Compliance
Die Zeitschrift für Compliance-Verantwortliche

Juli/August 2023

Inhalt

© IMAGO / Panthermedia

Aufmacher

Habemus Hinweisgeberschutzgesetz!
In diesen Tagen ist das Hinweisgeberschutzgesetz in Kraft getreten. Ein Regelwerk dessen es mit Blick auf die Einrichtung von Meldestellen „rein rechtlich" nicht unbedingt bedurft hätte. Der Repressionsschutz für gutmeinende hinweisgebende Personen, sei hingegen zweifellos nötig, schreibt Dr. André-M. Szesny in unserem Aufmacher. Nun gilt es mit dem lang diskutierten Gesetz umzugehen, denn „die ‚richtige' Arbeit fängt mit dem Eingang der Meldungen an".

Praxis

© IMAGO / Ikon Images

Ist es noch Compliance oder schon Security? – Überlappungen im Ethical & Criminal Risk Management
Anhand eines realen Praxisfalls eines mittelständischen Unternehmens werden thematische Überlappungen im Ethical & Criminal Risk Management aufgezeigt.

Recht

© Pixabay

Kein grundsätzliches Verwertungsverbot bei offener, nicht datenschutzkonformer Videoüberwachung
Das Bundesarbeitsgericht hat entschieden: In einem Kündigungsschutzprozess besteht grundsätzlich kein Verwertungsverbot in Bezug auf solche Aufzeichnungen aus einer offenen Videoüberwachung, die vorsätzlich vertragswidriges Verhalten des Arbeitnehmers belegen sollen.

Recht

© IMAGO / agefotostock

Der EU Data Act kommt
Der EU Data Act hat Ende Juni die letzte Hürde im EU-Gesetzgebungsverfahren genommen.

Veranstaltungen

15.09.2023 | Frankfurt am Main oder Online | **9. Deutscher Glücksspielrechtstag**

27. – 29.09.2023 | Düsseldorf oder Online | **Datenschutzkonferenz**

12.10.2023 | Frankfurt am Main | **Jahrestagung Logistik & Recht**

17.10.2023 | Frankfurt am Main | **Jahrestagung Geldwäsche und Recht**

10.11. & 23.11. 2023 | Webinar & Frankfurt am Main | **Praxisseminar zur CSRD-Berichterstattung: Nicht-finanzielles Reporting optimal umsetzen**

Habemus Hinweisgeberschutzgesetz!

In diesen Tagen ist das Hinweisgeberschutzgesetz in Kraft getreten. Ein Regelwerk dessen es mit Blick auf die Einrichtung von Meldestellen „rein rechtlich" nicht unbedingt bedurft hätte. Der Repressionsschutz für gutmeinende hinweisgebende Personen, sei hingegen zweifellos nötig, schreibt Dr. André-M. Szesny in unserem Aufmacher. Nun gilt es mit dem lang diskutierten Gesetz umzugehen, denn „die ‚richtige' Arbeit fängt mit dem Eingang der Meldungen an".

Whistleblowing ist kein leichter Schritt: Es liegt darum auch in der Hand der Unternehmen, ihre Beschäftigten zu ermutigen, Meldungen über Compliance-Verstöße intern abzugeben.

Was verbinden Sie mit Whistleblower-Hotlines? Denunziantentum und falsche Verdächtigungen? Böswillige Falschmeldungen und Angriffe feiger, weil anonymer Verbalheckenschützen? Ungerechtfertigte Verdächtigungen und blinden Verfolgungseifer? Schäden für das Vertrauen innerhalb der Belegschaft – keiner traut keinem mehr?

Sie haben Recht – diese Gefahren bestehen. Sie bestehen aber stets, völlig unabhängig davon, ob Sie in Ihrem Unternehmen eine Whistleblower-Hotline einrichten oder nicht. Denn Whistleblower suchen sich ihren Weg und wenden sich mit ihrem Anliegen an Vorgesetzte oder den Betriebsrat, und wenn das nichts nützt, an Behörden oder die Öffentlichkeit. Es liegt in Ihrer Hand, Ihre Beschäftigten zu ermutigen, Meldungen über Compliance-Verstöße oder auch nur einen Verdacht intern abzugeben, entsprechende Kanäle zu schaffen und sich damit in die Lage zu versetzen, selbst einzugreifen, wo es Not tut.

Anfang Juli tritt – EU-initiiert – ein Gesetz in Kraft, das öffentliche und private Beschäftigungsgeber verpflichtet, interne Meldestellen einzurichten. Ein langes, politisch motiviertes Hin und Her in Bundestag und Bundesrat mit abstrusen Argumenten gegen einzelne Vorschriften des Gesetzes aus der Ecke der Opposition und verfassungsrechtlich zweifelhaften Volten der Regierungsfraktionen führt nun endlich zu einer gesetzlichen Regelung über die Ausgestaltung des Schutzes nicht nur von hinweisgebenden Personen, sondern auch von Verdächtigten. Habemus Hinweisgeberschutzgesetz!

Dr. André-M. Szesny, LL. M., ist Partner bei Heuking Kühn Lüer Wojtek in Düsseldorf. Zu seinen Beratungsschwerpunkten zählen Wirtschafts- und Steuerstrafrecht, Compliance und Interne Ermittlungen. Er ist Co-Sprecher des Arbeitskreises Kapitalmarktstrafrecht der Wirtschaftsstrafrechtlichen Vereinigung e. V., hat einen Lehrauftrag an der Universität Liechtenstein (Wirtschaftsstrafrecht) und ist Autor zahlreicher Veröffentlichungen zum Wirtschaftsstrafrecht.

An der Legitimation interner Meldestellen, wie das HinSchG sie jetzt gesetzlich vorschreibt, besteht kein Zweifel – meines Erachtens hätte es rein rechtlich eines besonderen Gesetzes insoweit nicht bedurft. Es gibt die dunklen Ecken in jeder Organisation, in Unternehmen, in Behörden, in Vereinen und Verbänden, in die keiner schaut, in denen sich Dreck ansammelt und Schimmel und wo sich unbeobachtet wähnende schwarze Schafe wohlfühlen. Die Schäden für Arbeitgeber, für Beschäftigte, für Kunden, für Lieferanten und für Wettbewerber durch Betrug, Veruntreuung, Mobbing, sexuelle Nötigung, Korruption, Kartelle, Steuerhinterziehung können immens sein. Organisationen, die es zulassen und fördern, dass ihre Beschäftigten ohne Angst über Straftaten oder andere schwere Verstöße oder auch nur über einen entsprechenden Verdacht berichten dürfen, haben die Möglichkeit, frühzeitig einzugreifen und tiefergehende Schädigungen zu vermeiden. Oftmals befürchtete „Meldeschwemmen" habe ich bislang nicht erlebt. Unterlassen Unternehmensleiter es hingegen, Meldungen nachzugehen oder verhindern sie sie sogar, verletzen sie ihre Legalitäts- und ihre Aufsichtspflichten und verantworten die deshalb entstehenden Vertiefungsschäden mit. Und die damit einhergehenden Reputationsverluste.

Deshalb ist es gut, dass das HinSchG – und dafür ist das Gesetz zweifellos nötig – gutmeinende hinweisgebende Personen einem Repressionsschutz unterstellt.

Eine Meldestelle ist schnell eingerichtet. Fragen wie die Zulässigkeit anonymer Meldungen, die Möglichkeit gemeinsame, gegebenenfalls gruppenweit zentrale Meldestellen einzurichten, die datenschutz- und kollektivarbeitsrechtlichen Aspekte – all das ist Technik, dafür sind Juristen da. Mit der Einrichtung der Meldestelle werden bereits wichtige Signale gesetzt. Ein webbasiertes Formular reicht rechtlich aus, und in der Tat schreiben manche hinweisgebenden Personen lieber online, als dass sie sprechen. Doch manch ein Whistleblower möchte erst einmal „reden", um einschätzen zu können, was da eigentlich passiert mit der eigenen Meldung. Welche Meldekanäle zu welchem Unternehmen passen, ist eine strategische, unternehmenskulturelle Frage, die individuell zu beantworten ist.

Doch die „richtige" Arbeit fängt mit dem Eingang der Meldungen an. Das Vertrauen der Belegschaft in ein Hinweisgebersystem verlangt den verantwortungsvollen, sensiblen und fachkundigen Umgang mit Verdachtsmeldungen.

Vorverurteilung und Verfolgungseifer sind fehl am Platze. Auch Bagatellisierung und Gleichgültigkeit sind ein „no go". Unvoreingenommenheit, Vertraulichkeit, Objektivität und Unabhängigkeit sind das Gebot der Stunde – jetzt erst recht, nachdem zum 2. Juli in Stein gemeißelt ist, dass Beschäftigungsgeber Meldestellen haben müssen.

Dr. André-M. Szesny

Ist es noch Compliance oder schon Security? – Überlappungen im Ethical & Criminal Risk Management

Mit dem im Folgenden dargestellten realen Praxisfall eines mittelständischen Unternehmens werden thematische Überlappungen im Ethical & Criminal Risk Management aufgezeigt. Unternehmen sollten diese Überschneidungen für sich benennen und herausarbeiten, wer im konkreten Fall zuständig wäre bzw. das Know-How hätte, den unterschiedlichen Herausforderungen zu begegnen.

Kriminelle Machenschaften können vielfältig sein: Wie genau Unternehmen auf solche Vorgänge reagieren, sollte auch mit Blick auf mögliche Überschneidungen zwischen Compliance und Security bewertet werden.

Aufgrund ignorierter Überlappungen, nicht definierter Schnittstellen und mangelnder interner Kommunikation verfestigt sich in den Abteilungen Compliance und Corporate Security oftmals ein ausgeprägtes Silodenken. In der Konsequenz strengt dann beispielsweise Compliance eine Ermittlung an, ohne über das fachliche Ermittlungs-Know-How zu verfügen. Das, obwohl in der Sicherheitsabteilung evtl. ehemalige Zielfahnder der Polizei arbeiten. Oder Corporate Security erhält im Rahmen eines eigenen Security Audits Kenntnis von vorsätzlichen Sanktionsverletzungen und Menschenrechtsverstößen an einem ausländischen Standort, meldet diese jedoch nicht dem Compliance-Manager.

Dabei zeigen sich schon im Vergleich der ISO 37301 Richtlinie und der Leitfäden/Standards 2000-1 und 2000-2 zum Wirtschaftsgrundschutz deutliche thematische Überschneidungen zwischen Compliance und Unternehmenssicherheit. Konkret und aus der Praxis lassen sich folgende Überlappungen in Aufgaben und Kompetenzen identifizieren:

- Non-compliance Investigations
- Förderung sozialer und ethischer Werte
- Verhinderung von Straftaten
- Korruptionsprävention
- Terrorismus-Bekämpfung
- Geldwäscheprävention
- Anti-Fraud
- Bekämpfung von Wirtschaftskriminalität
- Informationsschutz

Zum konkreten Fall: An einem europäischen Standort eines Kunden konnte sich ein komplexes kriminelles Biotop mit einem monatlichen Schadensvolumen von ca. 40.000 EUR verfestigen, da Hinweisen von Whistleblowern nur mit großer zeitlicher Verzögerung nachgegangen wurde. Gemäß den Hinweisen verschiedener Whistleblower und den daraufhin angestrengten Ermittlungen, die auch technische Maßnahmen und mobile Observationen einschlossen, hatte sich innerhalb des Standorts ein komplexes und arbeitsteiliges System krimineller Machenschaften etabliert, das bis hinein in die deutsche Unternehmenszentrale reichte. An der Spitze dieser als organisierte Kriminalität zu bezeichnenden Struktur stand ein lokaler Angestellter, der zusammen mit weiteren internen und externen Komplizen eine parallele Logistikkette mit gestohlenen Roh- und Fertigwaren aufgebaut hatte.

De facto waren so die Integrität des Standorts und ein rechtskonformer Unternehmensbetrieb nicht länger gewährleistet und der Fall einer strafrechtlichen Managementhaftung bereits eingetreten. Der langfristig angelegte und organisierte Diebstahl aus dem Unternehmensareal entlang der Logistikkette wurde überdies noch durch ein nahezu filmreifes Potpourri an weiteren Straftaten flankiert. Diese beinhalteten unter anderem

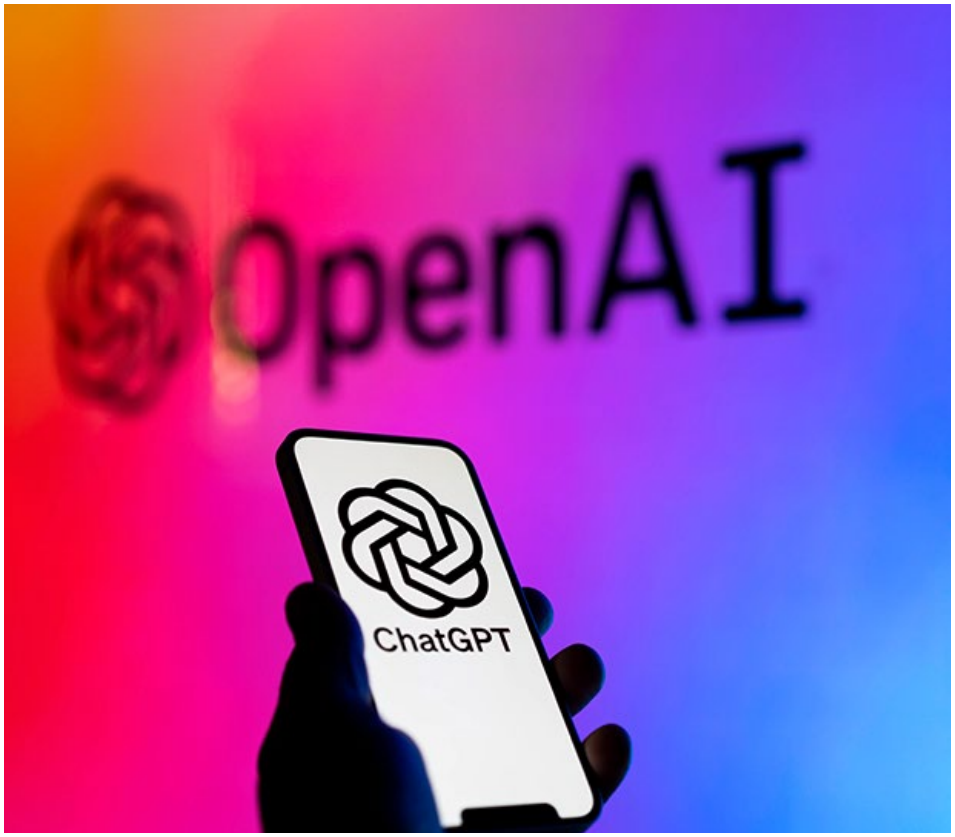
- die Vereinnahmung und Instrumentalisierung der gewerkschaftlichen Vertretung mit dem Ziel, das Management zu demotivieren,
- die Gewährung/Annahme von Vergünstigungen zulasten des Unternehmens. Gabelstapelfahrer, Lagerarbeiter, LKW-Fahrer, Mitarbeiter des externen Werkschutzes und der deutsche Logistikverantwortliche wurden regelmäßig mit Alkohol, Bargeld, Potenzmitteln und sogar Prostituierten bestochen,
- das Betreiben einer aus den Diebesgutverkäufen gespeisten „schwarzen Kasse" zwecks privater Bereicherung und Bestechungen,
- die Bedrohung des Standortmanagers mit physischer Gewalt,
- die gezielte Demotivation oder Erpressung von neu eingestellten Mitarbeitern, die nicht gewillt waren, die kriminellen Machenschaften zu decken,
- Ausschreibungsbetrug, um von nahen Verwandten betriebene Speditionen zu ungünstigen Konditionen als Dienstleister unter Vertrag zu nehmen und gleichzeitig mehr Kontrolle über den Warendiebstahl zu erhalten,
- die Anzeige vorgeblicher (aber tatsächlich nicht existenter) Gesetzesverstöße in den Bereichen Arbeitsschutz und Brandschutz, um über behördliche Prüfungen das Management zu belasten sowie
- Falschbilanzierung, Verstöße gegen Buchhaltungspflichten, Tatverschleierung mit Rechnungsstornos und Geldwäsche.

Nachdem alle Modi Operandi und der Täterkreis aufgeklärt bzw. identifiziert waren, wurden nun im nächsten Schritt Ad-hoc-Maßnahmen zur kurzfristigen Eindämmung der Kriminalitätsbelastung am Standort ergriffen. Hierbei mussten eventuelle Gegenmaßnahmen der kriminellen Struktur antizipiert und in der Ausgestaltung und zeitlichen Abfolge der Maßnahmen berücksichtigt werden. Über die Implementierung transparenter Prozessvorgaben, Security Maßnahmen und Personalwechsel, konnte der Standort sukzessive wieder in einen rechtskonformen und sicheren Regelbetrieb überführt werden. *Lars D. Preußer*

Dipl.-Pol. Lars D. Preußer, CPP, CCTP ist Inhaber der Boutique-Unternehmensberatung Laurentium GmbH, Berlin und arbeitet seit 1999 weltweit als Sicherheitsberater im Ethical & Criminal Risks Management für internationale Großkonzerne. Er begleitet seine Kunden mit individuellen und diskreten Problemlösungen in den Bereichen Risk Analysis, Corporate Security Management, Asset Tracing & Recovery, Crisis Management, und Investigations.

Künstliche Intelligenz und Compliance

Künstliche Intelligenz (KI) kann eine große Hilfestellung sein – auch für Compliance. Genauso kann sie aber zum Problem werden – ebenfalls aus Compliance-Sicht. Einen ersten kurzen Überblick gibt Prof. Dr. Stefan Behringer in diesem Beitrag.



© IMAGO / NurPhoto

ChatGPT: Das neue Tool kann viel, verbreitet aber auch erschreckend viele Fehlinformationen.

Chat GPT, inzwischen in Version 4 verfügbar, ist seit Ende 2022 in aller Munde. Der einfache Zugang gibt allen Interessierten die Möglichkeit, auszuprobieren, was Künstliche Intelligenz zu leisten imstande ist – und eben auch nicht leisten kann. Es ist erstaunlich, was das neue Tool kann. Aber es ist auch erschreckend, wie viele Fehlinformationen durch Chat GPT verbreitet werden. Künstliche Intelligenz kommt eben doch an seine Grenzen.

Für viele Berufsfelder und Bereiche des täglichen Lebens hat diese neue Technologie enorme Wirkungen, die heute in ihrer ganzen Tragweite noch nicht zu überschauen sind. Auch für die Funktionen im Bereich Risk, Fraud und Compliance ergeben sich erhebliche Herausforderungen. Künstliche Intelligenz kann präventiv wirken, Kontrollen übernehmen oder Informationen liefern. So können Chatbots Compliance Help Desks übernehmen, zumindest für standardisierbare Abfragen. Das Problem wird sein, dass Aussagen, was eindeutig verboten und erlaubt ist, gut automatisierbar sind. Aber die Zwischentöne, wo es keine ganz eindeutigen Regeln gibt, werden nur schwer durch Chatbots zu übernehmen sein.

Überlegungen, dass Künstliche Intelligenz Entscheidungsvorschläge macht, die auch genutzt werden können, die Einhaltung der Business Judgement Rule zu belegen, gibt es in der wissenschaftlichen Literatur. Dabei gehen manche Wissenschaftler so weit, die Verwendung von Algorithmen verpflichtend zu machen, um eine neutrale Entscheidung zu belegen. Da die Künstliche Intelligenz Stereotypen in ihre Entscheidungen einbezieht, ist dieser Vorschlag sicherlich (noch) nicht umsetzbar, zeigt aber die mögliche Tragweite eines Einsatzes von Künstlicher Intelligenz auf. Ausserdem kann die KI Muster entwickeln, die auf eigentlich irrelevanten Kriterien beruhen. Auch dadurch können Fehlentscheidungen entstehen. Das Problem dabei: Der verwendete Algorithmus ist nicht transparent nachvollziehbar.

Neben den Chancen eines Einsatzes von Künstlicher Intelligenz im Compliance-Management selbst, wird das Vordringen von KI Compliance noch auf andere Weise beschäftigen: Die Regulierung von Künstlicher Intelligenz selbst muss eingehalten werden und Teil jedes Compliance-Managements werden. Auch hier warten viele Herausforderungen auf Compliance-Manager. Hier ist zu schauen, wie sich die Regulierung entwickelt. Lernende Systeme, wie sie KI darstellen, entwickeln in ihrer Einsatzzeit ständig neue Muster, wie sie Entscheidungen treffen. Welche Muster das sind, hängt im Wesentlichen von den Daten ab, mit der die Künstliche Intelligenz arbeitet. Dies wiederum liegt nicht mehr im Einflussbereich des Herstellers der KI, sondern in den Händen des Anwenders. Insofern ist die Verantwortung für das, was das Produkt macht, nicht eindeutig zuzuordnen.

Prof. Dr. Stefan Behringer

© Hochschule Luzern

Prof. Dr. Stefan Behringer ist Chefredakteur der ZRFC (Zeitschrift Risk, Fraud & Compliance) sowie Leiter des Kompetenzzentrums Controlling am Institut für Finanzdienstleistungen Zug IFZ der Hochschule Luzern.

Mehr dazu und zu weiteren aktuellen Compliance-Themen erfahren Sie auf der Integrity Europe Konferenz am 26./27. Oktober 2023 am Institut für Finanzdienstleistungen Zug IFZ der Hochschule Luzern. Die Konferenz richtet sich an Praktiker*innen in Führungsrollen sowie an anwendungsorientierte Forscher*innen, die sich mit strategischen und / oder operativen Fragestellungen aus dem Themenfeld Compliance, Risikomanagement, Integrität, ESG und Corporate Governance befassen. In der diesjährigen Konferenz gibt es u. a. Präsentationen und Workshops zu Themen wie Umgang mit Whistleblowing-Mechanismen, Standardisierung und Digitalisierung im Compliance-Management oder das Verhältnis von ESG- und Compliance-Funktionen im operativen Geschäft. Zu den Referenten gehören u.a. Dr. Regina Hörmanseder (Global Compliance Officer & Head of Compliance, Primetals Technologies), Prof. Dr. Peter Kirchschläger, (Leiter des Instituts für Sozialethik ISE, Universität Luzern), Prof. Dr. Bartosz Makovicz, (Europa Universität Viadrina, Frankfurt (Oder)) und Sandra Middel (Head of Group Compliance Clariant).

Weiterführende Informationen gibt es unter: https://www.hslu.ch/de-ch/wirtschaft/agenda/veranstaltungen/2023/10/26/integrity-europe-konferenz/.

Jahrestagung **Logistik & Recht**
Digitalisierung & Nachhaltigkeit im Fokus

12. Oktober 2023 | dfv Mediengruppe, Frankfurt am Main

10 % Frühbucherrabatt bei Anmeldung bis 14. Juli!

HIGHLIGHT: Verleihung des LogR-Awards für herausragende wissenschaftliche Arbeiten

DIE THEMEN:

- Digitalisierung der Supply Chain
- Digitalisierung von Ursprungszeugnissen und Carnets ATA/CPD
- Neue Entwicklungen in der Automatisierung und Fördertechnik
- Digitalisierung von Güterzugabfertigung und Gefahrstofftransporten durch SmartTrain
- Mit der Blockchain-Technologie zu nachhaltigen Supply Chains: Chancen, Herausforderungen und rechtliche Aspekte

DIE SPEAKER:


Torsten Kutschke


Dr. David Saive


Sophie M. Staron


Dr. Axel T. Schulte


Dr.-Ing. Maximilian Austerjost


Prof. Dr. Dagmar Gesmann-Nuissl


Dr. Malte Passarge


Andrea Wedig


Nadine Collier-Peters


Johanna Wegner


Christoph Mangelmans


Dr. Maximilian Dorndorf

Veranstaltungsort:

dfv Mediengruppe
Mainzer Landstr. 251
60326 Frankfurt am Main

Abonnieren lohnt sich!

Für 149,- EUR LogR-Jahresabo abschließen und 200,- EUR Teilnahmegebühr sparen!

Teilnahmegebühr (zzgl. MwSt.):

529,- EUR	LogR-Abonnent*innen & Behördenvertreter*innen
729,- EUR	Normalpreis

Rabatte – so sparen Sie intelligent:

Frühbucherrabatt 10 % bei Buchung bis zum 14. Juli 2023
Mehrbucherrabatt 5 % bei Anmeldung von 3 oder mehr Teilnehmer*innen einer Kanzlei/Institution/Behörde/Kammer ab der 3. Anmeldung

Registrierung:

Deutscher Fachverlag GmbH
Frau Maria Belz
Mainzer Landstraße 251
60326 Frankfurt am Main

Telefon: +49 69 7595–1157
Fax: +49 69 7595–1150
E-Mail: Maria.Belz@dfv.de

Anmeldeschluss:

11. Oktober 2023.
Eine frühzeitige Anmeldung wird empfohlen.

Stornierung:

Die Anmeldung ist übertragbar.
Bei Stornierung bis zum 14. September 2023 (Eingangsdatum) wird eine Bearbeitungsgebühr von 75,- EUR zzgl. MwSt. erhoben. Danach ist die volle Teilnahmegebühr zu entrichten.

Der Preis schließt Veranstaltungsunterlagen und die Pausenverpflegung mit ein.
Die Teilnahmegebühr bitten wir erst nach Erhalt der Rechnung zu überweisen.

Sie haben die LogR noch nicht im Abo?

- 4 Ausgaben
- 149,- EUR pro Jahr
- inkl. Zugang zur Online-Datenbank

JETZT BESTELLEN:

☐ Ich möchte die LogR im Abonnement beziehen. Bitte liefern Sie ab sofort.

Weitere Informationen unter: www.ruw.de/LogR

JETZT QR-CODE SCANNEN UND DIREKT ANMELDEN!

Weitere Informationen zur Tagung und zur Bewerbung für den LogR-Award unter www.ruw.de/jt-logr

dfv Mediengruppe

Deutscher Fachverlag GmbH · Maria Belz
Mainzer Landstr. 251 · 60326 Frankfurt am Main

Kein grundsätzliches Verwertungsverbot bei offener, nicht datenschutzkonformer Videoüberwachung

Das Bundesarbeitsgericht (BAG) hat mit Urteil vom 29. Juni 2023 (Az.: 2 AZR 296/22) entschieden: In einem Kündigungsschutzprozess besteht grundsätzlich kein Verwertungsverbot in Bezug auf solche Aufzeichnungen aus einer offenen Videoüberwachung, die vorsätzlich vertragswidriges Verhalten des Arbeitnehmers belegen sollen. Das gilt auch dann, wenn die Überwachungsmaßnahme des Arbeitgebers nicht vollständig im Einklang mit den Vorgaben des Datenschutzrechts steht.

© Pixabay

Nicht zu übersehende Videokamera: Was hier aufgezeichnet wird, darf zum Nachweis eines Arbeitszeitbetruges herangezogen werden.

Zum konkreten Fall: Der Kläger war bei der Beklagten zuletzt als Teamsprecher in der Gießerei beschäftigt. Die Beklagte wirft ihm unter anderem vor, am 2. Juni 2018 eine sogenannte Mehrarbeitsschicht in der Absicht nicht geleistet zu haben, sie gleichwohl vergütet zu bekommen. Nach seinem eigenen Vorbringen hat der Kläger zwar an diesem Tag zunächst das Werksgelände betreten. Die auf einen anonymen Hinweis hin erfolgte Auswertung der Aufzeichnungen einer durch ein Piktogramm ausgewiesenen und auch sonst nicht zu übersehenden Videokamera an einem Tor zum Werksgelände ergab nach dem Vortrag der Beklagten aber, dass der Kläger dieses noch vor Schichtbeginn wieder verlassen hat. Die Beklagte kündigte das Arbeitsverhältnis der Parteien außerordentlich, hilfsweise ordentlich.

Mit seiner dagegen erhobenen Klage hat der Kläger unter anderem geltend gemacht, er habe am 2. Juni 2018 gearbeitet. Die Erkenntnisse aus der Videoüberwachung unterlägen einem Sachvortrags- und Beweisverwertungsverbot und dürften daher im Kündigungsschutzprozess nicht berücksichtigt werden.

Die Vorinstanzen haben der Klage stattgegeben. Die hiergegen gerichtete Revision der Beklagten hatte vor dem Zweiten Senat des Bundesarbeitsgerichts bis auf einen Antrag betreffend ein Zwischenzeugnis Erfolg. Sie führte zur Zurückverweisung der Sache an das Landesarbeitsgericht. Dieses habe nicht nur das Vorbringen der Beklagten zum Verlassen des Werksgeländes durch den Kläger vor Beginn der Mehrarbeitsschicht zu Grunde legen, sondern gegebenenfalls auch die betreffende Bildsequenz aus der Videoüberwachung am Tor zum Werksgelände in Augenschein nehmen müssen. Dies folge aus den einschlägigen Vorschriften des Unionsrechts sowie des nationalen Verfahrens- und Verfassungsrechts. Dabei spiele es keine Rolle, ob die Überwachung in jeder Hinsicht den Vorgaben des Bundesdatenschutzgesetzes bzw. der Datenschutz-Grundverordnung (DSGVO) entsprach. Selbst wenn dies nicht der Fall gewesen sein sollte, wäre eine Verarbeitung der betreffenden personenbezogenen Daten des Klägers durch die Gerichte für Arbeitssachen nach der DSGVO nicht ausgeschlossen. Dies gelte jedenfalls dann, wenn die Datenerhebung wie hier offen erfolgt und vorsätzlich vertragswidriges Verhalten des Arbeitnehmers in Rede steht. In einem solchen Fall sei es grundsätzlich irrelevant, wie lange der Arbeitgeber mit der erstmaligen Einsichtnahme in das Bildmaterial zugewartet und es bis dahin vorgehalten hat. Der Senat ließ offen, ob ausnahmsweise aus Gründen der Generalprävention ein Verwertungsverbot in Bezug auf vorsätzliche Pflichtverstöße in Betracht komme, wenn die offene Überwachungsmaßnahme eine schwerwiegende Grundrechtsverletzung darstelle. Dies sei vorliegend nicht der Fall gewesen.

„Das BAG unterstreicht einmal mehr, dass Zielrichtung des Datenschutzes eben nicht der Täterschutz ist. Bei der Prüfung eines Verwertungsverbots kommt es stets auf eine Abwägung der Schwere des Datenschutz-/Grundrechtsverstoßes mit dem arbeitgeberseitigen Interesse an der Verwertung an", ordnet Dr. Maximilian Koschker, Rechtsanwalt und Partner bei der internationalen Wirtschaftskanzlei CMS Deutschland, die Entscheidung ein. Das BAG habe das Interesse der Beklagten an der Auswertung der durch eine offene Videoaufzeichnung gewonnenen Erkenntnisse zu Recht als gewichtiger angesehen als ihre nicht schwerwiegenden und auch nicht vorsätzlichen Datenschutzverstöße: „Dem BAG kam es dabei für die Verwertbarkeit der Videoaufzeichnungen im Gegensatz zu den Vorinstanzen offenbar nicht darauf an, dass die Beklagte die unter anderem auf Hinweisschildern kundgetane Speicherdauer von maximal 96 Stunden missachtet und ältere Aufzeichnungen zur Beweisführung herangezogen hatte."

Koschker hebt noch einen weiteren Aspekt hervor: „Erwähnenswert ist noch, dass sich die Beklagte zur Begründung der streitgegenständlichen Kündigung auch auf Daten aus der elektronischen Zeiterfassung des Klägers stützte. Hier waren die Vorinstanzen zu dem Schluss gelangt, dass die Arbeitsgerichte an einer Verwertung dieser Daten gehindert seien, da die Beklagte in einer Betriebsvereinbarung zur elektronischen Zeiterfassung das Unterbleiben entsprechender Auswertungen gerade zugesichert hatte." Gerade hier werde es aus Sicht der Praxis besonders interessant: „Betriebsvereinbarungen mit Bezug zur elektronischen Verarbeitung von Mitarbeiterdaten enthalten vielfach die Aussage, dass unter Verstoß gegen die Vorgaben der Betriebsvereinbarung gewonnene Daten und Erkenntnisse nicht zu Lasten des Arbeitnehmers in Kündigungsschutzprozesse eingeführt werden dürfen." Bis dato sei die überwiegende arbeitsgerichtliche Rechtsprechung recht „großzügig" über derlei Vereinbarungen der Betriebsparteien hinweg gegangen und habe sich hieran nicht gebunden gefühlt. „Ob das BAG an dieser Stelle – im Einklang mit den Vorinstanzen – eine Zeitenwende einleitet oder aber ‚alles beim Alten' bleibe, lasse sich auf Grundlage der Pressemitteilung des BAG allein nicht beantworten. Der Volltext der Entscheidung liegt bislang nicht vor.

chk

Präsenz-Workshop inkl. Einführungs-Webinar

Praxisseminar zur CSRD-Berichterstattung:

Nicht-finanzielles Reporting optimal umsetzen

Grundlagen-Webinar: 10. November 2023
Online

10.00 Uhr	Begrüßung
10.15 Uhr	Neue gesetzliche Anforderungen an die nicht-finanzielle Berichterstattung von Unternehmen
11.15 Uhr	Umsetzungsmöglichkeiten und Konsequenzen bei Untätigkeit
12.15 Uhr	Offene Diskussion mit Referenten & Teilnehmenden
13.00 Uhr	Ende des Praxisseminars

Das Webinar dient der Einführung in das Thema und vermittelt die Grundlagen zur CSRD-Berichterstattung. Der Präsenz-Workshop baut darauf auf und vertieft die Inhalte weiter. Eine separate Teilnahme an beiden Formaten ist problemlos möglich.

Präsenz-Workshop: 23. November 2023
dfv Mediengruppe, Mainzer Landstr. 251, 60326 Frankfurt am Main

9.30 Uhr	Begrüßung
9.45 Uhr	Übersicht über die aktuellen und zukünftigen gesetzlichen Anforderungen der nicht-finanziellen Berichterstattung
10.45 Uhr	In Kleingruppen: Analyse von ausgewählten Berichten unterschiedlicher Unternehmen
11.45 Uhr	Besprechung der Ergebnisse und Zusammenstellung von „Best & Worst Disclosures“
12.45 Uhr	Mittagspause & Networking
14.00 Uhr	Praktische Herangehensweise an Datenerhebung und -darstellung im eigenen Lagebericht
16.30 Uhr	Besprechung der herausgearbeiteten Ergebnisse und Diskussionsrunde
17.00 Uhr	Ende des Workshops

Unsere Experten geben u.a. Antworten auf diese Fragen:

- Wie verändert die CSRD die Berichterstattung?
- Welche Informationen benötigt man für die nicht-finanzielle Berichterstattung?
- Wie bereitet man die Informationen im Lagebericht optimal auf?
- Was sind gute, was sind schlechte Beispiele für nicht-finanzielle Berichterstattung – und warum?
- Was ist 2024 mindestens zu tun? Und was danach?
- Wie kann man sich gegen Klimaklagen schützen?
- Welche Konsequenzen drohen Unternehmen und Geschäftsleitern bei nicht-compliance?
- Was sind zukünftige Entwicklungen in der EU und Deutschland?

Prof. Dr. Daniel Graewe
Rechtsanwalt

Henning Kuhlmann
Wirtschaftsprüfer/
Steuerberater

Zielgruppe:

Das Format richtet sich an alle, die mit dem Thema „nicht-finanzielle Berichterstattung“ sowie deren Umsetzung im Unternehmen befasst sind. Dazu zählen neben der Geschäftsleitung, den Gesellschaftern und Kontrollorganen auch Nachhaltigkeitsbeauftrage, Sustainability Manager, Rechtsabteilung, Controlling, Human Resources und andere. Neben den aktuellen Normen (CSRD, CSDDD) werden auch die neuen Nachhaltigkeitsstandards „ESRS“ thematisiert.

Preise:

Teilnahmegebühr (zzgl. MwSt.)	Abonnenten RuW und Behördenverteter	Regulär
Webinar	99,- EUR	149,- EUR
Workshop	599,- EUR	699,- EUR
Webinar + Workshop	639,- EUR	749,- EUR

Ihre Ansprechpartnerin:

dfv Mediengruppe
Mainzer Landstr. 251
60326 Frankfurt am Main
Frau Maria Belz
E-Mail: Maria.Belz@dfv.de
Tel.: +49 69 7595 1157

JETZT QR-CODE SCANNEN UND DIREKT ANMELDEN!

oder unter www.ruw.de/csrd-praxis

Eine Veranstaltung von:

Compliance Berater
Betriebs-Berater Compliance

Kooperationspartner:

GREEN WORKS
www.how-green-works.de

Der EU Data Act kommt

Der EU Data Act hat Ende Juni die letzte Hürde im EU-Gesetzgebungsverfahren genommen. In den so genannten Trilog-Verhandlungen konnten sich die Europäische Kommission, der Rat und das Parlament für ein Gesetz zur Regelung des Zugangs zu Daten, deren Austausch und Übermittlung einigen. Mit dem lange und breit diskutierten EU Data Act sollen europäische Unternehmen nun bei den Themen Datenkontrolle und Transparenz stärker in die Pflicht genommen werden und unter anderem umfangreichere Datenschutzmaßnahmen – vor allem beim Schutz von Geschäftsgeheimnissen – umsetzen. Doch die neuen Anforderungen sorgen bereits seit Längerem für starke Kritik aus der Wirtschaft, beschreiben Dr. Björn Herbers und Dr. Michael Kraus.

EU Data Act: Er soll die Datenwirtschaft der EU ankurbeln und den europäischen Cloud-Markt fördern.

Unter anderem seien Definitionen und Begrifflichkeiten teilweise unpräzise und es drohe eine hohe administrative Belastung für die Unternehmen selbst – mit negativen Auswirkungen auf Innovationsfähigkeit und Wettbewerbsfähigkeit. „Der Data Act ist ein Experiment. Er setzt auf umfassende Datenzugangsansprüche, ohne dass überhaupt klar ist, ob und welche Geschäftsmodelle darauf aufbauen können, kritisiert Dr. Björn Herbers, Partner und Rechtsanwalt im Brüsseler Büro der Wirtschaftskanzlei CMS. Eine der Herausforderungen bei den nun umzusetzenden Regeln, sei insbesondere der Schutz von Geschäftsgeheimnissen. „Die Industrie hat im Gesetzgebungsverfahren massive Sorge davor geäußert, dass über Datenzugangsansprüche ihre Geschäftsgeheimnisse abfließen", erläutert Herbers. Der Schutz von Geschäftsgeheimnissen sei deshalb bis zuletzt Knackpunkt der Verhandlung gewesen. Das sei auch ein kartellrechtliches Thema.

Dr. Michael Kraus, ebenfalls Partner bei der Wirtschaftskanzlei CMS, rät Unternehmen, bereits jetzt die Auswirkungen des Data Act auf ihr Geschäftsmodell zu prüfen und Umsetzungsmaßnahmen einzuleiten: „Es betrifft alle Teile des Unternehmens – Entwicklung, Vertrieb, Rechtsabteilung und unter strategischen und Compliance-Gesichtspunkten nicht zuletzt auch die Unternehmensführung. Verstöße gegen den Data Act sind bußgeldbewehrt und die Bußgeldregelungen entsprechen denen der DSGVO."

Der Data Act zwinge Unternehmen daher zu einer vorausschauenden Datenstrategie. Weil das Recht zur Datennutzung nur auf der Grundlage vertraglicher Vereinbarung zulässig sei, könnten Unternehmen geneigt sein, ihre Datenstrategie neu und restriktiv auszurichten. Das führe aber zu weniger verfügbaren Daten und laufe damit dem Ziel des Data Act zuwider, so Kraus. Denn der EU Data Act soll die Datenwirtschaft der EU gerade ankurbeln, indem Industriedaten freigegeben, ihre Zugänglichkeit und Nutzung optimiert und ein wettbewerbsfähiger und zuverlässiger europäischer Cloud-Markt gefördert werden, wie die EU-Kommission in einer Pressemitteilung beschreibt. Konkret umfasst der EU Data Act danach:

– Regelungen, die es den Nutzern vernetzter Geräte ermöglichen, auf die Daten zuzugreifen, die von diesen Geräten und den damit verbundenen Diensten erzeugt werden. Die Nutzer können diese Daten an Dritte weitergeben und damit den Anstoß für vielfältige Anschlussdienste und Innovationen geben. Gleichzeitig bleiben die Anreize für die Hersteller, unter Wahrung ihrer Geschäftsgeheimnisse in eine hochwertige Datenerzeugung zu investieren, bestehen.
– Vorschriften zum Schutz vor einseitig auferlegten missbräuchlichen Vertragsklauseln. Diese sollen EU-Unternehmen vor ungerechten Vereinbarungen schützen, faire Verhandlungen fördern und KMU in die Lage versetzen, selbstbewusster am digitalen Markt aufzutreten.
– Mechanismen, mit denen öffentliche Stellen auf Daten des privaten Sektors zugreifen und diese nutzen können, wenn dies bei öffentlichen Notständen (wie bei Überschwemmungen und Waldbränden) oder zur Erfüllung eines gesetzlichen Auftrags nötig ist und die erforderlichen Daten nicht ohne Weiteres auf andere Weise verfügbar sind.
– Neue Vorschriften, die den Kunden die Freiheit geben, zwischen verschiedenen Cloud-Datenverarbeitungsdienstleistern zu wechseln. Diese Vorschriften zielen darauf ab, den Wettbewerb und die Auswahl auf dem Markt zu fördern und gleichzeitig eine unerwünschte Anbieterbindung zu vermeiden. Darüber hinaus enthält das Datengesetz Schutzvorkehrungen, die unrechtmäßige Datenübermittlungen verhindern und für mehr Verlässlichkeit und Sicherheit in der Datenverarbeitungsumgebung sorgen sollen.
– Maßnahmen zur Förderung der Entwicklung von Interoperabilitätsstandards für den Datenaustausch und die Datenverarbeitung im Einklang mit der EU-Normungsstrategie.

Die politische Einigung, die das Europäische Parlament und der Rat erzielt haben, muss nun von den beiden Gesetzgebungsorganen noch förmlich gebilligt werden. *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, Kluth Rechtsanwälte; 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

Regeln zu Menschenrechten und Umweltauswirkungen

Das EU-Parlament hat Anfang Juni 2023 seine Position für die Verhandlungen mit den EU-Ländern über Regeln zur Integration von Menschenrechten und Umweltauswirkungen in die Unternehmensführung angenommen.

© IMAGO / Panthermedia

Zum Klimaschutz verpflichtet: Unternehmen müssen einen Übergangsplan zur Begrenzung der Erderwärmung umsetzen.

Die neuen Vorschriften gelten für in der EU ansässige Unternehmen, unabhängig von ihrer Branche, einschließlich Finanzdienstleistungen, mit mehr als 250 Beschäftigten und einem weltweiten Umsatz von über 40 Mio. EUR sowie für Muttergesellschaften mit mehr als 500 Beschäftigten und einem weltweiten Umsatz von über 150 Mio. EUR. Nicht-EU-Unternehmen mit einem Umsatz von mehr als 150 Mio. EUR, wenn mindestens 40 Mio. in der EU erwirtschaftet wurden, werden ebenfalls einbezogen.

Die Unternehmen müssen einen Übergangsplan zur Begrenzung der Erderwärmung auf 1,5°C umsetzen. Im Falle großer Unternehmen mit mehr als 1.000 Beschäftigten wird sich die Erfüllung der Ziele des Plans auf die variable Vergütung der Mitglieder der Unternehmensleitung (z. B. Boni) auswirken. Die neuen Vorschriften verpflichten die Unternehmen außerdem, sich mit den von ihren Handlungen Betroffenen, einschließlich Menschenrechts- und Umweltaktivisten, auseinanderzusetzen, einen Beschwerdemechanismus einzuführen und die Wirksamkeit ihrer Sorgfaltspflicht regelmäßig zu überprüfen.

Unternehmen, die die Vorschriften nicht einhalten, sind schadenersatzpflichtig und können von den nationalen Aufsichtsbehörden mit Sanktionen belegt werden. Zu den Sanktionen gehören Maßnahmen wie die namentliche Anprangerung („Naming and Shaming"), die Rücknahme der Waren eines Unternehmens vom Markt oder Geldstrafen von mindestens 5 % des weltweiten Nettoumsatzes. Nicht-EU-Unternehmen, die sich nicht an die Regeln halten, werden von der öffentlichen Auftragsvergabe in der EU ausgeschlossen.

Nach dem angenommenen Text sollen die neuen Verpflichtungen je nach Größe des Unternehmens nach drei oder vier Jahren gelten. Kleinere Unternehmen können die Anwendung der neuen Vorschriften um ein weiteres Jahr verschieben. *chk*

3 Monate Testlesen mit gratis Onlinezugang!

www.ruw.de/CB

Der **CB – Compliance Berater** richtet sich als praxisnahes Tool an alle Compliance-Verantwortlichen – wie z. B. **Compliance Officer, Risikomanager und Geschäftsleitung** – in Unternehmen, Institutionen und Verbänden.

Der **CB – Compliance Berater** bildet die 4 **Facetten von Compliance in jeder Ausgabe ab: Corporate Compliance, Risikoanalyse und -identifikation, Compliance Management** und **Haftung & Aufsicht**

Der **CB – Compliance Berater** liefert seinen Lesern zusätzlich eine Website mit aktuellen News und Standpunkten renommierter Autoren. Schauen Sie jetzt selbst auf compliance.ruw.de

Die **Online-Zeitschrift Compliance** compliance-plattform.de – Compliance ist eine ebenso wichtige wie spannende Aufgabe im Unternehmen, der unsere Redaktion ihre ganze journalistische Aufmerksamkeit widmet. Mit der Online-Zeitschrift werden Compliance-Verantwortliche monatlich kompetent und übersichtlich rund um ihr tägliches Arbeitsgebiet informiert.

Per Faxantwort an 069 7595-2770

Name: _____

Firma: _____

Abteilung: _____

Straße: _____

PLZ | Ort: _____

Telefon: _____

E-Mail: _____

Datum | Unterschrift: _____

Sichern Sie sich Ihr individuelles Vorteilsangebot und bestellen Sie jetzt den CB – Compliance Berater

☐ **Testabo:** 3 Monate kostenlos lesen + 1 Zugang zur Online-Datenbank

Sie erhalten die nächsten 3 Ausgaben der Fachzeitschrift „Compliance-Berater" kostenlos. Falls Ihnen der „Compliance-Berater" gefällt, brauchen Sie nichts weiter zu unternehmen. Wenn Sie nicht innerhalb der Testzeit abbestellen, beginnt im Anschluss ein Jahresabo. Zunächst für ein Jahr (11 Ausgaben) zum Vorzugspreis von derzeit 589,00 € inkl. aller Gebühren und MwSt. in Deutschland und anschließend bis auf Widerruf zum jeweils gültigen Jahrespreis. Das Abonnement kann bis 3 Monate vor Ablauf des Bezugszeitraumes schriftlich bei der Deutscher Fachverlag GmbH, Mainzer Landstr. 251, 60326 Frankfurt am Main gekündigt werden. Liegt dem Verlag zu diesem Zeitpunkt keine Abbestellung vor, verlängert sich das Abonnement automatisch um ein weiteres Jahr. Die Abonnementgebühren sind im Voraus nach Erhalt der Rechnung zahlbar.

☐ **Jahresabo:** 11 Ausgaben + 1 Zugang zur Online-Datenbank

Sie erhalten die nächsten 11 Ausgaben der Fachzeitschrift „Compliance-Berater", sowie den Zugang zur Online-Datenbank. Der Abonnementvertrag wird für mindestens ein Jahr abgeschlossen. Das Abonnement kann jederzeit bis 3 Monate vor Ablauf des Bezugszeitraumes schriftlich bei der Deutscher Fachverlag GmbH, Mainzer Landstr. 251, 60326 Frankfurt am Main gekündigt werden. Liegt dem Verlag zu diesem Zeitpunkt keine Abbestellung vor, verlängert sich das Abonnement automatisch um ein weiteres Jahr. Die Abonnementgebühren sind im Voraus nach Erhalt der Rechnung zahlbar und betragen 589,00 € inkl. aller Gebühren und MwSt. in Deutschland.

CB – Compliance Berater | Betriebs-Berater Compliance
kundenservice@ruw.de

dfv Mediengruppe