Governance

Governance, Compliance & ethische Prinzipien – Datenschutz & Informationssicherheit – Menschenrechte und nachhaltiges Lieferkettenmanagement

Wir richten unser Handeln an gesetzlichen Vorgaben aus, berücksichtigen Datensouveränität und integrieren menschenrechtliche sowie nachhaltige Standards in unsere Beschaffungsprozesse.

Gesamtzahl Korruptionsfälle im Jahr 2025:

0

Geldbußen oder sonstige Sanktionen aufgrund von Datenschutzverstößen oder Sicherheitsvorfällen 2025:

0

Überprüfung aller potenziellen Hochrisiko-Lieferanten mit Self-Assessments zu ESG-Aspekten:

100 %

Governance, Compliance & ethische Prinzipien

Wir handeln regelkonform im Hinblick auf alle anwendbaren Gesetze, gesellschaftlichen Richtlinien und unsere Wertvorstellungen.

Strategie

Verlässlichkeit, Integrität und Transparenz als Basis unseres Handelns

Verantwortungsvolle Unternehmensführung ist unser Leitprinzip – unsere Governance schafft den Rahmen dafür, verantwortungsvoll, nachhaltig und werteorientiert zu handeln. Nachhaltigkeit ist fest in allen Geschäftsbereichen verankert, Leitlinien und Kontrollmechanismen sichern **Integrität, Verlässlichkeit und Transparenz**. Sie sorgen dafür, dass ökologische, soziale und Compliance-Standards systematisch in den Managementprozessen verankert sind, geben klare Orientierung für alle Mitarbeitenden und schaffen verbindliche Regeln.

Wir handeln **gesetzeskonform und ethisch**. Wir verhindern Korruption und unlautere Geschäftspraktiken konsequent, bewahren die Integrität der Unternehmenskultur bei O_2 Telefónica und stellen die Umsetzung von Datenschutz- und Compliance-Standards sicher. Damit schützen wir unsere Reputation, das **Vertrauen unserer Stakeholder** und die Grundlage für langfristigen Unternehmenserfolg.

Richtlinien

Integrität leben und regelkonform handeln

Unsere Geschäftsgrundsätze dokumentieren die ethischen Grundlagen und sind der verbindliche Verhaltenskodex bei O_2 Telefónica – auch zu Nachhaltigkeitsthemen, wie Menschenrechte, Klimaverantwortung oder verantwortungsvolle Nutzung von digitalen Technologien.

Mit der Antikorruptionsrichtlinie, die sich an der **UN-Konvention gegen Korruption**, dem nationalen Strafrecht und den **OECD-Leitlinien** orientiert, bekennen wir uns klar zu **Null-Toleranz** gegenüber Bestechung und unlauteren Geschäftspraktiken. Zugleich definiert die Richtlinie Compliance-Organisation den Aufbau des **Compliance-Management-Systems** mit internen Strukturen, Rollen und Verantwortlichkeiten, um Gesetzesverstöße, Schadensersatzforderungen und Reputationsschäden vorzubeugen. Die Richtlinie zur Kartellrechtsprävention gibt einen Überblick über die gesetzlichen Regelungen und verbotenen Verhaltensweisen; sie ist für alle Mitarbeitenden verpflichtend. Die Richtlinie zu Geschenken und Einladungen sorgt dafür, dass wir **Interessenkonflikte minimieren**, während die Richtlinie zu Trainingspflichten die Trainingsanforderungen definiert, damit alle Mitarbeitenden unsere Standards kennen und leben.

Als Teil unserer verantwortlichen Unternehmensführung setzen wir auf ein nach ISO 22301 zertifiziertes **Business Continuity Management (BCM)**. Die BCM-Richtlinie regelt Impact- und Risikoanalysen sowie die Notfallplanung, damit kritische Geschäftsprozesse auch bei Störungen so resilient wie möglich bleiben. Das BCM-System wird regelmäßig auditiert, auch 2025 wurde die externe Zertifizierung bestätigt. Ergänzend sorgt das **IT Service Continuity Management (ITSCM) basierend auf ISO 27031** für die **Resilienz** unserer IT- und Netzwerk-Infrastruktur. 2025 wurde ein Regelprozess für Transparenz und Disaster-Recovery-Pläne etabliert.

Um unsere Unternehmenskultur aktiv zu leben und höchste Standards in Bezug auf Menschenrechte, Umweltschutz und Integrität zu fördern, haben wir ein **umfassendes Hinweisgebersystem** etabliert. Es ermöglicht die Meldung von Hinweisen zu menschenrechtlichen und umweltbezogenen Risiken gemäß dem Lieferkettensorgfaltspflichtengesetz (LkSG), zu Korruption oder Betrug laut Hinweisgeberschutzgesetz (HinSchG) sowie zu internen Regelungen. Das Hinweisgeber-verfahren beschreibt transparent, wie solche Meldungen erfolgen können – anonym und nicht-anonym an eine unabhängige Ombudsperson. Die Meldung ist in 21 Sprachen möglich und kann online, per Brief oder Telefon erfolgen. Zusätzlich stehen ein Human-Rights-Postfach sowie ein Compliance-Mailpostfach zur Verfügung. Die **Whistleblowing-Richtlinie** schützt hinweisgebende Personen, da ihnen keine Nachteile entstehen sollen. Weitere Informationen zu unseren Due-Diligence-Prozessen finden Sie im Kapitel Menschenrechte.

Ziele

Bis Ende 2025

- darf es keine **Korruptionsfälle** im Unternehmen geben,
- sollten mehr als 95 % unserer Mitarbeitenden die **Schulung zu den Geschäftsgrundsätzen** erfolgreich absolviert haben.

Performance

Wir bleiben unserem Anspruch treu

2025 verzeichneten wir wie im Vorjahr 0 **Korruptionsfälle** und haben damit unser Ziel erreicht.

85,4 % (2024: 94,7 %) der Mitarbeitenden haben die **Schulung zu den Geschäftsgrundsätzen** erfolgreich absolviert. Somit liegen wir trotz weiterhin guter Abschlussquote unter dem von uns angestrebten Wert.

Weitere Kennzahlen und Definitionen finden Sie in unserem interaktiven Kennzahlentool.

Maßnahmen

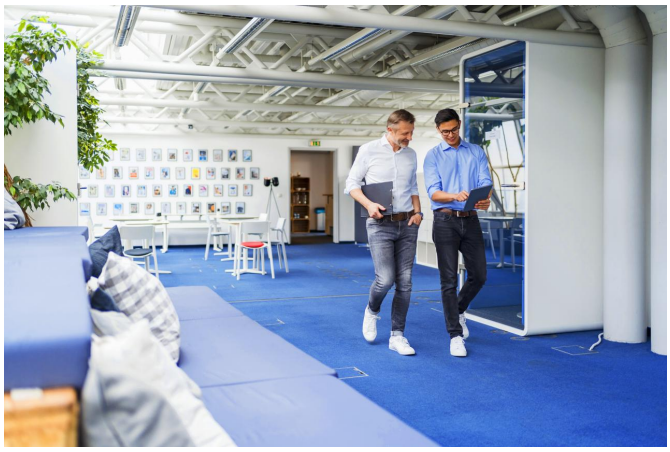
So sichern wir Integrität und Handlungsfähigkeit

Wir stellen uns robust auf: Für Krisenfälle oder Störungen ist im Rahmen unseres BCMs sowie auf Grundlage der Krisenmanagement-Richtlinie vorgesorgt. So sind alle wichtigen Datacenter und Core Sites örtlich voneinander getrennt, aber synchronisiert und darauf ausgelegt, 48 Stunden autark betrieben werden zu können. Für Katastrophenlagen stehen mobile Netzersatzanlagen, Pumpen und Klimageräte bereit. Zudem sind Notfall-Offices eingerichtet, die auch bei Ausfällen über Satellit mit dem Internet verbunden bleiben.

Wissen schafft Sicherheit: Die Schulung zu den Geschäftsgrundsätzen und Menschenrechten ist für alle Mitarbeitenden verpflichtend und wird alle drei Jahre wiederholt, ebenso das Training zum Allgemeinen Gleichbehandlungsgesetz (AGG). In der Schulung zu den Geschäftsgrundsätzen sind auch Korruptionsprävention, Kartellrecht und ESG-Themen, wie nachhaltiges Lieferkettenmanagement, Klimaverantwortung, Kreislaufwirtschaft oder verantwortungsvolle Nutzung von digitalen Technologien, enthalten. Zusätzlich bieten wir ein freiwilliges Intensivtraining zur Korruptionsbekämpfung, das den korrekten Umgang mit Geschenken und Einladungen sowie die Erkennung und Reaktion auf Bestechungsversuche vermittelt.

Das Senior Leadership Team bestätigt jährlich die Einhaltung der Anti-Korruptionsvorgaben im Rahmen des konzernweiten Zertifizierungsprozesses; Geschäftspartnerinnen und -partner verpflichten sich vertraglich zur Einhaltung entsprechender Antikorruptionsklauseln.

Förderung der Speak-up-Kultur und Stärkung von Compliance Bewusstsein: Wir beobachten laufend die Gesetzeslage und sensibilisieren zu Compliance und ethischem Handeln – durch Awareness-Maßnahmen, interne Kommunikation und das Whistleblower-System. Hinweise werden vertraulich behandelt und von einem geschulten Team bearbeitet. Auf diese Weise fördern wir die Verankerung ethischen Handelns in unsere Unternehmenskultur.



Business Value

Rechtssicherheit digital gedacht

Wir digitalisieren Rechts- und Compliance-Prozesse mit Legal-Tech-Tools und ermöglichen so eine revisionsgerechte Dokumentation für **Transparenz und Kontinuität** – bereichsübergreifend und künftig cloudbasiert. Dadurch beantworten wir Rechtsanfragen schneller, gestalten Prozesse effizienter und verbessern die **Compliance-Dokumentation** für mehr Vertrauen und Sicherheit. Klare digitale Workflows reduzieren Risiken bei Datenschutz und rechtlichen Prozessen. Geschäftskunden können von **verbessertem Datenschutz**, **verlässlicher Compliance** und **beschleunigten Reaktionszeiten** profitieren.

Nächste Schritte

Wir machen Compliance smart

Wir wollen Compliance-Prozesse weiter digitalisieren – mit **Legal-Tech sowie Self-Service-Plattformen** für Zertifikate und Audits für unsere Geschäftskunden. Schulungen werden durch Micro-Learning und Gamification ergänzt.

Datenschutz & Informationssicherheit

Wir setzen uns dafür ein, dass die Hoheit über ihre Daten bei unseren Kundinnen und Kunden bleibt und sie ihr digitales Leben souverän gestalten können.

Strategie

Aus Prinzip für Datensouveränität

Der **Schutz personenbezogener Daten** und die **Abwehr von Cyberrisiken** haben für uns höchste Priorität. Wir handeln gesetzeskonform, transparent und proaktiv, um Vertrauen zu schaffen und zu einer sicheren digitalen Gesellschaft beizutragen.

Richtlinien

Wir gehen auf Nummer sicher

Wir schützen personenbezogene Daten auf Basis anerkannter Standards und geltender Gesetze, wie z. B. der Datenschutz-Grundverordnung (DSGVO), dem Telekommunikationsgesetz (TKG) und der **ISO 27001:2022 Informationssicherheits-Managementsystem**. Der Konzernstandard Datenschutz bildet die Grundlage des Datenschutz-Managementsystems und zielt darauf, dass Daten nur rechtmäßig verarbeitet und nach aktuellem Stand der Technik geschützt werden. Ergänzt wird er durch interne Vorgaben, wie der Informationssicherheitspolitik, der Richtlinie Datenschutzvorfälle und der Richtlinie Krisenmanagement.

Unser Resilienz-Rahmenwerk beschreibt die grundlegenden **Security-Kontrollziele**, die wir in Richtlinien und Standards konkretisieren und aus denen wir Kontrollvorgaben ableiten. Die **Wirksamkeit der Maßnahmen zur Informationssicherheit** wird regelmäßig überprüft – unter anderem im Rahmen interner und externer Audits, wie z. B. dem **ISO 27001** Zertifizierungsaudits, Prüfungen der internen Revision oder interner Control Assessments.

Spezifische interne Vorgaben und Verfahren regeln den Umgang mit Bedrohungen, Schwachstellen und die Sensibilisierung der Mitarbeitenden für diese Themen. Diese Leitlinien bilden die Grundlage für ein **robustes Sicherheits- und Datenschutzmanagement**, das sowohl die Transparenz über die Datennutzung als auch den verantwortungsvollen Umgang mit Informationen sicherstellt. Informationssicherheit umzusetzen beinhaltet auch die technische und organisatorische Absicherung unserer Netz- und IT-Systeme. Dieser Ansatz wird durch das Cyber Fusion Center unterstützt, das umfassende Schutzmaßnahmen gegen Cyberangriffe koordiniert.

Ziele

Bis Ende 2025 haben wir uns zum Ziel gesetzt,

- dass **keine Datenschutzverstöße oder Sicherheitsvorfälle** auftreten, die Geldbußen oder sonstige Sanktionen zur Folge haben,
- die **Abschlussquote des Trainings** „Informationssicherheit" bei unseren Mitarbeitenden auf über 90 % zu steigern.

Performance

Ermutigende Ergebnisse

- 2025 kam es wie im Vorjahr zu **keinen Datenschutzverstößen oder Sicherheitsvorfällen**, die zu Bußgeldern oder anderen Sanktionen geführt hätten.
- Die Abschlussquote für das Training **Informationssicherheit** lag im Jahr 2025 bei 88,5 % (2024: 90 %) und damit knapp unter dem angestrebten Wert von über 90 %. Mit zahlreichen zusätzlichen Awareness-Maßnahmen als Ergänzung zum Pflichttraining haben wir das Sicherheitsbewusstsein unserer Mitarbeitenden weiter gestärkt.

Alle Kennzahlen und Definitionen finden Sie in unserem interaktiven Kennzahlentool.

Maßnahmen

Prävention, Überwachung, Reaktion: unser Resilienz-Dreiklang

Risiken von Anfang an minimieren: Wir setzen auf das Prinzip „Privacy by Design und Default", um personenbezogene Daten von Anfang an bestmöglich zu schützen. Durch die Minimierung von Datenverarbeitung und Zugriffsrechten lassen sich potenzielle Angriffsflächen verringern.

Sicherheit im Blick behalten: Unser Cyber Fusion Center (CFC) ist ein zentraler Knotenpunkt zur Verbesserung der Cybersicherheit. Hier werden Systeme und Netzwerke kontinuierlich überwacht, Bedrohungen identifiziert und Vorfälle schnell und koordiniert bearbeitet. Unterstützend überwacht das Network Operation Center (NOC) die Netzkomponenten, um Auffälligkeiten frühzeitig zu erkennen und die Stabilität unserer Dienste zu unterstützen.

Kompetenz gezielt stärken: Mit verpflichtenden und regelmäßig aktualisierten Schulungen zu Datenschutz und Informationssicherheit stärken wir das Bewusstsein unserer Mitarbeitenden für aktuelle Bedrohungen und regulatorische Anforderungen. 2025 wurden zahlreiche zusätzliche Maßnahmen zu unterschiedlichen Security-Themenfeldern angeboten, um den individuellen Bedarf zu adressieren und das Sicherheitsbewusstsein weiter zu stärken.

Bedrohungen proaktiv begegnen: Darüber hinaus nutzen wir Cyber Threat Intelligence (CTI) und das Threat Intelligence Program, um die sich wandelnde Bedrohungslandschaft zu analysieren. So können wir Risiken antizipieren und präventive Maßnahmen einleiten, um potenziellen Bedrohungen zuvorzukommen.

Dieser Dreiklang aus Prävention, Überwachung und schneller Reaktion stärkt den Schutz der digitalen Infrastruktur.

Datenschutz priorisieren: Als Telekommunikationsanbieter verarbeiten wir große Mengen an Mobilitäts- und Nutzungsdaten. Mit der Data Anonymization Platform (DAP) wurde ein mehrstufiges Verfahren entwickelt, das Daten anonymisiert. Mehr Informationen zum Schutz der Daten finden Sie hier.

Business Value

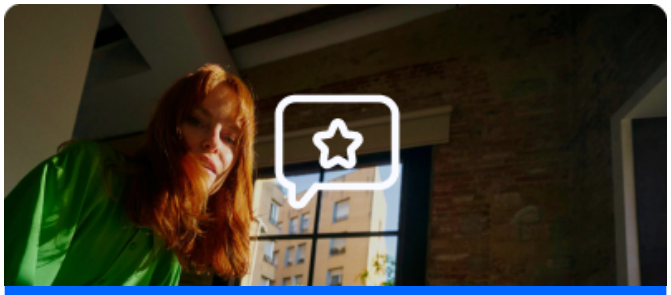
Gefahren im Blick

Mit unserem **Threat Intelligence Program** können wir Bedrohungen frühzeitig erkennen und präventiv handeln. Angreifertaktiken und Risiken werden fortlaufend analysiert, u. a. in den Kernthemen 5G Netzwerk, IoT, Ransomware, Lieferketten, Cloud-Sicherheit und Social Engineering. Auch neue Bedrohungen wie KI-basierte Angriffe, Malware-Trends und Phishing gegen Business-Tools werden erfasst. Das Programm liefert verwertbare Erkenntnisse für schnelle Entscheidungen, unterstützt die **Resilienz der digitalen Infrastruktur** und erhöht die Verlässlichkeit der Services für unsere Geschäftskunden.

Nächste Schritte

Mit Sicherheit gut gedacht

Wie bei Compliance wollen wir unsere KI-gestützten Risikoanalysen und Threat-Intelligence-Systeme erweitern, um die **Prävention weiter zu optimieren**. Die Self-Service-Plattformen sollen auch für Datenschutzanfragen und Sicherheitszertifikate genutzt werden können.



Business Impact Story: O_2 Telefónica ermöglicht sichere Netzarchitekturen für die öffentliche Verwaltung

ekom21, ein IT-Dienstleister für Kommunen und öffentliche Einrichtungen in Hessen, nutzt unsere SD-WAN-basierte Netzarchitektur mit integrierten Sicherheitsfunktionen – um den Zugriff auf Cloud-Dienste zu ermöglichen und den Betrieb sensibler Anwendungen technisch abzusichern.

→ **Hier geht es zur Geschichte: „Wir brauchten eine flexible und vor allem auch sichere Netzwerklösung"**

Menschenrechte und nachhaltiges Lieferkettenmanagement

Wir berücksichtigen Nachhaltigkeitskriterien in unseren Einkaufsvorgängen und setzen uns für ökologische, soziale und menschenrechtliche Standards in der Lieferkette ein.

Strategie

Menschenrechte schützen, Risiken mindern

Um die **Achtung der Menschenrechte** wirksam in unserem Konzern und in den eigenen Geschäftsaktivitäten zu verankern, arbeiten wir mit unserem Due-Diligence-Prozess zum Schutz der Menschenrechte. Der Prozess setzt die Anforderungen internationaler Rahmenwerke, wie den UN-Leitprinzipien und den OECD-Leitsätzen, sowie gesetzlichen Vorgaben, wie dem Lieferkettensorgfaltspflichtengesetz (LkSG), um. Die sechs Bausteine des Prozesses sind auf der O_2 Telefónica-Website für Menschenrechte beschrieben. Zudem haben wir ein **umfassendes Lieferkettenmanagement** etabliert. Lesen Sie dazu online mehr hier.

Richtlinien

Wir folgen verbindliche Standards

Neben den Geschäftsgrundsätzen definiert die Richtlinie Menschenrechte den Anspruch, internationale Standards, wie die **UN-Leitprinzipien, die OECD-Leitsätze und ILO-Normen,** in unsere Prozessen zu integrieren sowie menschenrechtliche Risiken systematisch zu identifizieren und angemessen zu mindern. Sie wird flankiert durch das Commitment zu Kinderrechten, das sich auf den Schutz von Kindern und Jugendlichen fokussiert und sich an den **UNICEF Grundsätzen Kinderrechte und unternehmerisches Handeln** orientiert.

Die O_2 Telefónica Grundsatzerklärung zur Achtung der Menschenrechte erläutert unsere Handlungsfelder und bekräftigt unser **Bekenntnis zu fairen Arbeitsbedingungen**. Sie formuliert Anforderungen zur **Vermeidung von Kinder- und Zwangsarbeit** sowie Diskriminierung, unterstützt die Einbindung von Arbeitnehmervertretungen und erläutert den Due-Diligence-Prozess als zentrales Element zur Überwachung der Umsetzung dieser Richtlinien.

Unsere Supply Chain Sustainability Policy ist ein verbindlicher Verhaltenskodex für Lieferanten und gilt für den Einkauf von Produkten und Dienstleistungen. Sie legt klare **ökologische, soziale und ethische Mindeststandards** fest, darunter insbesondere Menschen- und Arbeitsrechte, Umwelt- und Klimaschutz, Integrität im Geschäftsverhalten sowie Datenschutz. Die direkten Lieferanten sind angehalten, auch ihre Subunternehmen vertraglich zur Einhaltung vergleichbarer Standards und Regelungen zu verpflichten.

So verfolgen wir das Ziel, gemeinsam mit unseren Lieferanten resiliente und wettbewerbsfähige Lieferketten zu fördern.

Ziele

Bis Ende 2025 strebten wir an, dass

- nahezu alle potenziellen Hochrisiko-Lieferanten der O_2 Telefónica mit **Self-Assessments** zu ESG-Aspekten überprüft wurden,
- der Anteil **gelöster Beschwerden** und Hinweise zu Menschenrechtsthemen bei 100 % liegt.

Performance

Fortschritte, aber auch Handlungsbedarf

- 2025 lag der Anteil der potenziellen Hochrisikolieferanten, die ein **ESG-Self-Assessment** durchgeführt haben, bei 100 % (2024: 78 %).
- Der Anteil der **gelösten Hinweise und Beschwerden** zu Menschenrechtsthemen belief sich wie im Vorjahr auf 100 %.

Alle Kennzahlen und Definitionen finden Sie in unserem interaktiven Kennzahlentool.

Maßnahmen

Governance, Risikomanagement und Transparenz: So setzen wir Verantwortung um

Wir handeln im Einklang mit geltenden Gesetzen: Unser Due-Diligence-Prozess zum Schutz der Menschenrechte ermöglicht es, menschenrechtliche und umweltbezogene Risiken und Verstöße frühzeitig zu erkennen und geeignete Maßnahmen zu ergreifen, um diese zu verhindern, zu mindern oder – sofern bereits eingetreten – Abhilfemaßnahmen einzuleiten.

Bearbeitung von Hinweisen und Beschwerden: Einzelpersonen, Unternehmen und Organisationen können menschenrechtliche und umweltbezogene Risiken oder Verstöße melden. Alle relevanten Informationen finden sich auf unserer Webseite zum Hinweisgeberverfahren, die wir 2025 durch leicht verständliche Sprache und Infografiken für alle Stakeholder weiter zugänglicher gestaltet haben.

Kontrolle in Hochrisikoländern: Im Rahmen der Joint Alliance for CSR (JAC) führt die Telefónica, S.A. Group regelmäßige Audits bei Lieferanten durch. Diese prüfen die Einhaltung zentraler sozialer und arbeitsrechtlicher Standards, darunter faire Arbeitsbedingungen einschließlich angemessener Löhne und Arbeitszeiten sowie Gesundheit und Sicherheit am Arbeitsplatz. Die Audits definieren zudem notwendige Korrekturmaßnahmen, um identifizierte Risiken gezielt zu adressieren. Als Tochtergesellschaft der Telefónica, S.A. Group sind wir Teil der JAC und verfügen über direkten Zugang zu den Ergebnissen der Lieferantenaudits.

Zusammenarbeit mit Lieferanten: Nahezu 100 % der 2025 beauftragten Lieferanten, die über das Einkaufssystem abgewickelt wurden, haben sich zur Einhaltung der Supply Chain Sustainability Policy verpflichtet. Ergänzend setzen wir im Rahmen der jährlichen Risikoanalyse standardisierte Fragebögen für Hochrisikolieferanten ein, um die identifizierten prioritären Risiken zu erfassen. Diese Risiken umfassten im Jahr 2025: unangemessene Löhne, Ungleichbehandlung in der Beschäftigung, Missachtung der Vereinigungsfreiheit und das Recht auf Tarifverhandlungen sowie mangelhafte Gesundheit und Sicherheit am Arbeitsplatz. Durch den Dialog mit den Lieferanten präzisieren wir unsere Erwartungen zu Arbeitsbedingungen und Beschäftigungsstabilität.

Lieferantenmonitoring: Durch KI-gestütztes Screening identifizieren wir frühzeitig Risiken und kritische Ereignisse in der Wertschöpfungskette (siehe Abschnitt Business Value) und leiten bei Bedarf Maßnahmen ein.

Überprüfung interner Prozesse und Schulungen: Wir überprüfen kontinuierlich die Governance-Strukturen und Prozesse, um Transparenz und menschenrechtliche Sorgfalt zu verbessern. Regelmäßige Online-Trainings für Mitarbeitende und Lieferanten unterstützen die Umsetzung des LkSG.

Business Value

Für nachhaltige Partnerschaft: Echtzeit-Überwachung der Lieferkette

Wir haben unser KI-basiertes Lieferantenscreening weiterentwickelt, um Risiken in der Lieferkette transparent und effizient zu bewerten. Mithilfe moderner KI-Modelle analysieren wir Informationen aus Nachrichten, Social Media und vertrauenswürdigen Quellen in mehr als 180 Sprachen. So erkennen wir **potenzielle Menschenrechts- oder Umweltverstöße** frühzeitig und leiten kritische Hinweise in **Echtzeit** an den Einkauf weiter. Durch kontinuierliche Anpassung auf Basis von Nutzerfeedback stellen wir die Qualität der Risikoerkennung sicher.

Mithilfe eines KI-gestützten Lieferantenmonitorings zielen wir auf Transparenz und Sicherheit in der direkten Lieferkette. Wir tragen zur Unterstützung fairer und umweltfreundlicher Bedingungen bei der Herstellung von Produkten und der Erbringung von Dienstleistungen bei, wollen **Ausfall- und Compliance-Risiken reduzieren** und die **ESG-Konformität stärken**. So verfolgen wir das Ziel, Lieferanten zu verlässlichen Partnern zu entwickeln sowie durch Vertrauen und Wettbewerbsfähigkeit Mehrwert zu schaffen.

Nächste Schritte

Menschenrechtliche Sorgfaltspflicht konsequent vorantreiben

Wir lösen alle Hinweise und Beschwerden verantwortungsvoll, wollen die Quote der ESG-Self-Assessments bei Hochrisikolieferanten auf nahezu 100 % stabil halten und **bauen KI-gestützte Systeme für Risikoanalysen weiter aus**. Zudem intensivieren wir Sensibilisierungsmaßnahmen für interne Teams und Lieferanten, um internationale Standards konsequent umzusetzen.