## EU-Lieferkettengesetz beschlossen

**Nachricht vom 14.12.2023**

*Das Europaparlament und der Europäische Rat haben sich auf ein Lieferkettengesetz geeinigt.*

Die Regeln verpflichten Unternehmen, Sorgfaltspflichten insbesondere bezogen auf **Menschenrechte** und die **Umwelt** in ihre Richtlinien und **Risikomanagementsysteme** zu integrieren, teilten Parlament und Rat der EU jetzt mit [1]. Dabei sind Herangehensweise, Prozesse und Verhaltenskodizes zu beschreiben. Außerdem ist sicherzustellen, dass die Geschäftsmodelle dem Ziel entsprechen, die globale Erwärmung auf höchstens 1,5 Grad Celsius zu begrenzen.

Die Gesetzgebung gilt grundsätzlich für Unternehmen in der EU mit mehr als 500 Mitarbeitenden und einem weltweiten Umsatz von mehr als 150 Millionen Euro. Die Verpflichtungen treffen auch Unternehmen mit mehr als 250 Mitarbeitenden und einem Umsatz von mehr als 40 Millionen Euro, wenn mindestens 20 Millionen Euro in einem der folgenden Sektoren generiert werden:

- Herstellung und Großhandel von Textilien
- Bekleidung und Schuhen
- Landwirtschaft einschließlich Forstwirtschaft und Fischerei
- Herstellung von Lebensmitteln und Handel mit Rohstoffen
- Bergbau und Großhandel von Mineralressourcen
- Herstellung von entsprechenden Produkten und Bauwesen

„Unternehmen und ihre Leitungsorgane benötigen ein effektives Compliance-Management für ihre Supply-Chain zur systematischen Erfassung und Steuerung der neuen Vorgaben", stellt die Kanzlei CMS Deutschland. Für Unternehmen, die das Lieferkettengesetz in seiner aktuellen Fassung einhalten, werde es nicht schwierig sein, sich auf die neuen Regeln der Richtlinie umzustellen. Es sei deshalb völlig übertrieben, von einem europäischen Bürokratiemonster zu sprechen.

Aufgrund der neuen Richtlinie muss Deutschland sein Lieferkettengesetz nachschärfen, führt CMS weiter aus. Beispielsweise sollen Menschenrechte und Umwelt in weiterem Umfang als bisher geschützt werden. Neu sei auch die zivilrechtliche Haftung. „Unternehmen müssen betroffene Personen stärker einbeziehen. Und es werden mehr Unternehmen unter das Gesetz fallen. Aber die Sorgfaltspflichten bleiben im Wesentlichen dieselben", so CMS.

**Quelle**

[1] https://www.europarl.europa.eu/news/de/press-room/20231205IPR15689/corporate-due-diligence-rules-agreed-to-safeguard-human-rights-and-environment

## Regulierung Künstlicher Intelligenz trifft auch ChatGPT

**Nachricht vom 11.12.2023**

*Die EU-Mitgliedsstaaten haben sich jetzt auf eine europäische KI-Verordnung geeinigt. Der Artificial Intelligence Act (AI Act) ist das weltweit erste Gesetz zur Regulierung von Künstlicher Intelligenz.*

Künftig müssen KI-Anwendungen je nach Risiko, das von ihnen ausgeht, unterschiedlich hohe Anforderungen erfüllen, nennt der TÜV-Verband als zentralen Aspekt. Es sei positiv, dass auch besonders leistungsstarke KI-Basismodelle nicht von der Regulierung ausgenommen sind. Dazu zählt auch General Purpose AI wie **ChatGPT.** Über diesen Punkt war bis zum Schluss der Verhandlungen kontrovers diskutiert worden. Der Druck von Lobbys und Unternehmen, General Purpose AI nicht zu regulieren, sei enorm gewesen, heißt es aus Verhandlungskreisen. Nun sollen diese Grundlagenmodelle in zwei Risikoklassen eingeteilt werden und besondere Pflichten erfüllen, etwa bei der Weitergabe von Informationen, bei der Risikoanalyse und beim Dokumentieren der Daten, mit denen die KI trainiert wird.

Der jetzt verabschiedete AI Act teilt KI-Anwendungen in **vier Risikoklassen** ein. Die große Mehrheit der KI-Anwendungen wird als niedriges Risiko eingestuft, für die keinerlei Anforderungen gelten. KI-Systeme mit einem nicht akzeptablen Risiko wie Social-Scoring-Systeme werden dagegen komplett verboten. KI-Systeme mit einem begrenzten Risiko wie einfache Chatbots müssen bestimmte Transparenz- und Kennzeichnungspflichten erfüllen. Für KI-Anwendungen mit einem hohen Risiko, zum Beispiel in kritischen Infrastrukturen, in Bewertungssystemen im Personalwesen und für die Beurteilung der Kreditwürdigkeit, gelten strengere Sicherheitsanforderungen. Dazu zählen die Anforderungen in Bezug auf Nachvollziehbarkeit, Risikomanagement und Cybersicherheit.

Inwiefern KI im öffentlichen Raum etwa bei der Strafverfolgung zum Einsatz kommen darf, wurde kontrovers diskutiert. Das EU-Parlament wollte automatisierte Gesichtserkennung verbieten, doch viele Mitgliedsstaaten stemmten sich gegen ein mögliches Verbot. Die biometrische Identifizierung soll nun grundsätzlich möglich sein, wenn auch in engen Grenzen.

„Diese EU-Verordnung wird eine Blaupause für die weltweite Regulierung sein", kommentiert die Wirtschaftskanzlei CMS den Abschluss des AI Acts. Die Anforderungen an die Dokumentation stiegen enorm. Mittelfristig würden sich die Anbieter durchsetzen, die Compliance-by-Design berücksichtigen. Die übrigen würden vom Markt verschwinden.

## KI-Einsatz im Job gewinnt an Bedeutung – Große Mehrheit für gesetzliche Vorgaben

**Nachricht vom 30.11.2023**

*Die Haltung zu Künstlicher Intelligenz ist bei Nutzerinnen und Nutzern in Deutschland insgesamt aufgeschlossenen. Allerdings werden auch erhebliche Gefahren gesehen.*

Das ist das Ergebnis einer Forsa-Umfrage im Auftrag des TÜV-Verbands. Befragt wurden 1.008 Personen ab 16 Jahren.

Demnach sehen 78 Prozent beim Einsatz von KI-Technologie derzeit nicht abschätzbare Risiken. 92 Prozent glauben, dass mit dem Einsatz von KI kaum noch erkennbar sein wird, ob Fotos oder Videos echt oder gefälscht sind. Dass der Wahrheitsgehalt eines mit Hilfe von KI generierten Textes nicht mehr erkennbar ist, meinen 83 Prozent. 91 Prozent fordern eine Transparenz- und Kennzeichnungspflicht für Inhalte, die mit Hilfe von Künstlicher Intelligenz erzeugt wurden.

Das Sprachmodell ChatGPT haben der Umfrage zufolge 37 Prozent der Userinnen und User in Deutschland schon mal genutzt; 85 Prozent haben von dieser KI zumindest gehört. Zum Vergleich: Der Digitalverband Bitkom hatte zwei Wochen zuvor gemeldet [1], dass in Deutschland 78 Prozent von dem Chatbot gehört und 34 Prozent das Sprachmodell genutzt haben.

Laut der Umfrage im Auftrag des TÜV-Verbands erwartet fast die Hälfte der Erwerbstätigen, dass Künstliche Intelligenz in fünf Jahren eine große oder sehr große Rolle für ihre berufliche Tätigkeit spielen wird. Das aktuelle Ranking der Anwendungen sieht so aus:

- Unterhaltungszwecke (52 Prozent)
- Recherchen (44 Prozent)
- Schreiben von Texten (40 Prozent)
- Generierung und Bearbeitung von Fotos oder Videos (26 Prozent)
- Programmierung (12 Prozent)

Zu den Vorbehalten und Sorgen beim KI-Einsatz:

- 56 Prozent haben kein Vertrauen in die Ergebnisse generativer KI-Anwendungen.
- 83 Prozent plädieren für gesetzliche Vorgaben für den KI-Einsatz.
- 63 Prozent halten eine Weiterbildung zu Künstlicher Intelligenz für ihre berufliche Tätigkeit für sinnvoll.

„Unsicherheit besteht noch darüber, inwieweit KI-Systeme eine echte Gefahr für den eigenen Arbeitsplatz sind oder diesen wie Computer, Internet oder Smartphone schrittweise verändern werden", stellt der TÜV-Verband fest [2]. Gut die Hälfte der Erwerbstätigen ist der Meinung, dass KI-Systeme Routineaufgaben ihrer beruflichen Tätigkeit übernehmen werden oder das jetzt schon tun. 29 Prozent glauben, dass KI ihre berufliche Tätigkeit ganz oder teilweise ersetzen könnte.

### EU in finalen Verhandlungen über Regulierung

Mit dem AI Act steht eine europäische KI-Verordnung kurz vor dem Abschluss. Ein Streitpunkt in den finalen Trilog-Verhandlungen ist der Umgang mit KI-Basismodellen wie zum Beispiel ChatGPT. Der TÜV-Verband spricht sich für grundlegende Transparenzpflichten als Mindestanforderung aus. Als entscheidender Termin der Trilog-Verhandlungen gilt der 6.12.2023.

Der AI Act sieht vor, KI-Anwendungen in vier Risikoklassen einzuteilen.

### Inakzeptables Risiko

Alle KI-Systeme, die als eindeutige Bedrohung für die Sicherheit, den Lebensunterhalt und die Rechte von Menschen angesehen werden, sollen verboten werden, etwa soziale Bewertungen durch Regierungen und Spielzeug, das Sprachhilfe verwenden, die gefährliches Verhalten fördert.

### Hohes Risiko

Hochrisiko-Systeme umfassen KI-Technologie in folgenden Bereichen (mit jeweils einem Beispiel):

- kritische Infrastrukturen (Verkehr), die das Leben und die Gesundheit der Bürger gefährden könnten
- allgemeine oder berufliche Bildung, die den Zugang zu Bildung und beruflichem Verlauf des Lebens einer Person bestimmen kann (Bewertung von Prüfungen)
- Sicherheitskomponenten von Produkten (KI-Anwendung in robotergestützten Chirurgie)
- Beschäftigung (CV-Sortierungssoftware für Einstellungsverfahren)
- wesentliche private und öffentliche Dienstleistungen (Kreditwürdigkeit, bei der Bürgerinnen und Bürgern die Möglichkeit verweigert wird, ein Darlehen zu erhalten)
- Strafverfolgung, die in die Grundrechte der Menschen eingreifen kann (Bewertung der Zuverlässigkeit von Beweisen)
- Migrations-, Asyl- und Grenzkontrollmanagement (Überprüfung der Echtheit der Reisedokumente)
- Rechtspflege und demokratische Prozesse (Anwendung des Gesetzes auf konkrete Fakten)

### Begrenztes Risiko

Begrenztes Risiko bezieht sich auf KI-Systeme mit spezifischen Transparenzverpflichtungen. Bei der Verwendung von KI-Systemen wie Chatbots sollten Nutzerinnen und Nutzer sich bewusst sein, dass sie mit einer Maschine interagieren, damit sie eine informierte Entscheidung treffen können, fortzufahren oder zurückzutreten.

### Geringes oder kein Risiko

Der Vorschlag ermöglicht die kostenlose Nutzung von KI mit minimalem Risiko. Dazu gehören Anwendungen wie KI-fähige Videospiele oder Spamfilter. Die überwiegende Mehrheit der derzeit in der EU eingesetzten KI-Systeme fällt in diese Kategorie.

Die Europäische Kommission hat ihren Vorschlag für einen KI-Rechtsrahmen hier veröffentlicht [3].

Wie sich ChatGPT sinnvoll in Unternehmen einsetzen lässt, zeigt das Buch „ChatGPT in der Unternehmenspraxis [4] – Anwendungsbeispiele für Risikomanagement, Controlling und Compliance. Der Chatbot verfasst Aufsätze, Gedichte, Songtexte, Rezensionen, Interpretationen und Porträts. Er entwirft Verträge, Referenzen, Zeugnisse, Bewerbungen, Geschäftsberichte, Marketinganalysen, Strategieberichte, Vorträge, Skripte und Rechtsgutachten. Er generiert Website-Codes und kann beim Verfassen von Businessplänen, Governance-Konzepten, Risikomanagementsystemen, Notfallplänen und Gesetzen sehr hilfreich sein.

**Quelle**

[1] https://esv.info/aktuell/chatgpt-jeder-dritte-hat-die-ki-schon-mal-ausprobiert/id/131828/meldung.html
[2] https://www.tuev-verband.de/pressemitteilungen/ein-jahr-chatgpt-gut-ein-drittel-nutzt-die-ki-fuer-unterhaltung-recherchen-und-inspiration-viele-davon-misstrauen-den-ergebnissen
[3] https://digital-strategy.ec.europa.eu/de/policies/regulatory-framework-ai
[4] https://esv.info/978-3-503-23697-8

## Messbarkeit von Compliance-Zielen bislang oft unterbewertet

**Nachricht vom 20.11.2023**

*Nur mit klar definierten Compliance-Zielen wird die Organisation, insbesondere aber auch die Compliance-Abteilung in die Lage versetzt, ein wirksames Compliance Management System (CMS) einzurichten*

Das ist eine der zentralen Aussagen im Report „The Future of Compliance 2023", den Deloitte jetzt veröffentlicht hat. 84 Prozent der Befragten gaben an, dass Compliance-Ziele für den Erfolg ihres CMS eine wichtige Rolle spielen. Allerdings haben nur 61 Prozent solche Ziele definiert. Je größer und internationaler die Organisation aufgestellt ist, desto mehr dienen Compliance-Ziele auch der Vermittlung einer einheitlichen Compliance-Kultur, stellt Deloitte fest.

Weitere Erkenntnisse aus der Erhebung:

Unterschiedliche Zeithorizonte bei der Definition von Compliance-Zielen wirken sich nicht nur auf deren Formulierung, sondern auch auf die dahinterliegende Strategie und Umsetzung aus. 65 Prozent der teilnehmenden Organisationen mit entsprechenden Compliance-Zielen gaben an, dass sie Jahresziele definiert haben, gefolgt von mittelfristigen Zielen mit

51 Prozent, langfristigen mit 36 Prozent und kurzfristigen Zielen 32 Prozent. Deloitte empfiehlt, unterschiedliche Zeithorizonte zu berücksichtigen.

Die reine Quantifizierung der Compliance-Ziele hat sich in der Praxis nicht bewährt. Eine Mischung aus qualitativen und quantitativen Zielsetzungen hat sich durchgesetzt. 54 Prozent der Teilnehmenden mit definierten Compliance-Zielen gaben an, sowohl qualitative als auch quantitative Ziele zu verfolgen, 44 Prozent setzen eher auf qualitative Ziele. Nur zwei Prozent haben rein quantitative Ziele formuliert.

Die Messbarkeit von Zielen ermöglicht die Bewertung der Wirksamkeit von Maßnahmen. Allerdings spielt für 44 Prozent der Befragten die Messbarkeit lediglich eine eher bedeutende Rolle bei der Definition von Compliance-Zielen. Zehn Prozent sprechen dem Kriterium sogar keine Bedeutung zu.

Weitere Infos zum Report „The Future of Compliance 2023“ finden Sie hier [1].

**Quelle**

[1] https://www2.deloitte.com/de/de/pages/audit/articles/future-of-compliance.html

## Große Defizite beim Nachhaltigkeitsreporting – Inflation, Volatilität und Klimawandel sind größte Risiken

**Nachricht vom 16.11.2023**

*Investierende, die auch oder ausschließlich in Deutschland aktiv sind, sehen für die kommenden zwölf Monate Inflation, gesamtwirtschaftliche Volatilität und den Klimawandel als die größten Risiken für ihre Portfoliounternehmen an.*

Und: Fast alle Investorinnen und Investoren halten das Nachhaltigkeitsreporting von Unternehmen zumindest teilweise für unzuverlässig. Das sind einige der Kernergebnisse des PwC Global Investor Surveys 2023.

Gefragt nach den größten potenziellen Bedrohungen für ihre Portfoliounternehmen in den kommenden zwölf Monaten machten die Befragten vor allem diese Punkte geltend:

- 49 Prozent nannten die Inflation (30 Prozent stark betroffen, 19 Prozent extrem stark betroffen).
- 46 Prozent führten die gesamtwirtschaftliche Volatilität an (31 Prozent stark, 15 Prozent extrem).
- 41 Prozent sehen den Klimawandel als Schlüsselbedrohung (29 Prozent stark, 12 Prozent extrem).

Der Klimawandel ist für 54 Prozent der Befragten zugleich einer der wesentlichen Werttreiber für die kommenden drei Jahre. Dazu zählen auch der technologische Wandel (67 Prozent) und veränderte Kundenpräferenzen (56 Prozent).

90 Prozent sehen es als entscheidend für die Wertschöpfung an, dass Unternehmen Künstliche Intelligenz schneller als bisher für sich nutzen. Zugleich sind sie sich aber der Risiken bewusst, die mit dem KI-Einsatz einhergehen, allen voran unzureichende Governance-Prozesse, Kontrollen und Datensicherheit – gefolgt vom Risiko, das von falschen Informationen ausgeht.

Dabei ist das Bedürfnis nach verlässlichen Nachhaltigkeitsinformationen enorm, betont PwC im Global Investor Survey. Es sei klar erkennbar, dass die großen globalen Veränderungen, allen voran der Klimawandel und die Digitalisierung, auch die Entscheidungen der Investierenden immer stärker beeinflussen.

86 Prozent der Befragten sei mit Blick auf ihre Investmententscheidungen mindestens teilweise wichtig, wie Unternehmen nachhaltigkeitsbezogene Risiken und Chancen managen. Die Adressierung des Klimawandels ist für 44 Prozent einer der wichtigsten Bewertungsfaktoren, nur knapp hinter der Unternehmensführung mit 45 Prozent. 68 Prozent der Befragten sagen sogar, dass sie ihre Investmentanteile schon einmal abgestoßen haben, weil ein Unternehmen bezogen auf Nachhaltigkeitsaspekte nicht aktiv genug war – 71 Prozent erwägen, dies künftig zu tun.

98 Prozent sagen, dass die Unternehmensberichterstattung zur Nachhaltigkeit zumindest in gewissem Maße nicht untermauerte Behauptungen enthält; 17 Prozent von ihnen meinen sogar, dass dies in sehr großem Ausmaß der Fall ist; 40 Prozent konstatieren unzutreffende Angaben in großem Ausmaß.

Besonders unzuverlässig sind nach Ansicht der Befragten Nachhaltigkeitsangaben, insbesondere mit Blick auf Umwelt- und Sozialbelange, gefolgt von anderen verbalen Formen der Berichterstattung und Angaben zur Wesentlichkeitseinschätzung.

PwC Global Investor Survey kann hier angefordert werden [1].

**Quelle**

[1] https://www.pwc.de/de/deals/global-investor-survey-2023-ergebnisse-fuer-deutschland.html

## ChatGPT: Jeder Dritte hat die KI schon mal ausprobiert

**Nachricht vom 16.11.2023**

*ChatGPT wurde vor gut einem Jahr öffentlich zugänglich gemacht. In Deutschland haben mittlerweile 78 Prozent von dem Chatbot gehört, 34 Prozent habe das Sprachmodell auch schon genutzt.*

Das sind die Ergebnisse einer Befragung unter 1.004 Personen ab 16 Jahren im Auftrag des Digitalverbands Bitkom. Demnach haben es 10 Prozent bei einem Versuch belassen und nutzen ChatGPT nicht mehr, 11 Prozent nutzen das Tool selten und 13 Prozent häufig.

**Ergebnisse zur Nutzung:**

- 82 Prozent der ChatGPT-Nutzerinnen und -Nutzer setzen das Tool für private Zwecke ein.
- 50 Prozent nutzen ChatGPT auch beruflich, davon ein Drittel ohne Wissen des Arbeitgebers.
- Nur bei 24 Prozent der Erwerbstätigen gibt es im Unternehmen Regeln für den Einsatz von generativer KI.
- 29 Prozent haben im Job keine solchen Vorgaben, würden sich aber welche wünschen.
- 40 Prozent haben am Arbeitsplatz keine Regeln und möchten auch keine.

**Ergebnisse zum Nutzen:**

- 53 Prozent sagen, dass die Dialoge mit ChatGPT Spaß machen.
- 32 Prozent geben an, dass sie die Antworten der KI fasziniert haben.
- 13 Prozent meinen, dass ChatGPT ihnen bei Problemen geholfen hat.
- 20 Prozent beklagen, dass es zu viel Zeit kostet, hilfreiche Antworten von ChatGPT zu bekommen.
- 14 Prozent finden, dass der Chatbot ihre Fragen zu oft nicht richtig versteht.

„Auf den ersten Blick ist die Nutzung von generativer KI sehr einfach. Um aber hilfreiche Antworten zu bekommen, muss man lernen, der KI die notwendigen Hin-

tergrundinformationen zu vermitteln und Arbeitsaufträge präzise formulieren", resümiert Bitkom [1]. Außerdem sollten die Nutzerinnen und Nutzer wissen, wie sie die Ergebnisse schnell auf Richtigkeit überprüfen können.

Wie sich ChatGPT sinnvoll in Unternehmen einsetzen lässt, zeigt das Buch „ChatGPT in der Unternehmenspraxis – Anwendungsbeispiele für Risikomanagement, Controlling und Compliance" [2]. Der Chatbot verfasst Aufsätze, Gedichte, Songtexte, Rezensionen, Interpretationen und Porträts. Er entwirft Verträge, Referenzen, Zeugnisse, Bewerbungen, Geschäftsberichte, Marketinganalysen, Strategieberichte, Vorträge, Skripte und Rechtsgutachten. Er generiert Website-Codes und kann beim Verfassen von Businessplänen, Governance-Konzepten, Risikomanagementsystemen, Notfallplänen und Gesetzen sehr hilfreich sein [3].

**Quelle**

[1] https://www.bitkom.org/Presse/Presseinformation/Ein-Jahr-ChatGPT-Jeder-Dritte-hat-KI-Chatbot-ausprobiert
[2] https://esv.info/978-3-503-23697-8
[3] https://esv.info/aktuell/esv-im-dialog-sie-hoeren-recht-episode-10/id/130702/meldung.html

## Korruptionsbekämpfung: Richtlinienvorschlag der EU-Kommission in der Kritik

**Nachricht vom 13.11.2023**

*Der Rechtsausschuss des Bundestags hat sich mit einem Richtlinienvorschlag der EU-Kommission zur Bekämpfung der Korruption befasst.*

Die Sachverständigen äußerten sich überwiegend kritisch zu dem Vorschlag und mahnten teils erhebliche Nachbesserungen an, berichtet der Informationsdienst des Bundestags (hib). Mit der Richtlinie [1] will die Kommission neben einer Stärkung der Prävention und der Gewährleistung der Strafverfolgung auch die Definitionen von Straftaten im Zusammenhang mit Korruptionsdelikten harmonisieren und die strafrechtlichen Sanktionen verschärfen.

Ein wesentlicher Punkt in der Anhörung war hib zufolge [2] die Frage, ob die in Artikel 7 des Richtlinienvorschlags vorgesehene Gleichstellung von Amts- und Mandatsträgern im Bereich der Bestechung und Bestechlichkeit mit dem verfassungsrechtlich garantierten freien Mandat von Abgeordneten vereinbar sein würde. Aktuell wird in Deutschland die Bestechlichkeit und Bestechung von Mandatsträgern anders geregelt als die von Amtsträgern. Das Gros der Sachverständigen sah in diesem Regelungsvorschlag kein Problem in diesem Sinne. Angelika Allgayer, Richterin am Bundesgerichtshof, führte aus, dass der Richtlinienvorschlag zwar eine Gleichstellung bedeute, aber genügend Raum in der Umsetzung für strukturelle Unterschiede zwischen Abgeordneten und Mandatsträgern lasse. In den Verhandlungen zu der Richtlinie sollte ihrer Meinung nach aber auf eine Klarstellung hingewirkt werden, nach der keine vollständige Gleichstellung von Amts- und Mandatsträgern vorgesehen sei, sagte die Sachverständige.

Die Sachverständigen hatten weniger ein Problem mit dem Artikel 7, sondern vielmehr mit den übrigen Regelungen des Vorschlags. Der Entwurf sei inhaltlich unausgereift und „lässt kein strukturiertes Konzept erkennen", bemängelte etwa Professor Jörg Eisele von der Universität Tübingen. Professor Kilian Wegner von der Europa-Universität Viadrina Frankfurt/Oder sagte, die Richtlinie bedrohe die „Souveränität der Bundesrepublik in Strafrechtssachen" und dürfe in dieser Form nicht beschlossen werden. Professor Frank Zimmermann von der Universität Münster mahnte an, strafrechtliche Regelungen mit Bedacht einzusetzen. Die Richtlinie gehe damit an „etlichen Stellen" zu weit. Er warnte, dass Korruptionsvorwürfe rasch missbraucht werden könnten, um politische Gegner kaltzustellen.

Timo Lange von Lobbycontrol warb dafür, dass Deutschland bei der Korruptionsbekämpfung auf EU-Ebene „treibend vorangehen" solle statt zu bremsen. Lobbycontrol unterstütze das „grundlegende Ansinnen der EU-Richtlinie". Viele der aufgeworfenen Fragen seien lösbar. Der Kampf gegen Korruption sei wichtig, um die Demokratie zu schützen. So sei Korruption in besonderer Weise dazu geeignet, „das Vertrauen in die Demokratie, in demokratische Institutionen und Verfahren zu gefährden", so der Sachverständige. Ähnlich äußerte sich Anna-Maija Mertens für Transparency International. Sie verwies darauf, dass mit der Richtlinie die UN-Konvention gegen Korruption vollständig umgesetzt werden sollte. Es sei ein „große Chance", dass damit die richtigen Themen und Sachverhalte angegangen und geregelt würden.

**Quelle**

[1] https://germany.representation.ec.europa.eu/news/eu-kommission-will-korruptionsbekampfung-verstarken-2023-05-03_de
[2] https://www.bundestag.de/presse/hib/kurzmeldungen-977422

## Ransomware ist größte Bedrohung – Neue Risiken durch KI-Einsatz

**Nachricht vom 02.11.2023**

*Die Bedrohung im Cyberraum ist so hoch wie nie zuvor. Das ist das Fazit des Bundesamts für Sicherheit in der Informationstechnik (BSI) im jetzt veröffentlichten Bericht zur Lage der IT-Sicherheit in Deutschland. Darin geht es auch um den Einsatz Künstlicher Intelligenz.*

Bei Cyberangriffen mit Ransomware beobachtet das BSI eine Verlagerung der Attacken: Nicht mehr nur große, zahlungskräftige Unternehmen stehen im Mittelpunkt, sondern zunehmend auch kleine und mittlere Organisationen, dazu staatliche Institutionen und Kommunen.

Wie die Realwirtschaft setzen auch Cyberkriminelle zunehmend auf Arbeitsteilung, einen wachsenden Dienstleistungscharakter und eine enge Vernetzung über Länder- und Branchengrenzen hinweg. Mit dem Konzept des „Cybercrime-as-a-Service" agieren Cyberkriminelle immer professioneller, denn die Spezialisierung auf bestimmte Dienstleistungen ermöglicht es ihnen, ihre „Services" gezielt zu entwickeln und einzusetzen, teilt das BSI mit.

Das BSI registriert immer mehr Schwachstellen in Software. Diese Schwachstellen sind oft das Einfallstor für Cyberkriminelle auf ihrem Weg zu einer Kompromittierung von Systemen und Netzwerken. Mit der Anzahl stieg auch ihre potenzielle Schadwirkung: Immer mehr Lücken (etwa jede sechste) werden als kritisch eingestuft.

### Generative KI sorgt neben Chancen auch für neue Risiken

Tools mit Künstlicher Intelligenz wie ChatGPT, Bard und LlaMa sind einfach zu bedienen und liefern eine hohe Quali-

tät. Dabei können sie auch für kriminelle Zwecke missbraucht werden. So können sie dafür sorgen, dass manipulierte Bilder, Videos und Stimmen authentischer werden und dadurch schwerer zu entlarven sind. Auch kann KI Phishing-Mails glaubwürdiger machen, im Social Web zu Desinformationskampagnen beitragen und selbst Schadcode generieren. KI kann auch selbst zur Schwachstelle werden, wenn sie gehackt und missbräuchlich eingesetzt wird. Das stellt das Schwachstellenmanagement in Unternehmen und Behörden vor noch größere Herausforderungen.

Weitere Hintergründe und den vollständigen Bericht hat das BSI hier veröffentlicht [1].

**Quelle**

[1] https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

## Schnittstellen zum Austausch risikorelevanter Informationen – RMA startet Podcast

**Nachricht vom 01.11.2023**

*Viele Unternehmen haben es bislang versäumt, ein ganzheitliches Risikomanagement innerhalb der eigenen Organisation aufzubauen.*

Das ist häufig ein Phänomen in großen Unternehmen mit vielen separaten Governance-Funktionen, beobachtet Ralf Kimpel. Der Vorstandsvorsitzende der RMA Risk Management & Rating Association geht in der ersten Folge des neuen Podcasts „RMA on Air“ [1] genauer darauf ein.

In großen Organisationen werden unterschiedlichste Betrachtungen durch verschiedene Abteilungen durchgeführt und unterschiedliche Tools eingesetzt. „Es fehlt oft an einer Klammer, die das alles verbindet, zusammenführt und dann auch zusammenhält“, so Ralf Kimpel. Das sei eigentlich Aufgabe der Unternehmensleitung. Für diese Klammer könnten aber auch die Akteure im Risikomanagement sorgen. Letztendlich gehe es darum, die verschiedenen Systeme zu vernetzen. Zusammen mit dem Deutschen Institut für Interne Revision (DIIR) hatte die RMA das „Positionspapier Interne Revision und Risikomanagement“ [2] veröffentlicht und darin die verschiedene Organisationsformen mit ihren Vor- und Nachteilen dargestellt.

Danach befragt, wie sich akuter Anpassungsbedarf im Risikomanagement relativ schnell umsetzen lässt, um die Zukunftsfähigkeit von Unternehmen zu gewährleisten, verweist Ralf Kimpel auf Schnittstellen zum Austausch risikorelevanter Informationen zwischen verschiedenen IT-Systemen. Diese Schnittstellen seien heute wesentlich einfacher herzustellen als in der Vergangenheit. So sei etwa die Entwicklung von Dashboards, in denen sich die Informationen für Entscheidungstragende zusammenführen lassen, mit Low-Code-Ansätzen und entsprechenden Tools einfacher und schneller als zuvor.

Das Risikomanagement ist mit anderen Governance-Funktionen eng verzahnt. Neben der gemeinsamen Initiative mit dem DIIR pflegt die RMA auch einen regen Austausch mit dem Internationalen Controller Verein (ICV) [3]. Wünschenswert wäre jetzt noch ein Schulterschluss mit Compliance-Verbänden. Intern werde zeitnah eine neue Content-Management-Plattform eingeführt, um den Informationsaustausch unter den RMA-Mitgliedern zu verbessern. Auch E-Learning-Angebote und Nachwuchsförderung will die RMA ausbauen.

**Quelle**

[1] https://rma-ev.org/podcast-rma-on-air
[2] https://internerevisiondigital.de/ce/interne-revision-und-risikomanagement-empfehlungen-zum-zusammenwirken/detail.html
[3] https://esv.info/978-3-503-17400-3

## Lieferkettengesetz erfordert Umdenken im Risikomanagement

**Nachricht vom 25.10.2023**

*Mit dem Lieferkettengesetz (LkSG) werden Unternehmen zur Einhaltung von Menschenrechten und Umweltstandards in ihren globalen Lieferketten verpflichtet. Dazu sollen umfangreiche Handlungs-, Kontroll- und Berichtspflichten umgesetzt werden.*

Darauf weist das Beratungsunternehmen Rödl & Partner hin und stellt fest: Nicht zuletzt aufgrund einer zu erwartenden Ausweitung der Sorgfaltspflichten auf mittelbare Zulieferer, sollten diese schon jetzt in der Risikoanalyse berücksichtigt werden. Das Risikomanagement habe sicherzustellen, dass Unternehmen in ihren Lieferketten Risiken bezüglich potenzieller Verstöße gegen Menschenrechts- und Umweltstandards identifizieren, bewerten und angemessen steuern. Ein weiterer Schwerpunkt liege darauf, die Einhaltung der Sorgfaltspflichten sicherzustellen, indem angemessene Maßnahmen in allen relevanten Geschäftsprozessen verankert werden.

Während das Risikomanagement gemäß IDW PS 981 darauf ausgerichtet ist, Risiken zu erkennen, zu bewerten und zu steuern, die das Unternehmen selbst betrifft, fordert das LkSG Unternehmen dazu auf, ihren Blick von der Betrachtung der Risiken für den Geschäftserfolg des Unternehmens abzuwenden, so Rödl & Partner. Stattdessen sollen sie eine menschen- und umweltrechtliche Perspektive einnehmen, die den Fokus auf die Auswirkungen der Unternehmensaktivitäten, die Umwelt und die betroffenen Stakeholder richtet.

Eine Risikoanalyse diene zur präzisen Identifikation von Risiken innerhalb des eigenen Geschäftsbereichs des Unternehmens und der unmittelbaren Zulieferer. Die Analyseergebnisse lieferten Unternehmen Informationen darüber, in welchem Maß Menschenrechts- und Umweltrisiken in ihrem eigenen Geschäftsbereich und in der Lieferkette auftreten. Dies bilde die Grundlage für Entscheidungen bezüglich erforderlicher Ressourcen, Fachkenntnisse, Zuweisung von Verantwortlichkeiten und die Integration in wesentliche Geschäftsprozesse im Rahmen des Risikomanagements.

Die Risikoanalyse sei mindestens einmal jährlich durchzuführen – außerdem anlassbezogen, wenn das Unternehmen mit einer wesentlich veränderten oder wesentlich erweiterten Risikolage in der Lieferkette rechnen muss und zusätzlich auch dann, wenn das Unternehmen konkrete Informationen hat, die darauf hinweisen, dass bei einem mittelbaren Zulieferer Menschenrechtsverletzungen oder Verstöße gegen Umweltauflagen wahrscheinlich sind.

Rödl & Partner empfiehlt, bei der Risikoanalyse folgende Schritte zu beachten:

- Abstrakte Risikoanalyse: Risiken sind beispielsweise anhand von Stammdaten, Indizes zu Länder- und Branchenrisiken allgemein einzuordnen.
- Konkrete Risikoanalyse: Eine detaillierte Risikoanalyse der zuvor abstrakt

identifizierten Risiken. Dazu kann auf intern vorhandenes Wissen, Recherche von weiteren Daten, Fragebögen oder Zertifizierungen zurückgegriffen werden.
- Gewichtung und Priorisierung der Risiken: Maßgeblich sind dabei Art und Umfang der Geschäftstätigkeit, das Einflussvermögen auf den unmittelbaren Verursacher, die zu erwartende Schwere, Umkehrbarkeit und Eintrittswahrscheinlichkeit eines Risikos und der eigene Verursachungsbeitrag.

Zur Umsetzung der Risikoanalyse gemäß LkSG hat das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) eine Handreichung veröffentlicht [1], in der die Anforderungen des LkSG erläutert und Hilfestellungen zur Umsetzung gegeben werden.

Mit der Einführung des deutschen Lieferkettengesetzes haben viele andere Länder in und außerhalb der EU ähnliche Vorschriften erlassen. Auch die EU arbeitet an einem Rahmenwerk zur Regulierung globaler Lieferketten. Der entsprechende Gesetzesvorschlag deutet heute darauf hin, dass die rechtlichen Anforderungen in Deutschland verschärft werden könnten.

Die vollständige Mitteilung von Rödl & Partner finden Sie hier [2].

**Quelle**

[1] https://www.bafa.de/DE/Lieferketten/Risikoanalyse/risikoanalyse_node.html
[2] https://www.roedl.de/themen/lieferketten-compliance/perspektivenwechsel-risikoanalyse-management-internationale-geschaeftsbeziehungen

## Tipps zum Schutz gegen Ransomware

**Nachricht vom 25.10.2023**

*Jedes neunte Unternehmen in Deutschland, das Opfer von Ransomware wurde, hat daraufhin Lösegeld bezahlt. 44 Prozent der Ransomware-Opfer berichten, dass ihr Geschäftsbetrieb durch die lahmgelegten Computer und verlorenen Daten beeinträchtigt wurde, im Schnitt für rund 3 Tage.*

Das teilt der Digitalverband Bitkom auf Basis einer Befragung von 1.002 Unternehmen ab 10 Beschäftigten in Deutschland mit. „Wer Opfer von Ransomware wird, sollte auf keinen Fall bezahlen", sagt Susanne Dehmel, Mitglied der Bitkom-Geschäftsleitung. Man würde dadurch die kriminellen Organisationen stärken, die hinter den Attacken stehen, und ein interessantes Ziel für weitere Angriffe bleiben. Außerdem sei die Schadsoftware oft so schlecht programmiert, dass sich die Daten selbst nach Zahlung nicht oder nicht vollständig wiederherstellen lassen.

Hintergrund: Wenn „Ihr Computer ist gesperrt" oder „Ihre Daten sind verschlüsselt" auf dem Bildschirm erscheint, hat auf dem Computer eine Ransomware zugeschlagen. Die Folge: Daten auf den Festplatten sind verschlüsselt und meistens wurden auch noch Kopien davon zu den Tätern übertragen, die für die Wiederherstellung ein Lösegeld fordern – und andernfalls zudem mit der Veröffentlichung der häufig sensiblen Informationen drohen.

Ein wirksames Mittel gegen Ransomware-Attacken seien Backups. Wer aktuelle Sicherungskopien der Daten hat und auch geübt hat, diese wieder schnell in die Systeme einzuspielen, könne den Schaden deutlich reduzieren.

Insgesamt wurde 52 Prozent der Befragten innerhalb eines Jahres mit Ransomware angegriffen, 23 Prozent mit Schaden, 29 Prozent ohne. 11 Prozent haben sich an eine Strafverfolgungsbehörde gewandt. 49 Prozent gaben an, die Daten selbst wiederherstellen zu können. 7 Prozent haben auch ohne Zahlungen mit Hilfe der Täter wieder Zugang zu den Daten bekommen. Von 1 Prozent wurden Daten durch die Cyberkriminellen veröffentlicht.

## Geschäftsmodell-Review als Schlüsselaufgabe für Aufsicht und Führung

**Nachricht vom 24.10.2023**

*Die Schlüsselaufgabe kompetenter und professioneller Unternehmensführung und Aufsicht besteht darin, die relevanten Veränderungen zu identifizieren und für Chancen zu sorgen. Ein wesentliches Element dabei ist der Geschäftsmodell-Review.*

Ein Review setzt eine profunde Situationsdiagnose voraus. Worauf es darauf ankommt, erörtert Prof. Dr. Roman Stöger in der aktuellen Ausgabe der ZCG [1]. Im Zentrum steht die Frage, warum ein Unternehmen bisher erfolgreich war und welche Kompetenzen dies ermöglichten. Sollten dabei die Sichtweisen der Verantwortlichen grundlegend voneinander abweichen, wird es schwierig, ein gemeinsames Zukunftsbild zu entwerfen. Der Impuls für den Geschäftsmodell-Review muss von der unternehmerischen Gesamtführung kommen.

Die Einsatzmöglichkeiten des Geschäftsmodell-Reviews sind vielfältig. Es hängt vom situativen Kontext und den unternehmerischen Herausforderungen ab, wo der jeweilige Schwerpunkt gesetzt wird.
- **Kompetenzprofil für die Governance:** Der Geschäftsmodell-Review ist eine Kernaufgabe der Corporate Governance. Aufsicht und Top-Management sind für Positionsbestimmung, Navigation, Chancennutzung und Risikodiagnose verantwortlich.
- **Unternehmen-Geschäftsfeld-Funktion:** Der Geschäftsmodell-Review lässt sich auf ein ganzes Unternehmen oder auf einzelne Geschäftsfelder anwenden und hängt von der Größe und Komplexität der Organisation ab.
- **Schlüsselressourcen und -kompetenzen:** Wenn hinlänglich klar ist, wie das künftige Geschäftsmodell auszugestalten ist, können die Konsequenzen für Schlüsselressourcen und -kompetenzen abgeleitet werden, beispielsweise für die Personalentwicklung.
- **Kooperation und Akquisition:** Durch den Review wird klar, wo künftige Kooperations- und Akquisitionsfelder liegen.
- **Risikomanagement:** Durch die Betrachtung von Transformation und Wertstrom kommen Aspekte des Risikomanagements in die Diskussion: Gefahren, Entwicklungen, „blinde Flecken" und die Erfordernisse der künftigen Aussteuerung der Risiken.
- **Belegschaftsvertretung:** Die Belegschaftsvertretung sollte in die Review-Diskussion einbezogen werden.
- **Kommunikation:** Der Review ist ein Kommunikationsinstrument für relevante Stakeholder, weil konsequent aus dem Geschäft heraus argumentiert wird.

Der Geschäftsmodell-Review ist im Kern ein Business-Radar und zwingt zum Durchdenken des Umfelds, der Märkte, des Unternehmens und der Ressourcen. Indirekt ist er ein Assessment-Center sowohl für die Kompetenz der Governance als auch für eine Kultur der Verände-

rungsfähigkeit und der Lösungsorientierung.

Den vollständigen Beitrag lesen Sie in der ZCG 5/23 [2].

**Quelle**

[1] https://www.zcgdigital.de/

[2] https://zcgdigital.de/ce/geschaeftsmodell-review/detail.html

## Managed Services als Konzept bei Personalengpässen – Vor- und Nachteile

**Nachricht vom 13.10.2023**

*Managed Services können Unternehmen dabei helfen, Herausforderungen wie die Personalgewinnung zu bewältigen. Führungskräfte sind mit diesem Konzept jedoch oft nicht vertraut.*

Das ist das zentrale Ergebnis der jetzt veröffentlichten PwC Managed Services Studie 2023. Befragt wurden 100 Führungskräfte aus Deutschland von Januar bis März 2023.

Die Untersuchung zeigt, dass 38 Prozent der Teilnehmenden nur bedingt Kenntnisse von Managed Services haben. 21 Prozent gaben an, nichts über das Konzept zu wissen. Entscheiderinnen und Entscheider schätzen die Vorteile des Dienstleistungsmodells dementsprechend unterschiedlich ein, stellt PwC fest [1]. Während 90 Prozent der Nutzerinnen und Nutzer von Managed Services den Zugriff auf spezialisierte Ressourcen als Vorteil sehen, bestätigten das in der Gruppe der Nicht-Nutzenden nur 70 Prozent.

Bei vielen Unternehmen ist die schwierige Personalsituation ein Treiber für die Auseinandersetzung mit Managed Services. Für 85 Prozent ist die Suche nach den passenden Mitarbeitenden eine große Herausforderung. 79 Prozent glauben, dass Managed Services dabei helfen können, Personalengpässe zu vermeiden.

### Hintergrund

Durch Managed Services können Unternehmen Personalengpässe auf mehrere Arten vermeiden. **Vorteile:**

- Externes Wissen von Expertinnen und Experten wird verfügbar.
- Ressourcen lassen sich nach Bedarf aufstocken oder reduzieren.
- Der externe Support steht durchgehend zur Verfügung.
- Die Reaktionszeiten verkürzen sich.

Allerdings bestehen auch **Nachteile:**

- Die Nutzung von Managed Services kann teurer sein als die interne Verwaltung der IT.
- Unternehmen begeben sich in Abhängigkeit von Drittanbietern.
- Es können Probleme bei der Kommunikation auftreten.

Außerdem ist **zu bedenken,** dass

- die Leistungen an die Besonderheiten des eigenen Unternehmens angepasst sein sollten,
- die Sicherheitsvorkehrungen den Anforderungen und Standards des Unternehmens entsprechen,
- die vertragliche Bindung den Bedürfnissen und Zielen des Unternehmens anzupassen.

Ein **Konzept** für die Einführung von Managed Services kann aus folgenden Punkten bestehen:

- Einleitung und Zielsetzung
- Ist-Analyse
- Bedarfsanalyse und Auswahl des Managed Service Providers
- Festlegung der Managed Services
- Festlegung eines Service Level Agreements
- Kommunikation und Change Management
- Schulung und Integration
- Implementierung und Testing
- Überwachung und Verbesserung

In regelmäßigen Abständen sollten die Managed Services evaluiert und das Konzept angepasst werden, um sicherzustellen, dass die Ziele erreicht werden.

**Quelle**

[1] https://www.pwc.de/de/professional-managed-services/pwc-managed-services-studie-2023.html

## ESRS-Implementierung in den DAX 40-Unternehmen – Offene Fragen

**Nachricht vom 10.10.2023**

*Für Unternehmen besteht hinsichtlich der European Sustainability Reporting Standards (ESRS) wenige Monate vor der Einführung Klärungsbedarf.*

Das ist das zentrale Ergebnis einer Umfrage des Deutschen Rechnungslegungs Standards Committees (DRSC) unter den DAX 40-Unternehmen. Eine der größten Schwierigkeiten sehen die Unternehmen demnach in den Unklarheiten bezüglich der Berichtsanforderungen.

Die Ergebnisse im Einzelnen:

- Knapp die Hälfte der DAX 40-Unternehmen hat die Implementierung der ESRS im Finanzressort angesiedelt. In einigen Unternehmen stehen verschiedene Ressorts gemeinsam in der Verantwortung.
- Fast alle befragten Unternehmen haben das Projekt zur Implementierung der ESRS gestartet. Die Hälfte der DAX 40-Unternehmen hatte im Jahr 2022 begonnen, die anderen Unternehmen danach.
- Die erstmalige Wesentlichkeitsanalyse als Kern des ESRS-Implementierungsprojekts ist bei 75 Prozent der DAX 40-Unternehmen abgeschlossen oder in Bearbeitung. In fast ebenso vielen Unternehmen wurden Berichtsprozesse für Nachhaltigkeitsthemen etabliert.
- 80 Prozent der Unternehmen sehen große Schwierigkeiten in der „Unklarheit bezüglich der Berichtsanforderungen“ und in der „Datenqualität/Prüfbarkeit“.
- Fast alle befragten Unternehmen befassen sich neben den ESRS mit mindestens zwei weiteren Berichtsvorgaben.

Einen Kurzbericht zur Umfrage hat das DRSC hier veröffentlicht [1].

**Quelle**

[1] https://www.drsc.de/app/uploads/2023/09/20230929_Kurzbericht_DAX-40-Umfrage_ESRS-Implementierung.pdf

## Nachhaltigkeitsberichte im Fokus der Consultingbranche

**Nachricht vom 10.10.2023**

*Das Thema Nachhaltigkeit gewinnt auch im Consulting an Bedeutung. Das betrifft vor allem die Berichterstattung.*

In Anlehnung an den Deutschen Nachhaltigkeitskodex (DNK) hat der Bundesverband Deutscher Unternehmensberatungen (BDU) jetzt einen entsprechenden Branchenleitfaden entwickelt. Unternehmen mit Pflicht zur Nachhaltigkeitsberichterstattung sollen dabei unterstützt werden, die eigenen Aktivitäten mit Bezug zur Nachhaltigkeit zu erfassen, zu strukturieren, entsprechende Ziele in die

Unternehmensstrategie zu integrieren und konkrete Maßnahmen abzuleiten.

Unternehmensberatungen müssen sich in doppelter Hinsicht mit den drei Nachhaltigkeitsdimensionen auseinandersetzen, stellt der BDU fest: zum einen in Bezug auf ihre eigene Betriebsführung, zum anderen in ihrer Rolle als Multiplikator im Rahmen der nachhaltigen Transformation der Wirtschaft. Zu betrachten seien dabei einerseits das eigene Geschäftsmodell und das Unternehmensumfeld, andererseits die Märkte und Lieferketten, in denen Kunden und Kundinnen agieren.

In den einführenden Kapiteln des Branchenleitfadens werden zunächst beide Sichtweisen skizziert, bevor anschließend die einzelnen Kriterien aus Betriebsführungsperspektive fokussiert und veranschaulicht werden. Der Leitfaden steht hier zum Download [1].

**Quelle**

[1] https://www.bdu.de/media/357454/bdu_branchenleitfaden_nachhaltigkeit_final.pdf

## Markt für IT-Sicherheit wächst auf 9,2 Milliarden Euro

**Nachricht vom 10.10.2023**

*In der deutschen Wirtschaft sind die Ausgaben für IT-Sicherheit gegenüber dem Vorjahr um 13 Prozent auf 9,2 Milliarden Euro gestiegen.*

Für das kommende Jahr werde ein erneuter Anstieg um 13 Prozent erwartet, teilt der Digitalverband Bitkom jetzt mit. Zuletzt sei deutschen Unternehmen durch Sabotage, Spionage und Datendiebstahl ein jährlicher Schaden von 206 Milliarden Euro entstanden, davon 148 Milliarden Euro durch Cyberattacken. Die Angreifenden gingen immer professioneller und arbeitsteilig vor, dabei seien die Grenzen zwischen organisierter Kriminalität und staatlich gesteuerten Akteuren fließend.

Den größten Anteil an den Aufwendungen haben Ausgaben für IT-Sicherheitssoftware mit 4,3 Milliarden Euro, die um 18 Prozent gestiegen seien, stellt Bitkom fest. Aufwendungen für Dienstleistungen zur IT-Sicherheit hätten um 12 Prozent auf 4,0 Milliarden Euro zuleget. 0,9 Milliarden Euro entfallen auf IT-Sicherheits-Hardware.

Die vollständige Mitteilung hat der Digitalverband hier veröffentlicht [1].

**Quelle**

[1] https://www.bitkom.org/Presse/Presseinformation/Markt-IT-Sicherheit-waechst-mehr-9-Milliarden-Euro

## Arbeitszeiterfassung: Ausmaß an Flexibilität umstritten

**Nachricht vom 10.10.2023**

*Mit der gesetzlichen Umsetzung einer Entscheidung des Europäischen Gerichtshofs (EuGH) vom 14.5.2019 zur künftigen Erfassung der Arbeitszeiten von Beschäftigten hat sich jetzt der Bundestagsausschuss für Arbeit und Soziales befasst.*

Das berichtet der Informationsdienst des Bundestags (hib). In einer öffentlichen Anhörung reichten demnach die Stellungnahmen der Sachverständigen von einer möglichst detaillierten bis hin zu einer möglichst flexiblen gesetzlichen Neuregelung des Arbeitszeitgesetzes.

Gemäß EuGH-Urteil müssen die EU-Mitgliedstaaten die Arbeitgeber verpflichten, ein System einzuführen, mit dem die geleistete Arbeitszeit erfasst werden kann. Auf dieser Grundlage hatte das Bundesarbeitsgericht (BAG) festgestellt [1], dass die Arbeitgeber ein System einführen und anwenden müssen, mit dem Beginn und Ende der täglichen Arbeitszeiten einschließlich der Überstunden erfasst werden.

Eine große Rolle spielte in der Anhörung der gesetzlich nicht definierte Begriff der Vertrauensarbeitszeit. Aus Sicht von Isabel Eder vom Deutschen Gewerkschaftsbund ist diese in der Vergangenheit nur „pervertiert“ angewendet worden, die Beschäftigten seien mit einer Menge an zu bewältigenden Aufgaben alleingelassen worden. Insofern gebe es keinen Regelungsbedarf. Eine enge Auslegung des BAG-Urteils wäre nach Ansicht des DGB wünschenswert. Im Übrigen gebe es bereits jetzt genügend Flexibilisierungsmöglichkeiten im Arbeitszeitgesetz. Der DGB plädierte für die Beibehaltung des Achtstundentags, der von erheblicher Bedeutung für den Arbeits- und Gesundheitsschutz sei. Er sprach sich ferner für eine Begrenzung der täglichen Höchstarbeitszeit aus.

Dagegen unterstrich die Bundesvereinigung der Deutschen Arbeitgeberverbände (BDA), dass der Erhalt der Vertrauensarbeitszeit ein wichtiges Element der betrieblichen Praxis sei. Sie schlug vor, die Höchstarbeitszeit auf die Woche zu verteilen. Das BAG habe die Vertrauensarbeitszeit bestätigt, deshalb sollte daran festgehalten und nicht in Arbeitsverträge eingegriffen werden. Der Arbeitgeber habe nur zu ermöglichen, dass die Arbeitszeit erfasst werden kann. Er sei aber nicht verpflichtet, diese selbst zu erfassen.

Unterschiedliche Sichtweisen gab es auch bei den Jura-Professoren. Gregor Thüsing von der Universität Bonn sprach sich für tarifliche Öffnungsklauseln aus. Der EU-Gesetzgeber gehe von einer Wochen-Höchstarbeitszeit von 48 Stunden aus, kombiniert mit Ruhezeiten sei dies ein genügender Schutz.

Christiane Brors von der Universität Oldenburg sagte, auf Dauer länger als acht Stunden pro Tag zu arbeiten, sei ungesund. Mobiles Arbeiten führe zur Entgrenzung von Arbeit und Freizeit. Die Zunahme von psychischen Erkrankungen zeige, dass ein modernes Arbeitsrecht Begrenzungen brauche.

Thomas Klein von der Hochschule für Technik und Wirtschaft des Saarlands ging auf die Vertrauensarbeitszeit ein, von der nicht klar sei, „was es ist“. Wenn damit gemeint sei, dass die Beschäftigten ihre Arbeitszeit selbst festlegen, dann wäre dies nach dem EuGH-Urteil weiterhin möglich. Die Höchstarbeitszeiten dürften jedoch nicht überschritten werden.

Frank Bayreuther von der Universität Passau plädierte für eine klare gesetzliche Vorgabe, dass eine Behörde bei Verstößen ein Bußgeld verlangen kann. Er widersprach der Ansicht, der Arbeitgeber könne selbst entscheiden, ob er von der Arbeitszeiterfassung Gebrauch machen wolle oder nicht.

Video zur Anhörung und die Stellungnahmen der Sachverständigen hat der Bundestag hier veröffentlicht [2].

**Quelle**

[1] https://compliancedigital.de/ce/arbeitszeiterfassung-ausnahme-fuer-leitende-angestellte-erfordert-gesetzesaenderung/detail.html

[2] https://www.bundestag.de/dokumente/textarchiv/2023/kw41-pa-arbeit-zeitkonto-969674

## Aufsichtsrat als Teil eines integrierten Risikomanagements

**Nachricht vom 05.10.2023**

*Politische Krisen und Handelskriege bestimmen zunehmend die Agenda von Aufsichtsräten.*

Das ist das Ergebnis einer weltweiten Umfrage der Beratungsgesellschaft EY unter 500 Board- und Aufsichtsratsmitgliedern von Unternehmen mit mindestens einer Milliarde US-Dollar Umsatz. Demnach gaben 45 Prozent der Befragten an, mit starken oder sehr starken Auswirkungen von geopolitischen Krisen auf ihr Unternehmen und damit auch auf ihre Überwachungstätigkeit zu rechnen. In der vorangegangenen Befragung im Jahr 2021 lag der Anteil bei 34 Prozent.

Ähnlich stark gestiegen ist die Bedeutung von Lieferkettenunterbrechungen, die aktuell ebenfalls von 45 Prozent der Befragten als Top-Thema genannt wird. Vor zwei Jahren hielten 32 Prozent Lieferkettenunterbrechungen für eine Herausforderung, mit der sie sich im Rahmen ihrer Überwachung intensiv beschäftigen müssen.

Das dritte Top-Thema sind Cyberangriffe, deren Bedeutung mit 45 Prozent sehr hoch geblieben ist. Allerdings sehen viele Aufsichtsräte noch großen Handlungsbedarf: Lediglich 40 Prozent der Befragten haben nach eigenen Angaben ein sehr klares Verständnis der wichtigsten Cyberrisiken des Unternehmens. Nur 31 Prozent glauben, dass ihre Überwachung der möglichen Bedrohungen durch die digitale Transformation sehr effektiv ist.

„Die Vielzahl an Krisen, mit denen sich Unternehmen seit einigen Jahren konfrontiert sehen, hat erhebliche Auswirkungen nicht nur für die Arbeit des Managements, sondern auch für die Aufsichtsräte“, stellt EY fest. Aufsichtsräte müssten mehr Zeit aufwenden, das Unternehmen besser kennenzulernen, damit sie in der Lage sind, neben langfristigen Trends auch kurzfristige und überraschende Ereignisse zu bewerten.

Der Aufsichtsrat sollte einen vollständigen und integrierten Blick auf die Risiken eines Unternehmens haben, um sich auf Basis belastbarer Informationen mit Themen wie Nachhaltigkeit, Compliance und mit der entsprechenden Berichterstattung befassen zu können, zu der Unternehmen künftig viel stärker verpflichtet sind, so EY. Dafür müsse er sich intensiv mit dem Risikomanagement im Unternehmen verzahnen. Das Ziel sei ein integriertes Risikomanagement. Bis dahin sei der Weg bei vielen Unternehmen allerdings noch weit: Nur 57 Prozent der Aufsichtsräte treffen sich mindestens quartalsweise mit dem Chief Risk Officer.

Im Vergleich zur vorherigen Befragung haben die meisten der 13 abgefragten Risiken für die Unternehmensüberwachung an Bedeutung gewonnen. Besonders stark gewachsen ist das Risiko, dass neue Marktteilnehmer entstehen und dem Unternehmen Marktanteile abnehmen könnten: von 22 auf 42 Prozent. Genauso stark an Bedeutung gewonnen hat das Risiko einer falsch ausgerichteten Unternehmenskultur. Allerdings geben 60 Prozent der Befragten an, dass neu aufkommende Risiken bislang in ihrer Arbeit unzureichend berücksichtigt werden.