Compliance
Die Zeitschrift für Compliance-Verantwortliche

Juni 2026

Inhalt

Aufmacher

Mehr Vertrauen – weniger Bürokratie

Die Politik steht unter Druck: Bürgerinnen und Bürger, Unternehmen und Kommunen verlangen schnellere, digitale und bürgerfreundlichere Entscheidungen – bei gleichzeitig knappen Ressourcen. Vor allem aber erwarten sie, dass der Dschungel an Vorschriften, mit denen sie konfrontiert sind, gelichtet wird. Wie die Hessische Landesregierung hierauf reagiert, erläutert der Hessische Staatsminister Manfred Pentz in unserem Aufmacher.

Praxis

„Datenschutzverstöße können interne Ermittlungen selbst zum Risiko machen"
Seit Inkrafttreten des Hinweisgeberschutzgesetzes stehen interne Ermittlungen in einem besonderen Spannungsfeld. Eileen Baumann, Syndikusrechtsanwältin im Konzerndatenschutz der Deutschen Bahn AG, erläutert im Interview, welche rechtlichen Grenzen bei Mitarbeiterinterviews, E-Mail-Auswertungen und IT-forensischen Maßnahmen gelten.

Praxis

AMLA und der Wandel zur datengetriebenen Geldwäscheaufsicht
Mit der Anti-Money Laundering Authority (AMLA) in Frankfurt am Main beginnt ein neues Aufsichtsverständnis in der Bekämpfung von Geldwäsche und Terrorismusfinanzierung. Unter Vorsitz von Bruna Szego, zuvor Leiterin der Einheit für AML-Aufsicht und -Regulierung bei der Banca d'Italia, verfolgt die AMLA einen standardisierten, datengetriebenen Risikoanalyseansatz mit einheitlichen Datenpunkten und harmonisierten Risikokategorien.

Recht

KI-Kompetenz als Fundament wirksamer KI-Compliance
Die Förderung von KI-Kompetenz ist ein zentrales Anliegen der EU-KI-Verordnung. Im Zuge laufender Entbürokratisierungsbemühungen der EU („Digital Omnibus") wurde diskutiert, ob Unternehmen von ihrer primären Verantwortung zur Sicherstellung der KI-Kompetenz befreit werden sollten. Martin Schulz und Maximilian Vonthien beantworten diese Frage klar mit „nein" und zeigen, dass die Entwicklung von KI-Kompetenz durch adäquate Schulungen Bestandteil der Compliance-Pflicht ist.

Veranstaltungen

10.&11.06.2026 | Frankfurt am Main | **Deutsche Compliance Konferenz 2026**

11.06.2026 | München | **1. Münchner Data Litigation Forum**

23.06.2026 | Online | **Microsoft 365 & Copilot**

25.06.2026 | Online | **Compliance & KI 2.0**

29.06.2026 | kostenfreies Webinar | **Volle KI-Power, höchster Datenschutz**

08.07.2026 | kostenfreies Webinar | **Soll KI die Passwörter kennen?**

Mehr Vertrauen – weniger Bürokratie

Die Politik steht unter Druck: Bürgerinnen und Bürger, Unternehmen und Kommunen verlangen schnellere, digitale und bürgerfreundlichere Entscheidungen – bei gleichzeitig knappen Ressourcen. Vor allem aber erwarten sie, dass der Dschungel an Vorschriften, mit denen sie konfrontiert sind, gelichtet wird. Wie die Hessische Landesregierung hierauf reagiert, erläutert der Hessische Staatsminister Manfred Pentz in unserem Aufmacher.

© Salome Roessler

Manfred Pentz, Minister für Bundes- und Europaangelegenheiten, Internationales und Entbürokratisierung und Bevollmächtigter des Landes Hessen beim Bund.

Nach einer Umfrage des ifo Instituts 2025 sehen knapp 40 Prozent der Unternehmen die Entschlackung der Bürokratie als wichtigstes Themenfeld für die aktuelle Legislaturperiode im Bund. Um dieser Erwartung der Bevölkerung gerecht zu werden, hat die Hessische Landesregierung das Erste Bürokratieabbaugesetz mit 120 Einzeländerungen in 90 Gesetzen auf den Weg gebracht. Am 1.1.2026 ist es in Kraft getreten. Darin setzen wir insbesondere auf zwei Grundsätze:

1. „Vertrauen statt Misstrauen": Behörden verzichten auf pauschale Nachweispflichten (z. B. Geburtsurkunden, Führungszeugnisse) und setzen auf digitale Kopien oder Eigenerklärungen.

2. „Digital statt Papier": Die Schriftform wird in Verwaltungsverfahren grundsätzlich durch die Textform ersetzt – eine E-Mail reicht oft aus, da die händische Unterschrift entfällt. Das spart Zeit, Kosten und auch Nerven.

Ein dritter Grundsatz wird das Zweite Bürokratieabbaugesetz prägen, zu dem wir bereits Eckpunkte verabschiedet haben: „Orientierung am Regelfall, nicht an der Ausnahme". Die klare Formulierung von Regelungszielen soll die detaillierte Aufzählung sämtlicher denkbarer Sonderfälle im Gesetz ersetzen. So hat es die hessische Landesregierung in ihren „Zielen und Grundsätzen der Regulierung" festgelegt.

Die Umsetzung dieses Prinzips in die Tat ist allerdings nicht ganz einfach. Denn das Denken in Ausnahmen und Risikoszenarien und der daraus folgende Drang, kleinteilige, umfangreiche Regelwerke zu entwickeln, ist in der deutschen Regelungskultur fest verankert. Hier brauchen wir einen Kulturwandel in den Verwaltungen, ein „Umparken im Kopf", wie es ein Automobilhersteller mal genannt hat. Dieser Regelungsansatz kommt nicht nur in staatlichen Rechtsvorschriften zum Ausdruck. Das Problem stellt sich auch und sogar besonders drängend bei Standards und Regelwerken, die nicht von staatlichen Institutionen geschaffen wurden, sondern von privaten Normungsgremien. Ein Beispiel: Vor kurzem wurden in mehreren Presseberichten Vorgaben zur Mindesthöhe von Treppen thematisiert. Ausführungen hierzu finden sich unter anderem in der 49 Seiten langen DIN 18065 „Gebäudetreppen – Begriffe, Messregeln, Hauptmaße" und der 28 Seiten langen DGUV (Deutschen Gesellschaft für Unfallversicherungen) Information 208–005 „Treppen". Nach Angaben des Deutschen Normungsinstituts DIN umfasst allein das Deutsche Normenwerk rund 33.500 Normen; jedes Jahr werden in Deutschland etwa 2.000 neue oder überarbeitete DIN-Normen veröffentlicht. So sind beim Bauen nach Branchenschätzungen rund 3.900 Normen zu beachten. Zum Vergleich: Die Gesetze und Verordnungen des Hessischen Landesrechts umfassen etwa 19.000 Paragrafen. Wenn man sich den Umfang der Regelwerke von Normungsgremien vor Augen führt, nimmt sich diese Zahl fast schon bescheiden aus.

An sich sind diese Regelwerke nicht verbindlich. Wegen der zahlreichen Verweise in Gesetzen und Verordnungen auf den „Stand der Technik" erhalten sie faktisch dennoch häufig Rechtsqualität. Selbst wenn es an solchen Verweisen fehlt, beziehen sich Behörden häufig dennoch pauschal bei Auflagen und Kontrollen auf solche Standards. Gleiches gilt für die Rechtsprechung. Auch Sie als Compliance-Verantwortliche in den Unternehmen wird die Frage beschäftigen, wie sie mit den Festlegungen in solchen Regelwerken umgehen.

Das Problem: Zum einen ist die Zahl der Vorgaben sehr groß, zum anderen werden diese stetig weiterentwickelt und verschärft – mit Auswirkungen auf den Erfüllungsaufwand für die Unternehmen. Nach unserer Wahrnehmung überfordern solche starren Verweise auf den „Stand der Technik" Unternehmen und Kommunen. Wir werden daher in unserem Zweiten Bürokratieabbaugesetz solche Verweise aus den Hessischen Gesetzen und Verordnungen streichen. So beenden wir den Automatismus, dass privat geschaffene Normen ohne staatliche Prüfung verbindlich werden.

Im Dezember 2025 haben die Ministerpräsidentinnen und -präsidenten gemeinsam mit dem Bundeskanzler die Föderale Modernisierungsagenda beschlossen. Sie enthält 237 teilweise sehr konkrete Maßnahmen zum Bürokratieabbau – vom Abbau von Berichts- und Dokumentationspflichten, über die Beschleunigung von Verwaltungsverfahren hin zu Vereinfachungen beim Vergaberecht oder Datenschutz. Bei diesem und vielen weiteren Themen des Bürokratieabbaus bohren wir dicke Bretter. Was mich dabei optimistisch stimmt: Es gibt nicht nur in Hessen ein Momentum für die Entbürokratisierung: Bund und Länder ziehen an einem Strang. Die beste Zeit für Bürokratieabbau ist jetzt! *Manfred Pentz*

Mehr zu politischen Maßnahmen und dazu, wie Landesregierungen Unternehmen durch Entbürokratisierung unterstützen können, erfahren Sie bei der Deutschen Compliance Konferenz 2026 am 10. und 11. Juni 2026 in Frankfurt a.M. Lernen Sie hier auch Dr. *Tobias Miethaner* kennen, der die neu eingerichtete Stabsstelle Entbürokratisierung in der Hessischen Staatskanzlei bei Staatsminister *Manfred Pentz* leitet, und einer der hochkarätigen Referenten unserer Konferenz ist.

Informationen und Anmeldung:
www.ruw.de/dck

Compliance & KI 2.0 – Das Update

Bereit für den rechtssicheren Einsatz künstlicher Intelligenz nach der KI-VO

Basis- & Aufbau-Webinar

Eine Veranstaltung der Kommunikation & Recht

25. und 26. Juni 2026, 09.00 bis 12.00 Uhr | Zoom

weiterer Termin: 17. & 18. September

BASIS-WEBINAR Donnerstag, 25. Juni
KI-Compliance verstehen

- **Einführung und Rahmen der KI-Regulierung**
- **Technische Basics & Anwendungsmöglichkeiten von KI**
- **Grundlagen der Risikoklassifizierung und Folgecompliance**
  - Überblick und Anwendungsbeispiele
  - Compliance bei Hochrisiko-KI-Systemen
  - Anforderungen für sonstige KI-Systeme und KI-Modelle
  - Praktische Herausforderungen
- **Rahmen und Umsetzungsbeispiele von KI-Kompetenz nach Art. 4 KI-VO**
- **Fragestellungen beim Einsatz von GenAI**
- **Überblick zu datenschutzrechtlichen Fragestellungen**
- **Normative Schnittstellen der KI-VO**
- **Tipps und Praxisbeispiele**

AUFBAU-WEBINAR Freitag, 26. Juni
KI-Compliance in der Praxis

- **Das Omnibus-Paket auf der Zielgeraden**
  - Aktueller Entwicklungsstand und welche Auswirkungen hat dieser auf Ihre KI-Compliance
- **Deep dive und best practices bei der Verwendung von Hochrisiko-KI-Systemen**
  - Umsetzungsbeispiele von Compliance bei Hochrisiko-KI-Systemen und Normierungsstand
- **Nationales Durchführungsgesetz der KI-VO**
- **Einordnung und Verwendung von RAG-Systemen**
  - Compliance nach der KI-VO und datenschutzrechtliche Aspekte
- **Klassifizierung und Einordnung von Agentic AI**
- **Aufbau einer eigenen KI-Governance in der Organisation**
- **Wichtige Punkte bei Third-Party KI-Systemen**
- **Tipps und Praxisbeispiele**

SEMINARLEITER & MODERATOR

Dr. Robert Müller, LL.M.

Aufbau-Webinar auch einzeln buchbar!

Jetzt anmelden & KI-Kompetenzen nach Art. 4 KI-VO sichern!

Ihre Ansprechpartnerin:
Frau Maria Belz
Projektmanagerin

Deutscher Fachverlag GmbH
Tel.: +49 69 7595-1157
E-Mail: Maria.Belz@dfv.de

Teilnahmegebühren (zzgl. MwSt.):
359,– EUR Abonnent:innen K&R, CB, DSB
449,– EUR Normalpreis

Sie möchten auf das Basis-Webinar verzichten und nur am Aufbau-Webinar teilnehmen? Dann erhalten Sie **50 % Rabatt.** Weitere Informationen unter www.ruw.de/COKI.

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

// WIR FEIERN **80 JAHRE** /

R&W Fachkonferenzen

Eine Medienmarke der dfv Mediengruppe

„Datenschutzverstöße können interne Ermittlungen selbst zum Risiko machen"

Seit Inkrafttreten des Hinweisgeberschutzgesetzes stehen interne Ermittlungen in einem besonderen Spannungsfeld: Unternehmen müssen Verdachtsfällen aus Meldungen konsequent nachgehen – zugleich bewegen sie sich dabei in einem hochsensiblen datenschutzrechtlichen Rahmen. Eileen Baumann, Syndikusrechtsanwältin im Konzerndatenschutz der Deutschen Bahn AG, erläutert im Interview, welche rechtlichen Grenzen bei Mitarbeiterinterviews, E-Mail-Auswertungen und IT-forensischen Maßnahmen gelten.

© privat

Eileen Baumann ist Syndikusrechtsanwältin im Konzerndatenschutz der Deutschen Bahn AG und zertifizierte Datenschutzbeauftragte, Whistleblowing- und Compliance-Officer. Ihre Schwerpunkte liegen im Beschäftigtendatenschutz, Compliance und der Privacy Litigation.

Compliance: Interne Ermittlungen haben durch das Hinweisgeberschutzgesetz zusätzlich an Bedeutung gewonnen. Warum eigentlich?

Baumann: Weil interne Meldestellen nach dem HinSchG nicht nur Hinweise entgegennehmen, sondern auch angemessene Folgemaßnahmen ergreifen müssen. Dazu können nach § 18 Nr. 1 HinSchG ausdrücklich interne Untersuchungen gehören. Unternehmen stehen damit häufiger vor der Frage: Wie klären wir einen Verdacht effektiv auf – ohne Datenschutzrecht zu verletzen?

Compliance: Welche Konstellationen sind in der Praxis typisch?

Baumann: Oft geht es um Hinweise auf Compliance-Verstöße, Untreue, Korruption oder Datenschutzverletzungen. Sobald ein Hinweis plausibel erscheint, folgen meist erste Aufklärungsmaßnahmen: Interviews, E-Mail-Auswertungen oder IT-forensische Analysen. Genau dort beginnt aber das Spannungsfeld zwischen Aufklärungsinteresse und informationeller Selbstbestimmung der Betroffenen.

Compliance: Warum ist Datenschutz dabei ein so sensibles Thema?

Baumann: Weil interne Ermittlungen zwangsläufig personenbezogene Daten betreffen – von Hinweisgebern, beschuldigten Beschäftigten oder Zeugen. Die DSGVO gilt dabei uneingeschränkt. Anders als staatliche Ermittlungsbehörden können sich Unternehmen nicht auf Sonderbefugnisse berufen. Jede Maßnahme braucht eine belastbare Rechtsgrundlage und muss verhältnismäßig sein.

Compliance: Welche Rechtsgrundlagen kommen typischerweise in Betracht?

Baumann: Zentral ist zunächst § 26 Abs. 1 Satz 2 BDSG. Danach dürfen Beschäftigtendaten zur Aufdeckung von Straftaten verarbeitet werden, wenn ein dokumentierter tatsächlicher Verdacht besteht und die Maßnahme erforderlich ist. Wichtig ist: Bloße Vermutungen reichen nicht aus. Außerdem greift die Norm nur bei Straftaten – nicht bei bloßen Pflichtverletzungen.

Compliance: Und wenn gerade keine Straftat im Raum steht?

Baumann: Dann wird häufig auf Art. 6 Abs. 1 DSGVO zurückgegriffen, insbesondere auf lit. b, c oder f. Relevant ist etwa die Verarbeitung zur Erfüllung arbeitsvertraglicher Pflichten oder aufgrund berechtigter Interessen des Unternehmens. Zusätzlich kann sich die interne Meldestelle auf §§ 10, 13 HinSchG in Verbindung mit Art. 6 Abs. 1 lit. c DSGVO stützen, solange die Verarbeitung der Aufgabenwahrnehmung der Meldestelle dient.

Compliance: Könnte hier nicht auch auf § 26 Abs. 1 Satz 1 BDSG zurückgegriffen werden?

Baumann: Wegen der EuGH-Rechtsprechung bestehen erhebliche Zweifel an der Europarechtskonformität der Vorschrift. Der EuGH hat vergleichbare nationale Regelungen beanstandet, weil sie lediglich den Wortlaut der DSGVO wiederholen, ohne den Beschäftigungskontext näher auszugestalten. Deshalb sollte man sich bei internen Ermittlungen nicht mehr unkritisch auf § 26 Abs. 1 Satz 1 BDSG verlassen.

Compliance: Welche datenschutzrechtlichen Grundsätze werden in Ermittlungen besonders relevant?

Baumann: Vor allem Zweckbindung, Datenminimierung, Verhältnismäßigkeit und Vertraulichkeit. Unternehmen müssen sehr genau definieren, was eigentlich aufgeklärt werden soll. Daraus ergibt sich dann, welche Daten wirklich benötigt werden. Ein typischer Fehler ist es, zu breit zu ermitteln – etwa sämtliche E-Mails eines Mitarbeiters über Jahre hinweg auszuwerten, obwohl der Verdacht nur einen kurzen Zeitraum betrifft.

Compliance: Das klingt nach erheblichem organisatorischem Aufwand.

Baumann: Ja, aber dieser Aufwand schützt vor erheblichen Risiken. Datenschutzverstöße können interne Ermittlungen selbst zum Risiko machen und Bußgelder, Schadensersatzansprüche oder sogar strafrechtliche Risiken nach sich ziehen. Außerdem gefährden schlecht dokumentierte Ermittlungen die spätere Verteidigung vor Behörden oder Gerichten.

Compliance: Bleiben wir bei den Ermittlungsmaßnahmen. Was gilt für Mitarbeiterinterviews?

Baumann: Interviews sind datenschutzrechtlich ebenfalls Datenverarbeitungen. Anders als im Strafverfahren gibt es zwar keine klassische Belehrungspflicht nach § 136 StPO. Dennoch verlangen Transparenz und Fairness, dass Betroffene wissen, worum es geht und wie ihre Angaben verwendet werden. Gleichzeitig gilt auch im Arbeitsverhältnis der nemo-tenetur-Grundsatz: Niemand muss sich selbst belasten.

Compliance: Besonders konfliktträchtig dürfte die Auswertung von E-Mails sein.

Baumann: Absolut. Gerade wenn private Nutzung erlaubt oder geduldet wurde, ist besondere Zurückhaltung geboten. Unternehmen sollten die Sichtung strikt auf relevante Zeiträume, Personen und Suchbegriffe beschränken. Oft ist ein „Data Freeze" zunächst das mildere Mittel, bevor Inhalte ausgewertet werden. Der Grundsatz lautet immer: so wenig Eingriff wie möglich, aber so viel wie nötig.

Compliance: Wie sieht es bei Videoüberwachung oder IT-Forensik aus?

Baumann: Dort gelten besonders strenge Verhältnismäßigkeitsanforderungen. Eine flächendeckende Dauerüberwachung wegen Bagatellverdachts wäre klar unzulässig. Auch bei IT-forensischen Analysen muss sauber zwischen dienstlichen und privaten Daten getrennt werden – insbesondere bei „Bring your own device"-Konstellationen. Außerdem sind regelmäßig Mitbestimmungsrechte des Betriebsrats zu beachten.

Compliance: Was empfehlen Sie Unternehmen ganz praktisch?

Baumann: Interne Ermittlungen sollten nicht erst im Krisenfall organisiert werden. Sinnvoll sind klare Prozesse, Betriebsvereinbarungen und abgestimmte Datenschutzkonzepte. Der Datenschutzbeauftragte sollte früh eingebunden werden. Bei besonders eingriffsintensiven Maßnahmen kann zudem eine Datenschutz-Folgenabschätzung erforderlich sein.

Mehr zu Internen Ermittlungen als Folgemaßnahmen nach § 18 HinSchG und den vielfältigen weiteren praktischen Auswirkungen des Hinweisgeberschutzgesetzes erfahren Sie bei der Deutschen Compliance Konferenz 2026 am 10. und 11. Juni 2026 in Frankfurt a.M. im Themenblock „Drei Jahre Hinweisgeberschutzgesetz – Zeit für eine Evaluierung". Lernen Sie hier *Eileen Baumann* persönlich kennen, die gemeinsam mit Dr. *Timo Handel* referieren wird. Informationen und Anmeldung: www.ruw.de/dck

Hybrid-Veranstaltung: Teilnahme vor Ort sowie Online möglich!

Datenschutzkonferenz 2026

Praxis | Recht | Innovation

23. – 25. September 2026 | Hotel Kö59 Düsseldorf

ES ERWARTEN SIE UNTER ANDEREM DIESE THEMEN

- Entwicklungen im Datenschutzrecht aus rechts-politischer Sicht
- Folgen des digitalen Omnibus für die Praxis
- Datenschutz auch ohne Beauftragten?
- Videoüberwachung – Rechtliche Vorgaben und Enforcement
- AI Agents zwischen Autonomie und Aufsicht. Warum bestehende Datenschutz und Governance Konzepte nicht mehr ausreichen
- Wenn Aufsicht und Beratung aufeinandertreffen: Datenschutzfälle im Realitätscheck
- 10 Jahre Breyer – 10 Mythen zum Personenbezug
- KI braucht Daten. Der Datenschutz braucht Grenzen. Wer gewinnt?
- E-Mail-Marketing & Datenschutz in 2026: Risiken, Chancen & Best Practice
- Datenschutzherausforderungen eines internationalen Konzerns
- Der DSB-Tätigkeitsbericht: Vom Papiertiger zum Gamechanger
- Beschäftigtendatenschutz aus der Perspektive der Aufsicht
- AI und DSGVO – Datenschutz als Maßstab aller EU-Digital-rechtsakte?
- Melderegime im EU-Digitalrecht (KI-VO, DSGVO, BSIG, CRA und DORA)

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


Dr. Hans-Joachim Arnold
Lufthansa Group


Eileen Baumann
Deutsche Bahn AG


Stephan Hansen-Oest
Rechtsanwalt


Katja Horlbeck
HBDI


Prof. Dr. Tobias Keber
LfDi BaWü


Henrike Kopp-Teitge
BlnBDI


Carolin Loy
BayLDA


Dr. Jan-Peter Ohrtmann
PwC Legal


Dr. Aileen Pasquariello
L'Oréal Austria Germany


Dr. Ruben Plum-Schneider
BfDI


Wiebke Reuter
Taylor Wessing


Dr. Tobias Rothkegel
Osborne Clarke


David Sänger
GEA Group AG


Kathrin Schürman
Schürmann Rosenthal Dreyer


Olga Seewald
Capgemini Invent


Dr. Dominik Sorber
POELLATH


Michael Will
BayLDA


Nico Winter
Dentons


Dr. Markus Wünschelbaum
HmbBfDI


Tim Wybitul
Latham & Watkins


Sarah Johanna Zech
Allianz SE

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 über 15 Stunden nach § 15 FAO sowie 15 CPE-Credits für die IAPP-Zertifizierung werden erteilt.

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

// WIR FEIERN **80 JAHRE** /

R&W Fachkonferenzen

Eine Medienmarke der dfv Mediengruppe

AMLA und der Wandel zur datengetriebenen Geldwäscheaufsicht

Mit der Anti-Money Laundering Authority (AMLA) in Frankfurt am Main beginnt ein neues Aufsichtsverständnis in der Bekämpfung von Geldwäsche und Terrorismusfinanzierung. Unter Vorsitz von Bruna Szego, zuvor Leiterin der Einheit für AML-Aufsicht und -Regulierung bei der Banca d'Italia, verfolgt die AMLA einen standardisierten, datengetriebenen Risikoanalyseansatz mit einheitlichen Datenpunkten und harmonisierten Risikokategorien.

© IMAGO / HMB-Media

AMLA-Chefin Bruna Szego lässt keinen Zweifel daran, dass ihr Risikoanalyseansatz durch ihre frühere Tätigkeit bei der Banca d'Italia geprägt ist.

Vor einem Jahr hat die AMLA in Frankfurt am Main ihre Arbeit aufgenommen. Damit wird es Zeit, diese erste zentrale europäische Aufsichtsbehörde für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung in den Blick zu nehmen. Ziel der Behörde ist es, das öffentliche Interesse, die Stabilität und Integrität des Finanzsystems der Union sowie das reibungslose Funktionieren des Binnenmarkts zu schützen.

Die AMLA wurde im Rahmen des europäischen AML-Pakets eingerichtet, um die bislang fragmentierte Aufsicht innerhalb der EU zu vereinheitlichen und effektiver zu gestalten. Künftig übernimmt die Behörde die direkte Beaufsichtigung von rund 40 Kredit- und Finanzinstituten mit grenzüberschreitender Präsenz und hohem Residualrisikoprofil.

An der Spitze der Behörde steht Bruna Szego. Die Italienerin war zuvor viele Jahre in leitenden Positionen bei der Banca d'Italia tätig, zuletzt als Leiterin der Einheit für AML-Aufsicht und -Regulierung. Der von der AMLA verfolgte Risikoanalyseansatz knüpft deutlich an den italienischen Aufsichtsansatz an. Darum lohnt ein kurzer Exkurs:

Der Ansatz der Banca d'Italia zeichnet sich u. a. durch eine klare Strukturierung der Risikoanalyse aus: Risikoidentifizierung, Schwachstellenanalyse, Bestimmung des Residualrisikos und Abhilfemaßnahmen. Für die Einstufung der Risiken werden verbindliche Risikokategorien und vorgegebene Risikomatrizen genutzt.

Die Risikoanalyse nach Vorgaben der Banca d'Italia basiert auf zahlreichen objektiven und quantitativen Datenpunkten und erfolgt risikobasiert. Verpflichtete Institute müssen aggregierte Daten über ihre Geschäftstätigkeit regelmäßig übermitteln. Dadurch können Risiken sowohl auf institutsbezogener als auch auf geografischer oder sektoraler Ebene systematisch bewertet werden.

Dieser daten- und kennzahlenbasierte Ansatz findet sich nun auch im Aufsichtsverständnis der AMLA wieder.

Die AMLA verfolgt einen standardisierten Risikoanalyseansatz zur Erkennung, Bewertung und Überwachung von Geldwäsche- und Terrorismusfinanzierungsrisiken. Grundlage sind objektive Kriterien, harmonisierte Risikodefinitionen und -kategorien sowie einheitliche Datenpunkte.

Die Entwürfe technischer Regulierungsstandards nach Art. 40 Abs. 2 AMLD6 und Art. 12 Abs. 7 AML-VO enthalten die Datenpunkte und Kriterien, die sowohl von nationalen Aufsichtsbehörden als auch von der AMLA verwendet werden sollen. Dadurch entsteht ein gemeinsames Risikoverständnis innerhalb der EU.

Die für diesen neuen Ansatz notwendigen Referenzwerte basieren auf Kategorien von Risikofaktoren in Bezug auf Kundendaten und -strukturen, Produkten, Dienstleistungen, Transaktionen, Distributionswegen und geografischen Kriterien. Hinzu kommen Informationen über interne Kontrollen und Verfahren zur Minderung von Risiken.

Wesentlich ist dabei die stärkere Quantifizierung der Risikoanalyse. Die AMLA wendet sich damit von der bisherigen narrativen und richtlinienbasierten Bewertung ab und einem datengetriebenen Risikomodell zu. Risiken sollen systematisch, konsistent und nachvollziehbar bewertet werden.

Der standardisierte Risikoanalyseansatz stellt einen Paradigmenwechsel in der Geldwäscheaufsicht dar. Die bislang fragmentierten und teilweise lückenbehafteten Anforderungen nationaler Aufsichten werden hierdurch harmonisiert und präzisiert.

Der neue Ansatz ersetzt zunehmend die bisherigen Stichprobenkontrollen durch eine kontinuierliche datengetriebene Risikobewertung. Gleichzeitig reduziert die Harmonisierung individuelle Interpretationen der Institute und stärkt Transparenz und Vergleichbarkeit der Risikoprofile.

Besondere Bedeutung kommt der Datenqualität zu. Verpflichtete Institute müssen konsistente, aktuelle und vollständige Daten zu Kunden, Transaktionen, Risiken und Kontrollhandlungen verwenden. Minderwertige Datenqualität führt zu einem erhöhten Residualrisiko und kann intensivere Prüfungen nach sich ziehen.

Die AMLA verfolgt dabei einen Top-down-Ansatz, ergänzt durch institutsindividuelle Bottom-up-Risikobewertungen. Kredit- und Finanzinstitute haben ihre internen Risikomanagementsysteme so auszugestalten, dass diese in das europäische Gesamtbild integrierbar sind.

Für Kredit- und Finanzinstitute bedeutet der neue Ansatz einen deutlich erhöhten Fokus auf Datenqualität, Risikoanalyse und Governance-Strukturen. Die institutsinterne Risikoanalyse bleibt zentraler Bestandteil des Risikomanagements und wird zugleich stärker überprüfbar.

Die Nutzung strukturierter Risikomatrizen, standardisierter Datenpunkte und datengetriebener Risikoanalysen ermöglicht eine präzisere Einschätzung inhärenter Risiken sowie der entsprechenden Mitigierungsmaßnahmen.

Darüber hinaus gewinnen Risiko-Dashboards, Trendaussagen und Frühwarnindikatoren an Bedeutung. Risiken sollen nicht nur vergangenheitsbezogen bewertet, sondern im Sinne eines „looking-forward-Ansatzes" frühzeitig erkannt und gesteuert werden.

Die AMLA erkennt die Vorteile, die sich aus der institutsinternen Nutzung eines wesentlich stärker datengetriebenen Ansatzes ergeben und integriert diesen in den Leitlinien-Entwurf für die unternehmensweite Risikobewertung nach Art. 10 Abs. 4 AML-VO. Demnach sollen Datenpunkte, die der AMLA durch die Institute zur Verfügung zu stellen sind, auch für die institutseigene Risikoanalyse zur Ermittlung und Bewertung der inhärenten Risiken verwendet werden.

Compliance-Verantwortliche sollten ihre internen Risikoanalysen, Know-Your-Customer- und Customer-Due-Diligence-Prozesse sowie Governance-Strukturen frühzeitig an den standardisierten Risikoanalyseansatz der AMLA anpassen. Für die betroffenen Institute bedeutet dies zwar zunächst einen höheren Anpassungsaufwand, zugleich mittel- und langfristig jedoch mehr Klarheit, Synergien und (aufsichts-) rechtliche Sicherheit.

Hartmut T. Renz, STRATECO GmbH, Bad Homburg v. d. Höhe, und Andrea Kaßen, Sparkasse Duisburg

Lesen Sie hierzu auch den ausführlichen Fachbeitrag von *Hartmut T. Renz* und *Andrea Kaßen*, der als Zweiteiler im Compliance-Berater, Ausgabe 9 und 10/2026, am 20. August und am 17. September 2026 erscheinen wird.

CYBER//RESILIENT

Cyber-Security Anforderungen in der Produkt Compliance

Eine Veranstaltung von

Kommunikation & Recht und DATENSCHUTZ-BERATER

in Kooperation mit Osborne Clarke

10. November 2026 | Frankfurt am Main

Jetzt anmelden!

Get-together am Vorabend | Montag, 09. November 2026

ab 18.30 Uhr	**Gemeinsames Abendessen im traditionellen Apfelweinlokal „Kanonensteppel“** Textorstr. 20, 60594 Frankfurt (Sachsenhausen)

Programm | Dienstag, 10. November 2026

ab 08.30 Uhr	**Registrierung**
09.00 Uhr	**Begrüßung** Dr. Tobias Rothkegel, CIPP/E, Partner, Osborne Clarke Torsten Kutschke, Gesamtverlagsleiter Fachmedien Recht und Wirtschaft, dfv Mediengruppe
09.10 Uhr	**Überblick: Sachlicher Anwendungsbereich des Cyber Resilience Acts – Offene Fragen** Dr. Tobias Rothkegel, CIPP/E, Partner, Osborne Clarke
09.30 Uhr	**Der Cyber Resilience Act und Produkte mit digitalen Elementen im Anlagenbau: Ein Praxiseinblick – Von maßgeschneiderten Produkten, wesentlichen Änderungen und kommerziellen Auswirkungen des CRA** Peter Gaich, CIPP/E, Head of Legal – Data Protection & Digital Regulation, SSI Schäfer Gruppe
10.15 Uhr	**Kaffeepause**
10.45 Uhr	**Deep Dive: Herstellerpflichten rund um den Produkt Life Cycle** Mareike Christine Gehrmann, Partnerin, Taylor Wessing
11.30 Uhr	**CRA-Compliance entlang der Lieferkette – Herstellerpflichten zwischen Compliance, Kontrolle und Kooperation** Philipp Schröter, Director Legal Data Privacy & IT, Legal & Compliance, Miele & Cie KG
12.15 Uhr	**Gemeinsame Diskussion im Plenum**
12.45 Uhr	**Mittagspause**
13.45 Uhr	**Cyber Resilience Act: Zwischen Regulierung und Realität** Thomas Werner, Manager Cyber Security, UNITY Consulting & Innovation
14.30 Uhr	**Nutzung von Open Source und KI Komponenten in CRA-Produkten** Dr. Lina Böcker, Partnerin, Osborne Clarke
15.15 Uhr	**Kaffeepause**
15.45 Uhr	**Enforcement von CRA-Verstößen** **Enforcement von CRA-Verstößen und Verteidigungsstrategien dagegen** N. N. **CRA und Cybersicherheit in der Vertragsgestaltung und -durchsetzung** Prof. Dr. David Bomhard, Physiker, Partner, Aitava AI & IT Law **mit anschließender Diskussion**
17.00 Uhr	**Gemeinsame Diskussion im Plenum**
17.25 Uhr	**Zusammenfassung & Ausblick**
17.30 Uhr	**Ende der Konferenz**


Dr. Tobias Rothkegel


Torsten Kutschke


Peter Gaich


Mareike Christine Gehrmann


Philipp Schröter


Thomas Werner


Dr. Lina Böcker


Prof. Dr. David Bomhard

Ihre Ansprechpartnerin: Frau Maria Belz

Projektmanagerin
Deutscher Fachverlag GmbH
Tel.: +49 69 7595-1157
E-Mail: Maria.Belz@dfv.de

Teilnahmegebühren (zzgl. MwSt.):

499,– EUR Abonnent:innen DSB, K&R
599,– EUR Normalpreis

Fortbildungsbescheinigung nach § 15 FAO.

Veranstaltungsort:

dfv Mediengruppe
Mainzer Landstraße 251
60326 Frankfurt am Main

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

// WIR FEIERN **80 JAHRE** /

R&W Fachkonferenzen

Eine Medienmarke der dfv Mediengruppe

KI-Kompetenz als Fundament wirksamer KI-Compliance

Die Förderung von KI-Kompetenz ist ein zentrales Anliegen der EU-KI-Verordnung. Im Zuge laufender Entbürokratisierungsbemühungen der EU („Digital Omnibus") wurde diskutiert, ob Unternehmen von ihrer primären Verantwortung zur Sicherstellung der KI-Kompetenz befreit werden sollten. Martin Schulz und Maximilian Vonthien beantworten diese Frage klar mit „nein" und zeigen, dass die Entwicklung von KI-Kompetenz durch adäquate Schulungen Bestandteil der Compliance-Pflicht ist.

© IMAGO / Westend61

KI, das unbekannte Wesen? Unternehmen müssen durch adäquate Schulungen KI-Kompetenz vermitteln.

Mit der Verordnung über künstliche Intelligenz (KI-VO) hat die EU erstmals eine ausdrückliche Pflicht zur Sicherstellung von KI-Kompetenz eingeführt. Anbieter und Betreiber von KI-Systemen müssen gemäß Art. 4 KI-VO Maßnahmen ergreifen, um nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen.

Allerdings wurde im Zusammenhang mit den Entbürokratisierungsinitiativen der EU („Digital Omnibus") vom 19.11.2025 unter anderem eine Abschwächung dieser Regelung diskutiert. Der ursprüngliche Vorschlag der EU-Kommission für eine Änderungsverordnung („Digital Omnibus on AI") sah in Bezug auf Art. 4 KI-VO vor, die Verantwortung für die KI-Kompetenzentwicklung weitgehend auf Mitgliedstaaten und EU-Institutionen zu verlagern. Unternehmen sollten demnach vor allem durch staatliche Schulungsangebote unterstützt und motiviert werden. Nur für Hochrisiko-KI-Systeme hätte weiterhin die Pflicht bestanden, qualifiziertes Personal mit der menschlichen Aufsicht zu betrauen. Nach der nunmehr erzielten Einigung von Rat und Parlament wurde Art. 4 KI-VO allerdings nicht geändert, es bleibt vielmehr bei der bestehenden Pflicht zur KI-Kompetenzentwicklung.

Die Fortgeltung dieser Pflicht ist ausdrücklich zu begrüßen, denn die Bedeutung der KI-Kompetenz reicht weit über Art. 4 KI-VO hinaus. Die Geschäftsleitung muss schon zur Erfüllung ihrer allgemeinen Compliance-Pflicht die Einhaltung sämtlicher relevanter Normen (mit KI-Bezug) sicherstellen. Dies umfasst sowohl die Organisation als auch die Kontrolle einer angemessenen Schulung der Beschäftigten. Diese Schulungspflicht leitet die Rechtsprechung einerseits aus der allgemeinen Compliance-Pflicht der Leitungsorgane ab, andererseits aus ihrer Aufsichtspflicht nach §§ 130, 9 OWiG. So hat etwa das OLG Nürnberg im Haftungsfall eines GmbH-Geschäftsführers nach § 43 Abs. 2 GmbHG betont, dass bereits die unzureichende Anleitung oder Kontrolle von Mitarbeitenden eine haftungsrelevante Pflichtverletzung begründen kann. Der Bundesgerichtshof hat im Fall einer Aufsichtspflichtverletzung nach § 130 OWiG im Zusammenhang mit dem Export eines Medizinproduktes ausgeführt, dass geeignete organisatorische Vorkehrungen zur Haftungsvermeidung unter anderem in Schulungen der mit der Exportabwicklung befassten Mitarbeitenden liegen können (BGH, 29.5.2024 – 3 StR 507/22).

Diese allgemeinen Grundsätze zur Schulungspflicht lassen sich auf die Pflicht zur Entwicklung von KI-Kompetenz übertragen. Auch wenn Art. 4 KI-VO in der derzeitigen Fassung von der Sanktionsnorm des Art. 99 Abs. III-V KI-VO nicht explizit erfasst ist, kann ein Verstoß gegen die KI-Kompetenzentwicklungspflicht mittelbar sanktionsrelevant werden. Denn für Unternehmen und ihre Leitungsorgane entstehen erhebliche Haftungsrisiken, wenn die KI-Kompetenz nicht ausreichend sichergestellt wird. Dies gilt beispielsweise, wenn im Unternehmen mangels ausreichender KI-Kompetenz verbotene KI-Praktiken im Sinne des Art. 5 KI-VO existieren, wenn wegen fehlender KI-Kompetenz die erforderliche Wirksamkeit der menschlichen Aufsicht über Hochrisiko-KI-Systeme nicht funktioniert (Verletzung von Art. 26 Abs. 2 KI-VO) oder in dem Fall, dass mangels ausreichender KI-Kompetenz ein Schaden durch fehlerhafte Bedienung eines KI-Systems verursacht wird.

Diese Beispiele zeigen, dass Unternehmen und ihre Leitungsorgane in jedem Fall tragfähige Strategien und Konzepte für KI-Schulungen entwickeln sollten, um den rechtskonformen KI-Einsatz sicherzustellen. Die Legaldefinition der KI-Kompetenz in Art. 3 Nr. 56 KI-VO verdeutlicht, dass KI-Kompetenz nicht den Aufbau von Expertenwissen verlangt, sondern ein grundlegendes Verständnis der Funktionsweise von KI-Systemen sowie ein Bewusstsein für die damit verbundenen Chancen und Risiken. Diese Definition erfasst sowohl kognitive Fähigkeiten als auch ein praktisches Verständnis, das es ermöglicht, KI-Systeme in der Praxis sicher, verantwortungsvoll und rechtskonform einzusetzen.

Der Umfang der erforderlichen Kompetenz ist dabei kontextabhängig. Unternehmen, die KI-Systeme selbst entwickeln oder vertreiben, benötigen ein deutlich höheres Kompetenzniveau als Unternehmen, die KI lediglich unterstützend im Arbeitsalltag einsetzen. Gemeinsamer Kern bleibt jedoch stets die Notwendigkeit, durch Entwicklung von KI-Kompetenz einen rechtskonformen und verantwortungsvollen Einsatz von KI-Systemen dauerhaft zu gewährleisten.

Prof. Dr. Martin R. Schulz, LL.M. (Yale) und Dr. Maximilian Vonthien, LL.M. (Columbia)

Mehr zur Bedeutung der KI-Kompetenz für eine effektive KI-Compliance-Organisation, zur Verantwortung der Geschäftsleitung für die Sicherstellung von KI-Kompetenz und zu den Haftungsrisiken bei deren unzureichender Umsetzung lesen Sie in CB 2026, 208. In einem Folgebeitrag (erscheint in CB 8/2026) geben Prof. Dr. *Martin R. Schulz* und Dr. *Maximilian Vonthien* Empfehlungen zur Entwicklung von KI-Kompetenz im Rahmen eines KI-Compliance-Systems.

IMPRESSUM
Verlag
Deutscher Fachverlag GmbH, Mainzer Landstraße 251,
60326 Frankfurt am Main
Registergericht 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 Ruß
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, Hilti Corporation; Prof. Dr. Katharina Hastenrath, ZHAW Zürcher Hochschule für Angewandte Wissenschaften; Corina Käsler, 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 Niermann; 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