

Compliance

Die Zeitschrift für Compliance-Verantwortliche

Inhalt



© IMAGO / Zornar

2

Aufmacher

Compliance und ESG: Wie lassen sich beide miteinander verzahnen?
Compliance und die Nachhaltigkeitsthemen Environmental, Social und Governance (ESG) – gehören sie zusammen oder sollten sie getrennt behandelt werden? Dieser Frage nähert sich Prof. Dr. Katharina Hastenrath in unserem Aufmacher.

Recht



© IMAGO / analphoto

4

Cybersicherheit kritischer Infrastrukturen – Die NIS2-Richtlinie – Ein Überblick

Die im Jahr 2023 in Kraft getretene NIS2-Richtlinie (EU 2022/2555) verfolgt das Ziel, ein hohes, EU-weit einheitliches Niveau an Cybersicherheit zu gewährleisten. Dr. Dr. Fabian Teichmann gibt hier einen Überblick über Inhalt und Umsetzung der NIS2-Richtlinie, die den persönlichen und sachlichen Anwendungsbereich im Vergleich zur Vorgängerregelung erheblich erweitert.

Veranstaltung



© Kahlen-Pappas

6

Deutsche Compliance Konferenz 2025

Beste Voraussetzungen zum Austausch in der Compliance-Community: Impulse aus 15 Fachbeiträgen und vier hochkarätig besetzte Diskussionsrunden waren Grundlage für eine gelungene Deutsche Compliance Konferenz 2025 am 13. und 14. Mai.

Research



© IMAGO / Panthermedia

8

Studie: Wenig Vertrauen in Fähigkeiten beim Datenschutz

So schnell wie sich die Digitalisierung weiterentwickelt, so dringend muss der Datenschutz zu einem entscheidenden Geschäftsprinzip werden. Jedoch haben laut der ISACA-Studie „State of Privacy 2025“ nur 38 Prozent der europäischen Fachleute Vertrauen in die Fähigkeit ihres Unternehmens, sensible Daten zu schützen.

Veranstaltungen

Jetzt anmelden!

Praxisseminar zur KI und KI-Verordnung – Implementierung, AI-Compliance, Datenschutz & Durchsetzung

Weitere Informationen und Anmeldung unter www.ruw.de/ki-verordnung

24. Juni 2025 | 14.00 bis 18.45 Uhr | Düsseldorf

Eine Veranstaltung des

DATENSCHUTZ-BERÄTER

und **pwc**

23.06.2025 | Webinar | **Payment After Work: QR-Code-basierter Drittmisbrauch**

24.06.2025 | Düsseldorf | **Praxisseminar zur KI und KI-Verordnung**

25.06.2025 | Webinar | **Personenbezogene Daten im Fokus: So nehmen Sie Hackern ihre wichtigste Handelsware**

03.07.2025 | München | **1. Deutscher Entgelttransparenztag**

03.07.2025 | Frankfurt am Main | **Der Data Act – das neue Zugpferd der Datenwirtschaft?**

Compliance und ESG: Wie lassen sich beide miteinander verzahnen?

Compliance und die Nachhaltigkeitsthemen Environmental, Social und Governance (ESG) – gehören sie zusammen oder sollten sie getrennt behandelt werden? Dieser Frage nähert sich Prof. Dr. Katharina Hastenrath in unserem Aufmacher.

in kleineren Unternehmen. Beide Bereiche überschneiden sich im Punkt Governance, benötigen jedoch separate Expertise. Für die Zukunft müssen Compliance und ESG effizient zusammenarbeiten. Ob und wie Compliance und Compliance-Management-Systeme und die Nachhaltigkeit, die mittlerweile im Begriff ESG aufgegangen ist, aufeinander „verschmolzen“ werden können, dazu bestehen in der Wissenschaft und Praxis kontrovers diskutierte Ansätze. Alternativ bleiben die Themen nebeneinander bestehen oder es könnten nur Teilbereiche zusammengelegt werden.

Die strikte Trennung beider Bereiche birgt allerdings den Nachteil, dass gerade das Thema Governance viele inhaltliche Überschneidungen mit Compliance hat. Zudem müssten vorhandene Mitarbeiter im ESG-Bereich ausführlich in die neue Dimension der Tätigkeit eingearbeitet werden, was schon fast einen Studiengang erfordert, betrachtet man die Tragweite und hohen Bußen des Themas. Daher ist diese Variante jedenfalls aus Kostengesichtspunkten und möglichen Doppelbelastungen der operativen Mitarbeiter mit Abfragen und Prüfungen beider Bereiche nicht uneingeschränkt empfehlenswert.

Möglich wäre auch, dass die Compliance-Funktion einzelne Themen wie eine Risikoanalyse zu ESG-Themen übernimmt. Was theoretisch auf den ersten Blick denkbar erscheint, hält einem Praxistest allerdings nur sehr bedingt stand. Jeder, der bereits einmal eine Risikoanalyse durchgeführt hat, weiß, dass viele Erkenntnisse, die in dem finalen Risikobericht und der dazugehörigen Risikobewertung münden, der Ausfluss von feinen Nuancen und Einschätzungen aus persönlichen Interviews sind. Dies dann auf eine andere Funktion zu übertragen, also von der ausführenden Compliance-Funktion auf die ESG-Funktion, erscheint schwierig.

Grundsätzlich denkbar wäre, das neue Thema der verrechtlichten ESG auf die zentrale Compliance-Funktion zu übertragen. Im Unterschied zu den bestehenden Matrix-Compliance-Themen ist das Thema gerade nicht in einer vorhandenen Abteilung bereits umfassend betrachtet und bearbeitet. Dieser Ansatz kann allerdings nur funktionieren, wenn die Compliance-Funktion dann mit erheblichen zusätzlichen Ressourcen und Mitarbeitern ausgestattet wird. Die Themen sind zwar im Grundsatz gleich, nämlich mit einem Management-System zu minimierende Risiken, allerdings sind die Anforderungen im Detail erheblich andere.

Prof. Dr. Katharina Hastenrath

Wie diese Ideen weiterentwickelt werden können und mögliche Lösungsansätze dazu lesen Sie im Beitrag von Prof. Dr. Katharina Hastenrath „ESG-Pflichten als integrativer Teil der klassischen Compliance-Funktion?“ in der **Schwerpunktausgabe des Compliance-Beraters 2025 „Compliance und ESG“** auf Seite 140.



Können ESG- und klassische Compliance-Themen ein gemeinsames Räderwerk sein?

Blicken wir zunächst auf die Entwicklung der Compliance: Um die Jahrtausendwende wurde klar, dass Rechtsabteilungen nicht genühten, um Unternehmensskandale wie Korruption zu verhindern. Compliance-Abteilungen entstanden, jedoch oft ohne klare Aufgaben oder Systematik. Maßnahmen wie Schulungen und Codes of Conduct dominierten, während Kontrollen und Risikoanalysen fehlten. Ab 2010 etablierte der IDW PS 980 Compliance als Management-System (CMS) mit definierten Elementen wie Risikoanalyse und Überwachung. Das Berufsbild des CCO professionalisierte sich, und lokale Compliance-Officer wurden in Hochrisikoländern wie den USA eingeführt. Zudem erweiterte sich das CMS thematisch auf Kartellrecht, Datenschutz und Geldwäsche. Third-Party-Compliance brachte strengere Prüfungen von Geschäftspartnern durch Auditrechte und externe Kontrollen. Die Entwicklung der KI revolutioniert ab 2020 zunehmend das CMS und die Compliance. KI ermöglicht personalisierte E-Learnings, automatisierte Datenanalysen für interne Prüfungen und die Evaluation tausender Business-Partner. Zudem unterstützt KI Kulturabfragen

und bietet passgenaue Maßnahmen, um Risiken zu minimieren.

Schauen wir nun auf die Entwicklung der Nachhaltigkeit, die noch länger in die Vergangenheit zurückreicht. Die Nachhaltigkeitspolitik entwickelte sich von 1950 bis 2000 schrittweise. Internationale Meilensteine wie die UN-Umweltkonferenz 1972 und der Brundtland-Bericht 1987 prägten den globalen Diskurs. In Deutschland führten die Ölkrise und Katastrophen wie Tschernobyl zu Umweltgesetzen, der Gründung des Umweltministeriums und der Verankerung des Umweltschutzes im Grundgesetz. Ab 2000 wandelte sich der Fokus von freiwilligen Maßnahmen zu verbindlichen Regeln. Meilensteine waren die UN-Leitprinzipien für Wirtschaft und Menschenrechte sowie die CSR-Richtlinie der EU. Seit 2020 verschärfen Gesetze wie das Lieferkettengesetz und der EU-Green Deal die Anforderungen. Eine Revision soll wirtschaftliche Belastungen abfedern. Aus der ursprünglichen Freiwilligkeit wurde etappenweise eine Regulatorik mit härtesten Sanktionen bei Nichtbefolgung.

Ein Blick in die Vergangenheit, der Aufschluss über mögliche Handlungsoptionen der Zukunft gibt: Welche Ableitungen können wir ziehen?

Das CMS hat sich über 20 Jahre zu einem komplexen System entwickelt, bleibt jedoch mit stetigen Erweiterungen und der Integration von KI stark ausgelastet. Nachhaltigkeitsaufgaben haben sich von freiwilligen Maßnahmen zu streng regulierten Anforderungen gewandelt. 2025 sind ESG-Funktionen ebenso anspruchsvoll wie CMS-Themen, oft ohne ausreichende Qualifikation bei Mitarbeitern



Prof. Dr. Katharina Hastenrath ist Professorin für Compliance und Compliance-Management-Systeme an der ZHAW (Zürich/Schweiz); zuvor war sie (C)CO bei mehreren, internationalen deutschen Unternehmen. Sie berät zudem zu (strategischen) Compliance-Fragen.

Kostenlose Teilnahme für Abonnent:innen der RdZ – auch mit Probe-Abonnement!

„Payment After Work“ – die RdZ-Gesprächsreihe: QR-Code-basierter Drittmisbrauch

Montag, 23. Juni 2025 | Webinar

18.00 Uhr	Begrüßung Gabriele Bourgon , Chefredakteurin RdZ, dfv Mediengruppe
18.05 Uhr	Begrüßung und Moderation Prof. Dr. Sebastian Omlor , RdZ-Herausgeber
18.10 Uhr	QR-Code-basierter Drittmisbrauch Dr. Aurelia Philine Birne , Habilitandin und Wissenschaftliche Mitarbeiterin am Institut für das Recht der Digitalisierung der Philipps-Universität Marburg
18.40 Uhr	Offene Diskussion mit den Referierenden und Teilnehmenden
19.00 Uhr	Ende des Webinars



Gabriele Bourgon



Prof. Dr. Sebastian Omlor



Dr. Aurelia Philine Birne

Dieses Thema erwartet Sie:

Drittmisbrauch im Zahlungsverkehr äußert sich insbesondere in Form von Phishing-Angriffen, neuerdings durch Scannen schädlicher Quick-Response-(QR-)Codes (quishing). Kommt es in diesen Fällen zur täuschungsausführenden Ausführung von Zahlungsvorgängen, stellt sich insbesondere die Haftungsfrage zwischen Zahlungsdienstnutzer und Zahlungsdienstleister. Der Vortrag beschäftigt sich mit dem Quishing und seinen Erscheinungsformen sowie den möglichen zahlungsdienstrechtlichen Ansprüchen.

Über „Payment After Work“:

Die Zeitschrift Recht der Zahlungsdienste (RdZ) erscheint dreimal im Jahr: Ende Februar, Ende Juni und Ende Oktober. Jeweils ca. eine Woche vor Erscheinen der RdZ wird ein Thema der Ausgabe zum Gegenstand der Webinar-Reihe „Payment After Work“ gemacht. Die Autorinnen und Autoren stellen in einem Kurzvortrag ihre Kernthesen vor und diskutieren anschließend mit den Teilnehmenden. Die Moderation übernehmen im Wechsel die RdZ-Herausgeber Dr. Christian Conreder, Partner bei Rödl GmbH RAG StBG WPG, und Prof. Dr. Sebastian Omlor, Direktor des Instituts für das Recht der Digitalisierung an der Philipps-Universität Marburg.

Zielgruppen: Syndici bei Zahlungsdiensten, Personen, die Zahlungsdienste konzipieren, Berater im Bereich Zahlungsdienste (RA, StB, WP, Unternehmensberater) und Personen in Gesetzgebung, Justiz, Verwaltung, Wissenschaft und Verbänden, die mit Zahlungsdiensten befasst sind

Teilnahmegebühr: 99,- EUR (zzgl. MwSt.)

Jahres-/Probeabonnent:innen der RdZ nehmen kostenfrei teil.

Ihre Ansprechpartnerin: Maria Belz

Maria.Belz@dfv.de, Tel.: +49 69 7595-1157

Kennen Sie schon die RdZ – Recht der Zahlungsdienste?



Jetzt die RdZ im Probe- oder Jahresabo bestellen unter www.ruw.de/rdz-ueberuns und kostenfrei teilnehmen!

- 3 Ausgaben pro Jahr
- 339,- EUR zzgl. Versand
- inkl. Zugang zur Online-Datenbank mit allen Beiträgen seit der Erstausgabe 2020



**JETZT QR-CODE
SCANNEN UND
DIREKT ANMELDEN!**

oder unter
www.ruw.de/payment-after-work

Cybersicherheit kritischer Infrastrukturen – Die NIS2-Richtlinie – Ein Überblick

Die im Jahr 2023 in Kraft getretene NIS2-Richtlinie (EU 2022/2555) verfolgt das Ziel, ein hohes, EU-weit einheitliches Niveau an Cybersicherheit zu gewährleisten. Insbesondere Betreiber kritischer Dienstleistungen und wichtiger Unternehmen sollen durch anspruchsvolle IT-Sicherheitsmaßnahmen, Meldepflichten bei IT-Vorfällen und erweiterte Haftungsregeln für Leitungsorgane stärker in die Pflicht genommen werden. Der folgende Beitrag gibt einen Überblick über Inhalt und Umsetzung der NIS2-Richtlinie, beleuchtet in einem weiteren Teil (erscheint in der Juli-Ausgabe von Compliance) neue Pflichten – etwa zum Risikomanagement und zur 24-Stunden-Meldung.



Mit der NIS2-Richtlinie reagiert die EU auf die Zunahme von Cyberangriffen auf essenzielle Dienste.

Die NIS2-Richtlinie (Network and Information Security Directive 2) ist am 16. Januar 2023 in Kraft getreten und ersetzt die ursprüngliche NIS-Richtlinie von 2016. Als Teil der EU-Cyberstrategie reagiert sie auf die Zunahme von Cyberangriffen auf essenzielle Dienste in Europa. Die Richtlinie soll ein hohes gemeinsames Cybersicherheitsniveau in der EU erreichen und die Resilienz kritischer Infrastrukturen verbessern. Hierzu verpflichtet NIS2 die Mitgliedstaaten, ihre nationalen Cybersecurity-Vorschriften deutlich zu verschärfen und anzugleichen. Im Vordergrund steht das Ziel, Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der IT-Systeme kritischer Einrichtungen zu verhindern sowie die Auswirkungen von Sicherheitsvorfällen zu minimieren. Gleichzeitig sollen fragmentierte nationale Regelungen vereinheitlicht und ein „level playing field“ geschaffen werden, um Schlupflöcher durch laxere Vorschriften in einzelnen Mitgliedstaaten zu vermeiden.

Die NIS2-Richtlinie erweitert den persönlichen und sachlichen Anwendungsbereich im Vergleich zur Vorgängerregelung erheblich. Wesentliche Einrichtungen (essential entities) und wichtige Einrichtungen (important entities) in insgesamt 18 Sektoren unterliegen künftig den NIS2-Vorgaben. Erfasst sind neben den klassischen KRITIS-Branchen – etwa Energie, Verkehr, Finanzwesen, Gesundheitsversorgung, Trink- und Abwasser, Lebensmittelversorgung, digitale Infrastruktur und Telekommunikation – auch weitere Bereiche

der Wirtschaft. Hierzu zählen z.B. der Raumfahrtsektor, die Herstellung kritischer Produkte (etwa Pharmazeutika, Medizinprodukte, Chemikalien), Post- und Kurierdienste, Abfallentsorgung, Behörden und öffentliche Verwaltung sowie bestimmte IT-Dienstleister (z.B. Cloud- und DNS-Dienste).

Grundsätzlich erfasst NIS2 alle mittelgroßen und großen Unternehmen (i.d.R. mindestens 250 Mitarbeiter und 50 Mio. EUR Jahresumsatz) in den genannten Sektoren. Durch diese Size-Cap-Regel sind ca. 29.000 Unternehmen allein in Deutschland neu reguliert. Daneben bestehen einige Ausnahmen und Sondertatbestände: So können auch kleinere Einheiten erfasst sein, wenn sie z.B. als alleinige Anbieter eine kritische Dienstleistung erbringen oder als sog. „Alleinvertreter“ grenzüberschreitend tätig sind (etwa bestimmte Trust-Service-Provider). Insgesamt führt NIS2 zu einer erheblichen Ausweitung des Kreises verpflichteter Unternehmen im Vergleich zur bisherigen Rechtslage. Dies stellt Unternehmen – vor allem außerhalb der bisher schon als „kritisch“ eingestuften Betreiber – vor neue Compliance-Aufgaben.

Die Mitgliedstaaten mussten NIS2 bis zum 17. Oktober 2024 in nationales Recht überführen. In Deutschland wurde hierzu ein umfangreicher Regierungsentwurf für ein NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) erarbeitet und am 24. Juli 2024 vom Bundeskabinett beschlossen. Der Entwurf sieht eine grundlegende Novellierung des BSI-Gesetzes (BSIG) vor und umfasst über 240 Seiten. Die fristgerechte



RA Dr. Dr. Fabian Teichmann, LL.M., ist Managing Partner der Teichmann International (Schweiz) AG sowie Verwaltungsrat der Teichmann International (IT Solutions) AG. Seine Schwerpunkte liegen im Strafrecht, der Cybersecurity und der Unternehmenscompliance. Er ist zudem als Dozent an mehreren europäischen Hochschulen tätig.

Verabschiedung bis Oktober 2024 gelang jedoch nicht. Deutschland – wie 22 weitere EU-Staaten – hat die Umsetzungsfrist versäumt und sieht sich nun einem Vertragsverletzungsverfahren der EU-Kommission ausgesetzt. Die Verabschiedung des NIS2UmsuCG wird nun für 2025 erwartet. Ungeachtet dessen gilt es für betroffene Unternehmen, sich rechtzeitig auf die neuen Vorgaben vorzubereiten, da der deutsche Gesetzgeber ein Inkrafttreten unmittelbar nach Verkündung anstrebt. *RA Dr. Dr. Fabian Teichmann, LL.M.*

IMPRESSUM

Verlag

Deutscher Fachverlag GmbH, Mainzer Landstraße 251, 60326 Frankfurt am Main
Registrierungsgericht AG Frankfurt am Main HRB 8501

UStIdNr. DE 114139662

Geschäftsführung: Peter Esser (Sprecher), Thomas Berner, Markus Gotta

Aufsichtsrat: Andreas Lorch, Catrin Lorch, Dr. Edith Baumann-Lorch, Peter Rüb

Redaktion: Christina Kahlen-Pappas (verantwortlich),

Telefon: 0151 27 24 56 63, E-Mail: christina.kahlen-pappas@dfv.de

Verlagsleitung: RA Torsten Kutschke,

Telefon: 069 7595-1151, E-Mail: torsten.kutschke@dfv.de

Anzeigen: Mikhail Tsyganov,

Telefon: 069 7595-2779, E-Mail: Mikhail.Tsyganov@dfv.de

Fachbeirat: Gregor Barendregt, Carl Zeiss AG; Andrea Berneis, Berneis Legal & Compliance; Ralf Brandt, dievini patch Beteiligungs GmbH; Joern-Ulrich Fink, Regulatory Adherence & Compliance Policy Governance, Deutsche Bank AG; Otto Geiß, Deutsches Netzwerk Wirtschaftsethik; Mirko Haase, Hiltl Corporation; Prof. Dr. Katharina Hastenrath, ZHAW Zürcher Hochschule für Angewandte Wissenschaften; Corina Käslér, Senior Advisor, State Street Bank International GmbH; Dr. Karsten Leffrang, General Counsel Germany, Valeo; Prof. Dr. Bartosz Makowicz, Europa-Universität Viadrina Frankfurt/Oder; Thomas Muth, Muth-zur-Entwicklung; Stephan Niemann; Dr. Dietmar Prechtel, Osram GmbH; Dr. Alexander von Reden, Global Compliance, Miele Group; Hartmut T. Renz, Partner STRATECO GmbH; Dr. Barbara Roth, State Street Bank International; Jörg Siegmund, Getzner Textil AG; Eric S. Soong, Group Head Compliance & Corporate Security, Schaeffler Technologies AG & Co. KG; Dr. Martin Walter, selbstständiger Autor, Berater und Referent für Compliance-Themen

Jahresabonnement: kostenlos

Erscheinungsweise: monatlich (10 Ausgaben pro Jahr)

Layout: Uta Struhalla-Kautz, SK-Grafik, www.sk-grafik.de

Jede Verwertung innerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Keine Haftung für unverlangt eingesandte Manuskripte. Mit der Annahme zur Alleinveröffentlichung erwirbt der Verlag alle Rechte, einschließlich der Befugnis zur Einspeicherung in eine Datenbank.

1. Deutscher Entgelttransparenztag

Eine Veranstaltung des

**Compliance
Berater**

03. Juli 2025 | München

Jetzt anmelden!

PROGRAMM

Mittwoch, 02. Juli 2025

ab 19.00 Uhr **Get-Together im Ratskeller München** Marienplatz 8, 80331 München

Donnerstag, 03. Juli 2025

Moderation: *Dr. Michaela Felisiak & Dr. Dominik Sorber*

09.00 Uhr	Begrüßung & Einführung <i>Dr. Michaela Felisiak</i> , Eversheds Sutherland <i>Dr. Dominik Sorber</i> , POELLATH	13.30 Uhr	Speed-Dating „Umsetzung der Entgelttransparenzrichtlinie in den Unternehmen“ mit u.a. <i>Franziska Lorenz</i> , Allianz SE Reinsurance <i>Sophia Budde</i> , GANT <i>Dr. Michael Horcher</i> , Landesarbeitsgericht Hessen <i>Dr. Michaela Felisiak</i> , Eversheds Sutherland <i>Dr. Dominik Sorber</i> , POELLATH
09.15 Uhr	Worauf sollten sich Unternehmen, Tarifvertragsparteien, Beschäftigte und ihre Vertretungen vorbereiten? <i>Dr. Regine Winter</i> , Richterin am Bundesarbeitsgericht a. D.	14.30 Uhr	Gehaltscheck im Profi-Fußball: Hintergrundgespräch mit dem Geschäftsführer von Fortuna Köln <i>Niklas Müller</i> , Fortuna Köln <i>Markus Matt</i> , Journalist & HR-Experte
10.10 Uhr	Transparenz wirkt – Zwischen Kulturwandel und Unternehmensstrategie <i>Liza Torres</i> , accompio	15.00 Uhr	Kaffeepause
10.45 Uhr	Kaffeepause	15.30 Uhr	Zahlen Daten Fakten – oder wie räume ich den Vergütungskleiderschrank auf? <i>Raffaella Stutz</i> , Mercer
11.15 Uhr	Entgelttransparenz-RL – Auswirkungen auf das Verfahrensrecht und insbesondere die Beweislast <i>Dr. Michael Horcher</i> , Landesarbeitsgericht Hessen	16.00 Uhr	Frankreichs Weg zur Entgeltgleichheit: Rechtsrahmen, Urteile und Praxisbeispiele <i>Sylvia Cleff Le Divellec</i> , Cabinet ELAGE (Paris)
12.15 Uhr	Strafrechtliches Minenfeld Betriebsratsvergütung – neue Brisanz durch Entgelttransparenzrichtlinie?! <i>Dr. Oliver Sahan & Dr. Sascha Knaupe</i> , ROXIN	16.30 Uhr	Notfallplan & Checkliste zur Umsetzung der Entgelttransparenz-RL <i>Dr. Michaela Felisiak & Dr. Dominik Sorber</i>
12.45 Uhr	Mittagspause		

REFERIERENDE



Dr. Michaela Felisiak



Franziska Lorenz



Dr. Dominik Sorber



Sophia Budde



Dr. Regine Winter



Niklas Müller



Liza Torres



Markus Matt



Dr. Michael Horcher



Raffaella Stutz



Dr. Oliver Sahan



Sylvia Cleff Le Divellec



Dr. Sascha Knaupe

MEDIENPARTNER

**DATENSCHUTZ-
BERÄTER**

**Kommunikation
& Recht**

**Betriebs
Berater**



JETZT ANMELDEN UNTER
www.ruw.de/entgelt
oder QR-Code scannen

R&W
Fachkonferenzen

Eine Medienmarke der

dfv Mediengruppe

Deutsche Compliance Konferenz 2025

„Unsere Konferenz hat den Anspruch, aus der Praxis für die Praxis zu sein. Dazu müssen wir miteinander reden, uns austauschen, voneinander lernen. Das ist Ihre Konferenz, machen Sie was draus“, appellierte Jörg Bielefeld in seiner Begrüßung zur Deutschen Compliance Konferenz 2025 an die Tagungsteilnehmer. Beste Voraussetzungen hierfür lieferten die Impulse aus 15 Fachbeiträgen und vier hochkarätig besetzten Diskussionsrunden am 13. und 14. Mai. Einen ausführlichen Bericht zur DCK 2025 lesen Sie in Ausgabe 8 des Compliance-Beraters, der am 17. Juli erscheint.



Norbert Tutsch, Dr. Lars Kutzner, Kristina Konrad, Alexander Schmid und Erster Oberstaatsanwalt Karsten Wegerich (v.l.n.r.) diskutierten moderiert von Jörg Bielefeld über Compliance im Vertrieb.



Die Bedeutung der Boulevardpresse im Wirtschaftsstrafverfahren erläuterte Richter Prof. Dr. Matthias Jahn.



Prof. Dr. Dennis-Kenji Kipker hob den Stellenwert einer ganzheitlichen digitalen Resilienzstrategie hervor.



Kristina Konrad erläuterte am Beispiel Hamburg Compliance-Anforderungen kommunaler Unternehmen.



Zu Sanktionscompliance lieferten Norbert Tutsch und Alexander Schmid Praxisbeispiele.



Dr. Dietmar Deffert setzt bei der TUI AG auf eine „schnelle Eingreiftruppe“ bei Hinweisen auf Compliance-Vorfälle.



Marijke van der Most und Dr. Timo Handel berichteten zu Fallstricken und Best Practices beim Hinweisgeberschutz.



Sebastian Rünz referierte zu CSDDD, LKSG und den Effekten des Omnibus-Pakets der EU-Kommission.



„Alles was in NIS2 vorgeschrieben wird, sollten Sie sowieso machen“, mahnte Stefan Becker vom BSI (r.). Mit ihm in der Diskussion Eileen Müller.



Drei Strafrechtler zu den rechtspolitischen Entwicklungen: Jörg Bielefeld, Karsten Wegerich und Prof. Dr. Matthias Jahn.

© Christina Kahler-Pappas

Der Data Act – das neue Zugpferd der Datenwirtschaft?

Eine Veranstaltung von

DATENSCHUTZ-
BERÄTER

in Kooperation mit

PLANIT//LEGAL

03. Juli 2025 | Frankfurt am Main

Jetzt anmelden!

ES ERWARTEN SIE UNTER ANDEREM DIESE THEMEN

- Allgemeine Einführung in den Data Act
- Das Zusammenspiel zwischen Data Act und DS-GVO
- Datenzugang und -weitergabe nach dem Data Act sowie deren Grenzen
- Datennutzungsverträge – Inhalte auch im Hinblick auf die Kommissionsvorschläge und Umsetzung
- Unentgeltliche Herausgabe von Daten nach dem Data Act – das Ende
- Data Act am Beispiel der Automobil-Branche
- Cloud Switching: Interoperabilität bei Cloud-Diensten
- KI-Trainingsdaten aus dem Data Act
- Der Data Act – Umsetzung aus Sicht einer Datenschutzaufsichtsbehörde

FREUEN SIE SICH AUF NEUE IMPULSE DURCH DIESE UND VIELE WEITERE REFERENT:INNEN



Kirsten Ammon
PLANIT//LEGAL



Dr. Michael Eginger
Körber Supply Chain
Logistics GmbH



Susanne Enengl
Springtime
Technologies



Marc Stefan Fein
Kia Connect
GmbH



Thomas Fuchs
Der Hamburgische Beauftragte
für Datenschutz und
Informationsfreiheit



Dr. Tina Gausling
Simmons &
Simmons



Matthias Götz
Nikol & Goetz
Rechtsanwälte



Philippe Heinzke
CMS Hasche
Sigle



Carolin Loy
Bayerisches Landesamt
für Datenschutzaufsicht



Dr. Carlo
Piltz
Piltz Legal



Dr. Anna-
Kristina Roschek
PLANIT//LEGAL



Dr. Kristina Schreiber
Loschelder
Rechtsanwälte



Rebekka
Weiß
Microsoft

Ihr Ansprechpartner: Herr Jasha Baniashraf

Senior Projektmanager
Tel.: +49 69 7595-2773
E-Mail: Jasha.Baniashraf@dfv.de
Deutscher Fachverlag GmbH
Mainzer Landstr. 251
60326 Frankfurt am Main

Veranstaltungsort:

dfv Mediengruppe
Mainzer Landstraße 251
60326 Frankfurt am Main

**Frühbucherrabatt
bis 15. April 2025
sichern!**



**Inklusive Fortbildungsbescheinigung über
6 Stunden und 20 Minuten nach § 15 FAO.**



JETZT ANMELDEN UNTER
www.ruw.de/data-act
oder QR-Code scannen

R&W
Fachkonferenzen

Eine Medienmarke der

dfv Mediengruppe

Studie: Wenig Vertrauen in Fähigkeiten beim Datenschutz

So schnell wie sich die Digitalisierung weiterentwickelt, so dringend muss der Datenschutz zu einem entscheidenden Geschäftsprinzip werden. Jedoch haben laut der ISACA-Studie „State of Privacy 2025“ nur 38 Prozent der europäischen Fachleute Vertrauen in die Fähigkeit ihres Unternehmens, sensible Daten zu schützen. Dabei ist der Austausch personenbezogener Daten ein wichtiger Bestandteil moderner Geschäftsabläufe, so dass schwache Schutzmechanismen die Glaubwürdigkeit von Unternehmen untergraben und Misstrauen in Kundenbeziehungen schaffen. Die Auswirkungen spiegeln sich in den Umsätzen.



Datendiebstahl: Sensible Daten zu schützen, ist für viele Unternehmen keine leichte Aufgabe.



Chris Dimitriadis ist Chief Global Strategy Officer, ISACA.

Es gibt mehrere Gründe für die Vertrauenskrise unter den Datenschutzbeauftragten: 45 Prozent halten das Datenschutzbudget ihres Unternehmens für unterfinanziert und mehr als die Hälfte (54 Prozent) der Befragten rechnet mit weiteren Budgetkürzungen innerhalb des nächsten Jahres. Die Unterfinanzierung zeigt sich in Personalmangel: 52 Prozent der technischen Datenschutzteams geben an, unterbesetzt zu sein, und mehr als ein Drittel (37 Prozent) hat Schwierigkeiten, qualifizierte Datenschutzbeauftragte zu finden. Verschärft wird die Situation durch die Komplexität und Entwicklung der aktuellen Bedrohungslandschaft. Kein Wunder, dass zwei Drittel (66 Prozent) der befragten Fachleute angeben, ihre Arbeit sei heute stressiger als noch vor fünf Jahren.

Wichtige Meilensteine der regulatorischen Landschaft wie die EU-Gesetzgebung zur künstlichen Intelligenz, der Corporate Governance Kodex und die Datenschutz-Grundverordnung wirken sich positiv auf den Datenschutz in Europa aus. Diese Verordnungen bieten Organisationen Orientierung, um ihren Umgang mit dem Datenschutz zu optimieren.

Um jedoch Compliance zu erreichen und strenge Datenschutzstandards aufrechtzuerhalten, müssen Unternehmen die strukturellen Herausforderungen angehen – angefangen bei verstärkten Investitionen in Datenschutzmitarbeitende, die Zugang zu umfassenden Schulungen und Ressourcen erhalten. Organisationen, die Privacy by Design immer praktizieren, erreichen bei der Schließung der Qualifikationslücke im Bereich des Datenschutzes bereits entscheidende Fortschritte – 56 Prozent bieten Schulungen für Mitarbeitende an, die nicht im Bereich des Datenschutzes tätig

sind und in diesen Bereich wechseln wollen, verglichen mit 44 Prozent in Unternehmen, die Privacy by Design nicht praktizieren.

KI hat die Arbeitswelt in vielen Branchen verändert. Laut der ISACA-Studie „State of Privacy 2025“ setzen 37 Prozent der Unternehmen bereits KI für datenschutzrelevante Aufgaben wie Datenklassifizierung, Risikoanalyse und Compliance-Überwachung ein oder planen deren Einsatz. Die Technologie kann Prozesse beschleunigen, Routineaufgaben automatisieren und menschliche Fehler reduzieren.

Doch da KI-Technologien am Arbeitsplatz immer zugänglicher werden, stehen sie auch Cyberkriminellen offen. Allerdings sind nur 35 Prozent der Cybersicherheitsteams in Unternehmen an der Entwicklung von KI-Richtlinien beteiligt und 45 Prozent überhaupt nicht in die KI-Governance eingebunden. Aus Sicht des Datenschutzes ist es entscheidend, dass Unternehmen geschult werden, um mit den Angreifern Schritt zu halten, deren Angriffe zu erkennen und abzuwehren und zu verhindern, dass wichtige Daten in Gefahr geraten.

Es gibt drei grundlegende Schritte, die Unternehmen umsetzen sollten, um ihre Datenschutzteams zu unterstützen und sicherzustellen, dass sie effektiv arbeiten können.

Erstens: die Schließung der Qualifikationslücke. Fast die Hälfte (47 Prozent) der europäischen Organisationen bildet bereits Mitarbeitende, die nicht im Bereich des Datenschutzes tätig sind, zu Datenschutzbeauftragten aus. Bemerkenswert ist, dass 89 Prozent der Befragten Zertifizierungen gegenüber Hochschulabschlüssen (54 Prozent) den Vorzug geben.

Zweitens: die Nutzung neuer Technologien wie künstlicher Intelligenz. Investitionen in die Schulung

von Datenschutzexperten können dazu beitragen, wertvolle Ressourcen freizusetzen und eine sichere Nutzung zu gewährleisten.

Drittens: die Priorisierung des Datenschutzes. Angesichts neuer und anhaltender Bedrohungen müssen Geschäftsleitungen in Datenschutzteams investieren und den Datenschutz in ihre übergreifenden Unternehmensstrategien integrieren, um kostspielige, reputationsschädigende Auswirkungen in der Zukunft zu vermeiden.

Datenschutz ist eine geschäftliche Notwendigkeit. Unternehmen, die nicht in den Datenschutz investieren, riskieren Rufschädigung, behördliche Sanktionen und den Verlust des Kundenvertrauens. Führungskräfte müssen jetzt handeln und in Mitarbeitende, Prozesse und Technologien investieren, um eine robuste und zukunftsorientierte Datenschutzstrategie aufzubauen.

Chris Dimitriadis

Die Studie „State of Privacy 2025“ untersucht unter anderem die Priorisierung des Datenschutzes durch Vorstände, die Einhaltung von Datenschutzvorgaben, den Einsatz von Künstlicher Intelligenz im Datenschutz, Schulungen zum Datenschutzbewusstsein, Datenschutzverletzungen und die Rolle von „Privacy by Design“. Die Ergebnisse basieren auf der fünften jährlichen globalen Datenschutz-Umfrage von ISACA, die im September 2024 durchgeführt wurde. Mehr als 1.600 Personen aus dem Berufsfeld „Datenschutz“ nahmen an der Umfrage teil. 38 Prozent waren in Managementpositionen tätig, 29 Prozent gehörten zur oberen Führungsebene, 20 Prozent waren Einzelmitarbeitende und 12 Prozent Teil der Geschäftsleitung.

Hybrid-Veranstaltung: Teilnahme vor Ort sowie Online möglich!

Datenschutzkonferenz 2025

Praxis | Recht | Innovation

24. - 26. September 2025 | Hotel Kö59 Düsseldorf

ES ERWARTEN SIE UNTER ANDEREM DIESE THEMEN

- Datenerwerb im Unternehmenskauf – so geht's!
- Update Beschäftigendatenschutz
- Vom Chaos zur Perlenkette: Ein bereichsübergreifender Compliance-Prozess für mehr Awareness und Effizienz
- Verhandlungen, Verständigungen und Deals mit den Datenschutzbehörden
- Grenzenlose Unsicherheit? Drittlandtransfers zwischen Risiko und Regulierung
- Fotoaufnahmen im Unternehmensalltag: Zwischen Recht am eigenen Bild und Datenschutz
- KI und Datenschutz aus aufsichtsbehördlicher Perspektive
- Training von Datenschutzkoordinatoren im Unternehmen – Wertschätzung und Wissensvermittlung als Schlüssel für ein funktionierendes DSMS
- AI (Act) aus der Sicht des DSB
- The more the merrier? Herausforderungen bei der Datenschutzumsetzung in Netzwerken und ähnlichen Strukturen
- Aktuelles aus dem EDSA
- „Allein auf weiter Flur?“ – Der DSB zwischen Loyalitätsdruck und Behördenschutz
- Good Cop, Bad Cop? Datenschutzfälle aus Sicht der Aufsicht und der Beratung

FREUEN SIE SICH AUF NEUE IMPULSE DURCH DIESE UND VIELE WEITERE REFERENT:INNEN



Dr. Jens Ambrock
HmbBfDI



Dr. Jens Eckhardt
BvD e.V.



Anna Eickmeier
YPOG Rechtsanwältin



Dr. Diana Ettig
Spirit Legal



Daniel Gabel



Inna Gendelman
Scout24



Dr. Jan-Michael Grages
KNPZ Rechtsanwältin



Stephan Hansen-Oest
Rechtsanwalt



Dr. Nina Elisabeth Herbort
Short Law



Prof. Dr. Tobias Keber
LfDi BaWü



Carolin Loy
BayLDA



Dr. Carolin Monsees
Taylor Wessing



Dr. Flemming Moos
Osborne Clarke



Dr. Aileen Pasquariello
L'Oréal Austria Germany



Dr. Ruben Schneider
BfDI



Dr. Dominik Sorber
POELLATH



Dr. Lea Stegemann
Noerr



Laura L. Stoll
intersoft consulting
services AG



Henrike Teitge
BlnBDI



Mona Wrobel
TeamViewer
Germany GmbH



Tim Wybitul
Latham & Watkins

Ihr Ansprechpartner: Herr Jasha Baniashraf

Senior Projektmanager
Deutscher Fachverlag GmbH
Tel.: +49 69 7595-2773
E-Mail: Jasha.Baniashraf@dfv.de

Veranstaltungsort:

Hotel Kö59 Düsseldorf
Königsallee 59
40215 Düsseldorf

Eine Fortbildungsbescheinigung nach § 15 FAO für Ihre berufliche Weiterbildung wird erteilt.



JETZT ANMELDEN UNTER
www.datenschutzkonferenz.de
oder QR-Code scannen

R&W
Fachkonferenzen

Eine Medienmarke der
dfv Mediengruppe