



Bundesministerium für
wirtschaftliche Zusammenarbeit
und Entwicklung



**Partners in
Transformation**
Helpdesk Wirtschaft
und Menschenrechte

Praxishilfe: Unterstützung von Sorgfaltsprozessen mit IT-Tools und Softwarelösungen

Michaela Streibelt, Dr. Jana Heinze und Malte Drewes

Inhalt

Einführung: Potenziale und Grenzen der Unterstützung von Sorgfalt mit digitalen Tools	3
1. Überblick: Funktionen von IT-Tools	4
2. Spotlight Risikoanalyse	8
Anforderungen an die Risikoanalyse	8
Chancen und Herausforderungen von IT-Tools in der Risikoanalyse	9
Exkurs: Herausforderung bei der Einbeziehung der Perspektive potenziell Betroffener	11
Integration bestimmter Funktionen von Tools in die eigene Risikoanalyse – Schritt-für-Schritt-Anleitung	10
Schritt 1 - Definition des Prozesses der Risikoanalyse	10
Schritt 2 - Kritische Analyse der Funktionen und Daten von IT-Tools	12
Schritt 3 - Informationslücken identifizieren	12
Schritt 4 - Ergänzende Maßnahmen entwickeln	14
Allgemeine Hinweise zur Nutzung von Tools im Sorgfaltsprozess	15
Weiterführende Informationen	16

Einführung: Potenziale und Grenzen der Unterstützung von Sorgfalt mit digitalen Tools

Unternehmen stehen vor der Herausforderung, menschenrechts- und umweltbezogene Sorgfaltspflichten effektiv in ihre Prozesse zu integrieren und Risiken und Verletzungen in ihren Lieferketten frühzeitig zu erkennen. IT-Tools und Softwarelösungen versprechen hierbei Unterstützung, indem sie Abläufe optimieren, Daten systematisch erfassen und die Analyse komplexer Liefernetzwerke erleichtern.

Doch so vielversprechend digitale Lösungen sind, sie bringen auch Herausforderungen mit sich. Oftmals sind die erhobenen Daten lückenhaft oder basieren auf Selbstauskünften, so dass ein realistisches Bild der tatsächlichen Risiken schwer zu erhalten ist. Zudem besteht die Gefahr, dass Unternehmen sich zu stark auf technische Lösungen verlassen, ihre Managementverantwortung abgeben und den direkten Dialog mit Stakeholdern – insbesondere mit potenziell Betroffenen – vernachlässigen. Dies kann dazu führen, dass wichtige Informationen über menschenrechts- und umweltbezogene Risiken und Verletzungen, die nicht durch Softwarelösungen erfasst werden, übersehen werden.

Weitere Herausforderungen können sein, dass Unternehmen die Bewertungsmethodik der IT-Tools nicht vollständig nachvollziehen können. Des Weiteren sind viele Anwendungen nicht interoperabel, so dass sie sich nicht ohne Weiteres in die unternehmenseigenen Prozesse integrieren lassen. Nicht zuletzt können die Kosten und der Aufwand für die Implementierung vieler dieser Tools gerade für kleinere Unternehmen eine Hürde darstellen. Für diese Unternehmen ist es oft schwierig, die notwendigen Ressourcen für eine nachhaltige digitale Transformation bereitzustellen. Dies betrifft auch kleinere Unternehmen, die von ihren Kunden in das Tool eingebunden werden.

Aus diesen Gründen sollten digitale Lösungen nicht als Allheilmittel betrachtet werden. Vielmehr sollten sie als unterstützende Instrumente im Sorgfaltsprozess gesehen werden, die nur dann ihren vollen Wert entfalten, wenn sie mit einer eigenen fundierten menschenrechts- und umweltbezogenen Analyse und einem langfristigen Engagement für die Rechte der Betroffenen kombiniert werden. Nur so kann die Effektivität dieser Lösungen maximiert und die konstruktive Wahrnehmung der Verpflichtungen durch die Unternehmen sichergestellt werden.

Diese Praxishilfe beleuchtet die aktuellen Entwicklungen im Bereich digitaler Tools für die menschenrechts- und umweltbezogene Sorgfalt, stellt Anwendungsfälle vor und diskutiert Herausforderungen sowie offene Fragen im Umgang mit IT-Tools. Hierfür haben wir uns dem Thema in zwei Workshops mit Unternehmen und zivilgesellschaftlichen Organisationen gewidmet. Die Ergebnisse dieser Workshops finden Sie zusammengefasst in dieser Praxishilfe, um Unternehmen Orientierung bei Auswahl und Nutzung von IT-Tools zu bieten. Eine Beschreibung oder Bewertung einzelner Anbieter von IT-Tools erfolgt nicht.

1. Überblick: Funktionen von IT-Tools

Es gibt viele verschiedene IT-Tools zur Unterstützung von Sorgfaltsprozessen und entsprechend viele Funktionalitäten und Methoden, die sich in den Details unterscheiden. Mit IT-Tools, IT-Lösungen oder Softwarelösungen sind in diesem Zusammenhang IT-Programme gemeint, die Unternehmen im menschenrechts- und umweltbezogenen Sorgfaltsprozess unterstützen. Tools können in der Praxis beispielsweise bei der Datensammlung und -verwaltung, der Kommunikation mit Zulieferern und der Berichterstattung gegenüber der zuständigen Behörde eingesetzt werden. Im Einzelnen können die verschiedenen IT-Tools Unternehmen teilweise unterstützen bei:



Risikoanalyse



Präventions- und Abhilfemaßnahmen



Beschwerdeverfahren



Dokumentation



Berichterstattung

Ziel vieler IT-Tools ist es, Informationen zu sammeln, zu verwalten und diese für die Umsetzung der Sorgfaltsprozesse zu nutzen. Typische Einsatzfelder sind insbesondere Unterstützung im Rahmen der Risikoanalyse (z. B. Medienscreening, Analyse öffentlich verfügbarer Datenquellen), der Lieferantenmanagement (z. B. Lieferantenprofil, Fragebögen, spezifische Interventionen) oder bei der Dokumentation und Ableitung von Präventions- und Abhilfemaßnahmen in Zusammenarbeit mit Zulieferern (z. B. Schulungen, Codes of Conduct). Die Nutzung digitaler Tools entbindet Unternehmen nicht von ihren eigenen Sorgfaltspflichten.

Insgesamt wurde in den Workshops eine große Bandbreite verschiedener Anwendungen beschrieben. IT-Tools unterscheiden sich teils erheblich im Hinblick auf ihre Qualität und Einsatzmöglichkeiten. Für einige Unternehmen ist es dementsprechend gängige Praxis, dass mehrere Tools gleichzeitig im Einsatz sind, um verschiedene Use Cases abzudecken bzw. gewisse Kundenanforderungen zu erfüllen. Herausfordernd scheint die effektive Integration digitaler Tools in bestehende Unternehmensprozesse. In diesem Zusammenhang wurde vermehrt auf die Schwierigkeit der fehlenden Interoperabilität hingewiesen.

BAFA-Erläuterungen zum Einsatz von Tools

Die BAFA-Handreichung zu Standards, Audits und Zertifizierungen¹ verweist darauf, dass Software-Lösungen darauf angewiesen sind, dass ihre Daten validiert werden, um das in sie gesetzte Vertrauen zu rechtfertigen und aufrechtzuerhalten. Nutzen diese Tools Berichtsvorlagen, hängt die Aussagekraft der Ergebnisse von den verarbeiteten (verifizierten) Informationen ab. Beispielsweise sind Selbstauskünfte von Unternehmen nicht unabhängig überprüft, was ihre Aussagekraft einschränken kann. Zudem verweist das BAFA darauf, dass die Herkunft der Daten und die Methodik zur Risikobewertung nicht immer vollständig transparent und nachvollziehbar sind. Risiko-Screening-Tools können laut BAFA Schwierigkeiten haben, tiefere Lieferketten angemessen abzubilden. Dies liegt u. a. daran, dass relevante Daten fehlen oder nicht alle Zulieferer weltweit über die notwendigen technischen und personellen Ressourcen verfügen. Herausfordernd ist laut BAFA-Handreichung zudem die Erfassung menschenrechts- und umweltbezogener Risiken in informellen Sektoren.

Das BAFA betont, dass sich teilweise eine übermäßige Abhängigkeit („Overreliance“) von solchen Systemen ergibt: Unternehmen verlassen sich zu stark auf die bereitgestellten Informationen, ohne eigene Maßnahmen zur Risikoanalyse und -ermittlung zu ergreifen. Dies kann dazu führen, dass Risiken unzureichend erfasst werden und ein effektives Risikomanagement erschwert wird. Zudem führt ein alleiniger Rückgriff auf IT-Tools auch zu einer Fehlmessung des Gesetzes und Mehraufwand, wenn das Tool Vorgaben des Gesetzes nicht abdeckt.

Daher ist es laut BAFA essenziell, dass sowohl die Funktionsweise als auch die verarbeiteten Informationen möglichst transparent und nachvollziehbar überprüfbar sein müssen – ähnlich wie es bei Standards, Audits und Zertifizierungen erforderlich sei. Bei der Integration digitaler Tools in die Risikoanalyse sollen Unternehmen daher laut BAFA-Handreichung darauf achten, nicht blind auf die bereitgestellten Daten und Bewertungen zu vertrauen, sondern risikobasiert vorzugehen und zunächst eigenverantwortlich zu prüfen, ob und welche Instrumente für die Umsetzung des Gesetzes geeignet sind.

Digitale Lösungen sind zudem häufig kostspielig und erfordern spezifisches Fachwissen, das nicht immer verfügbar ist. Zudem fehlt es an Standardisierung und Qualitätskriterien für Anbieter von Softwarelösungen. Die Vielzahl an IT-Lösungen führt dazu, dass Datenformate und Bewertungsmethoden nicht immer kompatibel sind, was die Vergleichbarkeit und Nutzbarkeit der Daten erschwert. Insgesamt stellen verschiedene technische und finanzielle Hürden eine große Herausforderung dar, insbesondere für kleine und mittelständische Unternehmen (KMU).

¹https://www.bafa.de/DE/Lieferketten/Handreichungen/handreichungen_node.html, Seite 17. Letzter Zugriff 26.06.2025.



Risikoanalyse

Tools ermöglichen es Unternehmen, menschenrechts- und umweltbezogene Risiken strukturiert zu identifizieren und sich so einen Überblick zu verschaffen, welche Themen näher beleuchtet werden sollten. Durch den Einsatz von Datenbanken, Risiko-Mapping-Software oder automatisierten Analysetools können die Unternehmen große Datenmengen aus verschiedenen Quellen bündeln und auswerten, wodurch Risiken transparenter und vergleichbarer werden. Dadurch können Unternehmen wertvolle Einblicke gewinnen und gezielter vorgehen.

Automatisierte Screening-Tools, KI-gestützte Analysen und Risiko-Rating-Systeme können im Prozessschritt der Risikoanalyse helfen, relevante Daten aus verschiedenen Quellen zu sammeln und potenzielle Risiken frühzeitig zu erkennen. Durch den Einsatz von Software können Unternehmen so präzise Daten zu Arbeitsbedingungen, Umweltschutz und anderen Aspekten generieren und übersichtlich abbilden.

Im Rahmen der Datenanalyse ermöglichen bestimmte Mapping-Tools, menschenrechts- und umweltbezogene Risiken geografisch zu verorten und risikobehaftete Regionen oder Branchen gezielt zu identifizieren. Datenbanken mit Länder- und Sektor-Risikoprofilen ermöglichen so eine faktenbasierte Einschätzung der Herausforderungen in bestimmten Regionen oder Industrien. Digitale Lösungen können damit – je nach Umfang und Tiefe der Software – potenziell auch einen Beitrag zu mehr Transparenz über Zuliefererstrukturen leisten und dabei helfen, kritische Bereiche in der Lieferkette zu erkennen.



Jedoch stoßen viele Unternehmensvertreter:innen bereits beim Einsatz von Tools für die Analyse, Priorisierung und Risikobewertung an Grenzen. In den Workshops wurde betont, dass es häufig zusätzlich einer qualitativen Einschätzung durch das Unternehmen bedarf. Viele Tools decken vor allem die Stufe der direkten Zulieferer (Tier-1) ab und erfassen nur in seltenen Fällen auch die tiefe Lieferkette, sodass wichtige Teile der Risikoanalyse nicht durch den Einsatz digitaler Tools umgesetzt werden können. Zudem gibt es Risiken und Verletzungen in globalen Lieferketten, die durch IT-Lösungen nicht erfasst und mithin nicht in die Risikoanalyse einbezogen werden können, insbesondere im informellen Sektor.



Präventions- und Abhilfemaßnahmen

In der Phase der Maßnahmenumsetzung gibt es ebenfalls verschiedene Anwendungsmöglichkeiten. Eingesetzt werden Tools beispielsweise, um Standards bei Zulieferern zu überprüfen, Compliance-Anforderungen nachzuhalten oder Codes of Conduct, Zertifizierungen bzw. auditrelevante Dokumente zu speichern. Ein weiterer Vorteil ist die Bereitstellung von Informationen in mehreren Sprachen (z. B. Fragebögen oder Schulungen).



Jedoch bleibt der Einsatz insofern eingeschränkt als bei der Umsetzung von Maßnahmen insbesondere individuelle, kontextbezogene Lösungen, der Dialog mit Betroffenen und praxisnahe Anpassungen erforderlich sind und dies nur teilweise oder nicht durch Tools abgedeckt werden kann.



Schulungen und Sensibilisierung

E-Learning-Tools oder interaktive Trainingsplattformen können Beschäftigte für menschenrechts- und umweltbezogene Risiken sensibilisieren.



Jedoch bleibt hier immer auch die Frage, ob die richtigen Zielgruppen erreicht werden, insbesondere auch deshalb, weil viele IT-Anwendungen sich vor allem auf die direkten Zulieferer fokussieren und damit weite Teile der Lieferkette außer Acht lassen, die jedoch im Sinne eines risikobasierten Ansatzes eher in den Blick genommen werden sollten. Einige Unternehmen berichteten vom Einsatz der Tools in diesem Zusammenhang, betonten jedoch gleichermaßen auch die Notwendigkeit, ihren Einsatz durch weitere Maßnahmen zu flankieren.



Beschwerdeverfahren

Digitale Meldekanäle, Apps oder Chatbots können helfen, potenziell Betroffenen eine niedrigschwellige Möglichkeit zur Kontaktaufnahme zu bieten. Anonyme Whistleblower-Systeme mit mehrsprachiger Unterstützung erhöhen die Zugänglichkeit und Sicherheit für Betroffene. Im Workshop wurde betont, dass hier erste Ansätze pilotiert würden, dies jedoch noch nicht flächendeckend ausgerollt worden seien.



Monitoring und Dokumentation

Grundsätzlich ermöglichen es Softwarelösungen, menschenrechts- und umweltbezogene Risiken und Verletzungen, Maßnahmen und Fortschritte strukturiert zu erfassen und automatisch Berichte zu generieren. Digitale Lösungen können so bei der Dokumentation und im Compliance-Management eingesetzt werden. Digitale Dashboards und Tracking-Tools können helfen, Fortschritte bei der Umsetzung von Maßnahmen zu überwachen.



Jedoch sahen einige Unternehmensvertreter:innen hier gewisse Grenzen, denn teilweise würde sich das Scoring ändern (z. B., wenn Zulieferer Dokumente hochladen) ohne dass der Nutzer darüber informiert wird bzw. die Bewertung nachvollziehen kann. Auch die Nicht-Beantwortung von Fragen könne unter Umständen eine Risikoeinstufung nach sich ziehen.

Fazit

Insgesamt können Tools an verschiedenen Stellen im Sorgfaltsprozess eingesetzt werden und werden es auch in der Praxis. Sie müssen jedoch durch das Unternehmen hinsichtlich Qualität, Nutzen und Reichweite kontinuierlich überprüft und durch eigene Maßnahmen flankiert werden.

Die meisten Unternehmensvertreter:innen sahen den größten Mehrwert beim Einsatz von Tools in der Risikoanalyse. Im nächsten Abschnitt gehen wir näher auf die Einsatzmöglichkeiten für diesen Schritt des Sorgfaltsprozesses ein.

2. Spotlight Risikoanalyse

Viele IT-Anwendungen setzen bei der Risikoanalyse an und bieten hier für Unternehmen teilweise erhebliche Erleichterungen. Im folgenden Kapitel soll Unternehmen zunächst eine Orientierung gegeben werden, welche Anforderungen sich aus dem Lieferkettensorgfaltspflichtengesetz (LkSG) an die Risikoanalyse ergeben. Nach einer überblicksartigen Darstellung der Chancen und Herausforderungen von Tools im Rahmen der Risikoanalyse und Hinweisen zur Einbeziehung potenziell Betroffener folgt eine Schritt-für-Schritt-Anleitung, was bei der Integration von Tools in den Risikomanagementprozess zu beachten ist.

Anforderungen an die Risikoanalyse

Die jährliche sowie anlassbezogene Risikoanalyse in Bezug auf den eigenen Geschäftsbereich und unmittelbare Zulieferer (§ 5 LkSG) sowie die anlassbezogene Risikoanalyse in Bezug auf mittelbare Zulieferer (§§ 5 Abs. 4, 9 Abs. 3 LkSG) ist ein grundlegender Bestandteil des Risikomanagements nach dem LkSG. Mit ihr soll Kenntnis über die menschenrechts- und umweltbezogenen Risiken und Verletzungen im eigenen Geschäftsbereich und in der Lieferkette erlangt, bewertet und priorisiert werden. Die Risikoanalyse ist ein vorbereitender Schritt zur Ergreifung von Präventions- und Abhilfemaßnahmen. Das LkSG verpflichtet hierbei zu einer angemessenen Risikoanalyse und verankert damit einen risikobasierten Ansatz. Es verpflichtet gerade nicht dazu, alle (unmittelbaren) Zulieferer jährlich zu analysieren. Stattdessen müssen Unternehmen risikobasiert vorgehen und möglicherweise nur eine Auswahl von Zulieferern sowie Zulieferer mit unterschiedlich intensiven Maßnahmen untersuchen.

Mapping: Das LkSG gibt den Prozess der Risikoanalyse nicht im Detail vor. Es bietet sich jedoch an, diesen in verschiedene Schritte zu teilen. Eine bewährte Möglichkeit ist, zunächst mit einem Mapping zu beginnen, um sich einen Überblick über die eigenen Zulieferer, Lieferketten und -netze, mögliche Risikothemen und Stakeholder-Gruppen zu verschaffen. Dies kann zum Beispiel durch eine Heat-Map geschehen. Falls aufgrund der großen Anzahl an Zulieferern erforderlich, sollte auf Basis der Heat-Map eine Auswahl für die weiteren Schritte der Risikoanalyse getroffen werden.

Abstrakte und konkrete Risikoanalyse: Im nächsten Schritt sollte man sich mit einer abstrakten Risikoanalyse einen Überblick über mögliche Risikothemen verschaffen. Hierbei werden allgemein verfügbare Quellen zu Rate gezogen wie etwa Medienberichte, Berichte von Nichtregierungsorganisationen (NGOs), Berichte von Regierungsorganisationen oder wissenschaftliche Quellen. Diese bieten dann die Grundlage für Maßnahmen der konkreten Risikoanalyse, bei der es darum geht, die gewonnenen Informationen in Bezug auf konkrete Zulieferer oder Lieferketten und -netze nachvollziehbar zu machen. Ein weit verbreitetes Instrument hierfür sind Fragebögen zur Selbstauskunft oder Audits. Dabei ist zu beachten, dass die Aussagekraft von Fragebögen und angekündigter Audits nur beschränkt ist.²

Stakeholder: Im Rahmen der Risikoanalyse nach dem LkSG sind als weiterer Schritt auch Stakeholder einzubeziehen. Dies folgt aus der Anforderung der angemessenen Berücksichtigung der Interessen potenziell Betroffener gemäß § 4 Abs. 4 LkSG. Insbesondere bei der Risikoanalyse ist ein Einbezug potenziell Betroffener wichtig, da diese Auskunft über die Situation vor Ort, vor allem in Bezug auf ihre Situation (z. B. Arbeitszeiten, Löhne, Arbeitsschutz) geben können. In Situationen, in denen Zulieferer möglicherweise nicht wahrheitsgemäß Auskunft geben, sind sie ein wichtiges Korrektiv. Die Berücksichtigung der Interessen Betroffener kann durch direkte Konsultation aber auch durch Konsultation von legitimen Interessenvertretungen (wie z. B. Gewerkschaften oder NGOs) erfolgen.³

Chancen und Herausforderungen von IT-Tools in der Risikoanalyse



IT-Tools erleichtern Unternehmen die Umsetzung der menschenrechts- und umweltbezogenen Sorgfalt, insbesondere durch höhere Effizienz und Skalierbarkeit. Sie ermöglichen eine effiziente, systematische und automatisierte Erfassung großer Datenmengen aus komplexen Lieferketten. Der Einsatz von Tools kann sich vor allem für Unternehmen mit einer Vielzahl an Zulieferern lohnen. Einige Unternehmen sehen einen Mehrwert darin, mithilfe von Tools potenzielle menschenrechts- und umweltbezogene Risiken und Verletzungen frühzeitig erkennen und so Ressourcen gezielter einsetzen zu können, insbesondere zur Erfüllung von Sorgfaltspflichten in weit verzweigten Liefernetzwerken.



Digitale Lösungen erhöhen potenziell die Transparenz und erleichtern teilweise die Nachverfolgbarkeit von Produkten und Rohstoffen in komplexen Lieferketten. Allerdings liefern solche Tools in der Regel nur für formalisierte Tätigkeiten in der Lieferkette und in vielen Fällen begrenzt auf die direkten Zulieferer (Tier-1) verlässliche Daten.



Ein zentrales Problem ist hier die begrenzte Datenverfügbarkeit und -qualität. Viele Unternehmen haben nur begrenzte Informationen über tiefere Lieferkettenstufen und die vorhandenen Daten, die sie über IT-Tools erhalten, sind oft (noch) unvollständig oder veraltet. Wichtige Bereiche globaler Lieferketten – etwa Kleinstbergbau, landwirtschaftliche Feldarbeit oder Heimarbeit – werden von IT-Tools häufig nicht ausreichend erfasst. Da jedoch in vielen Industrien die Risiken häufig insbesondere in der tiefen Lieferkette liegen, können Softwarelösungen nur ein Teil der Analysegrundlage sein.

² Siehe https://www.bafa.de/DE/Lieferketten/Risikoanalyse/risikoanalyse_node.html, letzter Zugriff 26.06.2025.

³ Siehe „BAFA Fragen und Antworten zum Lieferkettengesetz“ https://www.bafa.de/DE/Lieferketten/FAQ/haeufig_gestellte_fragen_node.html, letzter Zugriff am 26.06.2025.

 Hinzu kommt, dass einige Unternehmensvertreter:innen auch teilweise Mängel bei der Zuverlässigkeit und Qualität der Daten angemerkt haben. Beispiele hierfür sind, dass die Struktur nicht immer auf Basis von NACE-Codes fußt, dass News Monitoring nicht nochmal auf Plausibilität überprüft wird und nicht immer öffentlich-finanzierte Quellen (z. B. Berichte von Regierungen, Vereinte Nationen oder NGOs) in ausreichendem Maße einbezogen werden. Eigens erhobene Daten über die Tools z. B. in Form von Fragebögen liefern auch nicht immer die erforderlichen Informationen für die Risikoanalyse.

 Viele Tools liefern in erster Linie die Rohdaten. Diese müssen dann vom Unternehmen in die unternehmenseigenen Prozesse überführt werden. Jedoch berichten Unternehmen auch teilweise davon, dass dies häufig nicht ohne weiteres möglich sei (Stichwort: fehlende Interoperabilität). Außerdem müssen Unternehmen Datenschutz und Datensicherheit beachten. Die Verarbeitung sensibler Lieferketteninformationen birgt Risiken, insbesondere, wenn Daten über Dritte oder Plattformanbieter verwaltet werden.

Integration bestimmter Funktionen von Tools in die eigene Risikoanalyse – Schritt-für-Schritt-Anleitung

Die folgenden Schritte können dabei helfen, die eigene Risikoanalyse mit digitalen Lösungen zu unterstützen.

SCHRITT 1 - DEFINITION DES PROZESSES DER RISIKOANALYSE

Zunächst sollten Unternehmen ihren Analyseprozess definieren. Dieser Schritt umfasst die Identifikation relevanter Risiken und Verletzungen, die Bewertung und Priorisierung derselben sowie die Festlegung von Verantwortlichkeiten. Ein strukturierter Ansatz hilft dabei, relevante menschenrechts- und umweltbezogene Risiken und Verletzungen systematisch zu erfassen, Prioritäten zu setzen und Zuständigkeiten festzulegen. Wichtig ist es, eine klare Zielsetzung zu definieren bevor ein Tool eingesetzt wird, d. h. sich klarzumachen, welche konkreten Risiken und Verletzungen identifiziert werden sollen und welche Entscheidungen hierauf basieren. Die Risikoanalyse sollte nicht isoliert betrachtet werden, sondern in die gesamte Sorgfaltspflichtenstrategie des Unternehmens eingebettet sein.

Exkurs: Herausforderungen bei der Einbeziehung der Perspektive potenziell Betroffener

Im Dialog mit NGOs wurde betont, dass die Perspektive potenziell Betroffener bei digitalen Tools bisher nur begrenzt berücksichtigt werde. Viele Lösungen konzentrierten sich auf Risikobewertungen basierend auf öffentlich verfügbaren Daten, Zertifizierungen oder Selbstauskünften von Unternehmen.

Partizipative Ansätze, die Betroffene direkt einbeziehen, sind noch selten, obwohl erste Fortschritte wie Beschwerdemechanismen via Apps und partizipative Monitoring-Ansätze erkennbar sind.

Ein großes Hindernis ist der fehlende Zugang zu digitalen Technologien, Sprach- und Kulturbarrieren sowie das mangelnde Vertrauen in digitale Systeme, insbesondere in ländlichen oder ressourcenschwachen Regionen. Datenschutz und Anonymität sind daher entscheidend, um die Teilnahme zu fördern.

Die Integration der Rückmeldungen in die Sorgfaltsprozesse der Unternehmen bleibt eine Herausforderung, da oft die nötigen Strukturen und Prozesse zur systematischen Einbindung potenziell Betroffener fehlen.

- ✓ Ein hybrider Ansatz, der digitale und analoge Formate kombiniert, könnte diese Barrieren überwinden und auch Menschen ohne digitale Kompetenzen erreichen.
- ✓ Kooperationen mit lokalen Organisationen wie NGOs und Gewerkschaften können Vertrauen aufbauen und die Akzeptanz erhöhen.
- ✓ Zudem sollten Betroffene aktiv in die Gestaltung der Tools einbezogen werden, um diese bedarfsgerecht und zugänglich zu machen.
- ✓ Gesetzliche Vorgaben oder Anreize könnten Unternehmen dazu anregen, partizipative digitale Lösungen verstärkt zu nutzen.
- ✓ Letztlich müssen Unternehmen sicherstellen, dass der Datenschutz gewahrt bleibt, um Repressionen zu verhindern. Vertrauen entsteht durch langfristiges Engagement und eine kontinuierliche Auseinandersetzung mit den Ursachen der Probleme.

Insgesamt bietet die Einbindung von Betroffenen in digitale Tools großes Potenzial, erfordert jedoch einen ganzheitlichen Ansatz, der sowohl technologische, soziale als auch ethische Herausforderungen adressiert.

SCHRITT 2 - KRITISCHE ANALYSE DER FUNKTIONEN UND DATEN VON IT-TOOLS

Im nächsten Schritt gilt es zu analysieren, welche Daten und Funktionen das entsprechende IT-Tool tatsächlich liefert bzw. liefern könnte. Unternehmen sollten hinterfragen, inwieweit diese Informationen für ihre spezifischen Anforderungen ausreichen und wo Ergänzungen notwendig sind.

Viele IT-Tools zur Unterstützung der Risikoanalyse fokussieren sich aktuell beispielsweise auf die Bereitstellung einer Heat-Map sowie das Versenden und Nachhalten von Fragebögen zur Selbstauskunft. In der Praxis bedeutet das, dass Zulieferer auf Aufforderung des Unternehmens nach Einrichten eines Accounts einen Fragebogen ausfüllen. Aufwände und Kosten entstehen für Zulieferer hierbei u. a. durch die fehlende Interoperabilität, die sie zwingt, immer wieder ähnliche aber in Details doch unterschiedliche Fragebögen auszufüllen.⁴

Bürokratische und oft wenig zielführende Aufwände entstehen auch dann, wenn Tools sog. „Gießkannenansätze“ verfolgen, Tools also etwa automatisch Fragebögen an alle im System eingepflegten direkten Vertragspartner:innen verschicken. Viele Tools ermöglichen es, die gesamte Kreditorenliste einzupflegen, in denen sich z. B. auch Behörden wie lokale Finanzämter finden. Teilweise besteht die Möglichkeit, Belege wie Audit-Reports oder interne Policies hochzuladen, wobei aktuell nur wenige Anbieter eine inhaltliche Überprüfung dieser Dokumente vornehmen. In einigen Fällen führt diese Praxis jedoch dazu, dass Zulieferer Policies entwickeln, die ein besseres Scoring ergeben, ohne dass die dort aufgeführten Themen für sie relevant sind oder vom Unternehmen umgesetzt werden.

Ein rein auf den Versand von standardisierten Fragebögen gestützter Ansatz ist zudem problematisch, da er potenzielle Lücken in der Risikoanalyse hinterlässt. Unternehmen müssen neben den unmittelbaren Zulieferern auch ihren eigenen Geschäftsbereich sowie anlassbezogen mittelbare Zulieferer berücksichtigen.

Unternehmen sollten daher gezielt hinterfragen, welche Daten das IT-Tool liefert, wie aktuell und zuverlässig diese sind und wo ergänzende Informationen erforderlich sind. Auch das BAFA betont den risikobasierten Ansatz, die Berücksichtigung der Betroffenenperspektive, die Abdeckung der Lieferkette und technische Anforderungen wie die Interoperabilität (siehe Infobox auf S. 5). In diesem Zusammenhang sollte das Unternehmen u. a. auch prüfen, ob Herkunft und Qualität der Daten zugänglich sind. Die Gestaltung und Logik des zugrundeliegenden Algorithmus der jeweiligen Software-Lösung muss für Anwender:innen nachvollziehbar sein.

Die folgenden Fragen geben Orientierung bei der Prüfung der Funktionen von Tools im Rahmen der Risikoanalyse (siehe Infobox auf der nächsten Seite).

SCHRITT 3 - INFORMATIONSLÜCKEN IDENTIFIZIEREN

Wie in Schritt 1 erläutert, sollten Unternehmen gezielt hinterfragen, welche Daten das IT-Tool liefert, wie aktuell und zuverlässig diese sind und wo ergänzende Informationen benötigt werden.

⁴ Dieses Problem besteht auch, wenn mehrere LkSG-pflichtige Kundenunternehmen sich mit jeweils eigenen Fragebögen zur Selbstauskunft an ihre Zulieferer wenden. Siehe „BAFA und Helpdesk Handreichung Zusammenarbeit in der Lieferkette“ https://www.bafa.de/DE/Lieferketten/Zusammenarbeit_in_der_Lieferkette/zusammenarbeit_in_der_lieferkette_node.html, letzter Zugriff am 26.06.2025.

Fragen zur Analyse der Funktionen von IT-Tools im Rahmen der Risikoanalyse

- ✓ Wird ein risikobasierter Ansatz verfolgt?
- ✓ Welche menschenrechts- und umweltbezogenen Risiken stehen im Fokus (z. B. Kinderarbeit, Zwangsarbeit, Diskriminierung)?
- ✓ Werden die richtigen Adressaten erreicht?
- ✓ Werden alle relevanten Stufen der Lieferkette und Regionen abgebildet? (einschließlich des eigenen Geschäftsbereichs und der tiefen Lieferkette)
- ✓ Wie ist die Qualität der gestellten Fragen?
- ✓ Berücksichtigt das Tool die unterschiedlichen Informationsanforderungen in der tiefen Lieferkette?
- ✓ Ist die Bewertungslogik transparent und nachvollziehbar?
- ✓ Können eigene Erwägungen in die Analyse einbezogen werden?
- ✓ Welche Entscheidungen sollen auf Basis der Analyse getroffen werden? (z. B. Anpassung der Beschaffung, Schulungen für Zulieferer, Audits)

Einige Anbieter setzen aktuell auf standardisierte Fragebögen, die im konkreten Einzelfall möglicherweise nur eine geringe Relevanz haben. Eingesetzt werden beispielsweise Fragebögen, die die einzelnen geschützten Rechtspositionen des LkSG in Ja-Nein-Fragen umgewandelt haben, wie beispielsweise „Beschäftigen Sie Kinder?“ oder „Halten Sie alle Gesetze ein?“ Solche Fragen sind mitunter wenig geeignet, um Rückschluss auf Risiken und Verletzungen zu geben und können für manche Unternehmen, in denen aufgrund der Branche und des Landes nur ein geringes bis gar kein Risiko für die Verletzung des abgefragten Menschenrechtes besteht, schlichtweg überflüssig sein (Bsp.: Kinderarbeit bei einem Lebensmittel-Importeur in Deutschland). Solche Ansätze führen unter Umständen auch dazu, dass durch den Fokus auf Tier-1-Zulieferer risikobehaftete vorgelagerte Zulieferer im Verborgenen bleiben.

Wenn zum Beispiel ein in Deutschland ansässiger Importeur von Schokolade angibt, dass Kinderarbeit und Zwangsarbeit bei ihm selbst keine Rolle spielen, besteht die Gefahr, dass diese Themen in Bezug auf vorgelagerte Zulieferer in Anbauländern unentdeckt bleiben. Ein solches Vorgehen erzeugt unnötigen bürokratischen Aufwand und ist zudem wenig zielführend, da nicht risikobasiert.

Zudem besteht die Gefahr, dass nicht die richtigen Zielgruppen erreicht werden. Fragebögen werden in der Regel durch das Management des Zulieferers ausgefüllt und nicht durch die Belegschaft. Die angemessene Berücksichtigung der Interessen Betroffener ist so nur sehr eingeschränkt möglich. Während einige Fragen sinnvollerweise an die Geschäftsführung des Zulieferers zu richten sind (Bsp.: Zertifikate, Policies und Managementprozesse), sollten Fragen in Bezug auf die Situation von Rechteinhabenden (z. B. Arbeitszeiten oder Formen der betrieblichen Mitbestimmung) zumindest auch an potenziell Betroffene oder ihre legitimen Interessenvertretungen gerichtet werden.

SCHRITT 4 – ERGÄNZENDE MASSNAHMEN ENTWICKELN

Sollte das eingesetzte Tool nicht alle relevanten Informationen liefern (siehe Herausforderungen Seite 9), sind ergänzende Schritte notwendig, um eine umfassende und fundierte Risikoanalyse zu gewährleisten.

Zu diesen ergänzenden Maßnahmen gehören beispielsweise:

1. **Gezielte, risikobasierte Fragebögen** für Zulieferer mit erhöhtem Risiko, um tiefere Einblicke in deren Arbeitspraktiken und mögliche menschenrechts- und umweltbezogene Risiken zu erhalten.
2. **Unternehmens- oder lieferkettenspezifische Fragenkataloge** ermöglichen die Erfassung maßgeschneiderter Informationen, die über Standardfragen hinausgehen.
3. **Vor-Ort-Besuche und Audits** für Hochrisikozulieferer, um sich einen Überblick über die Situation in der Fabrik oder auf dem Feld zu verschaffen und gezielt die Umsetzung von Maßnahmen entlang der Lieferkette anzugehen.
4. **Stakeholder-Konsultationen** fördern die Integration verschiedener Perspektiven. Der Dialog mit NGOs, Gewerkschaften und anderen relevanten Akteuren liefert wertvolle, praxisnahe Erkenntnisse für eine fundierte Risikoanalyse.

Je nach Kontext sind sehr unterschiedliche Präventions- und Abhilfemaßnahmen – in Abhängigkeit von Angemessenheit und Wirksamkeit – notwendig. Insofern ist die Liste an ergänzenden Maßnahmen nur als Anregung und nicht als vollständige Liste zu verstehen.

Allgemeine Hinweise zur Nutzung von Tools im Sorgfaltsprozess

Digitale Tools werden wie zu Beginn beschrieben auch in Bezug auf andere Sorgfaltspflichten eingesetzt. Folgende Hinweise helfen bei einem angemessenen und wirksamen Einsatz.

Eigene Expertise gezielt einbringen

Digitale Tools bieten wertvolle Unterstützung, doch sie dürfen die menschliche Beurteilung nicht ersetzen. Vorsicht ist insbesondere dann geboten, wenn sehr großzügige Compliance Versprechen durch einen Softwareanbieter gemacht werden. Es ist entscheidend, dass Unternehmen ihre eigene Expertise einfließen lassen – insbesondere bei der Priorisierung von Risiken und Verletzungen und der Entwicklung geeigneter Maßnahmen. Eine rein automatisierte Analyse kann wichtige Nuancen übersehen, die nur durch die fachkundige Einschätzung erfahrener Beschäftigter – etwa aus dem Einkauf – berücksichtigt werden können. Dies ist besonders wichtig, wenn es darum geht, welche Risiken und Verletzungen als besonders schwerwiegend erachtet werden und welche Maßnahmen am effektivsten sind. Unternehmen sollten die zuständigen Fachabteilungen und die Kolleg:innen daher aktiv in die Nutzung der Softwarelösungen einbinden und deren Anwendung kontinuierlich weiterentwickeln und nicht blind auf das Tool vertrauen.

Nahtlose Integration in bestehende Prozesse und technische Grenzen beachten

IT-Lösungen sollten in einem Unternehmen nicht isoliert oder als Insellösungen betrachtet werden. Vielmehr müssen sie sinnvoll in bestehende Risikomanagement- und Entscheidungsprozesse integriert werden. Nur so kann das Potenzial der Anwendungen vollständig ausgeschöpft werden. Digitale Lösungen sollten daher ein fester Bestandteil des Risikomanagementprozesses werden, um sicherzustellen, dass alle relevanten Daten und Erkenntnisse systematisch genutzt werden.

Kontinuierliche Überprüfung und Optimierung

Die Nutzung von digitalen Lösungen muss regelmäßig evaluiert werden, um sicherzustellen, dass sie weiterhin den sich verändernden Anforderungen und Rahmenbedingungen entsprechen. Eine kontinuierliche Überprüfung ermöglicht es, Schwächen frühzeitig zu identifizieren und gegebenenfalls Anpassungen vorzunehmen. Die sich schnell entwickelnde technologische Landschaft und neue gesetzliche Anforderungen erfordern eine regelmäßige Anpassung der eingesetzten Tools, um ihre Wirksamkeit langfristig zu sichern. Zudem hilft eine fortlaufende Optimierung dabei, den Nutzen der digitalen Lösungen kontinuierlich zu steigern und die Genauigkeit der Risikoanalyse zu verbessern.

Weiterführende Informationen



BAFA Handreichung Risikoanalyse:

Diese [Handreichung](#) des Bundesamts für Wirtschaft und Ausfuhrkontrolle (BAFA) bietet Unternehmen eine Anleitung zur Durchführung von Risikoanalysen im Rahmen des Lieferkettensorgfaltspflichtengesetzes (LkSG).



BAFA Handreichung Standards:

Diese [Handreichung](#) des BAFA bietet eine konkrete Orientierungshilfe in Bezug auf die Auswahl und Nutzung von Standards, Audits und Zertifizierungen als Instrumente zur Erfüllung der Sorgfaltspflichten nach dem LkSG.



BAFA und Helpdesk Handreichung Zusammenarbeit in der Lieferkette:

Diese [Handreichung](#), erstellt vom BAFA gemeinsam mit dem Helpdesk Wirtschaft und Menschenrechte, zeigt auf, wozu verpflichtete Unternehmen ihre Zulieferer nach dem LkSG auffordern können und wozu nicht. Sie enthält zudem Empfehlungen für eine konstruktive Zusammenarbeit.



BAFA FAQ Papier risikobasierter Ansatz:

Das BAFA hat [Fragen und Antworten](#) mit Klarstellungen zum risikobasierten Vorgehen im Rahmen der Risikoanalyse und zur Zusammenarbeit in der Lieferkette veröffentlicht.



CSR Risiko-Check:

Der CSR Risiko-Check ist ein [Online-Tool](#), das Unternehmen dabei unterstützt, die lokale Menschenrechtslage sowie Umwelt-, Sozial- und Governance-Themen zu bewerten.



BMWK/BMAS Dialogreihe faire Lieferketten:

Das Bundesministerium für Arbeit und Soziales hat gemeinsam mit dem Bundesministerium für Wirtschaft und Klimaschutz und dem Helpdesk Wirtschaft und Menschenrechte für Unternehmen und interessierte Wirtschaftsverbände die [Dialogreihe](#) #FaireLieferketten ins Leben gerufen.

Impressum

Helpdesk Wirtschaft und Menschenrechte

(umgesetzt von der DEG Impulse mit Unterstützung der GIZ)

DEG Impulse gGmbH
Kämmergasse 22
50676 Köln

E-Mail: kontakt@helpdeskwimr.de

Website: www.helpdeskwimr.de



Folgen Sie uns auf den Sozialen Medien und bleiben Sie über die aktuellen Entwicklungen zum Thema Wirtschaft und Menschenrechte informiert:



[Helpdesk Wirtschaft
und Menschenrechte](#)

Stand: 26. Juni 2025

