Falls Ihnen der Newsletter weitergeleitet wurde und Sie ihn regelmäßig beziehen möchten, besuchen Sie: www.compliance-plattform.de

Compliance

Die Zeitschrift für Compliance-Verantwortliche

September 2026

SCHWERPUNKT FINANCE

Inhalt

© IMAGO / Zoonar

Aufmacher

Was ist wirklich neu an der 9. MaRisk-Novelle?

Mit Rundschreiben 06/2026 (BA) vom 30. Juni 2026 hat die BaFin die 9. MaRisk-Novelle veröffentlicht. Eine vollständige Neugestaltung des Regelwerks ist sie nicht. Vielmehr bleibt die Grundstruktur der 8. MaRisk erhalten. Die wichtigsten Neuerungen beschreibt Prof. Dr. Dieter Krimphove in unserem Aufmacher.

Recht

© IMAGO / Shotshop

Finanzsektor: Bafin überwacht KI-Systeme
Die Bafin überwacht künftig KI-Systeme von Unternehmen des Finanzsektors. Zentrale Ziele sind dabei laut der Aufsichtsbehörde: Innovationen fördern, Grundrechte schützen.

Praxis

© IMAGO / ingimage

Ist die aktuelle Verschlüsselung noch eine wirksame Schutzmaßnahme?
Bei den technischen Maßnahmen zum Schutz von sensiblen Daten und Systemen zählt die Verschlüsselung zu den wichtigsten Sicherheitsmechanismen. Doch wie wirksam ist diese Schutzmaßnahme langfristig, wenn leistungsfähige Quantencomputer künftig in der Lage sein könnten, heute eingesetzte Verschlüsselungsverfahren zu brechen?

Research

© IMAGO / YAY Images

Report: Deutschland braucht eine stärkere Speak-up-Kultur
Vorschriften in den Bereichen Hinweisgeberschutz, KI-Governance und Datenschutz werden zunehmend komplexer. Die Ergebnisse des NAVEX Reports 2026 „Whistleblowing und Compliance in Europa: Datengestützte Einblicke und Benchmarks" zeigen, dass die größten Hürden inzwischen operativer Natur sind. Hier gewinnen Hinweisgebersysteme an Bedeutung.

Veranstaltungen

03.09.2026 | kostenfreier Netzwerkabend in Hamburg | **Der Sanierungsberater im Dialog**

16.09.2026 | Online | **EmpCo meets Tourism & Food Industry**

17.09.2026 | Online | **Compliance & KI**

23.09.2026 | Düsseldorf | **Datenschutzkonferenz 2026**

29.09.2026 | Saarbrücken | **IT.CON 2026 by CYBR360**

Was ist wirklich neu an der 9. MaRisk-Novelle?

Mit Rundschreiben 06/2026 (BA) vom 30. Juni 2026 hat die BaFin die 9. MaRisk-Novelle veröffentlicht. Eine vollständige Neugestaltung des Regelwerks ist sie nicht. Vielmehr bleibt die Grundstruktur der 8. MaRisk erhalten. Neu sind vor allem die stärkere Orientierung am Risikoprofil des jeweiligen Instituts, die neue Einteilung der Institute nach Größe und Bedeutung sowie die stärkere Einbindung von ESG-, IKT- und Modellrisiken. Die Novelle setzt damit zugleich die Europäisierung des Bankenaufsichtsrechts fort. Die wichtigsten Neuerungen beschreibt Prof. Dr. Dieter Krimphove in unserem Aufmacher.

© IMAGO / Zoonar

Strukturell neu: Institute werden nach Größe und Bedeutung in vier Kategorien eingeteilt.

Die Überarbeitung steht insbesondere im Zusammenhang mit den EBA-Leitlinien zur internen Governance (EBA/CP/2025/20) und zur Umwelt-Szenarioanalyse (EBA/GL/2025/04). Die MaRisk übernehmen damit zunehmend europäische aufsichtsrechtliche Standards.

Die BaFin verfolgt dabei ausdrücklich das Ziel, die MaRisk stärker prinzipienbasiert und weniger komplex auszugestalten. Erläuterungen und Beispiele wurden teilweise gestrichen, um den Instituten mehr Spielraum für risikoadäquate Lösungen zu geben (siehe Übersendungsschreiben der BaFin an die Verbände der Kreditwirtschaft vom 30. Juni 2026).

Die wohl wichtigste strukturelle Neuerung findet sich in AT 2.1 Tz. 1 MaRisk. Die Institute werden nach Größe und Bedeutung in vier Kategorien eingeteilt:

1. sehr kleine Institute mit einer Bilanzsumme bis 1 Mrd. Euro,
2. kleine Institute (Small and Non-complex Institutions - SNCIs),
3. übrige weniger bedeutende Institute (Less Significant Institutions - LSIs) und
4. bedeutende Institute (Significant Institutions - SIs).

Die MaRisk gelten für die Kategorien 1 bis 3. SIs unterliegen dagegen unmittelbar der europäischen Aufsicht und den einschlägigen EBA-Vorgaben; sie werden aus dem Anwendungsbereich der deutschen MaRisk herausgenommen.

Die Einteilung ist mehr als eine bloße Orientierungshilfe. Sie bestimmt die Intensität der aufsichtsrechtlichen Anforderungen und macht das Proportionalitätsprinzip zu einem tragenden Element der 9. MaRisk.

Die 9. MaRisk ist deutlich kompakter als ihre Vorgängerfassung. Zahlreiche Beispiele und Detailbeschreibungen wurden gestrichen. Dies betrifft insbesondere die Erläuterungsteile, die bislang häufig zur Konkretisierung einzelner Anforderungen herangezogen wurden. Die Folge ist – wie bereits angesprochen – ein größerer Gestaltungsspielraum der Institute, zugleich aber auch ein höherer Bedarf an eigener Auslegung und an Orientierung durch Verwaltungspraxis und Fachliteratur.

Die stärkere Prinzipienorientierung ist deshalb weniger ein vollständiger Systemwechsel als eine Verschiebung des Schwerpunkts: Nicht jede Einzelheit wird vorgegeben; entscheidender wird, ob die gewählte Lösung zum Geschäftsmodell, zur Komplexität und zum Risikoprofil des Instituts passt.

Die ESG-Anforderungen werden insbesondere in AT 2.2 Tz. 3 und AT 4.3.3 Tz. 7 MaRisk konkretisiert. Institute müssen Umwelt-Szenarioanalysen durchführen und deren Auswirkungen auf ihre Risikopositionen dokumentieren. Grundlage hierfür sind insbesondere die EBA-Leitlinien zur Umwelt-Szenarioanalyse (EBA/GL/2025/04).

Dabei werden ESG-Risiken nicht als isolierte zusätzliche Risikokategorie verstanden. Vielmehr sind Umwelt-, Sozial- und Governance-Faktoren in die bestehende Risikosteuerung einzubeziehen und in ihrer Wechselwirkung mit anderen Risiken zu betrachten. ESG wird damit Bestandteil der strategischen Steuerung, des Risikomanagements und der Governance des Instituts.

Eine weitere zentrale Neuerung ist die stärkere Einbindung von IKT-Risiken. Als IKT-Risiken fasst die MaRisk Bedrohungen der Integrität, Verfügbarkeit, Vertraulichkeit und Authentizität von Informations- und Kommunikationstechnologien, die den Geschäftsbetrieb und die digitale Resilienz eines Unternehmens beeinträchtigen können. AT 2.2 Tz. 1 Anm., AT 4.2 Tz. 2, AT 7.3 Tz. 1, AT 8.2 Tz. 1, BTO Tz. 7; BTO 2.2.1 Tz. 6 verlangen ihre systematische Berücksichtigung im Risikomanagement.

© privat

Prof. em. Dr. jur. Dieter Krimphove ist emeritierter Inhaber des Lehrstuhls „Europäisches und deutsches Wirtschaftsrecht", sowie Jean-Monet Professor „ad personam" und Professor der Donau-Universität Krems. Zu seinen Forschungsgebieten zählen neben Fragen der Rechtsvergleichung das deutsche und Europäische Banken- und Unternehmensrecht.

Besondere Bedeutung hat dabei AT 4.3.4 MaRisk. Die Vorschrift erfasst Modelle bzw. quantitative Methoden und bezieht ausdrücklich KI-gestützte Systeme, automatisierte Modelle und technologiegestützte Innovationen ein. Erfasst werden beispielsweise Kredit- und Scoringmodelle, Stresstests und Preisbildungsmodelle. Das Institut muss insbesondere die Eignung des Modells, seine Anwendungsregeln und seine Grenzen kennen und eine angemessene Validierung sicherstellen (AT 4.3.4 Tz. 1, 3-5).

Für die digitale Resilienz bleibt allerdings DORA das maßgebliche europäische Regelwerk. Die 9. MaRisk grenzt beide Regelungssysteme insbesondere in AT 4.2 und AT 9 voneinander ab. IKT-Dienstleistungen, die dem IKT-Drittparteienrisikomanagement nach Art. 28-30 DORA unterliegen, fallen grundsätzlich nicht zusätzlich unter die MaRisk-Auslagerungsanforderungen.

Die stärkere Proportionalität wirkt sich insbesondere auf sehr kleine und kleine Institute aus. Erleichterungen bestehen unter anderem bei Governance-Prozessen, Bearbeitungsprozessen, der Strategieentwicklung, Risikoerfassung und Risikocontrolling, der Outsourcing-Dokumentation sowie bei Stresstests. Auch die Berichtsanforderungen werden teilweise reduziert.

Damit wird ein zentraler Gedanke der Novelle praktisch umgesetzt: Die Anforderungen sollen nicht allein danach bestimmt werden, was abstrakt für ein großes, komplexes Institut sinnvoll ist, sondern danach, welche Risiken das konkrete Institut tatsächlich aufweist.

Die 9. MaRisk-Novelle ist keine Revolution, aber eine strukturell bedeutsame Weiterentwicklung. Für die Praxis bedeutet sie weniger Detailsteuerung, aber zugleich mehr Eigenverantwortung der Institute bei der Ausgestaltung eines ihrem Geschäftsmodell entsprechenden Risikomanagements. *Prof. em. Dr. jur. Dieter Krimphove*

Lesen Sie hierzu auch den ausführlichen Fachbeitrag von Prof. em. Dr. jur. Dieter Krimphove, der im Compliance-Berater (CB 2026, 381) erschienen ist.

6. Praxisseminar Geldwäschegesetz 2026

Das branchenübergreifende Jahresupdate

Eine Veranstaltung von

GELDWÄSCHE & RECHT und

29. September 2026 | Frankfurt am Main

Jetzt anmelden!

PROGRAMM

9.00 Uhr	**Begrüßung** Dr. Uta Zentes, Rechtsanwältin und Syndikusrechtsanwältin, Frankfurt a. M. Sebastian Glaab, Partner, Annerton Rechtsanwälte, Frankfurt a. M. Lars-Heiko Kruse, Partner, PwC Germany, Berlin
Themenblock 1: Daten als Erfolgsfaktor	
9.10 Uhr	**Informationspools – zum Stand der Dinge** Dr. Joachim Kaetzler, Partner, CMS, Frankfurt a. M.
9.50 Uhr	**Automatisierung der Risikoanalyse** Lars-Heiko Kruse, Partner, PwC Germany, Berlin
10.30 Uhr	**Kaffeepause**
Themenblock 2: Antworten zum EU AML Paket	
11.00 Uhr	**Inanspruchnahme Dritter zur Erfüllung von Sorgfaltspflichten gegenüber Kunden unter der AML-VO** Dr. Andreas Burger, Partner, Deloitte GmbH, Frankfurt a. M. Christian Paap, Rechtsanwalt und Syndikusrechtsanwalt, Deloitte GmbH, Hamburg
11.40 Uhr	**AML-VO-konforme Risikoanalyse: Schritt-für-Schritt-Aufbau eines harmonisierten EU-Risk Assessments** Carsten Lang, Head Financial Crime Prevention Germany, UBS Europe SE, Frankfurt a. M.
12.20 Uhr	**Neue Standards durch die AML-VO im KYC – Was kommt auf uns zu** Dr. Jacob Wende, CEO & Gründer, Regpit GmbH, Berlin Schriftleitung Geldwäsche & Recht
13.00 Uhr	**Mittagspause**
Themenblock 3: Strafrechtliche Fragen	
14.15 Uhr	**Aktuelle Fragen der Vermögensabschöpfung und Fragen des administrativen Ansatzes (Verbundeinsätze)** Jörg Lehnert, Leiter der Berliner Geldwäscheaufsicht von 2012–2025
14.55 Uhr	**Die geldwäscherechtliche Selbstanzeige gem. § 261 Abs. 8 StGB – praktische Anwendungsfälle und rechtlicher Rahmen** Dr. Thomas Richter, Fachanwalt für Strafrecht, RICHTER Rechtsanwälte, Frankfurt a. M. Tabitha Schulze-Bünte, RICHTER Rechtsanwälte, Frankfurt a. M.
15.35 Uhr	**Konvergenz von Sanktionsrecht und Geldwäschebekämpfung** Dr. Christian Schmies, Hengeler Mueller
16.15 Uhr	**Fazit**
16.30 Uhr	**Ende des Praxisseminars**


Dr. Uta Zentes


Sebastian Glaab


Lars-Heiko Kruse


Dr. Joachim Kaetzler


Dr. Andreas Burger


Christian Paap


Carsten Lang


Dr. Jacob Wende


Dr. Thomas Richter


Tabitha Schulze-Bünte


Dr. Christian Schmies

PARTNER

ANNERTON

CMS law·tax·future

pwc

MEDIENPARTNER

Compliance Berater

Recht der Zahlungsdienste

Betriebs Berater

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

// WIR FEIERN **80 JAHRE** /

R&W Fachkonferenzen

Eine Medienmarke der dfv Mediengruppe

Finanzsektor: Bafin überwacht KI-Systeme

Die Bafin überwacht künftig KI-Systeme von Unternehmen des Finanzsektors. Zentrale Ziele sind dabei laut der Aufsichtsbehörde: Innovationen fördern, Grundrechte schützen.

© IMAGO / Shotshop

Ein Auge auf die KI – hält ab sofort auch die Bafin.

Der deutsche Gesetzgeber erweitert das Mandat der Bafin, wie die Finanzaufsichtsbehörde selbst in einer Meldung Ende Juli mitgeteilt hat. Danach übernimmt die Bafin die Marktüberwachung für KI-Systeme, die in direktem Zusammenhang mit einer regulierten Finanztätigkeit stehen. Die neue Zuständigkeit erstreckt sich auf Kreditinstitute, Versicherer und andere Finanzunternehmen unter Aufsicht der Behörde.

Grundlage ist das Gesetz zur Durchführung der europäischen Verordnung über Künstliche Intelligenz, das am 29. Juli 2026 in Kraft getreten ist. Aufgrund ihres neuen Mandats werde die Bafin zukünftig überwachen, ob die beaufsichtigten Unternehmen die Anforderungen der KI-Verordnung einhalten.

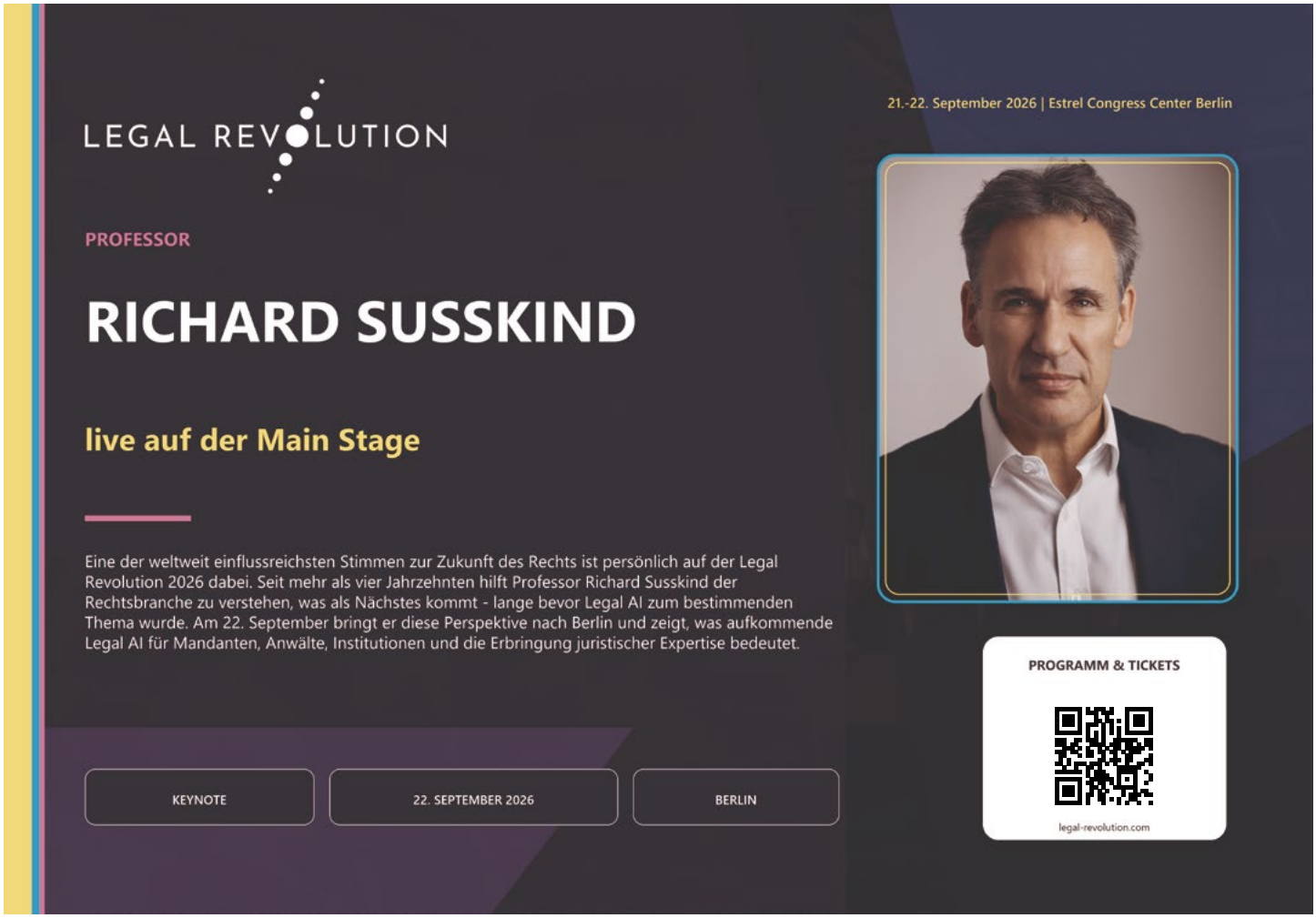
Die Marktüberwachung der Bafin umfasst zum Beispiel die Transparenzpflichten für KI-Systeme, die unmittelbar mit Menschen interagieren – wie etwa Chatbots in der Kundenkommunikation. Die Bafin werde zudem überwachen, ob die Regelungen der KI-Verordnung zu verbotenen KI-Praktiken eingehalten werden. Darüber hinaus umfasst die Marktüberwachung Hochrisiko-KI-Systeme. Dies sind beispielsweise Systeme, die Banken in der Kreditwürdigkeitsprüfung einsetzen oder die Versicherer für die Risikobewertung in der Lebens- und Krankenversicherung nutzen.

Die Bafin kündigt an, die Marktüberwachung für KI-Systeme eng mit ihrer laufenden Unternehmensaufsicht abzustimmen.

Bestimmte KI-Praktiken sind bereits seit dem 2. Februar 2025 verboten. Darunter fallen Systeme, die besonders schützenswerte Informationen über Menschen sammeln und bewerten, was zu einer ungerechtfertigten Benachteiligung von Menschen führen kann. Die ersten Transparenzpflichten der KI-Verordnung gelten seit dem 2. August 2026. Ab dem 2. Dezember 2027 greifen die Anforderungen an Hochrisiko-KI-Systeme.

Die Bafin erwartet von den Unternehmen, dass sie sich ausführlich mit der KI-Verordnung auseinandersetzen, weist aber gleichzeitig darauf hin, dass sich ihre Marktüberwachung auf KI-Systeme beschränke, die in direktem Zusammenhang mit einer regulierten Finanztätigkeit stehen. Andere KI-Anwendungen, etwa im Personalmanagement von Finanzunternehmen, fallen in den Zuständigkeitsbereich der Bundesnetzagentur.

Bei Verstößen gegen die KI-Verordnung kann die Bafin Bußgelder verhängen. *chk*



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 rechtspolitischer 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
- 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-Digitalrechtsakte?
- 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
SorberArbeitsrecht


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

9. MaRisk-Novelle: Mehr Gestaltungsspielraum, aber keine Entwarnung für die Compliance-Funktion

Am 30. Juni 2026 hat die Bafin die finale 9. MaRisk-Novelle veröffentlicht (Rundschreiben 06/2026 (BA)); das Ende der Übergangsfrist ist der 1. Januar 2027. Für Compliance-Verantwortliche lohnt sich der Vergleich mit der Konsultationsfassung (Konsultation 02/2026) vom 1. April 2026: An der zentralen Vorschrift zur Compliance-Funktion hat die Aufsicht noch einmal Hand angelegt.

© IMAGO / Pond5 Images

Die neue MaRisk unter der Lupe.

Die Konsultationsfassung hatte die Aufgabendefinition neu gefasst: Die Compliance-Funktion sollte beraten, unterstützen, „die Überwachung der Einhaltung im Rahmen eines strukturierten Prozesses sicherstellen", sowie „wesentliche rechtliche Risiken mit Compliance-Bezug identifizieren". Damit wäre die klassische „Hinwirkungspflicht" abgelöst und die strukturierte Überwachung erstmals auf Normtextebene erhoben worden.

Die finale Fassung geht diesen Schritt auf Normtextebene nicht mit. AT 4.4.2 Tz. 1 lautet nun: Jedes Institut muss über eine Compliance-Funktion verfügen, „um den Risiken, die sich aus der Nichteinhaltung rechtlicher Regelungen und Vorgaben ergeben können, entgegenzuwirken". Sie muss „auf die Implementierung wirksamer Verfahren zur Einhaltung der für das Institut wesentlichen rechtlichen Regelungen und Vorgaben und entsprechender Kontrollen hinwirken" sowie die Geschäftsleitung unterstützen und beraten.

Der Normtext der finalen Fassung kehrt damit im Kern zur bewährten Formulierung der 8. MaRisk-Novelle und ihrer Vorgängerversionen zurück. Der „strukturierte Prozess" ist nicht entfallen, sondern in die Erläuterungen verschoben: Danach muss die Compliance-Funktion insbesondere die Risiken aus der Nichteinhaltung wesentlicher rechtlicher Regelungen und Vorgaben identifizieren und im Rahmen eines strukturierten Prozesses sicherstellen, dass die jeweils betroffenen Bereiche die Einhaltung dieser Regelungen und Vorgaben überwachen. Das „insbesondere" stellt klar: Diese Aufgaben sind Ausprägungen der fortgeltenden Hinwirkungspflicht.

Eine Entwarnung ist das nicht. Die Erläuterungen sind gesicherte Verwaltungspraxis und Maßstab der Prüfungspraxis; die materielle Anforderung bleibt bestehen. Verändert hat sich die normhierarchische Verankerung und Institute gewinnen Spielraum, denn was ein „strukturierter Prozess" ist, definiert der Normtext nicht.

Bemerkenswert ist zudem die Klarstellung, dass die Überwachung bei den betroffenen Fachbereichen liegt; die Compliance-Funktion stellt diese sicher, nimmt die Umsetzung und Etablierung geeigneter 1st-Line Kontrollen jedoch nicht selbst vor. AT 4.4.2 Tz. 2 blieb im Vergleich zur Konsultationsfassung unangetastet: Die risikoorientierte Identifikation der wesentlichen rechtlichen Regelungen „in regelmäßigen Abständen" ist weiterhin im Normtext verankert.

Zwei praxisrelevante Neuerungen wurden unverändert in die Finalfassung übernommen:

Compliance-Beauftragter: AT 4.4.2 Tz. 4 verlangt die Benennung eines Compliance-Beauftragten, der für die Leitung und Erfüllung der Aufgaben der Compliance-Funktion verantwortlich ist. Bei sehr kleinen Instituten kann die Funktion auf einen Geschäftsleiter übertragen werden, sofern Maßnahmen zur Vermeidung von Interessenkonflikten implementiert sind, eine klare, größenabhängige Öffnung.

Zusammenarbeit zwischen Risk und Compliance (-Risk): AT 4.4.2 Tz. 5 etabliert erstmals ein ausdrückliches Kooperationsgebot: Die Compliance- und Risikocontrolling-Funktion „arbeiten zusammen und tauschen Informationen aus". Konkret verlangt dies zukünftig definierte Schnittstellen, abgestimmte Risikotaxonomien, belastbaren Datenaustausch, integre Datenhaushalte und die zunehmende Anlehnung an BCBS 239-Standards.

Auch die mit der Novelle neu eingeführte Kenntnisnahme des Compliance-Berichts durch das Aufsichtsorgan (AT 3.2 Tz. 2) wurde unverändert aus der Konsultation übernommen und ersetzt damit die analogen Vorgaben des AT 4.4.2 Tz. 7 der Vorgängerversion.

In AT 7.1 Tz. 1 hat die Bafin die Personalanforderung im Vergleich zur ursprünglichen Konsultationsfassung entschärft: Statt zu „gewährleisten, dass die Betriebsabläufe jederzeit störungsfrei durchgeführt werden" (Konsultationsfassung), muss die Personalausstattung nun „geeignet sein, um die Betriebsabläufe störungsfrei durchzuführen" – ein Wechsel von der Ergebnis- zur Eignungspflicht.

Abgesehen von den Detailänderungen bestätigt die Finalfassung die grundlegenden Entscheidungen der Konsultation: die Herausnahme bedeutender Institute (SIs) aus dem Anwendungsbereich der MaRisk, die Dreiklassensystematik der nationalen Beaufsichtigung und die konsequente Prinzipienorientierung. Die Novelle führt damit den von CRD VI und den EBA-Leitlinien zur internen Governance vorgezeichneten Konvergenzkurs klar fort und setzt diesen in die nationale Aufsichtspraxis um.

Prof. Dr. Frank Passing, Professor für Digitale Transformation an der IU (International University), Markus Müller, Director Compliance in der Funktion des Head of Compliance für PAYONE in Frankfurt a.M., und Finn Brüggemann, Legal & Compliance Experte bei der Fairfield & Archer GmbH

Eine vertiefte Analyse der Neuausrichtung der Compliance-Funktion im Spannungsfeld von CRD VI, EBA-Leitlinien zur internen Governance und MaRisk findet sich in der dreiteiligen Beitragsreihe von *Passing/Müller/Brüggemann* in CB 2026, 212, 269 und 304. Ergänzend steht im Compliance Glossary von Fairfield & Archer die Synopse „Von der MaRisk-Compliance zur Regulatory-Compliance" als dynamische Rechtsquellen-Gegenüberstellung zur Verfügung.

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), 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
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 Einspeisung in eine Datenbank.

Blick hinter die Kulissen der Compliance Audits

Was bei Compliance Checks wirklich zählt – Alle Ihre Fragen von Top-Auditoren beantwortet.

Eine Veranstaltung des Compliance Berater und kertos

16. Oktober 2026, 11.00 bis 12.00 Uhr | Webinar

Jetzt kostenlos anmelden!

Audit oder Compliance Check steht vor der Tür? Bringen Sie Ihre offenen Fragen mit!
Unsere Experten sprechen Klartext über TISAX®, C5, NIS2, EU AI Act oder ISO.

Viele Unternehmen bereiten sich monatelang auf ihr Audit vor oder investieren Zeit, um Compliance Anforderungen zu erfüllen. Häufig, ohne dabei zu wissen, worauf es wirklich ankommt. Wir zeigen Ihnen, welche Nachweise tatsächlich zählen und wo die häufigsten Lücken liegen, wenn es um eine solide Compliance geht.

WARUM DAS FÜR SIE RELEVANT IST

Ob NIS2, EU AI Act, TISAX®, C5 oder ISO – alle Frameworks haben gemeinsam, dass sie zu einem bestimmten Zeitpunkt klare Nachweise für die Einhaltung der Vorgaben erbringen müssen. Verstreute Excel-Tabellen oder PowerPoint-Präsentationen werden dabei selten akzeptiert. Auditoren und Behörden erwarten in diesem Moment eine Dokumentation, die strukturiert, vollständig und prüfbar ist.

DAS ERWARTET SIE

Auditor-Perspektive
Was Auditoren prüfen und was sie nicht interessiert

Konkrete Checklisten
Was Sie für die Erfüllung verschiedener Frameworks wirklich brauchen

Live Q&A
Ihre Fragen direkt, offen, praxisorientiert

Frameworks im Vergleich
Wo sich die Anforderungen überschneiden und wo nicht

FREUEN SIE SICH AUF

Antonia Glück
Information Security Expert
Kertos GmbH

Aron Lange
Founder & Auditor

Ihre Ansprechpartnerin: Frau Maria Belz
Projektmanagerin
Tel.: +49 69 7595-1157
E-Mail: Maria.Belz@dfv.de

Deutscher Fachverlag GmbH
Mainzer Landstr. 251
60326 Frankfurt am Main

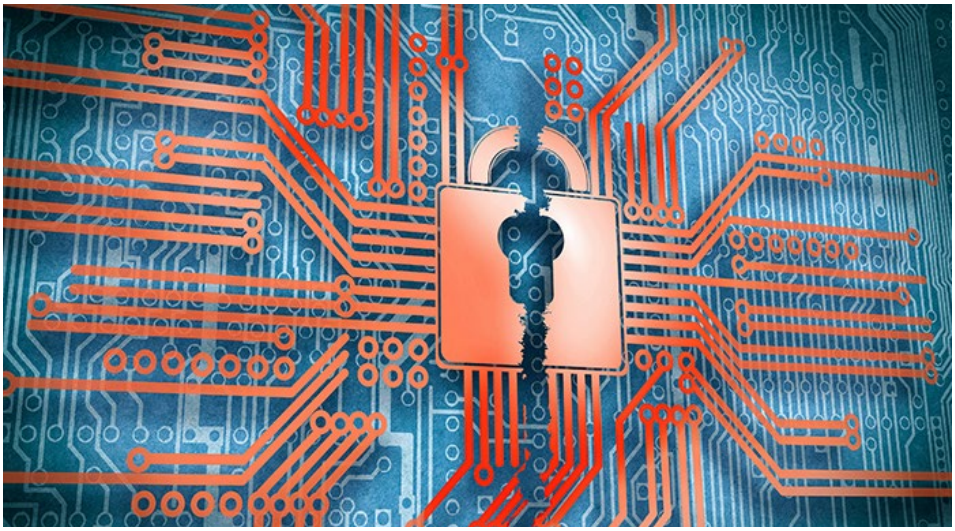
Die Teilnahme am Webinar ist kostenlos.

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

// WIR FEIERN **80 JAHRE** /
R&W Fachkonferenzen
Eine Medienmarke der dfv Mediengruppe

Ist die aktuelle Verschlüsselung noch eine wirksame Schutzmaßnahme?

Bei den technischen Maßnahmen zum Schutz von sensiblen Daten und Systemen zählt die Verschlüsselung zu den wichtigsten Sicherheitsmechanismen. Doch wie wirksam ist diese Schutzmaßnahme langfristig, wenn leistungsfähige Quantencomputer künftig in der Lage sein könnten, heute eingesetzte Verschlüsselungsverfahren zu brechen? Der nachfolgende Beitrag beleuchtet die damit verbundenen Risiken und zeigt auf, weshalb Organisationen sich bereits heute mit dem Thema Post-Quanten-Kryptographie auseinandersetzen sollten.



© IMAGO / ingimage

Vermeintlich sichere Verschlüsselungen könnten in der Zukunft aufbrechen.

Das Thema Daten- und Systemsicherheit ist heute auf allen Hierarchieebenen präsent. Einerseits nimmt die Bedrohungslage im Cyberraum stetig zu, andererseits steigen die gesetzlichen und regulatorischen Anforderungen an den Schutz von Daten kontinuierlich. Einen wesentlichen Impuls setzte unter anderem die Datenschutz-Grundverordnung (DSGVO), die seit Mai 2018 in der Europäischen Union gilt. Sie verlangt zum Schutz personenbezogener Daten angemessene technische und organisatorische Maßnahmen. Auch das revidierte Schweizer Datenschutzgesetz, das im September 2023 in Kraft trat, verfolgt diesen risikobasierten Ansatz.

Zu den klassischen technischen Schutzmaßnahmen gehört die Verschlüsselung. Dabei werden Daten so umgewandelt, dass sie nur mit einem passenden kryptographischen Schlüssel gelesen werden können. Die Verschlüsselung trägt wesentlich zur Sicherstellung der Vertraulichkeit und Integrität von Informationen bei und schützt Personendaten vor unbefugtem Zugriff. Verschlüsselungsverfahren spielen auch eine wesentliche Rolle beim Nachweis der Integrität des Autors oder Eigentümers von Daten und Systemen.

Genau diese Schutzwirkung wird jedoch durch ein Phänomen infrage gestellt, das unter dem Begriff „Harvest Now, Decrypt Later" (HNDL) oder „Jetzt ernten, später entschlüsseln" bekannt ist. Ein weiteres Bedrohungsszenario ist „Trust Now, Forge Later" (TNFL), was „Jetzt vertrauen, später manipulieren" bedeutet. Dabei werden verschlüsselte und digital signierte Daten bereits heute abgefangen oder entwendet und für eine spätere Entschlüsselung oder Manipulation gespeichert. Die Angreifer spekulieren darauf, dass zukünftige Quantencomputer die heute eingesetzten kryptographischen Verfahren brechen können. Besonders problematisch ist dies für Daten mit langen Aufbewahrungs- oder Vertraulichkeitsfristen, wie beispielsweise Gesundheits-, Kunden- oder Personaldaten. Dies betrifft auch Daten, die bereits vor vielen Jahren gesammelt wurden und noch einige Jahre sensibel bleiben werden.

Damit entsteht eine neue Form der Cyberbedrohung: Selbst, wenn verschlüsselte Daten heute nicht lesbar sind, könnte ihre Vertraulichkeit und Integrität in einigen Jahren gefährdet sein. Organisationen stehen deshalb vor der Herausforderung, ihre kryptographischen Verfahren rechtzeitig auf quantenresistente Alternativen umzustellen, bevor leistungsfähige Quantencomputer verfügbar werden.

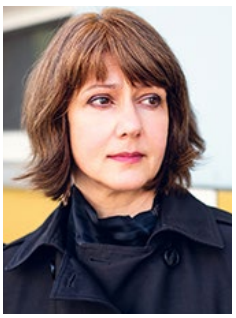
Post-quanten-sichere Kryptografie (PQC) wird schon seit den frühen 2000er Jahren erforscht. Das global führende National Institute of Standards and Technology (NIST) des U.S. Department of Commerce hat seit 2017 die ersten Kandidaten für Schlüsselaustausch und Digitale Signaturen evaluiert und im August 2024 drei ausgewählte Standards veröffentlicht. Die Standardisierung von zwei weiteren PQC-Verfahren läuft. Die ISO-Organisation in Genf und das European Telecommunications Standards Institute (ETSI) haben danach zusätzliche PQC-Standards veröffentlicht. Parallel haben verschiedene nationale und internationale Behörden Migrationsstrategien veröffentlicht. Die EU strebt an, kritische Systeme bis Ende 2030 auf PQC zu migrieren. Systeme mit mittlerem und geringem Risiko sollen bis Ende 2035 migriert werden. Das NIST verfolgt einen technischen Ansatz, nach dem bis 2030 alle Verfahren mit einer Sicherheit von 112 oder weniger Bit als veraltet gelten werden. Dabei steht die Bit-Sicherheit nicht für die Schlüssellänge, sondern für die Komplexität des effizientesten Angriffs auf das Verfahren. Das weit verbreitete Verfahren RSA-2048 fällt zum Beispiel unter diese Kategorie. Ab 2035 sind dann alle Verfahren nicht mehr compliant mit den NIST-Anforderungen, die nicht als post-quanten-sicher gelten. Angesichts der Komplexität unserer digitalen Infrastrukturen sind das sportliche, aber trotzdem notwendige Zeitpläne.

18 EU-Mitgliedsstaaten haben schon im November 2024 in Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography zur dringenden Priorisierung der PQC-Migrationen aufgerufen. Aufgrund neuer Entwicklungen im Quantum Computing hat z. B. Google es sich zum Ziel gesetzt, bis 2029 post-quanten-sichere Dienste anzubieten. Es wird empfohlen, mit sogenannten hybriden Verfahren zu beginnen. Das sind Verfahren, die PQC und klassische Kryptografie kombinieren.

Anja Schmitz und Xenia Bogomolec

© privat

Anja Schmitz ist Juristin und Partner/Senior Consultant bei der Projektas GmbH, mit Sitz in Zug/Schweiz. Sie berät im Bereich Corporate Governance, Compliance, Datenschutz & Projektmanagement, ein Schwerpunkt ihrer Arbeit liegt in der Umsetzung von Compliance-Projekten, dem juristischen Projektmanagement und der Management-Beratung.



© privat

Xenia Bogomolec ist Cybersichertsexpertin und Gründerin der Quant-X Security & Coding GmbH. Sie berät kritische Infrastruktur-Provider mit hohen regulatorischen Anforderungen in Cybersicherheit und leitet Technologietransfer-Projekte in Post-Quanten-Sicherheit, Quantenkryptographie und KI im Cybersicherheitskontext.

Praxisseminar: Datenschutz in der Unternehmensgruppe

Eine Veranstaltung des DATENSCHUTZ-BERATER

und RSM EBNER STOLZ

4. November 2026 | Köln

Jetzt anmelden!

Dienstag, 3. November 2026

Ab 19.00 Uhr	**Get-Together am Vorabend in einem Kölner Brauhaus** Kommen Sie bereits am Vorabend in lockerer Atmosphäre mit Referierenden und Teilnehmenden der Tagung ins Gespräch.

Mittwoch, 4. November 2026

09.00 Uhr **Begrüßung und Vorstellung der Referenten**

09.10 Uhr **Datenschutzorganisation neu gedacht: Erweiterung durch AI- & Datenregulierung**

- Zentrale vs. dezentralisierte Organisations-modelle/ Shared-Service-Zentren Modelle
- „Data Compliance" & AI-Richtlinie: DSMS-Schnittstellen und Praxisbeispiele
- Rollenkonflikte des DPO: Risiken und Lösungen (z. B. Rolle „AI-Officer")
- DPO-Dienstleistungsmodelle innerhalb von Gruppen, SLA-Konstrukte & pers. Haftung
- Teamstrukturen & Outsourcing, Ressourcenplanung & Führung in Matrixorganisationen (inkl. Data- & AI-Compliance)
- Stakeholder-Management & Reporting

10.45 Uhr **Pause & Networking**

11.05 Uhr **Operative Datenschutzprozesse: Steuern statt verwalten – durch Automatisierung, Outsourcing & AI**

- Accountability optimieren: Steuerung von RoPA, Threshold Analyis/ DPIA und AI Risk Assessments
- Risikoentscheidungen systematisieren: Business Judgement Rule in datengetriebenen Organisationen und die Rolle des DPO im Governance-Modell
- Incident-Management neu denken: Semi-automatisierte Bewertung, effiziente Eskalation & skalierbare Prozesse
- Betroffenenrechte effizient steuern: E2E-Optimierung, Insights, aufsichtsbehördliche Erwartungshaltung, gerichtliche Praxis

12.15 Uhr **Mittagspause auf Einladung von** RSM EBNER STOLZ

13.00 Uhr **Datenschutz im „Krisenmodus": Enforcement Lifecycle und Verfahrenssteuerung**

- Trigger-to-Enforcement: Aufsichtsbehördliche Untersuchungen – anlasslos/koordiniert, beschwerde- oder incident-getrieben (Ablauf & Beispiele)
- Litigation Readiness sicherstellen: Verfahren durch Playbooks, klare E2E-Verantwortlichkeiten und strukturierte Eskalationsmechanismen sicher und skalierbar managen (Praxisbeispiele)
- DPO „unter Druck": Rolle des DPO im Zusammenspiel mit Legal, Compliance und Management in kritischen Verfahrensphasen

14.30 Uhr **Pause & Networking**

14.50 Uhr **Datenschutz im Realbetrieb: Aktuelle Trends**

- Datenanalyse & Profiling: Grenzen des berechtigten Interesses (insb. im Zusammenhang mit AI-ADM)
- AI-Voice-Transcription – über (vermeintliche) Strafbarkeiten & berechtigte Interessen
- Agentic AI use cases im Kundenservice

… und ad hoc Fragen/Themen, die Sie im Unternehmen bewegen?

16.30 Uhr **Diskussions- & Fragerunde mit den Referenten und Teilnehmenden**

17.30 Uhr **Ende**

Ihre Referenten aus der Unternehmenspraxis

Björn Malinka, M.Sc.
Head of Global Privacy & Datenschutzbeauftragter, Bayer AG

RA Alexander Schultz, LL.M.
Head of Data Protection & AI Law, Datenschutzbeauftragter, E.ON Energie Deutschland

Moderator und Referent

RA Philipp M. Kühn
Rechtsanwalt & Partner, RSM Ebner Stolz

Ihr Ansprechpartner:
Herr Jasha Baniashraf
Senior Projektmanager
Tel.: +49 69 7595-2773
E-Mail: Jasha.Baniashraf@dfv.de

Veranstaltungsort:
RSM Ebner Stolz
Holzmarkt 1
50676 Köln

Teilnahmegebühren (zzgl. MwSt.):
649,– EUR Unternehmensvertreter:innen mit DSB-Abonnement*
749,– EUR Unternehmensvertreter:innen*
1.949,– EUR Normalpreis (Die Tickets für diese Kategorie sind limitiert.)
* Bitte beachten Sie die genaue Definition dieser Kategorie im Ticketshop.

Inklusive Fortbildungsbescheinigung über 7 Stunden und 15 Minuten nach § 15 FAO sowie 7 CPE-Credits für die IAPP-Zertifizierung.

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

R&W Fachkonferenzen

Eine Medienmarke der dfv Mediengruppe

Grenzüberschreitende Transformation im Private Banking

Privatbanken in ganz Europa sehen sich mit zwei parallelen Entwicklungen konfrontiert. Einerseits modernisieren viele Institute ihre Kernbankensysteme, konsolidieren Plattformen und integrieren neu erworbene Unternehmen. Andererseits entwickeln sich die regulatorischen Anforderungen sowohl auf europäischer als auch auf nationaler Ebene kontinuierlich weiter. Dies erfordert vor allem für Banken, die in mehreren Jurisdiktionen tätig sind regulatorische Compliance, Governance-Strukturen und operative Prozesse über verschiedene Märkte hinweg aufeinander abzustimmen.

© IMAGO / Dreamstime

Grenzüberschreitendes Bankgeschäft: Prozesse müssen über verschiedene Märkte hinweg aufeinander abgestimmt werden.

© Objectway

Karl im Brahm, CEO-Dach Objectway.

Für Banken, die in mehreren Jurisdiktionen tätig sind, geht Compliance über die bloße Erfüllung regulatorischer Verpflichtungen hinaus. Nationale Anforderungen beeinflussen das Kunden-Onboarding, Geeignetheitsprüfungen, Beratungsprozesse, die steuerliche Berichterstattung und das laufende Monitoring. Regulatorische Anforderungen prägen daher zunehmend das operative Tagesgeschäft, anstatt lediglich parallel dazu zu bestehen.

Dies hat erhebliche Auswirkungen auf Transformationsprogramme. Regulatorische Anforderungen sollten bereits bei der Gestaltung von Prozessen berücksichtigt und nicht erst nach deren Implementierung integriert werden. Compliance von Beginn an in operative Prozesse einzubetten, trägt dazu bei, konsistente Standards über verschiedene Märkte hinweg zu schaffen und gleichzeitig institutsspezifische Anforderungen einzelner Jurisdiktionen dort zu berücksichtigen, wo dies erforderlich ist.

Darüber hinaus führen Plattformkonsolidierungen und Integrationen nach Fusionen oder Übernahmen Organisationen zusammen, die häufig mit unterschiedlichen Datenmodellen, Produktstrukturen und regulatorischen Prozessen arbeiten. Während die technologische Integration ein wichtiger Bestandteil dieser Programme ist, ist die Entwicklung eines gemeinsamen Blueprints ebenso entscheidend.

Denn in Europa unterscheiden sich aufsichtsrechtliche Erwartungen, steuerliche Anforderungen und Berichtspflichten je nach Jurisdiktion. Für Banken und Finanzinstitute bedeutet dies: Ohne die Neugestaltung eines gemeinsamen Betriebsmodells führen diese Unterschiede häufig zu redundanten Prozessen, inkonsistenten Daten und zusätzlichen manuellen Kontrollen.

Die Definition von Governance-Rahmenwerken, Verantwortlichkeiten und Zielprozessen vor der Implementierung kann daher die Grundlage für einen Plattform-Blueprint schaffen, der den Kern standardisiert und zugleich die notwendige Flexibilität wahrt, um lokale Marktanforderungen sowohl hinsichtlich der regulatorischen Compliance als auch der operativen Steuerung während der gesamten Transformation zu berücksichtigen.

Grenzüberschreitende Betriebsmodelle erfordern sowohl zentrale Konsistenz als auch lokale Flexibilität. Die Standardisierung zentraler Prozesse verbessert Effizienz und Governance, während sich lokale regulatorische Anforderungen weiterhin von einer Jurisdiktion zur anderen unterscheiden.

Viele Privatbanken betreiben weiterhin mehrere Anwendungen, die ähnliche Geschäftsprozesse unterstützen oder sich überschneidende Kundendaten enthalten. Mit der Weiterentwicklung regulatorischer Anforderungen müssen Änderungen in solchen fragmentierten Umgebungen häufig gleichzeitig in mehreren Systemen umgesetzt werden.

Dies erhöht den operativen Aufwand und kann es erschweren, konsistente Daten, transparente Audit-Trails und standardisierte regulatorische Kontrollen sicherzustellen. Modernisierung trägt daher nicht nur zu einer höheren operativen Effizienz bei, sondern auch zu einer stärkeren Governance, einer verbesserten Datenqualität und größerer Transparenz für die interne Überwachung sowie für aufsichtsrechtliche Prüfungen.

Das grenzüberschreitende Bankgeschäft unterliegt einem kontinuierlichen regulatorischen Wandel. Ein Beispiel hierfür ist die Capital Requirements Directive VI (CRD VI), die einen harmonisierten europäischen Rahmen für die Erbringung zentraler Bankdienstleistungen durch Banken aus Drittstaaten einführt.

Während der übergeordnete Rahmen auf EU-Ebene vereinbart wurde, liegt die Umsetzung weiterhin in der Verantwortung der einzelnen Mitgliedstaaten, wodurch Unterschiede hinsichtlich des Zeitplans und der aufsichtsrechtlichen Auslegung entstehen.

Für international tätige Privatbanken bedeutet dies, dass regulatorische Veränderungen fortlaufend in Governance-Strukturen, Betriebsmodellen und der Planung technologischer Innovationen berücksichtigt werden müssen. Dies erfordert zugleich, Compliance und operative Resilienz als strategische Fähigkeiten und nicht lediglich als regulatorische Verpflichtungen zu verstehen.

Erst dann mit den Vorbereitungen für die Umsetzung zu beginnen, wenn neue Anforderungen bereits in Kraft treten, macht die Anpassung komplexer – insbesondere für Institute, die in mehreren Jurisdiktionen tätig sind.

Karl im Brahm

Der Kommentar erläutert ausführlich und praxisorientiert für alle tangierten Branchen die gesetzlichen und regulatorischen Vorgaben zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung im deutschen Recht.

Ergänzend werden wesentliche Grundlagen für den Umgang mit Finanzsanktionen dargestellt. Relevante Änderungen durch das EU-AML-Paket 2024 werden berücksichtigt. Die Kommentierung richtet sich in erster Linie an Personen, die täglich mit der Einhaltung und Umsetzung der Vorgaben beschäftigt sind.

Die Neuauflage berücksichtigt

- Sämtliche Auslegungs- und Anwendungshinweise zum GwG
- Rundschreiben der Aufsichtsbehörden, Guidelines der EBA
- Sämtliche aktuellen EU-Richtlinien und relevanten Umsetzungsgesetze, wie insbesondere
  - EU-AML-Paket 2024 (AML VO, AML-Richtlinie, AMLA VO, GTVO)
  - Finanzkriminalitätsbekämpfungsgesetz – FKBG
  - Erweiterte Kommentierung zu Finanzsanktionen inkl. Verpflichtungen nach dem EU-AML-Paket

Herausgegeben von

Dr. **Uta Zentes**, LL.M. ist als Rechtsanwältin und Head of Compliance tätig. Zuvor hatte sie über mehrere Jahre verschiedene Leitungspositionen in der Compliance-Funktion einer Großbank inne, bevor sie viele Jahre in Big Four-Gesellschaften in der Beratung bzw. Prüfung von Compliance-Themen tätig war. Frau Dr. Zentes ist Lehrbeauftragte, regelmäßig als Referentin tätig und Autorin zahlreicher Fachartikel zum Thema Geldwäscheprävention und Compliance.

RA **Sebastian Glaab** ist Rechtsanwalt und Partner bei Annerton Rechtsanwaltsgesellschaft mbH. Er berät insbesondere in den Themenfeldern Geldwäscheprävention, Wertpapier-Compliance, MaRisk-Compliance und Sanktionen. Aufgrund seiner langjährigen Tätigkeit als Compliance-Officer und Geldwäschebeauftragter in einem international tätigen Kreditinstitut verfügt Herr Glaab zudem über eine große praktische Expertise.

Zentes/Glaab (Hrsg.)
GwG – Geldwäschegesetz, GeldtransferVO, relevante Vorgaben aus KWG, VAG, StGB, AO, ZAG, AWG und Finanzsanktionen

4. Auflage 2025 | Frankfurter Kommentar
1.969 Seiten | Hardcover | € 289,00
ISBN: 978-3-8005-1937-8

Weitere Informationen
shop.ruw.de

Keine Buch-Neuerscheinung mehr verpassen? Abonnieren Sie doch gerne unseren Newsletter: **shop.ruw.de/newsletter**

dfv Mediengruppe
www.shop.ruw.de | Deutscher Fachverlag GmbH | Frankfurt am Main
Tel 08581 9605-0 | Fax 08581 754 | E-Mail info@suedost-service.de
R&W Fachmedien Recht und Wirtschaft

Report: Deutschland braucht eine stärkere Speak-up-Kultur

Vorschriften in den Bereichen Hinweisgeberschutz, KI-Governance und Datenschutz werden zunehmend komplexer. Die eigentliche Herausforderung besteht heute weniger darin, neue Regeln zu verstehen, sondern diese organisationsweit wirksam umzusetzen. Die Ergebnisse des NAVEX Reports 2026 „Whistleblowing und Compliance in Europa: Datengestützte Einblicke und Benchmarks" zeigen, dass die größten Hürden inzwischen operativer Natur sind. Vor diesem Hintergrund gewinnen Hinweisgebersysteme deutlich an Bedeutung. Sie liefern wertvolle Erkenntnisse über Risiken, Kontrollschwächen und kulturelle Entwicklungen innerhalb eines Unternehmens.

© IMAGO / YAY Images
Ein wichtiger Baustein, der manchen Unternehmen zur wirksamen Compliance noch fehlt: Speak-up-Kultur.

Grundlage der Analyse sind 2,37 Millionen Hinweisgebermeldungen aus mehr als 4.000 Organisationen sowie die Befragung von mehr als 1.100 Risiko- und Compliance-Verantwortlichen weltweit. Die Ergebnisse zeigen, Compliance-Verantwortliche in ganz Europa kämpfen heute nicht mehr mit mangelndem Bewusstsein für Compliance – sondern mit der zunehmenden Komplexität regulatorischer Anforderungen. Besonders häufig nennen sie sich überschneidende Vorschriften, Verzögerungen bei der Umsetzung, interne Abstimmungsprobleme und steigenden administrativen Aufwand als bedeutendste Auswirkungen der zunehmenden EU-Regulierungen.


© NAVEX
Oliver Riehl ist Regional Vice President Sales bei NAVEX.

In Deutschland sehen 43 % der Befragten die Integration neuer regulatorischer Anforderungen in bestehende Systeme als größte Hürde. Es folgen Abweichungen zwischen europäischen Vorgaben und ihrer nationalen Umsetzung (40 %) sowie mangelnde interne Abstimmung (37 %). Begrenzte Ressourcen und fehlende regulatorische Klarheit wurden von einem Drittel der Befragten genannt.

Mehr als die Hälfte der europäischen Unternehmen bewertet den Reifegrad ihrer eigenen Compliance-Programme inzwischen als „Verwaltend" oder „Optimierend". Compliance ist damit eine etablierte Unternehmensfunktion und nicht mehr lediglich ein sich entwickelnder Aufgabenbereich. Im internationalen Vergleich besteht jedoch weiterhin Potenzial, insbesondere bei der Weiterentwicklung und Skalierung bestehender Programme.

Wirksame Meldekanäle ermöglichen es Unternehmen, Probleme frühzeitig zu erkennen und zugleich gegenüber Aufsichtsbehören nachzuweisen, dass ihre Governance-Prozesse wie vorgesehen funktionieren.

Außerhalb Nordamerikas ist die webbasierte Meldung mittlerweile der wichtigste Meldeweg für Whistleblowing. Ein besonders interessantes Ergebnis der Studie betrifft das Meldeverhalten. In Kontinentaleuropa gehen durchschnittlich 0,85 Hinweise pro 100 Mitarbeiter ein – weltweit liegt der Durchschnitt bei 1,65. Dieser Unterschied lässt sich vor allem durch den Reifegrad der regulatorischen Anforderungen erklären. Während die EU erst 2021 umfassende Whistleblowing-Vorschriften eingeführt hat, verfügen Länder wie das Vereinigte Königreich (1999), die USA (2002) und Kanada (2007) bereits seit vielen Jahren über entsprechende Regelwerke.

Auf den ersten Blick könnten geringere Meldezahlen positiv wirken. Sie bedeuten jedoch nicht zwangsläufig weniger Vorfälle, sondern können auch auf eine geringere Sensibilisierung, weniger Meldekanäle oder eine weniger ausgeprägte Speak-up-Kultur hinweisen. Mit einem Anteil von 58 % verzeichnet Europa weltweit die höchste Quote an anonymen Meldungen. Anonymität ist zwar ein wichtiger Schutzmechanismus für Hinweisgebende. Gleichzeitig kann sie aber Ausdruck mangelnden Vertrauens in den Umgang mit Meldungen oder in den Schutz vor Vergeltungsmaßnahmen sein.

Positiv fällt hingegen die Qualität der Hinweise aus. Rund 45 % der Meldungen in Kontinentaleuropa werden bestätigt und liegen damit auf dem Niveau des weltweiten Durchschnitts. Dies spricht dafür, dass Hinweisgebende überwiegend berechtigte und substanzielle Sachverhalte melden.

Für eine wirksame Compliance-Kultur ist auch das Verhalten der Führungskräfte entscheidend. Zwar geben 63 % der europäischen Befragten an, dass ihre Unternehmensleitung Ethik und Compliance aktiv unterstützt. Beim Vorleben ethischen Handelns oder bei der konsequenten Einhaltung von Compliance-Grundsätzen unter wirtschaftlichem Druck liegt Europa jedoch weiterhin unter dem globalen Durchschnitt. Das weist auf eine bekannte Herausforderung hin: Viele Unternehmen haben zwar in Compliance-Strukturen investiert, doch das Engagement der Führungsebene hat sich nicht immer im gleichen Maße weiterentwickelt.

Hinweisgebersysteme sollten nicht isoliert als regulatorische Pflicht verstanden werden, sondern als Bestandteil einer integrierten Governance-Strategie. Meldedaten liefern wertvolle Hinweise auf Risiken und Schwachstellen, lange bevor daraus größere Compliance-Verstöße entstehen.

Ebenso wichtig ist eine effiziente Bearbeitung eingehender Hinweise. In Kontinentaleuropa dauert der Abschluss einer Untersuchung im Median 53 Tage – ein Wert, der trotz steigender Meldezahlen seit Jahren nahezu unverändert bleibt. Lange Bearbeitungszeiten erhöhen das Risiko, dass sich Probleme verschärfen oder erneut auftreten.

Mit der zunehmenden regulatorischen Komplexität wird es immer wichtiger, Compliance-Prozesse in bestehende Governance-, Risiko- und Technologieplattformen zu integrieren. Kennzahlen wie Meldevolumen, Anonymitätsquote, Bestätigungsrate und Bearbeitungsdauer liefern dabei wertvolle Hinweise auf den Reifegrad eines Compliance-Programms. Diese Kennzahlen helfen Unternehmen, über die reine Erfüllung regulatorischer Anforderungen hinauszugehen und widerstandsfähige, transparente und verantwortungsvoll geführte Organisationen aufzubauen.

Unternehmen sollten eine Kultur fördern, in der Mitarbeiter darauf vertrauen können, dass ihre Meldungen ernst genommen, fair bearbeitet und ohne negative Konsequenzen behandelt werden. Wirksame Compliance entsteht nicht allein durch Systeme, sondern durch Transparenz, Schulungen und Vertrauen. *Oliver Riehl*

Der Report kann hier eingesehen werden.

NIS-2-Pflichtschulung für Geschäftsleitungen

Eine Veranstaltung von R&W Fachkonferenzen

15. Oktober 2026, 10.00 bis 12.00 Uhr | Online-Schulung

Jetzt anmelden!

Cybersicherheit ist Chefsache. Von der Regulierung der NIS-2-Richtlinie und der Umsetzung im BSIG sind in Deutschland über 29.000 Unternehmen betroffen, viele erstmals. Neben klassischen Betreibern kritischer Infrastrukturen erfasst das Gesetz nun auch mittelständische Unternehmen etwa aus Maschinenbau, Lebensmittelproduktion, Chemie, Post- und Kurierdienstleistung oder Abfallentsorgung – bereits ab 50 Beschäftigten oder einem Jahresumsatz und einer Jahresbilanzsumme von je 10 Mio. Euro. Für die Leitungsorgane der regulierten Unternehmen gilt § 38 Abs. 3 BSIG: diese verpflichtet die Geschäftsleitung zu regelmäßiger Schulung.

DAS ERWARTET SIE:

In dieser Live-Schulung vermitteln wir, was das Gesetz von der Leitungsebene rechtlich verlangt. Der Fokus liegt auf den Rechtspflichten der Leitungsorgane – Risikoerkennung, Steuerungs- und Überwachungsverantwortung, Mindestmaßnahmen, Melde-, Registrierungs- und Dokumentationspflichten, Managemententscheidungen im Krisenfall sowie persönliche Haftung und Bußgelder.

Keine Schulung zum Absitzen: Live-Austausch mit den Referentinnen, Rückfragen ausdrücklich erwünscht, Vermittlung von Inhalten statt Referieren von Paragraphen.

Zielgruppe: Geschäftsführung, Vorstand und Leitungsorgane besonders wichtiger und wichtiger Einrichtungen aller Branchen – insbesondere auch Unternehmen, die erstmals unter die Cybersicherheitsregulierung fallen.

DIE THEMEN IM ÜBERBLICK:

- Überblick zur NIS-2-Richtlinie und zum Umsetzungsgesetz
- Betroffenheitsprüfung
- Pflichten der Geschäftsleitung: Risikomanagement (Steuerung und Überwachung), Melde-, Registrierungs- und Dokumentationspflichten
- Managemententscheidungen im Cyber-Krisenfall
- Persönliche Haftung
- Bußgelder

FREUEN SIE SICH AUF:

Larissa Normann
Partnerin
GÖHMANN Rechtsanwälte

Bettina Zerelles
Partnerin
GÖHMANN Rechtsanwälte

Teilnahmegebühren (zzgl. MwSt.):

369,– EUR Abonnent:innen eines Titels der Fachmedien Recht und Wirtschaft

399,– EUR Normalpreis

Teilnahmezertifikat zur Dokumentation der Einhaltung Ihrer Schulungspflicht

Ihre Ansprechpartnerin: Frau Maria Belz

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

Deutscher Fachverlag GmbH
Mainzer Landstr. 251
60326 Frankfurt am Main

Mit Unterstützung von GÖHMANN Rechtsanwälte · Notare

Medienpartner Compliance Berater | DATENSCHUTZ-BERATER | Kommunikation & Recht

JETZT ANMELDEN UNTER
www.ruw.de/NIS2-Pflicht
oder QR-Code scannen

// WIR FEIERN **80 JAHRE** /

R&W Fachkonferenzen

Eine Medienmarke der dfv Mediengruppe