Compliance

Die Zeitschrift für Compliance-Verantwortliche

April 2024

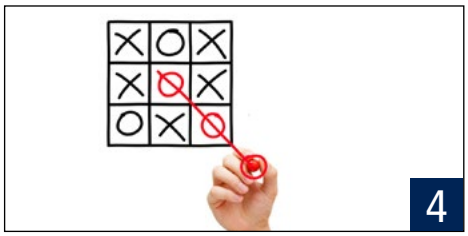
Inhalt

© IMAGO / Tetra Images

Aufmacher

Compliance Officer – ein unterschätzter Beruf
Wer hätte gedacht, dass einige Compliance-Skandale vor gut 20 Jahren für die Entstehung eines komplett neuen Berufsbildes mitursächlich werden. Ungefähr seitdem haben alle großen und viele mittelgroße Unternehmen Compliance-Management-Systeme (CMS) eingeführt. Während ihre Entwicklung und Verbesserung im Vordergrund standen, sind die für Compliance angestellten Personen in den Hintergrund geraten.

Kolumne



© IMAGO / Design Pics

Kolumne: Spielräume erkennen
Legal & Compliance und der Umgang mit Krisen – warum verschiedene Strategien richtig sind und was es mit K-Krisen und L-Krisen auf sich hat, erläutert Markus Jüttner in unserer monatlichen Kolumne.

Recht

© IMAGO / Tetra Images

Einigung über Europäische Lieferkettenrichtlinie erzielt
Vor wenigen Wochen schien es noch, dass die EU-Lieferkettenrichtlinie bis auf weiteres durch die Blockadehaltung – unter anderem – aus Deutschland auf Eis liegt. Am 15. März 2024 meldete die belgische Ratspräsidentschaft dann aber auf der Online-Plattform X: „Die Botschafter haben gerade die Corporate Sustainability Due Diligence Directive (CSDDD) bestätigt!"

International

© IMAGO / Steinach

Die EU-DSGVO gleich Schweizer DSG – oder etwa doch nicht?
Das revidierte Schweizer DSG ist am 1. September 2023 in Kraft getreten. Getrieben durch den technischen Fortschritt war das Gesetz zum einen ziemlich in die Jahre gekommen, zum anderen war das neue Datenschutzniveau, das die DSGVO mit sich gebracht hat, ein weiterer treibender Faktor für die Überarbeitung.

Veranstaltungen

18.04.2024 | Frankfurt am Main oder Online | **2. RAW SUMMIT – Future of Automotive Law**

07.05.2024 | Berlin | **Fashion Law 2024 – 1. Deutscher Moderechtstag**

11. & 12.06.2024 | Düsseldorf oder Online | **Deutsche Compliance Konferenz**

13.06.2024 | Berlin | **KI im Unternehmen**

13. & 14.06.2024 | Dresden | **Sanierungsberater Jahrestagung**

19.06.2024 | Webinar | **Das HinSchG und der Umgang mit Hinweisen**

Compliance Officer – ein unterschätzter Beruf

Wer hätte gedacht, dass einige Compliance-Skandale vor gut 20 Jahren für die Entstehung eines komplett neuen Berufsbildes mitursächlich werden. Ungefähr seitdem haben alle großen und viele mittelgroße Unternehmen Compliance-Management-Systeme (CMS) eingeführt. Während ihre Entwicklung und Verbesserung im Vordergrund standen, sind die für Compliance angestellten Personen in den Hintergrund geraten. Wer sind aber eigentlich diese Menschen, die als Compliance-Officer, Compliance-Beauftragte oder Compliance-Verantwortliche bezeichnet werden? Der Beantwortung dieser Frage widmet sich Prof. Dr. Bartosz Makowicz gleichsam mit einer Hommage an Compliance Officer.

Schon fast ein Held: Dem Compliance-Officer wird viel abverlangt.

Kann man nach fast zwei Dekaden von einem neuen und fest etablierten Berufsbild sprechen? Um die Frage zu beantworten, schauen wir erst einmal, was alles von Compliance-Verantwortlichen erwartet wird. Zunächst müssen sie ihre jeweilige Organisation, ihre Struktur und Prozesse sowie vor allem die Mitarbeitenden kennen und verstehen. Sie müssen also den Kontext des Unternehmens korrekt erfassen. Das ist die Basis, aber bei weitem nicht alles. Sie müssen nämlich auch in der Lage sein, die für ihr Unternehmen und seine Beschäftigten geltenden Rechtsnormen zu erkennen: Ob Geldwäsche, Wettbewerbsrecht, Lieferketten – hier sind sowohl der unionale, als auch der bundeseigene Gesetzgeber aktiver denn je, als würden sie an einem Wettbewerb der Regulatorik teilnehmen. Doch reichen rein juristische Kenntnisse auch nicht aus, vielmehr müssen sie anschließend die Risiken der Nichteinhaltung dieser Regeln sorgfältig evaluieren. An der Stelle müssen Fähigkeiten an den Tag gelegt werden, die jedenfalls nicht im Jurastudium vermittelt werden.

Und hier geht es erst richtig los: Denn nun müssen die ermittelten Compliance-Risiken mit sogenannten „geeigneten Vorkehrungen" adressiert werden. Was darunter zu verstehen ist, wagt uns weder der Gesetzgeber (Stichwort „VerSanG-E"), noch die Rechtsprechung zu sagen. Letztere hat immerhin einem effektiven CMS eine sanktionsmindernde Wirkung inzwischen bescheinigt. Vielmehr wird nun von denselben Personen, die schon so viel leisten müssen, eine praktisch grenzenlose Innovation verlangt. Und das kann alles bedeuten, denn ein CMS kann bekanntlich nur wirksam werden, wenn es passgenau ist: So sind sie primär Übersetzer und Kommunikatoren, wenn sie die abstrakten Rechtsnormen etwa in einem Verhaltenskodex abbilden; sie sind Berater, wenn konkrete Einzelfälle auftreten, oder Aufklärer, wenn Verdachtsfälle gemeldet werden – um nur einige ihrer Aufgaben zu erwähnen. Und dann heißt es noch: Berichten, berichten, berichten, womit sie für ein gutes Gewissen der Vorstände sorgen, die ja sonst persönlich haften könnten. Nicht zuletzt sind sie Designer, da alle Elemente auch zueinander passen müssen, wobei sie sich dabei an den gut strukturierten ISO-Standards orientieren können.

Auch wenn das CMS einmal implementiert ist, so gehen ihnen trotzdem – quasi on top – einige Sorgen durch den Kopf (und gemeint ist hier gar nicht die potenzielle strafrechtliche Haftung, die schon frühzeitig der BGHSt. ins Spiel brachte). Erstens die große Frage nach dem Warum? Warum werden Regeln gebrochen, selbst wenn das CMS gut läuft? Spätestens an der Stelle werden sie die Grundzüge der Verhaltenspsychologie für sich entdecken, die im Gewand des Integrity-Ansatzes ein CMS bestens ergänzen können. Zweitens werden sie sich sorgen, ob sie nicht bald durch die KI ersetzt werden. Dies wird aber noch lange nicht geschehen, wenn sie jetzt schon die vielfältigen KI-Werkzeuge in ihrem operativen Compliance-Job gekonnt einsetzen. Drittens wundern sich einige, dass sie seit dem Inkrafttreten des LkSG auch noch zu weltweiten Menschenrechts- und Umweltaktivisten geworden sind. Und schließlich fragen sie sich zurecht, wo eigentlich der Platz für Compliance in dem neuen ESG-Konzept ist? Dabei wird sie die Lektüre des DCGK nicht wirklich weiterbringen, in dessen neuster Fassung sie quasi zur Unter-Abteilung der internen Kontrolle „degradiert" wurden. Alles in allem recht turbulente Zeiten.

Einige Dinge stehen inzwischen aber fest, um nun zum Schluss der Mini-Hommage auf die Compliance-Officer zu kommen: Nach rund zwei Dekaden ist ebenso wenig das CMS aus der Governance-Struktur, wie die Compliance-Officer aus dem Unternehmensalltag wegzudenken. Das neue Berufsbild steht – zumindest in den Konturen, denn lange noch ist es nicht fertig gezeichnet. Fest steht ferner auch, dass kaum ein anderer Beruf derart herausfordernd, dynamisch und interdisziplinär ist, wie der Compliance-Job. Führt man all die Fähigkeiten, die von Compliance-Officers verlangt werden und all die guten Dinge zusammen, die sie für ihre Unternehmen tun, so müssten sie eigentlich jetzt schon als Helden gefeiert werden!

Prof. Dr. Bartosz Makowicz

Prof. Dr. Bartosz Makowicz, Leiter des berufsbegleitenden und interdisziplinären Masterstudiengangs „Compliance & Integrity Management" sowie des Viadrina Compliance Center an der Europa-Universität Viadrina Frankfurt (Oder): www.compliance-master.de.

AI in Prozessen von IT-Sicherheitsteams: Effizienz und Genauigkeit steigern

Die zunehmende Verfügbarkeit und Leistungsfähigkeit von AI-Tools machen sie zu unverzichtbaren Hilfsmitteln für IT-Sicherheitsteams. AI-Algorithmen unterstützen Experten dabei, große Datenmengen zu analysieren, potenzielle Angriffe zu erkennen und Risiken durch Drittanbieter zu identifizieren. Sie ermöglichen das Scannen von Netzwerken nach Schwachstellen, die Automatisierung von Reaktionen auf Vorfälle und die Erkennung bedrohlicher Anomalien, was Sicherheitsteams einen Wettbewerbsvorteil verschafft.

Auswahl relevanter Prompts für die Optimierung von Sicherheitsprozessen mit AI

Der Schlüssel zur Nutzung eines AI-Modells für die Sicherheit des Unternehmens liegt im sogenannten „Prompting", bei dem dem Modell klare Anweisungen für seine Aufgabe gegeben werden. Mit folgendem Vorgehen können die effektivsten Ergebnisse erzielt werden:

- Sicherheitsziele festlegen: Die Prompts sind so zu formulieren, dass relevante Bedrohungen erkannt und identifiziert werden können. Vage oder mehrdeutige Prompts führen zu ungenauen Ergebnissen.
- Umfang der Sicherheitsaufgabe definieren: Beispielsweise kann ein Netzwerk-IP-Bereich angegeben oder festgelegt werden, auf welche Geräte zugegriffen werden soll.
- Kontext bieten: Das Modell braucht ein Verständnis über die Umgebung und die Sicherheitsherausforderungen, mit denen es konfrontiert wird.
- Analysen und Empfehlungen anfragen: Vom Modell sollten nicht nur Rohdaten erbeten werden, sondern auch eine Analyse der Daten und Empfehlungen, um spezifische Bedrohungen zu identifizieren und Abhilfestrategien vorzuschlagen.
- Ergebnisse überprüfen und validieren: AI-Modelle können Fehler machen. Sie sollten in Verbindung mit einer menschlichen Überprüfung und Entscheidungsfindung verwendet werden.

Abschaffung manueller Prozesse durch Mustererkennung

Die vermehrte Verwendung von AI-Tools anstelle manueller Analysen resultiert aus der Fähigkeit von Algorithmen des maschinellen Lernens (ML). Sie können große Datenmengen effizient analysieren und Muster erkennen. Diese Algorithmen können dabei helfen, subtile oder weitläufige Datenabweichungen sowie Angriffsmuster zu identifizieren, die für Menschen nur schwer erkennbar sind.

Um die manuelle, auf menschlicher Arbeit basierende Analyse zu stärken und zu ergänzen, können IT-Sicherheitsteams ML-Algorithmen wie folgt nutzen:

- Erkennung verdächtiger Aktivitäten im Netzwerkverkehr (z.B. Spitzen im Datenverkehr, Änderungen im Zugriff oder Zugriffsanfragen, die nicht mit den üblichen Aufgaben in Zusammenhang stehen)
- Analyse von Sicherheitsprotokollen (z.B. unbefugter Zugriff auf sensible Daten)
- Aufdeckung von Insider-Bedrohungen (z.B. sensible Unternehmensdaten offenlegen).

Dennoch sollten jegliche Ergebnisse stets von menschlichen Sicherheitsanalysten überprüft werden, um eine angemessene Interpretation und Einordnung in den realen Kontext sicherzustellen. Darüber hinaus ist es entscheidend, dass IT-Sicherheitsteams ML-Algorithmen kontinuierlich trainieren und die Qualität der Ergebnisse durch sorgfältige Datenauswahl sicherstellen, indem sie die Daten sorgfältig kuratieren, bereinigen und vorbereiten, idealerweise unter Verwendung von tatsächlichen Protokollen und forensischen Analysen historischer Ereignisse.

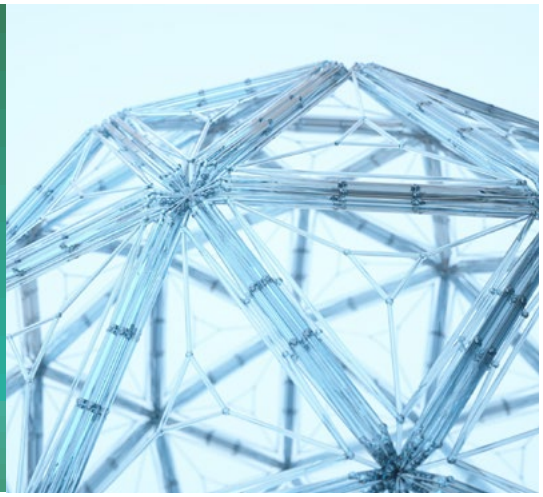
Verbesserte Sicherheitserkennung dank AI

AI-Tools tragen wesentlich zur Erhöhung der Sicherheit bei, indem sie Cyber-Bedrohungen in Echtzeit identifizieren, die Reaktion auf Vorfälle automatisieren und potenzielle Schwachstellen erkennen. Dies verkürzt die Zeit, die für die Erkennung, Eindämmung und Behebung von Cyberangriffen benötigt wird und gibt Angreifern weniger potenzielle Angriffsfläche.

Durch ihre Fähigkeit, große Datenmengen zu analysieren, Muster zu erkennen und aus Erfahrungen zu lernen, bieten AI-Tools eine wertvolle Ergänzung für das Sicherheitsportfolio jedes Unternehmens.

Von Tim Mullen, Chief Information Security Officer & Julian Head, Director of Information Security Architecture

Weiteres praktisches Wissen, wie AI effektiv in die täglichen Abläufe von IT-Sicherheitsteams integriert werden kann, bietet das AI Playbook von OneTrust. Es behandelt eingehend die verschiedenen Aspekte der AI-Nutzung, einschließlich potenzieller Risiken und bewährter Methoden, um sicherzustellen, dass AI-Anwendungen den aktuellen Compliance-Anforderungen entsprechen. Laden Sie das AI-Playbook herunter, um einen Leitfaden für den bestmöglichen Datenschutz zu erhalten und die unternehmensweite Nutzung von AI zu optimieren.



Kolumne: Spielräume erkennen

Legal & Compliance und der Umgang mit Krisen – warum verschiedene Strategien richtig sind und was es mit K-Krisen und L-Krisen auf sich hat, erläutert Markus Jüttner in unserer monatlichen Kolumne.

Viele Compliance-Manager und Syndici haben das Gefühl, dass die Krisen kein Ende nehmen und zum „New Normal" werden. Globale, aber auch lokale Ereignisse und eine hohe Dynamik führen zu einer Kumulation von Entscheidungsnöten. Wie in der letzten Kolumne geschrieben (Compliance Ausgabe März 2024, S. 5), ist in solchen Krisensituationen oftmals nicht ein Plan die Lösung, sondern strategisches Handeln. Allerdings wird dabei häufig der Fehler begangen, sich keine Gedanken darüber zu machen, mit welcher Art von Krise bzw. Problem man konfrontiert ist; dabei ist dies Voraussetzung für eine erfolgreiche Krisenbewältigung.

Strategieeigenschaften für den erfolgreichen Umgang mit einer K-Krise und einer L-Krise

K-Krise	L-Krise
Entschlossenheit	Nachdenken
Erfahrung	(Organisations-) Klugheit
Die Dinge „von vorne" betrachten.	Die Dinge auch „vom Ende her" inspizieren.
Dogmatimus	Flexibilität
Sich von „Freunden" beraten lassen (die das gleiche Mindset haben).	Sich von „Feinden" beraten lassen (die Alternativen aufzeigen).
Gruppendenken	Vielfalt von Ansichten
Eher optimistische Herangehensweise („Wir schaffen das!").	Eher pessimistische Herangehensweise („das und das könnte schiefgehen").
Igel	Fuchs

So sollte man nach Dörner (2013) zwischen K-Krisen (Kurzfristkrisen) und L-Krisen (Langfristkrisen) unterscheiden: Erstere kennt man zu genüge, wenn beispielsweise eine Whisteblowermeldung eingeht, die dann unverzüglich zu investigieren ist, ein Unfall passiert, ein hohes Compliance-Risiko oder anderes Schadensereignis sich plötzlich realisiert etc. In vielen Organisationen wird dann bei größeren Ereignissen dieser Art ein Krisenstab einberufen mit – zu Recht – klaren Aufgaben und Rollenverteilungen. Bei Langfristkrisen hingegen handelt es sich nicht um derartige akute „Notfälle". Die Umsetzung vieler neuer Gesetze, die steigenden Anforderungen an Compliance (vgl. jüngst KG Berlin, 22.1.2024 – 3 Ws 250/21, 161 AR 84/21 zur Verbandshaftung wegen eines Datenschutzverstoßes), die fortwährende Anpassung an Organisations- oder Marktveränderungen, der Umgang mit den gestiegenen ESG-Erwartungen externer Stakeholder, der Digitalisierungsdruck usw. sind Kennzeichen einer Langfristkrise. Es handelt sich mithin um Probleme, deren Lösung nicht unter unmittelbarem hohem Zeitdruck steht. Man hat in der Regel Wochen, Monate oder gar Jahre Zeit, sich auf die neuen Umstände einzustellen, Lösungen zu suchen und das sog. „Operating Model" der Legal- & Compliance-Abteilung danach auszurichten.

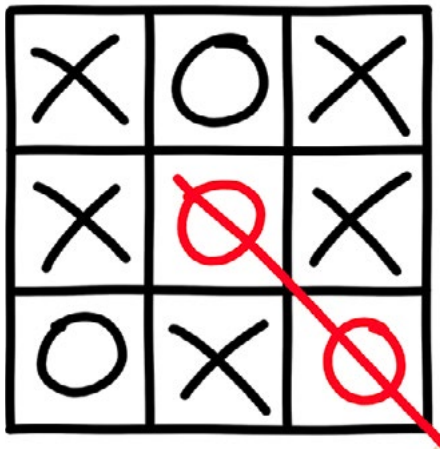
Nun ist es so, dass sich die Strategien zur erfolgreichen Bewältigung dieser beiden Situationen grundlegend unterscheiden. Bei einer K-Krise ist entschlossenes Handeln gefragt. Zögern, Zweifeln oder Zaudern sind keine Tugenden während eines Notfalls. Entscheidungsstärke und Erfahrung sind gefragt. Anders ist es bei einer L-Krise. Hier sind Abwarten, Zweifeln und Zögern nicht schädlich – im Gegenteil. Das Sammeln von Informationen, das Nachdenken über verschiedene Handlungsoptionen und Alternativen führt in der Regel zu besseren Lösungen. Luhmann sagte mal, „Umwege des Denkens ersparen Umwege des Handelns" – ein sehr guter Ratschlag für den Umgang mit L-Krisen. Gefragt ist hier also eine (Organisations-) Klugheit und Erfahrung nur insoweit als sie nicht zu einem Dogmatismus führt. Dies lässt sich anhand der Tabelle unten links veranschaulichen.

Mit den zuletzt genannten – Igel und Fuchs – aus der Tabelle sind zwei Problemlösungsstrategien gemeint, die hier ebenfalls weiterhelfen. „So hat der Psychologe Philip Tetlock aufgezeigt, dass jene Experten realitätsnäher urteilten, deren Denkstil dem des Fuchses entsprach. Offen zu sein für unterschiedliche Sichtweisen, vorschnellen Verallgemeinerungen zu widerstehen und mehrere Wahrheiten gelten zu lassen, zahlt sich offenbar aus. Allerdings, so Tetlocks Ergebnisse, wird dem Igel aufgrund seiner Klarheit und visionären Kraft öffentlich mehr Anerkennung gezollt. Daher ist es auch nicht verwunderlich, dass in Spitzenämtern von Wirtschaft und Politik weniger Füchse als Igel zu finden sind, wie eine andere Studie nahelegt. Wer nach oben kommen will, braucht offenkundig ein klares Profil. Mehrdeutigkeit und Zweifel werden da rasch als Schwäche interpretiert. Zwangsläufig müssen alternative Denkansätze zurücktreten und Widersprüche minimiert werden. In einer komplexen Welt ist aber Vorsicht geboten, wenn Handlungen oder Ereignisse auf einige wenige Grundprinzipien zurückgeführt werden. Typische Igel-Einstellungen zeigen sich in Aussagen wie: „Am Ende des Tages geht es doch immer nur um ABC." Oder: „Letzten Endes zählt nur XYZ." (Meynhardt, 2022)

Zusammenfassend ist also festzuhalten, dass es nicht die eine Krisenbewältigungsstrategie für Legal & Compliance gibt, sondern (mindestens) zwei. Die Strategie zum Umgang mit akuten, dringenden Problemen ist eine andere als die zur Lösung von solchen Problemen, die nicht unter erheblichem Zeitdruck stehen.

Markus Jüttner

Markus Jüttner ist Rechtsanwalt und Partner des Fachbereichs Forensic & Integrity Services, Ernst & Young GmbH. Er berät Unternehmen in Fragen der Compliance, der Kultur und der Integrität.
markus.juettner@de.ey.com



Spielräume erkennen: Es gibt (mindestens) zwei Strategien zur Krisenbewältigung. Welche wann die richtige ist, hängt vom zu lösenden Problem ab.

Forensic Technology

Digitale Transformation: Wie gut kennen Sie neue Betrugsrisiken und -muster?

Die Geschäftswelt dreht sich um künstliche Intelligenz (KI) und die Transformation wesentlicher Betriebsabläufe, die Effizienz in puncto Kosten und Prozesse sowie einen Wettbewerbsvorteil verspricht. Mit dieser Entwicklung steigen auch die Risiken für Betrugsszenarien – eine der aktuellen Herausforderungen für die Interne Revision, Corporate Compliance und Investigationsabteilungen. Gleichzeitig bringen Technologien Chancen: Sie sind Hilfsmittel, wenn es darum geht, Investigationen intelligenter durchzuführen. Unternehmen müssen sich daher fragen: **Verfügen wir über die richtigen Technologien und das passende Know-how, um auch neue Fraud-Schemen zu erkennen, aufzuklären und gravierende finanzielle Verluste und Reputationsschäden zu verhindern? Anita Kim-Reinartz, Leiterin Forensic Services bei PwC, gibt Einblicke in Herausforderungen und Lösungsansätze.**

KI spürt zügig Schwachstellen auf

KI-Tools erstellen inzwischen typische Fraud-Muster – mit erschreckendem Ergebnis. So gibt es bereits eine Reihe an KI-Funktionalitäten, die in unterschiedlichsten Varianten zum Einsatz kommen. Klassisch waren fehlgeschlagene Betrugsszenarien ein Hinweis auf ein gutes Kontrollsystem und erhöhten die Hürden erneuter Versuche. Das wird zunehmend obsolet, denn KI birgt hier das Potential, in Sekundenschnelle Methoden zu überarbeiten und auf Schwachstellen abzuzielen.

Eine sorgfältige Aufdeckung dieser Methoden und ein Präventionsmodell mit „waffengleichen" Mitteln ist von enormer Wichtigkeit für jedes Unternehmen. Interne Investigations-Teams müssen sowohl ihre eigene Organisation entsprechend aufstellen als auch ihre technische Ausstattung und Kompetenzen up to date halten:

1. **Transformation der eigenen Prozesse,** um die Effizienz und die Effektivität der Aufdeckung und Investigation der Betrugsschemen zu steigern
2. **Upskilling** des Teams im Hinblick auf neue Technologien, KI und Methoden, um diese effektiv in einer Investigation einsetzen zu können
3. Entwicklung eines hohen Maßes an **Verständnis für digitalisierte Prozesse im Unternehmen** und deren Risiken sowie Manipulationsmöglichkeiten

© privat

Anita Kim-Reinartz,
Leiterin Forensic Services
PwC Deutschland

Herausforderung angenommen

Egal, ob Unternehmen selbst das Thema Investigation angehen oder externe Unterstützung benötigen: Für beide Fälle bietet PwC Hilfestellungen an. Wir unterstützen in der Transformation von Investigations-Abteilungen. Und wir bieten mit Forensic Technology Solutions unsere Expertise an, wenn zur Untersuchung von Verdachtsfällen elektronische Daten zu erfassen, zu analysieren oder auszuwerten sind. Denn allein mit KI beschäftigen wir uns seit über zehn Jahren.

Zeit, Budget, die richtige Teamaufstellung, aber auch der sorgfältige Einsatz von Technologie: Unternehmen haben in der internen Aufklärung etliche Herausforderungen zu meistern, um die Basis für jede fundierte Investigation aufzubauen. Denn angesichts steigender Wirtschaftskriminalität müssen Unternehmen jederzeit handlungsfähig sein. Der Austausch mit externen Beratern kann hierbei äußerst nützlich sein.

www.pwc.de/forensicservices

Einigung über Europäische Lieferkettenrichtlinie erzielt

Vor wenigen Wochen schien es noch, dass die EU-Lieferkettenrichtlinie bis auf weiteres durch die Blockadehaltung – unter anderem – aus Deutschland auf Eis liegt. Am 15. März 2024 meldete die belgische Ratspräsidentschaft dann aber auf der Online-Plattform X: „Die Botschafter haben gerade die Corporate Sustainability Due Diligence Directive (CSDDD) bestätigt!"

© IMAGO / Tetra Images

Nebel um EU-Lieferkettenrichtlinie lichtet sich: Auch die entschärfte Fassung rückt weiterhin den Umweltschutz in den Fokus.

Trotz der Enthaltung Deutschlands hatte sich schließlich eine ausreichende Mehrheit der EU-Staaten für die Unterstützung des Richtlinien-Entwurfs ausgesprochen. Über die Details des neuen Gesetzes in der ursprünglichen Fassung hatte Compliance bereits in der März-Ausgabe berichtet.

Der am 15. März angenommene Entwurf ist gegenüber dieser Fassung allerdings entschärft. Er basiert auf einem Kompromisstext des Generalsekretariats des Rates, der vor allem folgende Änderungen vorsieht:

Der neue Entwurf gilt für Unternehmen ab 1.000 Beschäftigten und einem Jahresumsatz von 450 Mio. Euro. Zuvor nahm die Richtlinie bereits Unternehmen mit mehr als 500 Arbeitnehmern und einem Nettoumsatz von mehr als 150 Mio. EUR in die Pflicht.

Darüber hinaus sollten ursprünglich auch Unternehmen ab 250 Arbeitnehmern und einem Umsatz von 40 Mio. EUR aktiv werden müssen, wenn 20 Mio. EUR des Umsatzes in Hochrisikosektoren erwirtschaftet werden. Diese Einbeziehung der Hochrisikobranchen ist in der neuen Version nun nicht mehr vorgesehen.

Die Zahl der Unternehmen, die direkt von der neuen EU-Lieferkettenrichtlinie betroffen sind, hat sich damit erheblich gegenüber dem ursprünglichen Entwurf reduziert. Zudem wurde ein stufenweiser Ansatz eingeführt: Eine 3-jährige Umsetzungsfrist für Unternehmen mit mehr als 5.000 Mitarbeitern und 1,5 Mrd. Euro Umsatz; eine 4-jährige Umsetzungsfrist für Unternehmen mit mehr als 3.000 Mitarbeitern und 900 Mio. Euro Umsatz sowie eine 5-jährige Umsetzungsfrist für Unternehmen mit mehr als 1.000 Mitarbeitern und 450 Mio. Euro Umsatz.

Trotz dieser Entschärfungen gehen die Vorgaben der EU-Richtlinie (wie berichtet) deutlich über die des deutschen Lieferkettensorgfaltspflichtengesetzes (LkSG) hinaus. Auf europäischer Ebene rückt z.B. der Schutz der Umwelt deutlich stärker in den Fokus, während das LkSG den Schutz von Menschenrechten in den Mittelpunkt stellt. Außerdem sieht die EU-Richtlinie – anders als das LkSG – zivilrechtliche Haftungstatbestände vor, die bei Verstößen gegen die Sorgfaltspflichten greifen.

Das Europäischen Parlament muss nun noch im April 2024 über die CSDDD abstimmen, um der Richtlinie vor den Neuwahlen im Juni den Weg zu ebnen. *chk*

IMPRESSUM
Verlag
Deutscher Fachverlag GmbH, Mainzer Landstraße 251, 60326 Frankfurt am Main
Registergericht AG Frankfurt am Main HRB 8501
USt-IdNr. DE 114139662
Geschäftsführung: Peter Esser (Sprecher), Sönke Reimers (Sprecher), Thomas Berner, Markus Gotta
Aufsichtsrat: Andreas Lorch, Catrin Lorch, Dr. Edith Baumann-Lorch, Peter Ruß
Redaktion: Christina Kahlen-Pappas (verantwortlich), Telefon: 069 7595-1153, E-Mail: christina.kahlen-pappas@dfv.de
Verlagsleitung: RA Torsten Kutschke, Telefon: 069 7595-1151, E-Mail: torsten.kutschke@dfv.de
Anzeigen: Matthias Betzler, Telefon: 069 7595-2785, E-Mail: Matthias.Betzler@dfv.de
Fachbeirat: Gregor Barendregt, Carl Zeiss AG; Andrea Berneis, Berneis Legal & Compliance; Ralf Brandt, LTS Lohmann Therapie-Systeme AG / Drug Delivery Systems Beteiligungs GmbH; Joern-Ulrich Fink, Central Compliance Germany, Deutsche Bank AG; James H. Freis, Jr., Chief Compliance Officer, Deutsche Börse AG; Otto Geiß, Fraport AG; Mirko Haase, Hilti Corporation; Dr. Katharina Hastenrath, Frankfurt School of Finance & Management; Corina Käsler, Head of Compliance, State Street Bank International GmbH; Olaf Kirchhoff, Schenker AG; Torsten Krumbach, msg Systems AG; Dr. Karsten Leffrang, Getrag; Prof. Dr. Bartosz Makowicz, Europa-Universität Viadrina Frankfurt/Oder; Thomas Muth, Muth-zur-Entwicklung; Stephan Niermann; Dr. Dietmar Prechtel, Osram GmbH; Dr. Alexander von Reden, BSH Hausgeräte GmbH; Hartmut T. Renz, Citi Chief Country Compliance Officer, Managing Director, Citigroup Global Markets Europe AG; Dr. Barbara Roth, Chief Compliance Officer, UniCredit Bank AG; Jörg Siegmund, Getzner Textil AG; Eric S. Soong, Group Head Compliance & Corporate Security, Schaeffler Technologies AG & Co. KG; Elena Späth, AXA Assistance Deutschland GmbH; Dr. Martin Walter, selbstständiger Autor, Berater und Referent für Compliance-Themen; Heiko Wendel, Rolls-Royce Power Systems AG; Dietmar Will, Audi AG.
Jahresabonnement: kostenlos
Erscheinungsweise: monatlich (10 Ausgaben pro Jahr)
Layout: Uta Struhalla-Kautz, SK-Grafik, www.sk-grafik.de

COMPLIANCE COCKPIT

Die Plattform für effektive Compliance-Programme

- Third Parties / Risiken
- Whistleblowing
- Approvals
- Policies

Erfüllen Sie Ihre Sorgfaltspflichten gemäß LkSG sowie das HinSchG mit dem EQS Compliance COCKPIT.

Beschäftigtendatenschutz auf dem Prüfstand – Ein Interview

Vor gut einem Jahr, im März 2023, hat der EuGH die deutschen Regelungen zum Beschäftigtendatenschutz kritisiert und für teilweise unvereinbar mit Europarecht erachtet, gleichzeitig diskutiert der Gesetzgeber – wieder einmal – über ein neues Beschäftigtendatenschutzgesetz. Dr. Stefan Brink (SB), ehemaliger Landesbeauftragter für den Datenschutz in Baden-Württemberg, spricht in diesem Interview mit Dr. Frank Schemmel (FS) über die aktuellen Entwicklungen und die neuesten Erkenntnisse aus Berlin. Dr. Stefan Brink war über sein wissenschaftliches Institut wida in das bisherige Gesetzgebungsverfahren eingebunden und hat sich bereits in seiner Zeit als Leiter einer Datenschutzbehörde intensiv mit diesem Thema befasst.


© Privat

Dr. Frank Schemmel, Compliance Officer (Univ.) ist Senior Director Privacy, Compliance & Public Affairs bei DataGuard in München. Schwerpunkt seiner Arbeit sind Datenschutz, Informationssicherheit, Whistleblowing und die rechtlichen Herausforderungen der Digitalisierung.


© Privat

Dr. Stefan Brink, war zuletzt Landesbeauftragter für den Datenschutz und die Informationsfreiheit in Baden-Württemberg. Zuvor war er unter anderem als Richter am Verwaltungsgericht Koblenz und als Wissenschaftlicher Mitarbeiter beim Bundesverfassungsgericht tätig. Von 2008 bis 2016 war er Leiter Privater Datenschutz beim LfDI Rheinland-Pfalz.

FS: Der EuGH hat im März 2023 eine Vorschrift im Hessischen Datenschutzgesetz, die fast inhaltsgleich mit unserem § 26 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist, als sehr kritisch und nicht vereinbar mit Europarecht eingestuft. Was ist dem EuGH da so übel aufgestoßen? Und was muss der Gesetzgeber nun unternehmen, um das wieder glatt zu bügeln?

SB: Da muss er einiges tun. Artikel 88 Abs. 1 DSGVO besagt, ihr könnt den Bereich Beschäftigtendatenschutz national regeln, aber ihr müsst es spezifischer tun. Und da war der § 26 Abs. 1 BDSG jedenfalls in seiner etwas schlichten Einfalt mit Sicherheit dem Europäischen Gerichtshof nicht genug. Genauso wie das Hessische Datenschutzgesetz letztlich nichts geregelt hat außer dem Erforderlichkeitsprinzip. Aber wir brauchen die nationale Regelung nicht, um so eine Norm aus der DSGVO zu wiederholen. Das war die eine Kritik.

Die zweite Kritik ergibt sich aus Artikel 88 Abs. 2 DSGVO. Danach müssen nämlich immer dann, wenn national Beschäftigtendatenschutz geregelt wird, besondere Schutzvorschriften vorgesehen werden. Und auch da ist der Europäische Gerichtshof nicht fündig geworden.

FS: Ein Referentenentwurf für ein neues Beschäftigtendatenschutzgesetz ist in der Mache und soll dieses Jahr noch kommen. Wie ist deine Einschätzung, nachdem wir schon viele Anläufe genommen haben: Wie stehen die Chancen, dass dieser Anlauf nach mehreren Versuchen endlich von Erfolg gekrönt ist?

SB: Es sieht tatsächlich so aus, als hätte sich das Bundesarbeitsministerium, das ja federführend ist, mit dem Bundesinnenministerium geeinigt, sodass möglicherweise sogar noch in diesem Jahr die Ressorts-Anhörung beginnen kann. Aber das ist nur der erste Schritt. Spannend wird es dann endgültig, wenn er ins Parlament kommt. Die Koalition hat eine Menge Probleme. Ob sie sich dieses schwierige Thema „Beschäftigtendatenschutz" wirklich auflädt, wenn absehbar ist, dass es auch innerhalb der Koalition erhebliche Differenzen gibt – das werden wir sehen.

FS: Spielen wir „Wünsch dir was". Wenn du jetzt konkret damit beauftragt werden würdest, ein Eckpunktepapier zu erstellen zum neuen Beschäftigtendatenschutzgesetz, was wäre darin enthalten?

SB: Natürlich gibt es ein paar Punkte, die aus meiner Sicht unbedingt rein müssten in so ein Beschäftigtendatenschutzgesetz. Ich glaube zum Beispiel, dass das Thema Screening am Arbeitsplatz ganz dringend reguliert werden müsste. Da passiert in der Praxis sehr viel, was falsch ist, wo auch zu stark in die Beschäftigtenrechte eingegriffen wird und der Arbeitgeber nicht wirklich eine Rechtsgrundlage hat.

Ich würde darüber hinaus die Transparenzanforderung der DSGVO in den Vordergrund stellen und alle heimlichen Überwachungsmaßnahmen des Arbeitgebers, auch wenn sie im Moment vom Bundesarbeitsgericht noch für zulässig erachtet werden, verbieten. Ich glaube, die DSGVO lässt solche intransparenten Überwachungsmaßnahmen überhaupt nicht zu. Und schließlich würde ich insbesondere im Bewerbungskontext klarer regeln, was der Arbeitgeber an Informationen über den Bewerber einsammeln darf. Stichwort: Nutzung von Social Media. Wie stark darf er dem Bewerber hinterher ermitteln? Ich glaube, da brauchen wir dringend klare gesetzliche Vorgaben.

Dr. Frank Schemmel und
Dr. Stefan Brink

§ 26 Abs. 1 BDSG: Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Das Interview erscheint in voller Länge am 25. April 2024 in der Mai-Ausgabe des Compliance-Beraters (CB 5/2024). Dort tauschen sich Dr. Stefan Brink und Dr. Frank Schemmel außerdem aus zu den Themen: Datenschutz ist kein Tatenschutz, die datenschutzrechtliche Einwilligung im Arbeitskontext sowie Betriebsrat und Datenschutz.

Die EU-DSGVO gleich Schweizer DSG – oder etwa doch nicht?

Das revidierte Schweizer DSG ist am 1. September 2023 in Kraft getreten. Getrieben durch den technischen Fortschritt war das Gesetz zum einen ziemlich in die Jahre gekommen, zum anderen war das neue Datenschutzniveau, das die DSGVO mit sich gebracht hat, ein weiterer treibender Faktor für die Überarbeitung. Grundsätzlich lässt sich sagen, dass das Schweizer DSG und die DSGVO wohl gute Freunde sind – dennoch gibt es Unterschiede und diese werden im nachfolgenden Beitrag näher betrachtet.

Das Schweizer DSG: Eine Annäherung an die europäischen Regeln war unvermeidlich, dennoch sind die Unterschiede erheblich.

Das Schweizer Bundesgesetz über den Datenschutz (DSG) gilt für private Verantwortliche sowie Bundesorgane. Die revidierte Version hat zwischenzeitlich auch den ersehnten Angemessenheitsbeschluss seitens der EU im Januar 2024 erhalten. Die jeweiligen Kantonalen Datenschutzgesetze, die für die öffentlichen Organe der Kantone und der Gemeinden eine Anwendung finden, ziehen ebenfalls nach und befinden sich derzeit größtenteils noch in der Revision. Wer jetzt jedoch davon ausgeht, dass das Schweizer DSG nur eine Kopie der DSGVO oder allenfalls die „kleine Schwester" ist, irrt. In vielen Bereichen erfolgte zwar eine Annäherung an die DSGVO, jedoch sind die grundlegenden Prinzipien unterschiedlich. Während die DSGVO dem Leitsatz folgt „alles ist verboten, außer es ist erlaubt", hat das Schweizer DSG einen anderen, pragmatischeren Blick auf die Dinge und folgt dem Ansatz „grundsätzlich ist alles erlaubt, außer es ist verboten". Die wichtigsten Unterschiede werden nachfolgend erläutert, wobei diese nicht abschließend sind.

Ein großer Unterschied besteht bei den Sanktionen – in deren Höhe sowie beim Adressaten. Das neue Schweizer DSG hat die Bußen sowie die strafbewehrten Tatbestände deutlich ausgebaut, sodass nun Bußen von bis zu 250.000 CHF für private Verantwortliche möglich sind (früher max. 10.000 CHF). Nach dem aktuellen Meinungsstand richtet sich die Buße direkt gegen die handelnden Personen, also das Management, und sind auch nicht versicherbar. Die DSGVO hingegen sieht Bußen bis zu 20 Mio. EU oder 4 % des weltweiten Gesamtjahresumsatzes des Unternehmens vor und richtet diese direkt an die Organisation.

Einigkeit zwischen den beiden gesetzlichen Grundlagen besteht hingegen beim Thema Datenschutzverletzungen, also dass ein sog. „Data Breach" gemeldet werden muss. Jedoch werden die Frist und der Meldungsempfänger unterschiedlich definiert. Die DSGVO sieht eine strikte Frist vor, d.h. die Meldungen müssen innerhalb von 72 Stunden erfolgen, und zwar an die jeweilige zuständige EU-Aufsichtsbehörde. Die Schweiz lässt die Leine etwas länger und schreibt vor, dass die Meldung schnellstmöglich erfolgen muss, und zwar an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB).

Einen weiteren Unterschied gibt es beim Datenschutzbeauftragten: Gemäß der DSGVO ist die Bestellung unter der Erfüllung bestimmter Voraussetzungen eine Pflicht. Das Schweizer DSG nimmt eine Unterscheidung vor – private Verantwortliche können freiwillig entscheiden, ob sie einen Datenschutzbeauftragten einsetzen wollen, während diese bei Bundesorganen obligatorisch sind und gewisse fachliche Anforderungen erfüllen müssen. Um die beratende Rolle, die der Datenschutzbeauftragte einnimmt, zu unterstreichen, ist mit der Revision des Schweizer DSG der Fachbegriff auf „Datenschutzberater" angepasst wurden.

Auch bei der Datenübermittlung ins Ausland bestehen Unterschiede. Dabei unterscheidet das Schweizer DSG zwischen den regulierten Drittländern, d.h. diejenigen die über ein angemessenes Datenschutzniveau aus Schweizer Sicht verfügen und den unregulierten Drittländern, welche die Datenschutzanforderungen nicht erfüllen. Die Entscheidungshoheit über diese Klassifizierung hat neu der Bundesrat. Die regulierten Drittländer sind im Anhang 1 der Verordnung über den Datenschutz abschliessend aufgezählt (sog. „Länderliste"). Bei der DSGVO entscheidet die Europäische Kommission. Werden Daten in unregulierte Drittländer übertragen sind die Standardvertragsklauseln der EU einzusetzen. Dies gilt im Wesentlichen auch für die Schweiz, da der EDÖB die Standardvertragsklauseln anerkannt hat, jedoch müssen diese noch um das sog. „Swiss Finish" ergänzt werden, damit diese ihre Wirkung entfalten.

Auch bei der Datenschutzerklärung gibt es Unterschiede. Grundsätzlich entspricht das Transparenzgebot des DSG in seinen Zielsetzungen dem der DSGVO, jedoch ist es in der Schweiz weniger im Detail geregelt. Somit können bestehende Datenschutzerklärungen, die gemäß der DSGVO erstellt wurden, genutzt werden. Sie müssen jedoch noch um die jeweiligen Länder, in die Personendaten exportiert werden, sowie um die Angabe, auf welcher Grundlage der Export in einen unregulierten Drittstatt erfolgt, ergänzt werden. Hier ist es wichtig im Hinterkopf zu haben, dass die jeweiligen Länderlisten der DSGVO und des Schweizer DSG nicht deckungsgleich sind. Insoweit steckt auch beim Thema Datenschutz der Teufel häufig im Detail.

Anja Schmitz

Anja Schmitz ist Juristin und Senior Consultant sowie Partner der Projektas GmbH mit Sitz in Zug/Schweiz. Sie ist spezialisiert auf die Themen Corporate Governance, Compliance und Datenschutz sowie dem Business Continuity Management. Ein Schwerpunkt ihrer Arbeit liegt in der Projektleitung, der praktischen Umsetzung von rechtlichen Anforderungen und der Management-Beratung.

10. Hanseatischer Compliance Tag

Mittwoch, 29. Mai 2024 | 13:00 – 18:00 | Handelskammer Hamburg

11:00 Uhr	**Mitgliederversammlung Pro Honore e.V.** (nur für Mitglieder)
12:00 Uhr	**Imbiss & Erfrischung**
13:00 Uhr	**Eintreffen und Registrierung** der Tagungsteilnehmer
13:30 Uhr	**Begrüßung** **Christian Graf** | Leiter Recht Handelskammer Hamburg **Dr. Malte Passarge** | Geschäftsführer Pro Honore e.V. | Hamburg
13:45 Uhr	**Key Note: Zur Bedeutung der Zeitenwende und aktuellen Bedrohungslage für die Wirtschaft** **Kapitän zur See Michael Giss** Kommandeur des Landeskommandos | Hamburg
14:15 Uhr	**Aktuelle Compliance-Herausforderungen für KMU** **Rechtsanwalt Dr. Malte Passarge |** Partner Huth Dietrich Hahn | Hamburg
15:00 Uhr	**Zertifizierung von CMS nach dem Hamburger Compliance Zertifikat** **Prof. Dr. Stefan Behringer** | HSLU | Luzern
Anschließend	**Diskussion**
16:00 Uhr	**Kaffeepause**
16:30 Uhr	**Aktuelle normative Fragen zu KI** **Prof. Dr. Peter G. Kirchschläger** | Institut für Sozialethik | Universität Luzern
17:15 Uhr	**Aktuelle Bedrohungslage in der IT-Security** **André Knieper** | Manager Security Advisory avodaq AG | Hamburg
Anschließend	**Diskussion**
18.00 Uhr	**Ende und Ausklang** bei Wein und Gebäck






Speisen, Getränke, Dokumentation und Teilnahmezertifikat sind im Tagungspreis enthalten (**280,- € zzgl. 19,60 € MwSt.**)
Mitglieder von PRO HONORE e.V. zahlen den halben Preis. Wir bitten um Anmeldung per **Fax** an **040 41525-111**,
per **E-Mail** an **info@pro-honore.de** oder
online unter **https://www.pro-honore.de/leistungen/hanseatischer-compliance-tag**.

Veranstalter: PRO HONORE
Medienpartner: Compliance Berater
Förderer: HK Hamburg, Creditreform, HUTH DIETRICH HAHN

www.hanseatischer-compliance-tag.de

EU-Kommission überprüft Einhaltung des Digital Services Act

Die EU-Kommission überprüft, ob Plattformen und Suchmaschinen das Gesetz über Digitale Dienste (DSA) einhalten. Betroffen sind AliExpress, Bing, Google Search, Facebook, Instagram, Snapchat, TikTok, YouTube und X.

© IMAGO / NurPhoto

EU-Kommission macht mit dem Digital Services Act ernst: Nicht nur TikTok, YouTube und X müssen danach Auskunft geben.

Gegen AliExpress hat die Kommission ein förmliches Verfahren eingeleitet. Es wird geprüft, ob AliExpress gegen das Gesetz über digitale Dienstleistungen (DSA) verstoßen hat. Es geht um mehrere Bereiche, die mit dem Management und der Minderung von Risiken, der Moderation von Inhalten und dem internen Mechanismus zur Bearbeitung von Beschwerden, der Transparenz von Werbung und Empfehlungssystemen, der Rückverfolgbarkeit von Händlern und dem Datenzugang für Forscher zusammenhängen.

In einem förmlichen Auskunftsersuchen soll LinkedIn nähere Angaben darüber geben, wie der Dienst das Verbot einhält, Werbung auf der Grundlage von Profiling unter Verwendung besonderer Kategorien personenbezogener Daten zu präsentieren. LinkedIn muss außerdem informieren, wie es sicherstellt, dass seinen Nutzern alle erforderlichen Transparenzanforderungen für Anzeigen zur Verfügung gestellt werden.

Die Kommission hat im Rahmen des DSA förmliche Auskunftsersuchen an Bing und Google Search (Sehr große Online-Suchmaschinen, Very Large Online Search Engines, VLOSE) sowie an Facebook, Instagram, Snapchat, TikTok, YouTube und X (Sehr große Online-Plattformen, Very Large Online Platforms, VLOP) gerichtet. Die Kommission fordert diese Dienste auf, mehr Informationen über ihre jeweiligen Maßnahmen zur Eindämmung von Risiken vorzulegen: Hier geht es z.B. um so genannte „Halluzinationen", bei denen KI falsche Informationen liefert, um die virale Verbreitung von Deepfakes sowie die automatische Manipulation von Diensten, die Wähler in die Irre führen kann.

Die Kommission fordert außerdem Informationen und interne Dokumente zu den Risikobewertungen und Maßnahmen zur Risikominderung. Hier geht es um Auswirkungen generativer KI auf Wahlprozesse, die Verbreitung illegaler Inhalte, den Schutz der Grundrechte, geschlechtsspezifische Gewalt, den Schutz von Minderjährigen, das psychische Wohlbefinden, den Schutz personenbezogener Daten, den Verbraucherschutz und das geistige Eigentum. Die Fragen beziehen sich sowohl auf die Verbreitung als auch auf die Erstellung von generativen KI-Inhalten. *chk*

EU-Kommission zum Schutz vor Fälschungen

Die Europäische Kommission hat eine Toolbox zur Bekämpfung von Produkt- und Markenpiraterie angenommen. Die Empfehlung der Kommission bezieht sich darauf, wie Nachahmungen sowohl offline als auch online bekämpft und das Recht am geistigen Eigentum besser geschützt werden können.

© IMAGO / Manngold

Fälschungen: Längst nicht mehr nur ein Thema bei Straßenverkäufen.

Zu den vorgeschlagenen Maßnahmen gehören unter anderem:
– Benennung einer zentralen Kontaktstelle für Fragen der Durchsetzung von Rechten des geistigen Eigentums und Ausweitung der Nutzung bestehender Instrumente wie des vom Amt der **Europäischen Union für geistiges Eigentum** (EUIPO) bereitgestellten Portals für die Durchsetzung von Rechten des geistigen Eigentums.
– Ermutigung der Unterzeichner der **Vereinbarung über den Verkauf nachgeahmter Waren** im Internet, den Status eines „vertrauenswürdigen Hinweisgebers" im Rahmen des Gesetzes über digitale Dienste (DSA) anzustreben und so sicherzustellen, dass ihnen bei der Übermittlung von Meldungen illegaler Inhalte Vorrang eingeräumt wird.
– Anpassung der Verfahren zur Bekämpfung neuer Fälschungspraktiken, Behandlung von Themen wie Spiegelwebsites mit dynamischen Unterlassungsklagen, Optimierung des Informationsaustauschs in Gerichtsverfahren und Gewährleistung eines angemessenen Schadensersatzes, einschließlich materieller und immaterieller Schäden.
– Förderung der alternativen Streitbeilegung für alle Streitigkeiten im Bereich des geistigen Eigentums, die eine kostengünstige und effiziente Option bietet, insbesondere für grenzüberschreitende Streitigkeiten und KMU.
– Neubewertung und mögliche Anhebung der Höchststrafen für schwere Straftaten im Bereich des geistigen Eigentums.
– Entwicklung von Verfahren zur schnelleren, kostengünstigeren und umweltfreundlicheren Lagerung und Entsorgung von Fälschungen.
– Integration von Inhalten des geistigen Eigentums in die nationalen Ausbildungspläne, insbesondere für Strafverfolgungs- und Wirtschaftsstudien.
– Im Rahmen des KMU-Fonds, werden die Kosten erstattet, die KMU entstanden sind, die sich bei der Durchsetzung ihrer Rechte im Falle einer Verletzung von Rechten des geistigen Eigentums oder bei der Vermeidung der Verletzung von Rechten des geistigen Eigentums durch Sachverständige beraten lassen.
– Die Kommission wird in enger Zusammenarbeit mit der Industrie und den Mitgliedstaaten eine Checkliste mit Leitlinien dazu entwickeln, wie KMU KI nutzen können, ohne ihre immateriellen Vermögenswerte zu gefährden.

Im Jahr 2019 machten nachgeahmte Produkte fast 6 Prozent aller EU-Einfuhren aus und erreichten einen Wert von 119 Mrd. Euro, was zu einem geschätzten Verlust von 670.000 direkten Arbeitsplätzen und 15 Mrd. Euro an Steuereinnahmen führte.

chk

Neue EU-Verbraucherschutz-Regeln in Kraft

Am 27. März 2024 sind die neuen EU-Verbrauchervorschriften in Kraft getreten. Verbraucher sollen dadurch besser über die Lebensdauer und die Reparierbarkeit von Produkten informiert und vor Greenwashing geschützt werden. Die Mitgliedstaaten sind verpflichtet, die Richtlinie bis zum 27. März 2026 in nationales Recht umzusetzen.

Die neuen Regeln richten sich gegen Praktiken wie irreführende „Grünfärberei" oder falsche Aussagen über Produkte, deren Haltbarkeit nicht den Erwartungen entspricht. Es wird ein harmonisiertes Etikett mit Informationen über die gewerbliche Haltbarkeitsgarantie der Hersteller eingeführt, das auch einen Verweis auf das gesetzliche Gewährleistungsrecht enthält. Außerdem werden vage Umweltaussagen verboten. Das bedeutet: Unternehmen können nicht mehr behaupten, dass sie „grün" oder „umweltfreundlich" sind, wenn sie nicht nachweisen können, dass sie es wirklich sind.

Die EU-Kommission hat die Richtlinie zur Stärkung der Verbraucher für den ökologischen Wandel am 30. März 2022 vorgeschlagen. Sie ist Teil eines Pakets von vier Vorschlägen, zusammen mit dem Vorschlag für eine Ökodesign-Verordnung und den Richtlinienvorschlägen zu Umweltaussagen und zur Förderung der Reparatur von Waren (Recht auf Reparatur).

chk

FASHION LAW 2024

1. Deutscher Moderechtstag

Dienstag, 7. Mai 2024 – Berlin

9:00 Uhr **Begrüßung & Einführung**
Torsten Kutschke, Gesamtverlagsleiter Recht und Wirtschaft,
RA Fabian Reinholz, HÄRTING Rechtsanwälte,
Ulrike Wollenschläger, Chefin vom Dienst Business TextilWirtschaft

9:30 Uhr **Die deutsche Textil- und Modeindustrie: ESG-Transformation & regulatorische Herausforderungen**
RA Batzorig Daarten, Leiter Recht und Steuern, Gesamtverband textil+mode
Anne Göbel, Leitung CSR, Gesamtverband textil+mode

10:15 Uhr **Green Claims in der Fashionwelt – Werbung mit klimaneutraler Mode und Greenwashing als Haftungsfall**
RA Svyatoslav Gladkov, HÄRTING Rechtsanwälte

11:00 Uhr **Kaffeepause**

11:15 Uhr **Aktuelle Entwicklungen im Bereich LkSG und Sorgfaltspflichten**
RA Dr. Jens Nusser, LL.M., Franßen & Nusser Rechtsanwälte

12:00 Uhr **Traumjob Mode-Influencerin – berufliche und rechtliche Herausforderungen**
RA Kerem Bakir, HÄRTING Rechtsanwälte
Tessa Saueressig, .comTessa
Bekannte Influencerin aus der Modewelt

12:45 Uhr **Mittagspause**

13:45 Uhr **Fashion x Corporate – Labelgründung, Finanzierung und Collaborations**
RAin Dorothea Wentz, HÄRTING Rechtsanwälte

14:30 Uhr **Insolvenz und Sanierung im Fashionbusiness – Scheitern oder Chance?**
RA Dr. Christoph Weber, BBL Brockdorff Rechtsanwälte

15:15 Uhr **Kaffeepause**

15:30 Uhr **AI in Fashion**
Julia Holterhus, Legal Counsel Marketing, Creative and Media Law, Zalando

16:15 Uhr **Mode in der Zukunft – Digital Fashion, Virtual Try On & Metaverse-Couture**
RAin Leonore Hilchenbach & RAin Inga Sievers, HÄRTING Rechtsanwälte

17:00 Uhr **Podiumsdiskussion unter Einbeziehung des Publikums**
Themenfestlegung kurzfristig nach Aktualität

17:30 Uhr **Zusammenfassung und Ausblick**

ab 17:45 Uhr **Get-together und Ausklang bei Drinks & Canapés**


Torsten Kutschke


RA Fabian Reinholz


Ulrike Wollenschläger


RA Batzorig Daarten


Anne Göbel


RA Svyatoslav Gladkov


RA Dr. Jens Nusser

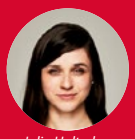

RA Kerem Bakir


Tessa Saueressig


Bekannte Influencerin aus der Modewelt


RAin Dorothea Wentz


RA Dr. Christoph Weber


Julia Holterhus


RAin Leonore Hilchenbach


RAin Inga Sievers

Veranstaltungsort
HÄRTING Rechtsanwälte
Chausseestraße 13, 10115 Berlin

Melden Sie sich jetzt an! www.ruw.de/fashion-law

Weitere Informationen und Anmeldung:
Frau Lena Wehrmann
Deutscher Fachverlag GmbH
Telefon: 069/7595-2784
E-Mail: Lena.Wehrmann@dfv.de

Teilnahmegebühr:
499,- € für Abonnenten der TextilWirtschaft und aller R&W-Titel
599,- € regulärer Preis

Eine Veranstaltung von:
R&W Fachmedien Recht und Wirtschaft
HÄRTING
TextilWirtschaft

Mit freundlicher Unterstützung von:
esystems