter persönlicher Einbindung des Complianceverantwortlichen, damit eine zentrale Transparenz für die gesetzlichen Vertreter gewährleistet ist.
   iii. Festlegung von zulässigen Rahmenbedingungen für Sponsoring und Spenden.
   iv. Zulässige Zuwendungen, wie angemessene Einladungen zu Geschäftsessen.
   v. Prozesse zur Registrierung von gegebenen oder erhaltenen Zuwendungen sowie zur Registrierung von Treffen mit öffentlichen Amtsträgern.

6. Interessenkonflikte:

a) Definition von relevanten Interessenkonflikten, z. B. familiäre Verbindungen zu Vertragspartnern der NGO oder Eigentümerschaft eines Unternehmens, welches ein Vertragspartner der NGO ist.
b) Verpflichtung und Prozess zur Meldung potenzieller Interessenkonflikte.
c) Prozesse zum Umgang mit auftretenden Interessenskonflikten.

7. Umgang mit Geschäftspartnern:

a) Verpflichtung zu dem Verbot jeglicher Korruption in allen Verträgen mit Geschäftspartnern.
b) Durchführung von Due-Diligence-Prüfungen vor Vertragsabschluss mit Geschäftspartnern und Lieferanten.
c) Regelmäßige Überprüfung der Geschäftspartnerbeziehungen und Partnerorganisationen.

8. Sanktionen bei Verstößen:

a) Klare Darstellung der Konsequenzen bei Verstößen:
   i. Disziplinarmaßnahmen bis hin zur Kündigung.
   ii. Strafrechtliche Schritte.
   iii. Anonyme Kommunikation von Verstößen.

9. Awareness:

a) Klare Definition der Rollen und Verantwortlichkeiten.
b) Beschreibung des Governance-Modells, inkl. klarer Verantwortlichkeiten in organisationalen Einheiten und / oder Regionen.
c) Mitarbeitende und Führungskräfte als erste Verteidigungslinie.
d) Compliance-Abteilung als zweite Verteidigungslinie und zentraler Ansprechpartner.
e) Interne Audit als dritte Verteidigungslinie.

10. Schulungen und Kommunikation:

a) Verpflichtende Schulungen zur Korruptionsbekämpfung für alle Mitarbeitenden und Partner.
b) Regelmäßige Auffrischungen und gezielte Trainings in Risikogebieten.

11. Aktualisierung und Überprüfung der Richtlinie:

a) Analyse von Verstößen etc.
b) Verfahren zur regelmäßigen Überprüfung und Anpassung der Richtlinie.
c) Verantwortlichkeit der Compliance-Abteilung für die Aktualisierung in Abstimmung mit der Geschäftsleitung.

D. CHECKLISTE: ABLAUF FALLMANAGEMENT BEI EINEM MÖGLICHEN COMPLIANCE VERSTOSS

1. Vertraulichkeit bewahren:

- Um mögliche Hinweisgebende (Whistleblower) und die Integrität des Untersuchungsprozesses zu schützen, sollte der/die Compliance-Verantwortliche den Vorfall und mögliche Anschuldigungen mit höchster Vertraulichkeit behandeln und nur einem kleinen, gezielten Personenkreis zugänglich machen.

2. Externe Unterstützung:

- Im Falle eines ersten Verdachts auf einen Verstoß gegen Richtlinien sollte der/die Compliance-Beauftragte abwägen, ob die Untersuchung durch eine unabhängige externe Drittpartei (z. B. eine Anwaltskanzlei oder spezialisierte Beratungsfirma) durchgeführt werden sollte. Dies ist häufig empfehlenswert, da interne Untersuchungen nur von qualifiziertem und hierfür geschultem Personal durchgeführt werden sollten, und externe Untersuchungen darüber hinaus einen höheren Grad an Unabhängigkeit sicherstellen können.

3. **Risikoanalyse:**
- Je nach Kontext, in dem die Anschuldigung erhoben wird, sollte vor Einleitung einer Untersuchung analysiert werden, welche Risiken für die Beteiligten (Betroffene, hinweisgebende Person, Beschuldigte, interne / externe Untersuchende) entstehen und wie diese abgemildert werden können. Dies ist insbesondere in Ländern mit nicht ausreichender Rechtssicherheit notwendig, um Schaden von allen Beteiligten fernzuhalten.

4. **Untersuchung einleiten:**
- Der/ Die Compliance-Beauftragte sollte im nächsten Schritt unverzüglich eine interne oder externe Untersuchung einleiten, um mögliche Vorwürfe zu überprüfen.

5. **Meldung an Führungsebene:**
- Der Verdacht sollte an die Führungsebene der NGO gemeldet werden (insofern die Führungsebene selbst nicht in den Vorwurf verwickelt ist), um Transparenz sicherzustellen und relevante Maßnahmen (z. B. fristlose Kündigungen) zu koordinieren.

6. **Meldung an Behörden:**
- Falls nationales oder internationales Recht fordert, dass der Vorfall bzw. der Verdachtsfall an die zuständigen Behörden gemeldet wird, muss diese rechtliche Vorgabe eingehalten werden.

7. **Vorbeugung für die Zukunft:**
- Ausgehend von der Untersuchung sollte die NGO bzw. die für Compliance zuständige Person Maßnahmen ergreifen, um Compliance Verstöße in Zukunft zu verhindern (Schulungen, Richtlinienanpassung, Risikoanalysen, etc.).

8. **Berichterstattung:**
- Nach Abschluss der Untersuchungen sollte ein schriftlicher Bericht den Vorfall, die Untersuchung sowie die getroffenen Maßnahmen zusammenfassen.

E. WEITERFÜHRENDE LITERATUR

(1) DICO-Standards

Thema	Titel	Datum	Kurzbeschreibung
Kapitel 2: Mindestanforderungen an ein Compliance Management System	Standard CMS	März 2021	Allgemeine Empfehlungen für die Ausgestaltung von Compliance-Management-systemen.
	S05 - Standard Schulungskonzepte	Februar 2021	Pragmatische Arbeitshilfe für die Vorbereitung von einzelnen Compliance-Schulungen oder kompletten Schulungskampagnen.
	S11 – Standard Hinweisgebersysteme	März 2021	Allgemeine Empfehlungen zur Ausgestaltung eines Hinweisgebersystems.
	S14 Richtlinienmanagement	Februar 2014	Praktische Umsetzungshilfe zum Management unternehmensinterner Regelungen.
2.2 Compliance Risiken	S01 – Geschäftspartner-Compliance	Juli 2019	Grundsätze zur Ausgestaltung der Geschäftspartner-Compliance mit abgeleiteten Anforderungen, die je nach Risikoprofil der NGO angepasst werden können.
	S09 – Standard Risikoanalyse	Januar 2020	Rahmenbedingungen und Anforderungen an die Organisation und Durchführung einer Compliance-Risikoanalyse
	S16 - Lieferketten Compliance	August 2022	Praxishilfe und Orientierung zur Umsetzung von gesetzlichen Lieferketten-Sorgfaltspflichten zu Menschenrechts- und Umweltrisiken in der Lieferkette
	A07 - Sanktionslisten im Rahmen der Geschäftspartnerprüfung	Oktober 2016	Beschreibung praktischer Maßnahmen zur Sicherstellung der Geschäftspartner-Compliance unter Verwendung von Sanktionslisten
	A06 – Grundlagenpapier: Einführung in die Exportkontrolle	Dezember 2024	Einführung in Exportkontrollmaßnahmen und Richtlinien, besonders relevant bei Export von Hilfsgütern, die Dual-Use Gütern sein könnten in Krisenregionen
	A11 – Mögliches Muster einer Sanktionslistenprüfung bei geplantem Liefervertrag	Januar 2018	Bezugnehmend auf A07

3.2.1 Korruption	Korruptionsprävention - Ein Leitfaden für Unternehmen	März 2021	Überblick über wirksame Anti-Korruptionsmaßnahme und deren Implementierung in Unternehmen. In vielen Fällen können diese auch leicht auf NGOs transferiert werden. Besonders Kapitel zwei zu wirksamen Compliance-Systemen sind für NGO's relevant, da Thematiken wie aktives Sponsoring seltener im alltäglichen Geschäftsbereich aufkommen.
	Anti-Korruptions-Compliance und Integrity Management in Hochrisikoländern	Januar 2023	Verdeutlichung der erhöhten Risiken in Hochrisikoländern und erste Handlungsempfehlungen durch angepasste Compliance- und Whistleblower-Systeme.
3.2.2 Geldwäsche und Terrorismusfinanzierung	Leitlinie: L12 Geldwäsche-Compliance für Güterhändler	August 2021	Überblick über Präventions- und Überwachungsmaßnahmen für Geldwäsche, die für Unternehmen gelten, die Güter handeln. Besonders das Geldwäsche Compliance-Management-System kann auch auf NGO's angewendet werden.
	Bericht über die Risiken im Bereich der Geldwäscherei und Terrorismusfinanzierung bei Non-Profit-Organisationen	Juni 2017	Beispiele für Terrorismusfinanzierung und Geldwäsche durch NPOs in der Schweiz. Empfehlungen: Erweiterung der Handelsregisterpflicht auf risikobehaftete Vereine im Bereich Terrorismusfinanzierung und Mitgliederlistenpflicht für eingetragene Vereine, Konsequente Bekämpfung von Geldwäsche und Terrorismusfinanzierung, Sensibilisierung des NPO-Sektors.
	International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations	Februar 2025	FAFT-Standrads: Empfehlung, fortlaufende Risikobewertungen durchzuführen und einen risikobasierten Ansatz zu verfolgen, um das Potenzial für Missbrauch im Bereich der Terrorismusfinanzierung im NGO-Sektor zu verstehen. Sicherstellung der operationellen Transparenz in NGO-Aktivitäten und Führung genauer Aufzeichnungen zur Rechenschaftspflicht. NGOs über Minderungsstrategien belehren und Sicherstellung der Einhaltung relevanter Gesetze.
3.2.3 Menschenrechte und Diskriminierung jeder Art	30 FAQ zum Menschenrechtsbeauftragten	August 2022	Überblick über die wichtigsten Berührungspunkte eines Menschenrechtsbeauftragten. Für NGO's besonders relevant: Haftungs- und Qualifikationsfragen
	Soziale Mindeststandards in der Lieferkette	02/2021	Überblick über aktuelle Entwicklungen, besonders relevant: Sorgfaltspflichten für Auftraggeber
3.2.6 Umwelt-, Menschenrechts-	Arbeitspapier A22: Leitfragen und Anregungen zur Ausgestaltung einer ESG-Governance	November 2024	Gezielte Anregungen zur Ausgestaltung eines ESG-Governance Systems. Für NGO's besonders Reporting und Konsequenzen relevant

und Governance-Risiken (ESG)	Positionspapier ESG	Juni 2023	Überblick über mögliche Ausgestaltungen eines ESG-Compliance Systems, für NGO's vermutlich Gesamtsteuermodell am relevantesten

(2) Externe Quellen

Thema	Titel	Datum	Kurzbeschreibung	Link
3.2.1 Korruption	Anti-Korruptions-Compliance und Integrity Management In Hochrisikoländern Herausforderungen und Lösungsansätze	März 2022	Überblick über die Risikogebiete und Aufzeigen möglicher Lösungsansätze durch CMS und angepasste Drittparteienprüfung – diese sollten auch NGO's durchführen, so sie denn in Hochrisikoländern aktiv sind	Hyperlink: *„https://www.htwg-konstanz.de/fileadmin/pub/ou/kicg/News/KICG_Kompendium_2022_Compliance_u_Integrity_in_Hochrisikolaendern.pdf"*
3.2.5 Gewalt gegen Erwachsene/Machtmissbrauch	Dokumentensammlung und Trainingsmaterialien zum Thema (englisch)	NA	Tools für international arbeitende NGOs	Hyperlink: https://safeguardingsupporthub.org/#

Über DICO:

DICO – Deutsches Institut für Compliance e.V. wurde im November 2012 in Berlin auf Betreiben führender Compliance-Praktiker und -Experten gegründet und hat als gemeinnütziger Verein Mitglieder aus allen Branchen in Deutschland, darunter namhafte DAX-Unternehmen, Wirtschaftsprüfungs- und Beratungsgesellschaften sowie aus der Wissenschaft. DICO versteht sich als unabhängiges interdisziplinäres Netzwerk für den Austausch zwischen Wirtschaft, Wissenschaft, Politik und Verwaltung und sieht sich als zentrales Forum für die konsequente und praxisbezogene Förderung und Weiterentwicklung von Compliance in Deutschland.

DICO fördert Compliance in Deutschland, definiert in diesem Bereich Mindeststandards, begleitet Gesetzgebungsvorhaben und unterstützt zugleich die praktische Compliance-Arbeit in privaten und öffentlichen Unternehmen, fördert Aus- und Weiterbildung und entwickelt Qualitäts- sowie Verfahrensstandards.

DICO

DICO – Deutsches Institut für Compliance
Bergstraße 68
D-10115 Berlin
info@dico-ev.de
www.dico-ev.de