

- die in § 2 Abs. 2 und 3 genannten Risiken (inklusive Auffangtatbestand in § 2 Abs. 2 Nr. 12) sowie
- die Risikobewertungsmethodik erläutern und handhabbar machen. Idealerweise wird den Verantwortlichen anschließend ein Handout sowie der erstellte Risikokatalog (→ Rn. 41) ausgehändigt.

2. Abstrakte Risikobetrachtung

S. zunächst → Rn. 66 ff. zum Hintergrund, der praktischen Relevanz und der konkreten Durchführung der abstrakten Risikobetrachtung. Praktisch relevant ist die abstrakte Risikobetrachtung vor allem im Rahmen der Risikoanalyse bei unmittelbaren Zulieferern. Das bedeutet aber nicht, dass sie nicht auch im Rahmen der Risikoanalyse im eigenen Geschäftsbereich im Einzelfall zum Tragen kommen kann. Insoweit kann 1:1 auf die Ausführungen hierzu in der **BAFA-Handreichung zur Umsetzung einer Risikoanalyse** nach den Vorgaben des LkSG (dort S. 13) verwiesen werden. Dort heißt es (Hervorhebungen durch den Autor):

Die „abstrakte Risikobetrachtung ist zwar auch im Rahmen der regelmäßigen Risikoanalyse **im eigenen Geschäftsbereich grundsätzlich zulässig**. Voraussetzung hierfür ist jedoch, dass die vom Anwendungsbereich des LkSG betroffene Gesellschaft so **viele Tochtergesellschaften/Filialen/Standorte** hat, dass eine individuelle Betrachtung aller Töchter/Einheiten (zumindest zunächst) nicht zumutbar erscheint bzw. die Gesellschaft ihren risikobasierten Ansatz plausibel darlegen kann. Die abstrakte Risikobetrachtung dient der Identifizierung von Gesellschaften/Filialen/Standorte im eigenen Geschäftsbereich mit einer erhöhten Risikoexposition für eine konkrete Risikobetrachtung wie sie im Rahmen von Schritt 2 beschrieben wird.“

Wie auch bei den unmittelbaren Zulieferern bedeutet dieses priorisierte Vergehen jedoch nicht, dass diese Gesellschaften/Filialen/Standorte überhaupt nicht mehr vom LkSG-Risikomanagement erfasst sind. Vielmehr hat die berichtspflichtige Gesellschaft gemäß ihrer Pflicht zur Einrichtung eines wirksamen Risikomanagements (§ 4 Abs. 1) dafür Sorge zu tragen, dass die **relevanten Mitarbeiter:innen in ausnahmslos** allen vom eigenen Geschäftsbereich umfassten Gesellschaften/Filialen/Standorten für die nach dem LkSG geschützten Rechtspositionen **sensibilisiert** und damit befähigt sind, entsprechende Risiken zu identifizieren und an die hierfür zuständigen Stellen im Konzern zu berichten. Die relevanten Mitarbeiter:innen müssen mithin – bspw. durch Schulungen, E-Learnings, Workshops, Einzelgespräche und Handreichungen – befähigt werden, Menschenrechts- und/oder umweltbezogene Risiken zu erkennen. Darüber hinaus muss im Rahmen eines unternehmens-/konzernweiten Berichtswesens dafür gesorgt sein, dass erkannte Risiken zuverlässig und zeitnah den zuständigen Stellen gemeldet werden. Das Gleiche gilt für die Implementierung eines effektiven Beschwerdemechanismus sowie ggf. für Präventivmaßnahmen, wenn und weil diese auch in den nicht-priorisierten Gesellschaften/Filialen/Standorten sinnvoll Anwendung finden (etwa Richtlinien).

Gesellschaften, die im Sinne eines risikobasierten Ansatzes zunächst auf eine abstrakte Risikobetrachtung setzen und die konkrete Risikobetrachtung nur bei priorisierten Gesellschaften/Filialen/Standorten durchführen, sind verpflichtet, **schrittweise** zu einer verbesserten Informationslage über den gesamten eigenen Geschäftsbereich zu gelangen und damit den Prozess der konkreten Risikobetrachtung im Rahmen der Risikoanalyse **auf alle Gesellschaften/Filialen/Standorte** im eigenen Geschäftsbereich **auszuweiten**.“

Aus dem Vorstehenden wird deutlich, dass eine abstrakte Risikobetrachtung iRd Risikoanalyse im eigenen Geschäftsbereich nur bei Konzernstrukturen mit einer Vielzahl von bestimmend beeinflussten konzernangehörigen Gesellschaften zulässig sein dürfe. Ein dauerhaftes „**Ausklammern**“ bestimmter Gesellschaften ist in **keinem Fall zulässig**. Vielmehr erlaubt die abstrakte Risikobetrachtung hier (nur)

ein schrittweises Vorgehen und „entlastet“ die Obergesellschaft in größeren Konzernen insoweit, dass sie die Risikoanalyse im eigenen Geschäftsbereich nicht bereits im ersten Jahr bei allen relevanten Gesellschaften durchgeführt haben müssen.

3. Konkrete Risikobetrachtung

39 Nach der abstrakten Risikobetrachtung – soweit sie wie soeben (→ Rn. 34 ff.) erläutert im Rahmen der Risikoanalyse im eigenen Geschäftsbereich ausnahmsweise zulässig ist – folgt als zweiter Schritt die konkrete Risikobetrachtung. Gehören zum eigenen Geschäftsbereich nicht so viele Tochtergesellschaften/Filialen/Standorte, dass eine abstrakte Risikobetrachtung zulässig in Betracht kommt, bildet die konkrete Risikobetrachtung den ersten Schritt der LkSG-Risikoanalyse. Sie besteht aus den **Teilschritten** der **Identifikation** (→ Rn. 40 ff.) und **Bewertung** (→ Rn. 49 ff.) von Risiken (in der BAFA-Handreichung Risikoanalyse (S. 12) wird der Schritt der konkreten Risikobetrachtung wie folgt beschrieben: „Konkrete Ermittlung von Risiken und ihre Gewichtung sowie Priorisierung anhand der in § 3 Abs. 2 genannten Kriterien.“). Die genannten Teilschritte unterscheiden sich hinsichtlich Methodik und Prozessablauf im Grundsatz nicht von der Identifikation und Bewertung von Risiken bei klassischen Risikomanagementsystemen oder Compliance Management Systemen (dazu → § 4 Rn. 7 ff.). Insofern muss bei der Identifikation und Bewertung von LkSG-Risiken nicht das sprichwörtliche Rad neu erfunden werden. Vielmehr kann auf in der Praxis bewährte (und im Unternehmen idealerweise bereits vorhandene) Methoden und Vorgehensweisen aufgesetzt werden.

a) Identifikation von Risiken

40 Nicht identifizierten Risiken kann nicht durch entsprechende Präventionsmaßnahmen vorgebeugt werden. Die sachgerechte Risikoidentifikation ist daher der erste und zentrale Schritt der Risikoanalyse und bildet die Grundlage für die Entwicklung eines wirksamen LkSG-Risikomanagementsystems. Dabei geht es um die **Sammlung** aller LkSG-relevanten, mithin der in § 2 Abs. 2 und 3 aufgelisteten Risiken. Im Rahmen der Identifikation sind alle LkSG-Risiken zu dokumentieren, deren Realisierung nicht praktisch ausgeschlossen werden kann, dh ungeachtet ihrer konkreten Eintrittswahrscheinlichkeit oder Schadenswirkung. Es sollte in diesem ersten Teilschritt also bewusst noch **keine Bewertung** einzelner identifizierter Risiken erfolgen.

aa) Erstellung eines Risikokatalogs

41 In der Praxis haben Mitarbeiter:innen, die mit der Risikoidentifikation betraut werden, regelmäßige Schwierigkeiten damit, die im Gesetz häufig recht abstrakt beschriebenen Risiken zu identifizieren (Beispiel: „*Verbot der Herbeiführung einer schädlichen Bodenverunreinigung*“, § 2 Abs. 2 Nr. 9). Die häufigste Frage, die der Autor bei entsprechenden Risikoworkshops hört, ist regelmäßig: „Haben Sie dafür ein Beispiel?“. Daher hat sich in der Praxis als **Hilfestellung für die Risikoidentifikation** die Erstellung eines Risikokatalogs bewährt. Dabei geht es darum, idealerweise für jede der in § 2 Abs. 2 und 3 genannten geschützten Rechtspositionen bzw. Risiken **beispielhafte Risikobeschreibungen** zu entwerfen, die im Unternehmen denkbar wären. An diesen beispielhaften Risikobeschreibungen können sich die Mitarbeitenden, denen die Aufgabe der Risikoidentifikation im eigenen Geschäftsbereich übertragen wird, orientieren. Mit der Erstellung eines Risikokatalogs betraut werden regelmäßig die Gruppenfunktionen/Fachabteilungen, denen die festgelegten Risikokategorien zugeordnet worden sind (→ Rn. 27 f.). Die nachfolgende Abbildung zeigt beispielhaft einen Ausschnitt aus einem Risikokatalog.

| Nr. | Typ | gesetzl. Anknüpfung | Risikohinzeichnung | Relevanz | Risikobeschreibung | Ursachen | Präventionsmaßnahmen |
|-------|--------------------|---------------------------------|-----------------------------------|----------|--|--|--|
| HR_01 | Menschenrechtisiko | Kinderarbeit | Kinderarbeit unter 15 Jahren | Ja | Ein Kind unter 15 Jahren arbeitet. | | * Die Altersgrenze der Schulpflicht im jeweiligen Land prüfen. * Im Einschulungsprozess das Alter des Bewerbers prüfen (Ausweis o. Ä.). * Bei der legalen Beschäftigung Minderjähriger/Heranwachsender: * Die Angemessenheit der Tätigkeit oder Tätigkeitsstätte für Minderjährige prüfen. * Einen Verantwortlichen als Ansprechpartner und zur Kontrolle der Angemessenheit der Tätigkeit bestimmen. * Enge Absprachen und vertragliche Regelungen mit den Erziehungsberechtigten treffen. |
| HR_02 | Menschenrechtisiko | Kinderarbeit | Kinderarbeit während Schulpflicht | Ja | Ein/e Minderjährige/r mit mind. 15 Jahren arbeitet vor Ablauf der Schulpflicht. | | |
| HR_03 | Menschenrechtisiko | Besonders schlimme Kinderarbeit | Sklaverei bei Kindern | Nein | Ein Kind verrichtet Arbeiten mit hoher körperlicher Belastung, bspw. das Tragen oder Bewegen schwerer Lasten, Arbeiten mit schweren Gerät. | * Kinder können jüngerer beschäftigt werden. * Kinder können bestmögliche Tätigkeiten besser ausführen. | |
| HR_04 | Menschenrechtisiko | Besonders schlimme Kinderarbeit | Sklaverei bei Kindern | Nein | Ein Kind arbeitet unter belastenden Umständen, bspw. mit lauten Maschinen, bei großer Hitze, in Enge oder Dunkelheit. | * Es herrscht ein Mangel an Arbeitskräften. * Von Kindern wird weniger Widerstand erwartet. | * Das Recht des Beschäftigungsortes prüfen und anwenden. * Ggf. an internationalen Standards, die über das Recht des Beschäftigungsortes hinaus gehen, orientieren. * Verantwortliche auf persönliche Eignung prüfen und schulen. * Angemessene Vertragsdokumente zur Beschäftigung konzipieren. * Angemessenen Beschwerde- und Hinweisgebersystem implementieren. * Speak-up-Kultur fördern. |
| HR_05 | Menschenrechtisiko | Besonders schlimme Kinderarbeit | Sklaverei bei Kindern | Nein | Ein Kind arbeitet unter gefährlichen Umständen, bspw. durch große Maschinen, schwere Gegenstände, Naturgewalten wie Wasser. | | |
| HR_06 | Menschenrechtisiko | Besonders schlimme Kinderarbeit | Sklaverei bei Kindern | Nein | Ein Kind arbeitet in einem unzureichenden zeitlichen Umfang oder bekommt keine angemessenen Ruhepausen. | | |
| HR_07 | Menschenrechtisiko | Besonders schlimme Kinderarbeit | Sklaverei bei Kindern | Ja | Ein Kind arbeitet, ohne dass die Arbeitsbedingungen vertraglich geregelt sind. | | |

Abb. 2: Ausschnitt aus einem beispielhaften Risikokatalog

Nachstehend werden die in der Praxis **wichtigsten Informationskanäle** zur Risikoidentifikation skizziert, wobei stets mehrere Informationskanäle parallel eingesetzt werden sollten:

bb) Risiko-Reporting

Jedes Risikomanagementsystem ist nur so wirksam wie die Berichterstattung zu aktuellen, neuen und veränderten Risiken. Ein wirksam gestaltetes kontinuierliches (ggf. konzernweites) Risiko-Reporting liefert fortwährend Informationen mit Relevanz für die Risikoidentifikation. Risiko-Reporting besteht in der **periodischen** (zB monatlichen oder quartalsweisen) Berichterstattung sowie der **anlassbezogenen** Berichterstattung bei besonderen Ereignissen. **Berichterstatter** sind die Risk Manager bzw. Risk Owner in den Geschäftsbereichen, Tochtergesellschaften, Filialen und Standorten. Die Berichterstattung erfolgt jeweils an die Person, welche die übergeordnete koordinierende Rolle für das LkSG-Risikomanagement hat.

Ein **wirksames Risiko-Reporting** sollte folgende Grundvoraussetzungen erfüllen:

- eindeutige Festlegung der für das Reporting Verantwortlichen (Berichterstatter und Adressaten) sowie
- klar festgelegte einheitliche Reporting-Ziele und Reporting-Intervalle,
- Schulung und Einweisung der Verantwortlichen
- einheitlich und klar definierte Mess- und Bewertungskriterien für Risiken,
- präzise Festlegung der Kriterien der Ad-hoc-Berichterstattung,
- Verwendung von unternehmensweit einheitlichen Reporting-Formaten,

cc) Fragebogengestützte Informationsgespräche:

Die Risikoidentifikation wird in der Praxis regelmäßig auch mittels fragebogengestützter Informationsgespräche durchgeführt, die mit den Risk Managern/Risk Ownern in allen relevanten Geschäftsbereichen/Tochtergesellschaften/Filialen/Standorten stattfinden.

dd) Risiko-Workshops

Ein bewährtes Instrument im Rahmen der Risikoidentifikation und -bewertung sind Risiko-Workshops. Sie führen neben ihrem primären Einsatzzweck (Identifizierung und Bewertung von (neuen) Risiken) stets zu einem verbesserten Risikoverständnis der Beteiligten und zu wichtigen Erkenntnissen über den Zusammenhang

verschiedener Einzelrisiken und Risikoparameter. Einsetzbar sind Risiko-Workshops in allen Unternehmensbereichen. Sie können sowohl auf Ebene der Geschäftsleitungen im Rahmen der **Top-down**-Beurteilung von Risiken durchgeführt werden als auch **Bottom-up** auf allen Ebenen darunter. In Abhängigkeit von den gesetzten Zielen können aber auch gemischte Workshops durchgeführt werden.

ee) Beschwerdeverfahren

- 48 In der **BAFA-Handreichung zur Umsetzung einer Risikoanalyse nach den Vorgaben des LkSG** (S. 4) heißt es zu Recht, dass „*auch Informationen zu Risiken und tatsächlichen Pflichtverletzungen, die durch die Bearbeitung von Hinweisen und Beschwerden gewonnen wurden*“, iRd Risikoanalyse zu berücksichtigen sind. Ein effektives Beschwerdeverfahren ist notwendiger und zentraler Bestandteil einer sachgerechten Risikoidentifikation und damit eines wirksamen LkSG-Risikomanagementsystems. Mitarbeitenden, Zulieferer und vor allem Betroffene sollen auf diese Weise die Möglichkeit erhalten, geschützt Hinweise auf Risiken bzw. Sorgfaltspflichtverstöße in der Lieferkette des Unternehmens zu geben.

b) Bewertung von Risiken

- 49 Gem. § 5 Abs. 2 S. 1 sind die ermittelten menschenrechtlichen und umweltbezogenen Risiken angemessen zu gewichten. Nach der Risikoidentifikation ist damit die systematische **Risikobewertung der nächste Schritt** zur Durchführung einer wirksamen LkSG-Risikoanalyse. Alle im Rahmen der Risikoidentifikation gesammelten (und dokumentierten) LkSG-Risiken müssen hierbei bewertet werden. Hierbei sind gemäß § 5 Abs. 2 S. 2 „*insbes. die in § 3 Absatz 2 genannten Kriterien maßgeblich*“, nämlich:
- Art. und Umfang der Geschäftstätigkeit
 - Eintrittswahrscheinlichkeit
 - Einflussmöglichkeit
 - Schwere der Verletzung nach Grad, Anzahl der Betroffenen und Unumkehrbarkeit
 - Verursachungsbeitrag des Unternehmens zu einzelnen Risiken oder Risikobereichen
- 50 **Ausschlaggebend** für eine wirksame Risikoanalyse ist aber letztlich, dass **Eintrittswahrscheinlichkeit** und **Schwere der Verletzung einzeln** (!) bewertet werden: Wie die BAFA-Handreichung Risikoanalyse (S. 4 Fn. 12) klarstellt, ist das Kriterium „Art. und Umfang der Geschäftstätigkeit“ (dazu → § 3 Rn. 73 f.) übergreifend und mit Blick auf die Vorbereitung der Risikoanalyse zu berücksichtigen, nicht als konkretes Kriterium zur Bewertung und Priorisierung. Das leuchtet unmittelbar ein: Art und Umfang der Geschäftstätigkeit kann bspw. bei der Frage eine Rolle spielen, welche finanziellen und personellen Ressourcen ein Unternehmen aufwenden muss, um für größere Transparenz in der Lieferkette zu sorgen. Hier wird man bspw. von einem DAX-40 Unternehmen mit einem Milliardenumsatz im zweistelligen Bereich größere Bemühungen erwarten als von einem mittelständischen Unternehmen, dessen Umsatz eher im unteren dreistelligen Millionenbereich liegt.
- 51 Ebenfalls mit Blick auf die Wirksamkeit der Risikoanalyse **zu vernachlässigen** sind **Einflussmöglichkeit** (dazu → § 3 Rn. 90 f.) und **Verursachungsbeitrag** (dazu → § 3 Rn. 131 f.). Denn mit Blick auf die Zielsetzung des LkSG („*Verbesserung der weltweiten Menschenrechtslage entlang von Lieferketten*“; BT-Drs. 19/28649, 1) und dem Umstand, dass es iRd LkSG-Risikomanagementsystems auf die Interessen der Betroffenen ankommt (vgl. § 4 Abs. 4), können diese beiden Kriterien nicht ausschlaggebend sein. Dies verdeutlicht folgende Überlegung: Sollte ein Unternehmen beschließen, Maßnahmen zur Minimierung jedes in seiner Lieferkette identifizierten Risikos zu ergreifen, unabhängig von einem Verursachungsbeitrag oder der Einflussmöglichkeiten, kann diesem Unternehmen kein Sorgfaltspflichtverstoß angelastet

werden mit dem Argument, es habe diese beiden in § 3 Abs. 2 genannten Kriterien bei der Risikobewertung nicht berücksichtigt. Denn das Unternehmen leistet in diesem Fall sogar mehr als es nach dem Gesetz eigentlich müsste, weil es nicht verursachte Risiken eigentlich gar nicht adressieren müsste (vgl. BT-Drs. 19/28649, 43).

Aus der maßgeblichen Sicht der Betroffenen und somit für eine wirksame Risikoanalyse **erforderlich** ist **allein**, dass **Eintrittswahrscheinlichkeit** und **Schwere der Verletzung** einzeln bewertet werden, „*bspw. mittels einer Skala bzw. einer Heatmap*“ (BAFA, Handreichung Risikoanalyse, S. 12). Das sind im Grundsatz genau die beiden Kriterien, die auch bei der Bewertung identifizierter Risiken im Rahmen klassischer Risikomanagementsysteme und Compliance Management Systeme angewendet werden (vgl. BAFA-Handreichung Risikoanalyse, Fn. 17, 18, jeweils mit dem Verweis auf die beiden IDW Standards PS 980 und PS 981). Daher empfiehlt es sich, nach Möglichkeit die im konkreten Unternehmen bereits existierende Methodik zur Bewertung von Compliance-Risiken oder der RMS-Risiken auf die Bewertung von LkSG-Risiken zu übertragen. Hierbei ist jedoch eines zu beachten: Anders als bei der Risikobewertung im Rahmen von Compliance Management Systemen und klassischen Risikomanagementsystemen (dort spricht man von „Schadenspotenzial“) geht es nicht um die Bewertung möglicher Schäden für das Unternehmen (sog. **Outside-In Perspektive**), sondern um die Bewertung möglicher Schäden für die Betroffenen (sog. **Inside-Out Perspektive**, → § 4 Rn. 15).

Entsprechend dem **Top-down/Bottom-up-Prinzip** (→ Rn. 45) sollten idealerweise unterschiedliche Unternehmensebenen in die Risikobewertung einbezogen werden. Stets sollten die Einschätzungen der am nächsten an den risikorelevanten Prozessen arbeitenden Mitarbeitenden (regelmäßig die Risk Owner) beachtet werden. Daneben sollten etwa die relevanten Bereichs-/Standortleitende oder die Geschäftsleitung der Tochtergesellschaften oder die Gruppenfunktionen (regelmäßig die Risk Manager) einbezogen werden, etwa dergestalt, dass sie eine Plausibilitätskontrolle der von den Risk Ownern vorgenommenen Risikoidentifikation und -bewertung vornehmen.

Für die Wirksamkeit der Risikobewertung ist es essenziell, dass die Risikobewertung „*nachvollziehbar nach einer konsistent angewandten Systematik*“ und für alle Beteiligten konzernweit nach denselben **Bewertungskriterien** für Eintrittswahrscheinlichkeit und Schwere der Verletzung erfolgt. Eine einheitliche Vorgabe der Risikobewertungsmethode macht nicht zuletzt deshalb Sinn, weil eine **Priorisierung** nur dann sinnvoll möglich ist, wenn alle relevanten Risiken nach der gleichen Methode bewertet worden sind.

Üblicherweise wird bei der Risikobewertung iRv Compliance Management Systemen und klassischen Risikomanagementsystemen zwischen Brutto- und Netto- risiko unterschieden: Die Bestimmung der Eintrittswahrscheinlichkeit und Schadenshöhe einzelner Risiken wird zunächst ohne Berücksichtigung der Wirkung und Wirksamkeit etwaiger bereits vorhandener Steuerungsmaßnahmen vorgenommen (sog. **Brutto- risiken**). Sodann wird bei der Bewertung die Wirkung der bereits umgesetzten Steuerungsmaßnahmen zur Minimierung des Risikos mit einbezogen und auf diese Weise das sog. **Nettorisiko** ermittelt. Abhängig von der Höhe des so bestimmten Nettorisikos und dem aus Sicht der Geschäftsleitung vertretbaren Maß an Risikobereitschaft ist die Konzeption und Umsetzung neuer oder die Anpassung bestehender Maßnahmen und Prozesse erforderlich.

Die Risikobewertung sollte unter **fachkundiger Reflektion** und **Moderation** erfolgen. Hier empfiehlt sich die Einbindung des Compliance Office und/oder der Risikomanagement-Abteilung, weil diese Abteilungen mit der Methodik der Risikoanalyse vertraut sind und regelmäßig die größte Erfahrung bei der Risikoanalyse besitzen. Freilich können auch externe Fachleute eingebunden werden.

c) Priorisierung von Risiken

Im Anschluss an die Bewertung erfolgt bei der klassischen Risikoanalyse iRv Compliance Management Systemen oder Risikomanagementsystemen regelmäßig

eine Priorisierung ist einer Staffelung bzw. der Bildung einer Rangordnung der einzelnen Risiken nach Risikointensität, also Eintrittswahrscheinlichkeit und (materielles und immaterielles) Schadenspotenzial. In der Praxis wird dies regelmäßig mit plakativen Lösungen, bspw. einer Heatmap, veranschaulicht. § 5 Abs. 2 S. 1 spricht auch iRd LkSG-Risikoanalyse davon, dass die ermittelten menschenrechtlichen und umweltbezogenen Risiken angemessen zu gewichten „und zu priorisieren“ sind. Die Priorisierung ist allerdings iRd LkSG-Risikoanalyse **kein zwingender Schritt**, wie sich aus der Gesetzesbegründung klar ergibt. Danach sind die Risiken, „**wenn notwendig**, zu priorisieren. Auf dieser Grundlage kann das Unternehmen entscheiden, welche Risiken es zuerst adressiert, sollte es nicht in der Lage sein, alle Risiken gleichzeitig anzugehen.“ Sprich: Nur in dem Fall, dass in der Lieferkette des Unternehmens so viele menschenrechtliche und/oder umweltbezogene Risiken bestehen, dass es nicht alle gleichzeitig angehen kann, soll – ist eines risikobasierten Ansatzes – eine Priorisierung vorgenommen werden.

III. Jährliche Risikoanalyse bei unmittelbaren Zulieferern

58 Die vorstehend (→ Rn. 21 ff.) beschriebene Risikoanalyse im eigenen Geschäftsbereich bereitet betroffenen Unternehmen – verglichen mit der bei unmittelbaren Zulieferern – in aller Regel wenig Schwierigkeiten. Dies liegt daran, dass sie sich mit Blick auf Methodik und Prozessablauf nicht wesentlich von der Risikoanalyse im Rahmen des Compliance Management Systems oder des klassischen Risikomanagementsystems unterscheidet. Anders ist dies bei der Risikoanalyse mit Blick auf die unmittelbaren Zulieferer (zum Begriff → § 2 Rn. 186 ff.). Sie stellt erfahrungsgemäß eine der **größten Herausforderungen bei der Umsetzung des LkSG** für Unternehmen dar. Dies hat vor allem **zwei Gründe**:

- Die **große Anzahl** der unmittelbaren Zulieferer – jedes größere mittelständische Unternehmen erreicht schnell eine Anzahl unmittelbarer Zulieferer im fünfstelligen Bereich
- Die **mangelnde Transparenz**, mithin das Fehlen notwendiger Informationen für die Risikoanalyse – oftmals kennen Unternehmen nicht einmal die Produktionsstätten ihrer Zulieferer

59 Mit Blick auf die durchzuführenden Schritte unterscheidet sich die Risikoanalyse bei unmittelbaren Zulieferern gleichwohl nicht von der im eigenen Geschäftsbereich: Auch hier beginnt der Umsetzungsprozess mit vorbereitenden Maßnahmen (dazu sogleich → Rn. 60 f.), gefolgt von der abstrakten (→ Rn. 66 f.) und konkreten Risikobetrachtung (→ Rn. 79 f.).

1. Vorbereitende Maßnahmen

a) Bestimmung von Zuständigkeiten

60 Wie bereits oben (→ Rn. 22) erläutert, ist die klare und überschneidungsfreie Zuordnung von Zuständigkeiten eine der zentralen Voraussetzungen eines wirksamen Risikomanagementsystems und notwendige Vorbereitungsmaßnahme für die Durchführung der Risikoanalyse. Regelmäßig obliegt die Zuständigkeit für die Durchführung der Risikoanalyse aus naheliegenden Gründen bei der **Einkaufs-** bzw. **Procurement-Abteilung**. In Konzernstrukturen sind entsprechende zuständige Personen (Risk Manager/Risk Owner) nicht nur beim zentralen Einkauf der Obergesellschaft zu bestimmen. Denn unmittelbare Zulieferer von bestimmend beeinflussten konzernangehörigen Gesellschaften sind zugleich unmittelbare Zulieferer der Obergesellschaft. Sofern also der Einkauf im Konzern – was erfahrungsgemäß die Regel ist – jedenfalls nicht 100 % zentral gesteuert wird, sind auch in den bestimmend beeinflussten konzernangehörigen Gesellschaften, welche direkte Vertragsverhältnisse mit Lieferanten pflegen, entsprechende **Risk Manager/Risk Owner** zu benennen. Je nach Größe der konzernangehörigen Gesellschaft sowie der Anzahl der direkten Vertragspartner kann der ernannte Risk Manager/Risk

Owner für die direkten Vertragspartner personenidentisch mit dem Risk Manager/ Risk Owner in der Gesellschaft sein, der für die Risikoanalyse im eigenen Geschäftsbereich verantwortlich ist (→ Rn. 22).

Beispiel: Die X AG mit über 3000 Arbeitnehmern in Deutschland hat 2 Tochtergesellschaften (A GmbH und B GmbH), über die sie bestimmten Einfluss ausübt. Die A GmbH hat 600 Arbeitnehmer, 2.500 direkte Vertragspartner und eine Einkaufsabteilung mit einem Leiter und 6 Mitarbeitenden. Die B GmbH hat nur 20 Arbeitnehmer, ca. 40 direkte Vertragspartner und keine Einkaufsabteilung. In diesem Beispiel kann es Sinn ergeben, bei der A GmbH einen Risk Manager (zB Mitglied der Geschäftsführung) und einen Risk Owner (fachlich geeigneter Mitarbeitenden) für die Risikoanalyse im eigenen Geschäftsbereich zu benennen sowie daneben einen Risk Manager (Leiter Einkauf) und einen Risk Owner (Mitarbeitenden des Einkaufs) für die Risikoanalyse bei den 2.500 direkten Vertragspartnern, die als unmittelbare Zulieferer der X AG zu qualifizieren sind und daher vom Scope der Risikoanalyse umfasst sind. Hingegen dürfte es bei der B GmbH aufgrund der geringen Mitarbeiterzahl sowie der überschaubaren Lieferantenzahl genügen, nur einen Risk Manager (Mitglied der Geschäftsführung) für die Risikoanalyse sowohl im eigenen Geschäftsbereich als auch bei unmittelbaren Zulieferern zu bestimmen.

b) Überblick über die Beschaffungsstruktur

Ausweislich der Gesetzesbegründung zu § 5 (BT-Drs. 19/28649, 44) sollen sich betroffene Unternehmen in einem ersten Verfahrensschritt einen Überblick über ihre Beschaffungsstruktur verschaffen. Dies könne – so die Gesetzesbegründung weiter – „in Form eines Risikomappings nach Geschäftsfeldern, Standorten, Produkten oder Herkunftsländern erfolgen.“ Dieses Risikomapping, das iRd abstrakten Risikobetrachtung (dazu sogleich → Rn. 66 f.) durchgeführt wird, ist nur dann möglich, wenn i) die Grundgesamtheit aller unmittelbaren Zulieferer bestimmt worden ist und ii) bestimmte Mindestinformationen über diese Zulieferer zusammengetragen worden sind. Diese Mindestinformationen sind in der nachstehenden Abbildung dargestellt.








| | Zulieferer | Relevanz für das LkSG |
|---|--|--|
|  | Eingetragener Firmensitz | Länderrisiken (Indizes) |
|  | Betriebs-/Produktionsstätten (falls bekannt) | Länderrisiken (Indizes) |
|  | Branche (nach NACE Codes, Level 2) | Industrierisiken (Indizes) |
|  | Auftragsvolumen im letzten Geschäftsjahr | Definition der Nichtaufnahmegrenze |
|  | Anzahl der Bestellungen im letzten Geschäftsjahr | Qualität der Geschäftsbeziehung (Einflussmöglichkeit/Verursachungsbeitrag) |
|  | Datum des Ersteintrags des Lieferanten | Dauer der Geschäftsbeziehung (Einflussmöglichkeit/Verursachungsbeitrag) |
|  | Lieferintervall (falls angegeben) | Qualität der Geschäftsbeziehung (Einflussmöglichkeit/Verursachungsbeitrag) |

Abb. 3: Notwendige Informationen für die Durchführung des Risikomappings

Aus der vorstehenden Tabelle wird ersichtlich, dass es sich bei den zusammenzutragenden Informationen um solche handelt, über die das Unternehmen selbst verfügen dürfte. Eine – wie auch immer geartete – Informationsbeschaffung bei den Zulieferern (zB mittels Fragebogen) sollte also in diesem Stadium der Risikoanalyse noch nicht erforderlich sein und bei der Vielzahl der Zulieferer in der Regel

auch nicht zumutbar iSd Angemessenheitskriteriums. Für das Zusammentragen der Informationen über die unmittelbaren Zulieferer sind idR die festgelegten Risk Manager/Risk Owner aus dem Einkauf (→ Rn. 60) zuständig.

- 65 Wie bereits oben (→ Rn. 58) erwähnt, ist die regelmäßig enorme Anzahl der unmittelbaren Zulieferer eine der größten Herausforderungen für Unternehmen bei der Durchführung der Risikoanalyse. Der Gedanke ist daher zumindest nicht fernliegend, dass im Einzelfall ein Unternehmen versucht sein könnte, seine Beschaffungsstruktur so umzugestalten, dass die Zahl der unmittelbaren Zulieferer (signifikant) reduziert wird. Diese potenzielle Gefahr hat offenbar auch der Gesetzgeber erkannt und zur Vorbeugung in § 5 Abs. 1 S. 2 formuliert: In Fällen, in denen ein Unternehmen eine **missbräuchliche Gestaltung** der unmittelbaren **Zuliefererbeziehung** oder ein **Umgehungsgeschäft** vorgenommen hat, um die Anforderungen an die Sorgfaltspflichten im Hinblick auf die unmittelbaren Zulieferer zu umgehen, gilt ein mittelbarer Zulieferer als unmittelbarer Zulieferer. In der Gesetzesbegründung (BT-Drs. 19/28649, 44 unten f.) heißt es dazu: „*Anzeichen für missbräuchliche Gestaltungen oder ein Umgehungsgeschäft sind insbesondere, wenn der zwischen dem Unternehmen und dem unmittelbaren Zulieferer auftretende Dritte keiner nennenswerten eigenen Wirtschaftstätigkeit nachgeht oder keine auf Dauer angelegte Präsenz in Gestalt von Geschäftsräumen, Personal oder Ausstattungsgegenständen unterhält.*“ Eine (jedenfalls theoretisch) naheliegende Konstellation, die demnach wohl auch der Gesetzgeber im Blick hat, ist, dass das Unternehmen eine Einkaufsgesellschaft gründet, auf die sie keinen bestimmenden Einfluss ausübt und sämtliche Verträge mit Lieferanten auf diese überträgt. Dann wäre (nur) die Einkaufsgesellschaft unmittelbarer Zulieferer iSd § 2 Abs. 7 und sämtliche bisherigen unmittelbaren Zulieferer nunmehr mittelbare Zulieferer iS von § 2 Abs. 8. In der Praxis nicht selten anzutreffen sind Unternehmen, die ihre Waren und Dienstleistungen tatsächlich weitestgehend über eine (regelmäßig in Luxemburg sitzende) Einkaufsgesellschaft beziehen, was in erster Linie steuerrechtliche Gründe hat. Jedenfalls sofern – was der Regel entspricht – diese Konstellation bereits bestand, bevor es das LkSG gab, kann von einer missbräuchlichen Gestaltung keine Rede sein. Auch im Übrigen dürfte die praktische Relevanz des § 5 Abs. 1 S. 2 überschaubar sein.

2. Abstrakte Risikobetrachtung

- 66 Die abstrakte Risikobetrachtung ist aus Sicht der dem LkSG unterfallenden Unternehmen ein zentraler Schritt der Risikoanalyse bei unmittelbaren Zulieferern. Denn in diesem Schritt geht es darum, aus der regelmäßig mind. im mittleren vierstelligen Bereich liegenden Anzahl der Zulieferer mit einem angemessenen und wirksamen Ansatz die sogenannten **Hochrisiko-Zulieferer** zu identifizieren, bei denen potenziell eher mit menschenrechtlichen und umweltbezogenen Risiken zu rechnen ist. Nur so kann das Unternehmen iS eines **risikobasierten Ansatzes** seine Ressourcen zielgerichtet bei **Zulieferern mit einer voraussichtlich erhöhten Risikodisposition** einsetzen. In der BAFA-Handreichung (BAFA, Handreichung Risikoanalyse, S. 14) wird dieser Schritt der Risikoanalyse bewusst als abstrakte „Betrachtung“ (und nicht abstrakte „Analyse“) von Risiken bezeichnet. Denn es werden bei Lichte betrachtet keine Risiken bei Zulieferern analysiert. Vielmehr werden Quellen (zB **Indizes** und **Rankings**, Länderberichte, Berichte von Regierungsorganisationen etc.) betrachtet, in denen wiederum eine Bewertung oder Analyse vorgenommen worden ist. Anhand dieser Quellen werden bspw. mittels typischer Länder- und Branchenrisiken mit Blick auf die nach dem LkSG geschützten Rechtspositionen bzw. Risiken die Zulieferer priorisiert, die anschließend einer näheren Betrachtung unterzogen werden sollen. Bei diesen handelt es sich dann definitionsgemäß um die vom Unternehmen definierten sogenannten Hochrisiko-Zulieferer. Eine für die abstrakte Risikobetrachtung **hilfreiche Quellen** sind im **Anhang II der BAFA-Handreichung** zur Risikoanalyse (S. 20) aufgeführt. In den nachstehenden Tabellen sind weitere hilfreiche Quellen aufgeführt.