Point of Compliance
Das Risikomanagement-Magazin

AUSGABE 1/2026

PoC

DZ CompliancePartner

Folgen Sie der DZ CompliancePartner GmbH auf Social Media.

IMPRESSUM

PoC – Point of Compliance
Das Risikomanagement-Magazin,
Ausgabe 38, 1/2026
ISSN: 2194-9514
Herausgeber: DZ CompliancePartner GmbH, Wilhelm-Haas-Platz, 63263 Neu-Isenburg, Telefon 069 580024-0, Telefax 069 580024-900, www.dz-cp.de
Handelsregister HRB 11105, Amtsgericht Offenbach, USt.-IdNr.: DE201150917
Geschäftsführung: Jens Saenger (Sprecher), Dirk Pagel

Verantwortlich i. S. d. P.: Jens Saenger
Redaktion: Gabriele Seifert, Leitung (red.)
Redaktionsanschrift: DZ Compliance-Partner GmbH, Redaktion Point of Compliance, Wilhelm-Haas-Platz, 63263 Neu-Isenburg, Telefon 069 580024-0, Telefax 069 580024-900, E-Mail: poc@dz-cp.de
Weitere Autoren dieser Ausgabe:
Derya Isikli-Mustafa, Abel Measho, Annika Poschwatta, Jens Saenger, Jörg Scharditzky, Eugenia Scherbanev, Lars Schinnerling, Thomas Schirmer, Thomas Schröder, Benjamin Wellnitz

Bildnachweise: iStockphoto.com/Devrimb, www.verbraucherzentrale.de, DZ Compliance-Partner GmbH
Gestaltung: DZ CompliancePartner GmbH
Druck: Thoma Druck, Dreieich

Redaktionsschluss: 3. März 2026
Auflage: 3.500 Exemplare

Der Wendepunkt in der europäischen Digitalpolitik: Mit der KI-Verordnung setzt die Europäische Union weltweit Maßstäbe für die Regulierung Künstlicher Intelligenz. Der Anspruch ist klar: Innovation ermöglichen und zugleich Grundrechte schützen. Dieser Balanceakt entscheidet auch darüber, ob Europa im globalen Wettbewerb nicht nur Regeln festsetzt, sondern auch Innovationsstandort bleibt (siehe Seite 4).

Zudem bieten KI-Technologien enorme Chancen – von effizienteren Verwaltungsprozessen bis hin zu neuen Geschäftsmodellen im Mittelstand. Ein strategisches Chancenmanagement wird damit zur Führungsaufgabe: Unternehmen müssen Potenziale systematisch identifizieren, Risiken bewerten und Kompetenzen aufbauen. Regulierung schafft dabei nicht nur Grenzen, sondern auch Vertrauen (siehe Seite 18).

Gleichzeitig verschärfen KI und Digitalisierung die Risiken in der Geldwäsche- und Betrugsprävention. Internationale Geschäftsbeziehungen sind komplexer denn je und kriminelle Akteure nutzen automatisierte Systeme für Täuschung und Verschleierung. Hier sind robuste Compliance-Strukturen, transparente Datennutzung und grenzüberschreitende Zusammenarbeit gefragt. Europas Antwort muss lauten: technologieoffen, wertebasiert und entschlossen (siehe Seite 22).

Hinzu kommen verschärfte Anforderungen an den Umgang mit Interessenkonflikten im Wertpapiergeschäft gemäß Wertpapierhandelsgesetz, die eine klare Governance und wirksame Kontrollmechanismen verlangen (siehe Seite 9). Auch aus Sicht der Bankenaufsicht rückt eine gelebte Risikokultur nach den MaRisk stärker in den Fokus – sie ist das Fundament für verantwortungsvolle Innovation und nachhaltige Stabilität im Finanzsystem (siehe Seite 12).

Ich wünsche Ihnen eine anregende Lektüre.

Herzlichst
Ihr Jens Saenger

Jens Saenger
Sprecher der Geschäftsführung

EU-Digitalpolitik: Regulierung von KI, Daten und digitalen Diensten und der Einfluss auf den Finanzsektor

Die rasante Entwicklung von KI und in der Datenverarbeitung verändert die Geschäftslandschaft grundlegend. Dabei sind Daten der Katalysator der digitalen Transformation. Die Europäische Union reagiert mit einer Vielzahl von Vorschriften und Richtlinien. Doch welchen Einfluss hat das auf den Finanzsektor?

Dieser Beitrag gibt einen Überblick über die wichtigsten EU-Regulierungen im Bereich KI, Daten sowie digitale Dienste und analysiert ihre Auswirkungen auf die Finanzbranche.

1. EU AI Act

Der EU AI Act stellt eine der umfassendsten und bedeutendsten Regulierungen im Bereich der Künstlichen Intelligenz (KI) dar. Sein primäres Ziel besteht darin, allgemeine Rahmenbedingungen für das Inverkehrbringen, die Inbetriebnahme und die Nutzung von KI-Systemen und KI-Modellen mit allgemeinem Verwendungszweck zu etablieren. Der EU AI Act bezieht sich ausschließlich auf KI-Systeme und KI-Modelle mit allgemeinem Verwendungszweck und wurde entwickelt, um sicherzustellen, dass diese sicher, transparent und ethisch vertretbar sind.

Ein zentrales Merkmal des EU AI Act ist sein risikobasierter Ansatz. Dieser Ansatz zielt nicht darauf ab, die KI-Technologie selbst zu regulieren, sondern vielmehr deren Einsatzbereiche.[1] Durch diese Differenzierung wird eine flexible und anpassungsfähige Regulierung ermöglicht, die den spezifischen Risiken und Herausforderungen verschiedener Anwendungsbereiche gerecht wird.

Die Marktüberwachung obliegt derzeit der Bundesnetzagentur. Es ist noch nicht abschließend geklärt, ob in speziellen Fällen, insbesondere im Finanzsektor, die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zuständig sein wird. Diese Aufteilung der Verantwortlichkeiten würde sicherstellen, dass die Regulierung sowohl umfassend als auch spezialisiert ist, um den besonderen Anforderungen der jeweiligen Branchen gerecht werden zu können.

Der EU AI Act markiert somit einen bedeutenden Schritt in Richtung einer harmonisierten und verantwortungsvollen Nutzung von KI-Technologien innerhalb der Europäischen Union.

2. Data Governance Act (DGA)

Der Data Governance Act (DGA) ist ein strategischer Ansatz zur Neugestaltung der europäischen Datenökonomie. Ziel ist es, ein koordiniertes und rechtskonformes Datenökosystem aufzubauen, das die Datenmobilität über physische Speicherorte hinweg ermöglicht.

Dies ist besonders wichtig für die schnelle Entwicklung von KI-Technologien und unterstützt eine auf den Menschen ausgerichtete, vertrauenswürdige und sichere Datengesellschaft und -wirtschaft.[2]

Durch den DGA werden geeignete Mechanismen implementiert, um die Weiterverwendung von Daten des öffentlichen Sektors, die bislang nicht als offene Daten verfügbar sind, zu erleichtern.

Die Integration dieser Daten in Innovationsprozesse bietet Unternehmen und Einzelpersonen in verschiedenen Sektoren, wie Gesundheit, Mobilität, Umwelt und Finanzen, wesentliche Vorteile: Durch die intelligente Nutzung von Daten können effizientere Lebens- und Arbeitsweisen entwickelt werden, die nicht nur die Produktivität steigern, sondern auch nachhaltige Lösungen für aktuelle Herausforderungen bieten.

Der DGA ist von entscheidender Bedeutung für die schnelle und nachhaltige Entwicklung von KI-Technologien. Durch die Bereitstellung eines sicheren, transparenten und rechtlich klar definierten Rahmens für die Datenverwendung können Unternehmen und Forschungseinrichtungen leichter auf Daten zugreifen und diese nutzen. Dies fördert nicht nur die Innovation, sondern auch die Entwicklung einer auf den Menschen ausgerichteten, vertrauenswürdigen und sicheren Datengesellschaft und -wirtschaft.

Der Regulierungsrahmen richtet sich an multiple Stakeholder, darunter Wirtschaftsteilnehmer, Technologieunternehmen sowie öffentliche und private Dateninfrastrukturen.

Die Bundesnetzagentur trägt die aufsichtsrechtliche Hauptverantwortung für den Data Governance Act in Deutschland. Sie wird dabei von anderen spezialisierten Behörden unterstützt, die jeweils spezifische Aspekte der Datenregulierung abdecken. Beispielsweise fällt in den Zuständigkeitsbereich der Bundesbeauftragten für den Datenschutz und die Informationssicherheit die Sicherstellung der Datenschutzkonformität.

3. Data Act

Der Data Act ist eine Vorschrift für einen fairen Datenzugang und eine faire Datennutzung. Er ist seit dem 12. September 2025 gültig und unmittelbar anwendbar. Ziel des Data Act ist es, sektorübergreifende Rahmen für die gemeinsame Nutzung von Daten zu schaffen. Durch die Regelung, wer unter welchen Voraussetzungen auf Daten zugreifen kann, soll die Innovation gefördert, die Wertschöpfung verbessert[3] und gleichzeitig ein fairer und sicherer europäischer Datenbinnenmarkt geschaffen werden.[4]

Der Data Act markiert einen wichtigen Meilenstein in der europäischen Datenpolitik und hat weitreichende Auswirkungen auf neue Technologien wie KI.

Durch den erleichterten Zugang zu großen Datenmengen aus verschiedenen Sektoren, welche für das Trainieren von KI-Modellen erforderlich sind, können KI-Systeme besser, präziser und leistungsfähiger werden.

Zudem fördert der Data Act die Innovation im KI-Sektor. Somit werden insbesondere für Start-ups die gleichen Zugangsmöglichkeiten geschaffen für namhafte Unternehmen, wodurch der Wettbewerb gefördert und die Entwicklung von neuen KI-Anwendungen beschleunigt wird. Dies wird eine Auswirkung auf viele Branchen, so auch den Finanzsektor, haben.

Schlussendlich wird durch die klaren Regulierungen und die Förderung eines fairen Datenzugriffs das Vertrauen in KI-Systeme gestärkt, was deren Akzeptanz und Verbreitung fördert.

Der Data Act stellt somit eine zentrale Säule für die zukünftige Entwicklung einer datengetriebenen und wettbewerbsfähigen europäischen Wirtschaft dar, insbesondere im Bereich der KI-Technologien.

Adressat sind insbesondere Hersteller von vernetzten Produkten, auch Internet of Things oder IoT-Produkte genannt, und Anbieter von verbundenen Diensten und andere Nutzer.[5]

Fraglich ist, inwiefern der Data Act auf den Finanzsektor eine Auswirkung haben könnte, da in der Regel dieser eher selten Hersteller von vernetzten Produkten sein wird. Zwar stellt ein Finanzunternehmen keinen vernetzten Kühlschrank her, jedoch kann eine Banking-App unter Umständen unter den Data Act fallen oder aber durch Anwendungen und Dienste als Software-as-a-Service gelten. Beispielsweise kann ein Institut auch durch Finanztransaktionen oder Abschlüsse von Versicherungsverträgen als Hersteller oder Datenverarbeitungsdienst eingestuft werden und damit in den Adressatenkreis fallen.

Die Bundesnetzagentur ist die zuständige Aufsichtsbehörde.[6] Aber die Landesdatenschutzaufsichtsbehörden würden parallel weiterhin die Aufsicht haben, sofern personenbezogenen Daten betroffen sind.[7]

4. Digital Services Act (DSA)

Der Digital Services Act (DSA) stellt einen zentralen Bestandteil der europäischen Digitalpolitik dar und ist seit dem 17. Februar 2024 unmittelbar anzuwenden. Der DSA verfolgt mehrere zentrale Ziele, darunter

- die Festlegung von Grundregeln für das Marktverhalten von Anbietern digitaler Dienste,
- die Schaffung von Abwehrmöglichkeiten für Verbraucher zur Sicherstellung ihrer Rechte im digitalen Raum,
- die Etablierung eines sicheren und vertrauenswürdigen Umfelds, in dem die Grundrechte aller Nutzer digitaler Dienste gewährleistet sind, sowie
- die Verpflichtung von Plattformen, illegale Inhalte zu entfernen und das Risiko zu minimieren, dass solche Inhalte auf die Plattformen gelangen.

Der Digital Services Act (DSA) stellt strenge Anforderungen an die Datenqualität und -sicherheit, wobei durch die Entfernung illegaler Inhalte und die Minimierung von Risiken die Integrität der Daten für KI-Modelle verbessert wird und somit präzisere und zuverlässigere KI-Systeme ermöglicht werden.

Weiterhin wird die Transparenz und Verantwortlichkeit bei der Nutzung von digitalen Diensten gefördert, indem Anbieter von KI-Technologien gem. Art. 24 DSA verpflichtet werden, ihre Systeme und Datenverarbeitungsprozesse klar und verständlich darzulegen,[8] wodurch das Vertrauen der Nutzer gestärkt und Missbrauch verhindert wird.

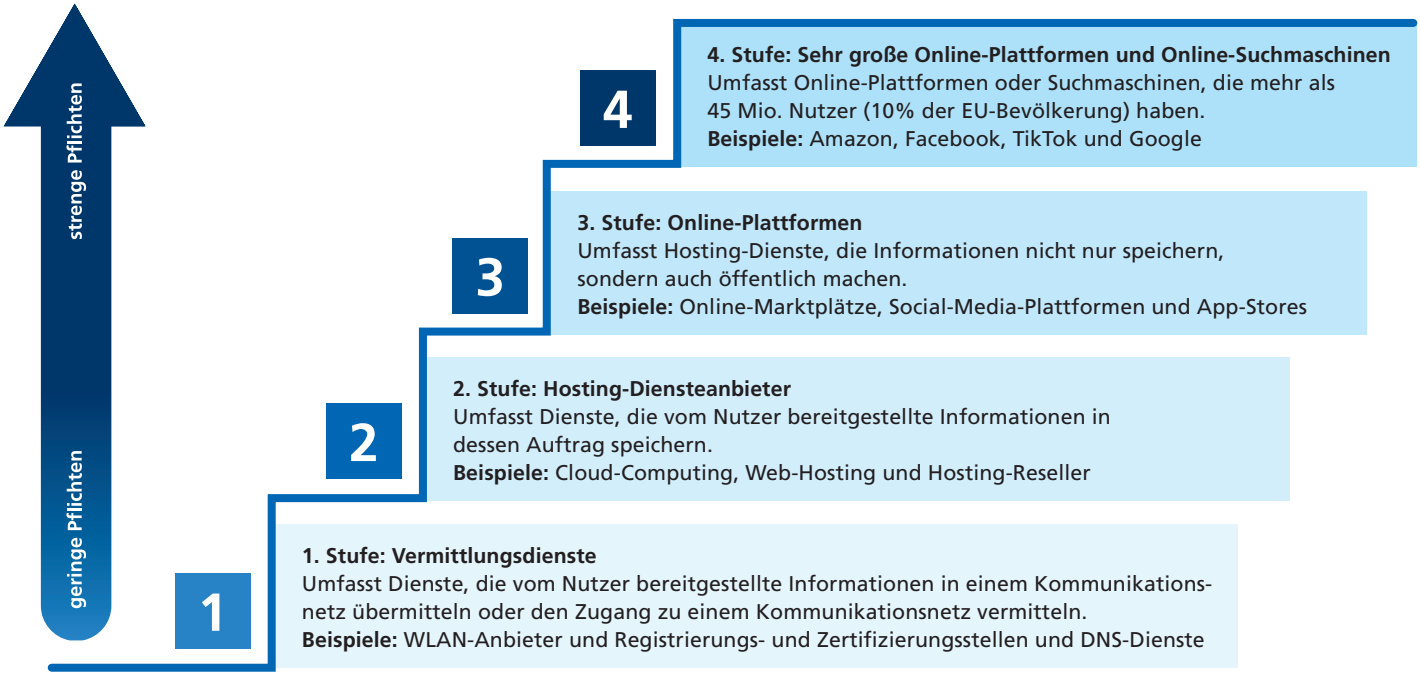
Der DSA verpflichtet gem. Art. 23 DSA zur Bekämpfung illegaler Inhalte und minimiert das Risiko ihrer Verbreitung auf Plattformen. Das ist besonders für KI-Systeme wichtig, die auf großen Datenmengen basieren. Die strengen Vorgaben des DSA tragen zur Sicherheit und Integrität dieser Systeme bei und schützen die Nutzer.

Durch die klaren Regeln und Verbraucherschutzmechanismen im DSA werden ebenfalls Innovationen und Wettbewerb im KI-Sektor gefördert.

Adressat sind primär Online-Plattformen und Suchmaschinenbetreiber, die digitale Dienste anbieten.

Adressat können aber auch sämtliche Anbieter von Vermittlungsdiensten sein. Damit sind Dienste gemeint, die Daten für ihre User speichern bzw. übertragen oder Informationen verarbeiten. Dabei gelten für größere Online-Plattformen weitaus strengere Vorgaben, da die Pflichten

Abb. 1. **Die vier Stufen des DSA (Digital Services Act)**



Quelle Grafik: https://www.e-recht24.de/datenschutz/13247-digital-services-act.html#

entsprechend der Einstufung des Anbieters bestimmt werden. Der DSA regelt dabei vier Stufen (siehe Grafik auf Seite 6).

Finanzunternehmen könnten unter Umständen unter den DSA fallen, wenn sie bspw. digitale Dienste anbieten. Dies wäre bei Finanzdienstleistungsplattformen der Fall. Ein weiteres Beispiel wäre das Anbieten von Crowdfunding-Diensten als Vermittler.

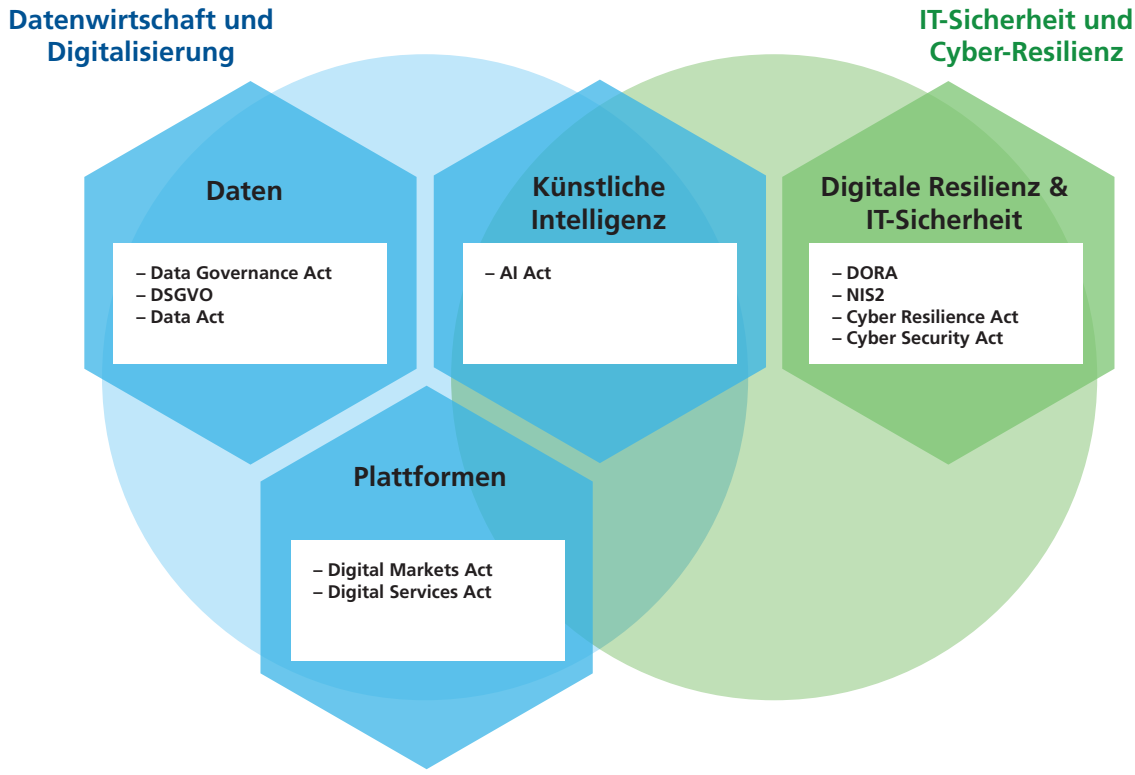
In Deutschland ist die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) für die Überwachung und Einhaltung des Digital Services Act (DSA) zuständig.

5. Digital Markets Act (DMA)

Der Digital Markets Act (DMA) ist im November 2022 in Kraft getreten und seit dem Mai 2023 gültig. Ziel ist es, einheitliche Wettbewerbsbedingungen auf dem digitalen Markt zu etablieren. Zu den Kernzielen gehören die Förderung eines fairen Wettbewerbes, die Stärkung der Innovation sowie die Erweiterung der Verbraucherrechte. Dabei stehen die marktbestimmenden großen Plattformdienste, sogenannte Gatekeeper, im Fokus des Gesetzes. Die Einstufung einer Plattform als Gatekeeper erfolgt auf Basis der Anzahl der aktiven Nutzer und des Jahresumsatzes. Plattformen, die diese Kriterien erfüllen, sind beispielsweise die bekannten Tech-Riesen wie Amazon, Apple, Meta und Microsoft. Diese Unternehmen besitzen eine dominante Marktstellung, die es ihnen ermöglicht, den Wettbewerb zu beeinflussen und potenziell zu beeinträchtigen. Durch den DMA sollen diese Gatekeeper verpflichtet werden, ihre Marktmacht nicht missbräuchlich einzusetzen. Dies umfasst Maßnahmen zur Förderung der Interoperabilität, zur Bereitstellung von Datenzugang und zur Transparenz bei Werbung und Algorithmen. Der DMA zielt darauf ab, neue Unternehmen und Innovationen zu ermutigen, indem faire und transparente Bedingungen geschaffen werden, unter denen alle Marktteilnehmer agieren können.

Der DMA fungiert als spezifisches Wettbewerbsregulierungsinstrument, das über traditionelle kartellrechtliche Ansätze hinausgeht. Er zielt auf eine proaktive Marktgestaltung durch präventive Regulierungsmechanismen.[9]

Abb. 2. **Abhängigkeiten von Digitalwirtschaft und IT-Sicherheit**



Obwohl Banken nicht direkt Adressaten des DMA sind, können sie mittelbar von dessen Regelungen profitieren. Ein Beispiel hierfür ist die Öffnung von iPhone-Geräten für alternative Zahlungsmethoden neben Apple Pay, wodurch Banken ihre eigenen Zahlungslösungen anbieten können. Diese Entwicklung kann zu einer Stärkung des Wettbewerbs und einer größeren Vielfalt an Zahlungsmöglichkeiten für Verbraucher führen.

Zuständige Stelle der Einhaltung und Sanktionierung ist primär die Europäische Kommission. Für Verbraucher oder Mitbewerber besteht die nationale Beschwerdemöglichkeit über das Gesetz gegen Wettbewerbsbeschränkungen (GWB).

6. Weitere Regelungen aus der Cybersicherheit

Weitere Rahmenwerke sind die DORA, NIS2, der Cyber Security Act und der Cyber Resilience Act, die die Grundprinzipien der Cybersicherheit erfassen. Sie stellen einen ganzheitlichen Schutz des digitalen Ökosystems dar. Auf sie wird jedoch in diesem Beitrag nicht näher eingegangen.

7. Rangfolge der europäischen digitalen Regulierungsrahmen

Die EU-Regulierung bilden ein komplexes Regelwerk mit mehren Ebenen. Dabei verfolgen sie zwar unterschiedliche Ziele, jedoch bezwecken sie zusammen einen verantwortungsvollen Umgang mit Daten und Technologien:

- DSGVO (Datenschutz): Grundlage für den Schutz personenbezogener Daten.
- Data Governance Act und der Data Act (Datenaustausch & -nutzung): aufbauend auf der DSGVO und regelt den Datenaustausch.
- EU AI-ACT (KI-Risiken): Nutzung von Datenregeln und die DSGVO, um KI-Risiken zu minimieren.
- Der Digital Services Act und der Digital Markets Act (Plattformen & Wettbewerb): Verhaltensregeln auf Plattformen, das von den Daten- und KI-Regeln beeinflusst wird.

Fazit

Während Regulierungen oft als Herausforderungen wahrgenommen werden, bieten sie auch Chancen für die Entwicklung neuer Geschäftsmodelle und die Stärkung der Wettbewerbsfähigkeit. Gleichzeitig müssen sich die Finanzunternehmen mit den neuen Regularien auseinandersetzen. Letztlich bilden die Regularien die Basis für die – insbesondere in der Finanzbranche zwingend erforderliche – Umsetzungssicherheit und damit für das notwendige Vertrauen in die neue Technologie. ▬

Derya Isikli-Mustafa
Beauftragte Datenschutz, zertifizierte Datenschutzauditorin und KI-Expertin,
E-Mail: derya.isikli-mustafa@dz-cp.de

[1] Zur weiteren Vertiefung Isikli in PoC 1/2024, PoC 2/2025 und PoC 2/2023.
[2] ErwGr 2 Data Governance Act
[3] Große FAQ zum Data Act: Das sollten Unternehmen wissen (https://www.ra-plutte.de/data-act/)
[4] Große FAQ zum Data Act: Das sollten Unternehmen wissen (https://www.ra-plutte.de/data-act/)
[5] Data Act: Was Finanzunternehmen wissen müssen (https://www.srd-rechtsanwaelte.de/blog/data-act-in-der-finanzbranche-neue-chancen-und-pflichten)
[6] https://www.bundestag.de/dokumente/textarchiv/2026/kw13-de-datennutzung-1156734
[7] Europäischer Data Act | Der Landesbeauftragte für den Datenschutz Niedersachsen (https://www.lfd.niedersachsen.de/startseite/datenschutzrecht/datenschutzrelevante_gesetzgebung/europaischer-data-act-244809.html)
[8] Verordnung - 2022/2065 - EN - EUR-Lex (https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022R2065)
[9] https://www.bundeskartellamt.de/DE/DigitalWirtschaft/RegelnDigitalwirtschaft/regelndigitalwirtschaft_node.html

Interessenkonflikte im Wertpapiergeschäft

Rechtliche Pflichten und praktische Lösungen

Interessenkonflikte zählen zu den zentralen Risiken im Wertpapiergeschäft von Banken, da sie das Vertrauen der Kunden und die Integrität des Marktes unmittelbar berühren. Die MiFID-II-Regulierung verpflichtet Institute daher zu einer systematischen Identifikation, Vermeidung und (soweit unvermeidbar) Offenlegung solcher Konflikte.[1]

Im Rahmen unserer Mehrmandanten-Dienstleistertätigkeit stellen wir regelmäßig fest, dass die praktische Umsetzung dieser Vorgaben in den Instituten zu Herausforderungen führen.[2] Hier werden insbesondere in der Bestandsaufnahme oftmals nicht alle bankindividuell angebotenen Wertpapier- und Wertpapiernebendienstleistungen aufgeführt.

Der Artikel untersucht die rechtlichen Rahmenbedingungen und typische Konfliktfelder und zeigt auf, welche organisatorischen Maßnahmen für ein wirksames Interessenkonfliktmanagement erforderlich sind.

Interessenkonflikte in der Praxis

Interessenkonflikte entstehen, wenn unterschiedliche Interessen aufeinandertreffen und dadurch das Risiko besteht, dass

- Kundeninteressen beeinträchtigt werden könnten,
- Bankinteressen den Kundeninteressen zuwiderlaufen,
- Eigene Interessen von Mitarbeitenden gegenüber Kundeninteressen bevorzugt werden,
- Interessen verschiedener Kunden kollidieren,

Mögliche Konfliktfelder ergeben sich ggf. durch

- Wertpapierberatung & Vertrieb,
- Mehrfachrollen von Mitarbeitenden,
- Vertrieb eigener Produkte,
- vertrauliche Informationen,
- Vergütungssysteme,
- Provisionsmodelle (UnionDepot Komfort, MeinDepot etc.).

Die implementierten Prozesse sowie die organisatorischen, personellen und verhaltensbezogenen Maßnahmen zur Prävention von Interessenkonflikten leisten einen wesentlichen Beitrag zum Schutz der Kunden. Das etablierte Verfahren zur Identifikation von Interessenkonflikten verfolgt das Ziel, potenzielle Konflikte frühzeitig zu erkennen und ihrer Entstehung vorzubeugen. Ein im Hause systematisch und fortlaufend geführtes Interessenkonfliktmanagement gewährleistet einen kontinuierlichen Überprüfungsprozess, bei dem die Bedürfnisse der Kunden stets im Mittelpunkt stehen.

Ausgangslage

Der Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR) stellt zur Erfüllung der regulatorischen Anforderungen im Rahmen des Interessenkonfliktmanagements vielfältige Musterdokumente bereit. Dabei wird ausdrücklich darauf hingewiesen, dass sich die Muster-Interessenkonfliktgrundsätze sowie die Muster-Kundeninformationen ausschließlich auf jene Wertpapier-(neben)dienstleistungen beziehen, die von der zugrunde gelegten Muster-Standardbank angeboten werden.[3]

Die Empfehlung des BVR lässt sich wie folgt zusammenfassen: Sollten zusätzliche Wertpapier(neben)dienstleistungen angeboten werden, die über das Angebot der Muster-Standardbank hinausgehen, besteht Handlungsbedarf [4]. In diesem Fall ist die betreffende

Wertpapier(neben)dienstleistung in die bankinternen Interessenkonfliktgrundsätze sowie die Kundeninformation aufzunehmen.

Praxisorientierte Umsetzung

Die zunehmende Dynamik von Markt- und Produktentwicklungen innerhalb des genossenschaftlichen Finanzsektors hat in den vergangenen Jahren dazu beigetragen, dass innovative Finanzprodukte – wie beispielsweise der digitale Anlage-Assistent der Union Investment „MeinInvest" – schrittweise in den Instituten eingeführt wurden.

Da die seitens des BVR zur Verfügung gestellten Musterdokumente für ein standardisiertes Produktangebot entwickelt wurden, sind bei Aufnahme bankindividueller Produkte und Dienstleistungen entsprechende Anpassungen und Ergänzungen in den Muster-Interessenkonfliktgrundsätzen sowie den Muster-Kundeninformationen vorzunehmen.

Bezugnehmend auf die vorbeschriebene Ausgangslage haben wir uns daher umfassend mit den individuellen Erweiterungen der Geschäftsmodelle innerhalb der Bankenlandschaft auseinandergesetzt und die sich daraus ergebenden notwendigen Ergänzungs- und Anpassungsbedarfe identifiziert.

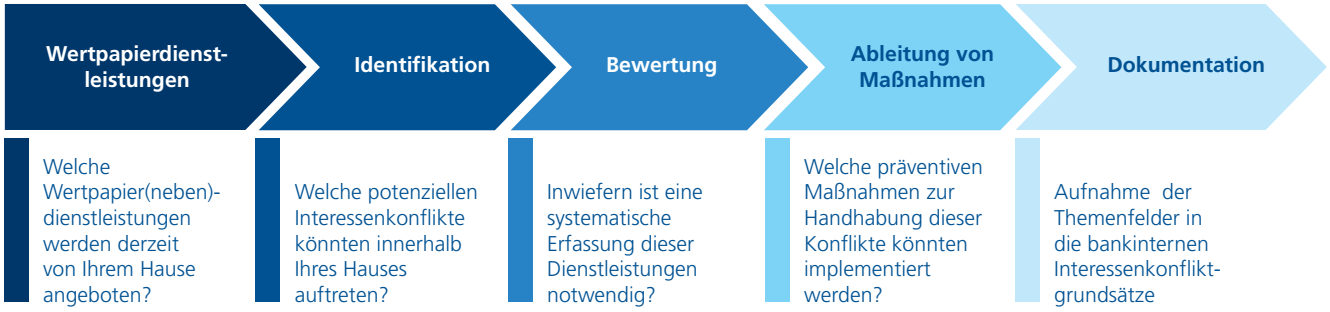
Im Ergebnis konnten Ergänzungsmuster für Institute entwickelt werden, deren Strukturen oder Geschäftsmodelle von der sogenannten Muster-Standardbank abweichen. Im Rahmen der Auslagerung WPHG-Compliance stellen wir diese Dokumente unseren Mandanten zur Verfügung.

Die von uns konzipierten Inhalte lassen sich in bestehende bankinterne Dokumentationen integrieren und bankindividuell adaptieren. Durch die systematische Zusammenführung der standardisierten Themenfelder mit den optionalen, institutsabhängigen Ergänzungen wird eine vollumfängliche Abdeckung sämtlicher relevanter Geschäftsbereiche gewährleistet.

Empfehlung zur Überprüfung der Interessenkonfliktgrundsätze[5]

Sofern nachfolgend aufgeführte Wertpapierdienstleistungen bzw. -nebendienstleistungen Bestandteil des Produktangebotes sind, empfehlen wir eine Überprüfung und ggf. Anpassung der Interessenkonfliktgrundsätze:

Abb. 1. **Beispielhafte Analyse der bestehenden Situation**



- Finanzportfolioverwaltung (eigenes Portfoliomanagement/VermögenPlus mit bankindividueller Steuerung)
- Ausgelagerte Finanzportfolioverwaltung (MeinInvest, VermögenPlus und FirmenkundenInvest)
- Beratung von bankeigenen Investmentvermögen (Fonds Advisory)
- All-In-Fee-Depotmodelle (UnionDepot Komfort und MeinDepot/ MeinDepot Premium)
- Wertpapierleihe

Hierbei wird ausdrücklich darauf hingewiesen, dass keine Gewähr für die Vollständigkeit dieser Aufstellung übernommen wird.

Zur Wahrung der aufsichtsrechtlichen Anforderungen ist es notwendig, eine gründliche Analyse vorzunehmen, um etwaige Interessenkonflikte zu identifizieren und angemessene Maßnahmen zur Vermeidung derselben zu ergreifen.

Fazit

Die fortlaufende Auseinandersetzung mit dem Thema Interessenkonflikte ist eine wichtige Aufgabe der Institute. Bestehende Regelungen sind kritisch zu hinterfragen und insbesondere bei der Neueinführung von Produkten, Dienstleistungen oder Geschäftsmodellen sind potenzielle Interessenkonflikte frühzeitig zu analysieren und zu berücksichtigen.

Durch die regelmäßige, mindestens jährliche Überprüfung wird sichergestellt, dass neue Risiken frühzeitig erkannt werden, bestehende Maßnahmen auf ihre Angemessenheit überprüft werden und Transparenz sowie Integrität in der Kundenbeziehung dauerhaft gewahrt bleiben.

Die DZ CompliancePartner steht den Instituten hierbei unterstützend zur Seite und begleitet sie mit fachlicher Expertise und praxisnahen Orientierungshilfen. ▬

Abel Measho
Beauftragter WpHG-Compliance,
E-Mail: abel.measho@dz-cp.de

Annika Poschwatta
Analystin WpHG-Compliance,
E-Mail: annika.poschwatta@dz-cp.de

[1] § 80 WpHG; Art. 33 ff. DelVO (EU) 2017/565
[2] Gemeint sind die im Rahmen der laufenden Überwachung durchgeführten Kontrollhandlungen der Beauftragten WpHG-Compliance der DZ Compliance Partner.
[3] vgl. hierzu BVR-RS vom 13.05.2022 sowie die Umsetzungshinweise zur Aktualisierung der Muster-Interessenkonfliktgrundsätze der Bank vom 22.06.2022.
[4] Z. B. wenn die Bank die Vermögensverwaltung erbringt.
[5] Positionierung der DZ CompliancePartner

Risikokultur – im Fokus der Aufsicht

Überblick und Stand der Entwicklung

Als Ursachen für die globale Finanzmarktkrise im Jahr 2008[1] sind Defizite in der Unternehmensführung (Governance) sowie mangelhafte kulturelle Grundlagen im Umgang mit Risiken und ein darauf aufbauendes Versagen in den Instituten zu nennen. Um dem entgegenzuwirken, hatte die Aufsicht im Rahmen ihrer Aufgaben zur Gewährleistung eines sicheren und effektiven Finanzsystems nicht nur den Grundstein zur Schaffung der MaRisk-Compliance-Funktion im Jahr 2012[2] gelegt, sondern mit der CRD IV im Jahr 2013 erstmals eine Erwartungshaltung formuliert, wonach eine solide Risikokultur als Teil des Risikomanagements auf allen Unternehmensebenen zu fördern ist.[3]

2017 hat die BaFin mit der fünften MaRisk-Novelle dann zunächst die Entwicklung, Förderung und Integration einer angemessenen Risikokultur als Aufgabe der Geschäftsleitung im Rahmen ihrer Gesamtverantwortung für eine ordnungsgemäße Geschäftsorganisation in die MaRisk aufgenommen.[4]

Als „Risikokultur" werden hierbei die Normen, Einstellungen und Verhaltensweisen eines Institutes auf das Risikobewusstsein, die Risikobereitschaft und das Risikomanagement sowie Kontrollen definiert, die für Entscheidungen über Risiken maßgeblich sind.[5]

Mit der sechsten MaRisk-Novelle im Jahr 2021 hat die BaFin kleine Änderungen und Klarstellungen im Hinblick auf die Risikokultur eingefügt, wobei diese maßgeblich die Berücksichtigung von ESG-Risiken sowie die Forderung nach einer Überwachung (und Dokumentation) der Risikokultur betreffen. 2023 wurde schließlich mit der siebten MaRisk-Novelle das Thema Überwachung der Risikokultur auf allen Ebenen des Instituts in die MaRisk aufgenommen.

Im Rahmen des Nationalen Aufsichtsprogramms 2025–2027 haben die Bundesbank und die BaFin das Thema Governance, das auch die Aspekte der Risikokultur beinhaltet, als einen zentralen Schwerpunkt der nationalen Bankenaufsicht definiert.[6]

Insgesamt wird Governance damit als Schlüsselfaktor für eine effektive und zukunftsfähige Bankenaufsicht gesehen. Eine solide Governance trägt wesentlich dazu bei, Risiken frühzeitig zu erkennen, Fehlsteuerungen zu vermeiden und Vertrauen in das Bankensystem zu stärken.

Ziele und Elemente einer angemessenen Risikokultur

Allgemein beschreibt die Risikokultur die Art und Weise, wie Mitarbeitende eines Instituts im Rahmen ihrer Tätigkeiten mit Risiken umgehen sollen. Die Identifizierung von und der bewusste Umgang mit Risiken soll durch eine nachhaltige Risikokultur gefördert werden.

Stichpunktartig lassen sich die Ziele der Risikokultur folgendermaßen beschreiben:

- Auseinandersetzung mit den Risiken des operativen Geschäfts (finanzielle/nichtfinanzielle Risiken)
- Schaffung und Förderung eines Risikobewusstseins, welches das tägliche Denken und Handeln prägt
- Entscheidungsprozesse führen zu Ergebnissen, die unter Risikogesichtspunkten ausgewogen sind
- Schaffen von nachhaltigen Geschäftsmodellen

- Etablieren von institutsspezifischen Werten wie Vertrauen, Professionalität und Kundennähe
- Schaffung eines Verantwortungsbewusstseins der Mitarbeitenden im Hinblick auf das Eingehen von Risiken
- Sensibilisierung für Mängel, die dann durch ergebnisorientierte und frühzeitige Maßnahmen zu beheben sind

Die Risikokultur steht nicht isoliert da und ist auch kein neuer Risikomanagementansatz, sondern ist eines von meheren Risikomanagement-Elemente, zusammen mit Interner Governance und Risikomanagement:

Risikokultur	Risikomanagement	Interne Governance
Führung	**Identifikation**	**Strategie**
Verantwortlichkeiten	**Analyse/Quantifizierung**	**Funktionstrennung**
Kommunikation	**Bewertung**	**Kompetenzsystem**
Anreize	**Bewältigung/Steuerung**	**IKS**
	Überwachung & Reporting	**Richtlinien/SfO**
		Berichtswesen

Bei der Frage, ob die Risikokultur eines Hauses angemessen ist, orientiert sich die Aufsicht an den folgenden vier Indikatoren[7], wobei diese weder als abschließend noch als Checkliste zu verstehen sind.[8]

Indikatoren für eine angemessene Risikokultur:[9]

1. Leitungskultur: „Vorleben" der gewünschten Risikokultur und Bekenntnis zu risikoangemessenem Verhalten durch Vorstand und Führungskräfte
2. Verantwortlichkeiten der Mitarbeiterinnen und Mitarbeiter: Tätigkeiten ausrichten am Wertesystem, am festgelegten Risikoappetit und an den bestehenden Risikolimits
3. Offene Kommunikation und kritischer Dialog:
   a. Konstruktive Anregungen und Kritik, alternative Standpunkte offen kommunizieren
   b. Mitarbeitenden ermöglichen, vertrauliche Bedenken über Vorgehensweisen im Institut zu äußern
4. Angemessene Anreizstrukturen schaffen: unterstützende Motivation durch materielle und immaterielle Anreize, sich entsprechend dem Wertesystem zu verhalten und innerhalb der festgelegten Risikolimits und Risikotoleranzen zu agieren

Die Indikatoren der Risikokultur werden durch konkrete, nachhaltige Maßnahmen sichtbar, greifbar und nachprüfbar.

Maßnahmen zur Etablierung und Stärkung der Risikokultur

Seitens der Aufsicht gibt es keine „definierte“ oder „vorgeschriebene“ Risikokultur. Risikokultur ist individuell und abhängig von dem Geschäftsmodell, den Produkten und Kunden, der Eigentümerstruktur und/oder einer Verbundzugehörigkeit sowie dem Proportionalitätsprinzip. Die Risikokultur einer regional tätigen Volksbank Raiffeisenbank sieht anders aus als die einer international agierenden Großbank.

Mit der fünften MaRisk-Novelle[10] hat die Aufsicht die Verantwortlichkeit für das Thema Risikokultur beim Vorstand angesiedelt: Die Mitglieder des Vorstands haben die wichtigste Vorbildfunktion (Tone from the Top); ihre Äußerungen und ihr Verhalten sollen ein Wertesystem widerspiegeln, das die Grundlage für die Risikokultur im Institut darstellt.

Der Vorstand sollte

- fortlaufend verdeutlichen, dass von den Mitarbeitenden ein ethisch und ökonomisch einwandfreies Verhalten erwartet wird, das durch
  - die Einhaltung der festgelegten Risikotoleranzen und der gesetzlichen Vorgaben sowie
  - die gesellschaftliche Erwartungshaltung an Banken geprägt ist;
- das Thema Risikokultur in einer Geschäfts- und Risikostrategie implementieren;
- für eine angemessene Unternehmensstruktur als Teil der Governance sorgen,
  - die sich an den Strategien des Unternehmens ausrichtet und
  - die Transparenz über die Geschäftsaktivitäten und Risiken des Instituts sicherstellt;
- institutsspezifische Werte entwickeln und kommunizieren, die auf den langfristigen und nachhaltigen Geschäftserfolg ausgerichtet sind, wie: Vertrauen – Professionalität – Nachhaltigkeit – Qualität – Regionalität – Kundennähe – Mitgliederverpflichtung;
- Kommunikation, offenen Dialog und Vertrauen auf allen Ebenen fördern („eine Bank – ein Team“):
  - im Aufsichtsrat, im Vorstandsteam, im Führungskreis und unter den Mitarbeitenden,
  - zwischen Vorstand und Aufsichtsrat, Vorstand und Führungskräften, Führungskräften und Mitarbeitenden;
- nachhalten, dass die Führungskräfte die Werte der Risikokultur an die Mitarbeitenden kommunizieren;
- ein offenes und kollegiales Führungskonzept etablieren;
- transparente und nachhaltige Vergütungssysteme einrichten;
- für ein umfängliches Internes Kontrollsystem mit klaren Verantwortlichkeiten sorgen.

Allerdings endet das Thema Risikokultur nicht beim Vorstand, sondern alle Bereiche einer Bank einschließlich Aufsichtsrat sind Teil der Risikokultur und somit „mitverantwortlich“, wenn auch in unterschiedlichen Funktionen und Aufgaben:

Dem Aufsichtsrat obliegt die Pflege eines vertrauensvollen, offenen Austauschs im Gremium und mit dem Vorstand über die Beurteilung und Begrenzung der Risiken der Bank. Er soll Impulse für die Werte der Bank geben, beurteilen, ob der Vorstand die Risikopositionen richtig einschätzt und wie die risikominimierenden Prozesse oder Kontrollen ausgestaltet sind. Ganz allgemein ist es dabei die Aufgabe des Aufsichtsrats, zu prüfen, ob und welche Maßnahmen zur Schaffung und Förderung einer Risikokultur im Haus etabliert wurden.

Führungskräften als Bindeglied zwischen Geschäftsleitung und Mitarbeitenden kommt analog zum Vorstand eine Vorbildfunktion zu. Sie sollen zum einen das Wertesystem und die Risikolimits kennen und beachten und zum anderen das Wertesystem und die Risikokultur zu den Mitarbeitenden transportieren. Ihre Aufgabe im Kontext mit Risikokultur ist es, eine offene Kommunikation zu fördern, eine gute Fehlerkultur und Feedbackmöglichkeiten zu etablieren sowie die Risiken innerhalb ihrer Zuständigkeiten zu identifizieren, zu bewerten und zu kontrollieren. Dazu gehört aber auch, klare Verantwortlichkeiten festzulegen und den Mitarbeitenden die Konsequenzen etwaiger Verstöße zu kommunizieren.

Eine hervorgehobene Rolle kommt den Kontrolleinheiten zu. Sie sollen in besonderer Weise die Werte der Risikokultur vorleben und den Vorstand beraten und unterstützen.

Mitarbeitenden obliegt, das Wertesystem, den festgelegten Risikoappetit und die bestehenden Risikolimits in ihrem Verantwortungsbereich zu beachten und ihr Verhalten daran auszurichten sowie allgemein die relevanten Vorschriften zu kennen und zu beachten. Dazu gehört auch, zu hohe oder nicht gewünschte Risiken nicht einzugehen, risikominimierende Prozesse und/oder Kontrollen nicht zu umgehen und an (Pflicht-)Schulungen teilzunehmen. Ein Grundstein für die Implementierung einer wirksamen Risikokultur wird im Onboarding-Prozess gesetzt, da hier in der Regel der erste dauerhafte Kontakt zwischen Institut und (neuem) Mitarbeitendem erfolgt.

Für die notwendige Berichterstattung über die Risikokultur bietet sich der Jahresbericht des MaRisk-Compliance-Beauftragten an und/oder der Bericht im Zusammenhang mit dem operationellen Risiko seitens der Risikocontrolling-Funktion.[11]

Das Thema Risikokultur ist kein einmaliger Prozess, sondern ein regelmäßiger bzw. wiederkehrender Zyklus, insbesondere, wenn z. B. eine angestrebte „Ziel-Risikokultur“ noch nicht erreicht ist oder die Risikokultur noch nicht im angemessenen Umfang im Institut gelebt wird.[12]

Überwachung einer angemessenen Risikokultur in den Instituten

Im Rahmen der siebten MaRisk-Novelle im Jahr 2023 wurde das Thema Überwachung der Risikokultur auf allen Ebenen des Institutes in die MaRisk aufgenommen. Aufgabe des Vorstandes ist es somit auch, zu überwachen, ob durch die Mitarbeitenden die Risikokultur in ihrer täglichen Arbeit beachtet wird. Damit korrespondiert eine Rechenschaftspflicht der Mitarbeitenden gegenüber dem Vorstand hinsichtlich der Einhaltung der Risikokultur.[13] Wie eine Überwachung der Risikokultur innerhalb eines Hauses erfolgt, schreibt die Aufsicht nicht vor, insoweit gilt Methodenfreiheit. Es liegt im Ermessen der Institute, wie sie einen angemessenen Überwachungsprozess ausgestalten. Aus Institutssicht sollte es um eine effiziente Umsetzung der Risikokultur einschließlich Überwachung gehen. Dies kann beispielsweise durch Überwachung des Mitarbeitendenverhaltens in Bezug auf die Einhaltung der schriftlich fixierten Ordnung erfolgen, es bieten sich sowohl anlassbezogene als auch stichprobenartig durchgeführte Kontrollen an. Klassische Beispiele einer Überwachungshandlung für Risikokultur sind Mitarbeitendenbefragungen oder Selbstbewertungen in regelmäßigen Mit-arbeitergesprächen.

Praxisbeispiele der Risikokultur in den Instituten

In unserer Praxis als MaRisk-Compliance-Beauftragte beobachten und begleiten wir vielfältige gute Prozesse zur Risikokultur und deren Überwachung. Die nachfolgende Abbildung zeigt eine graphische Übersicht von Praxisbeispielen zu guter Risikokultur.

Aktuelle Entwicklungen

Die EZB hat in der zweiten Jahreshälfte 2024 ein Konsultationsverfahren zum Leitfaden „Governance und Risikokultur“ durchgeführt,[14] allerdings ist der für Mitte 2025 avisierte Leitfaden aktuell noch nicht veröffentlicht worden.[15] Es bleibt abzuwarten, ob und mit welchem Inhalt die EZB den Leitfaden veröffentlicht und wie die nationale Aufsicht damit umgeht.

Maßnahmen für die Etablierung und Förderung der Risikokultur in der Geschäfts- und Risikostrategie

Risikobegrenzende Kompetenzsysteme

- Risikoüberwachung mittels Zielkennzahlen / Schwellenwerten / Risikolimits
- Auswertung der Beschwerden und der Schadensfälle → Nachverfolgung der Maßnahmen

Transparente, konsequente – auf nachhaltige Erfolgsbeiträge ausgerichtete – Vergütungssysteme

Verhaltenskodex (Wertesystem)

- Zielvereinbarungs- und Zielerreichungsgespräche (die quantitativen/qualitativen Ziele verdeutlichen die Verantwortung des Einzelnen für die Gesamtheit und sind mit den Bankzielen verknüpft)
- Mitarbeiterentwicklungsgespräche
- Selbstbewertungen durch Mitarbeitende

Schulungen für neue Mitarbeitende zu risikoangemessenem Verhalten

- Mitarbeiterversammlung, Weekly, Town Hall Meeting
- Thematisierung der Risikokultur in den regelmäßigen Besprechungen der Teams/Abteilungen/Bereiche
- Entwicklung der Risikokultur z. B. als Bestandteil eines Strategieworkshops

- Mitarbeiterbefragungen („Wir-Gefühl“)
- Führungskräftebefragungen

Im Rahmen des Projekts „Geno Next Level“ wurde ein Vorstands- und Aufsichtsratskodex entwickelt, der in der Mitgliederversammlung des BVR im Jahr 2027 beschlossen werden soll.[16]

Zusammenfassung und Handlungsempfehlungen

Das Thema Risikokultur ist nicht neu, hat aufgrund von Ereignissen in der jüngsten Vergangenheit aber an Bedeutung gewonnen. Adressat einer angemessenen Risikokultur und verantwortlich für diese ist jeder in einem Institut: vom Azubi über den Vorstand bis hin zum Aufsichtsrat. Risikokultur lässt sich auch nur schwer in Zahlen messen und bedeutet nicht die Quantifizierung der wesentlichen Risiken. Risikokultur ist institutsindividuell und keine einmalige Aufgabe, sondern dauerhaft zu betrachten und zu gewährleisten, wobei es praxisbewährte Mittel zur Implementierung und Aufrechterhaltung einer angemessenen Risikokultur gibt. Sprechen Sie uns gerne an. ▬

Jörg Scharditzky
Abteilungsleiter MaRisk-Compliance,
E-Mail: joerg.scharditzky@dz-cp.de

Eugenia Scherbanev
Beauftragte MaRisk-Compliance,
E-Mail: eugenia.scherbanev@dz-cp.de

Thomas Schirmer
Beauftragter MaRisk-Compliance,
E-Mail: thomas.schirmer@dz-cp.de

[1] Und weiterer Skandale, z. B. Panama Papers und Cum/Ex- bzw. Cum/Cum-Geschäfte.

[2] BaFin-Rundschreiben 10/2012 (BA) vom 14.12.2012, Tz. AT 4.4.2 (https://www.bundesbank.de/resource/blob/598760/825c3c1518cdc5fce74f732fc0d05cc4/472B63F073F071307366337C94F8C870/2012-12-14-rundschreiben-data.pdf)

[3] Und die zuständigen Behörden in die Lage zu versetzen sind, sich der Angemessenheit der internen Unternehmensführungsregeln zu versichern; RL 2013/36/EU (Bankenrichtlinie – CRD IV) vom 26.06.2013, Rn. 54.

[4] Damit setzte die BaFin auch die Empfehlungen des Baseler Ausschusses für Bankenaufsicht aus dessen Prinzipen zur Corporate Governance aus dem Jahr 2015 um.

[5] Diese Definition baut auf einem Vorschlag des Financial Stability Board aus dem Jahr 2014 auf und wird auch in den EBA-Guidelines zur Internen Governance verwendet, EBA/GL/2021/05, 02.07.2021, S. 11, 14, 28.

[6] https://www.bundesbank.de/de/aufgaben/bankenaufsicht/einzelaspekte/aufsichtsschwerpunkte/schwerpunkte-der-bankenaufsicht-799612

[7] Formuliert bereits im Jahr 2014 vom Financial Stability Board (FSB) und ebenfalls in den EBA-Leitlinien wiedergegeben, EBA/GL/2021/05, 02.07.2021, S. 28 f.

[8] Hannemann u.a., MaRisk, TB 1, 2025, AT 3, Rn. 68

[9] Die Indikatoren stehen nicht isoliert da, sondern sind miteinander verzahnt, auch können institutseigene Indikatoren hinzukommen, z. B. Risikoappetit. Es kommt auch weniger auf eine Quantifizierung der Indikatoren an als auf eine qualitative Bewertung.

[10] MaRisk vom 27.10.2017, AT 3 Tz. 1

[11] Häufig wird der Risikocontrolling-Funktion die operative Verantwortung für die Umsetzung der Risikokultur übertragen, auf jeden Fall sollten das Risikocontrolling und die Compliance-Funktion beteiligt werden.

[12] Denkbar ist auch, einen andauernden „Regelkreis“ aufzusetzen.

[13] Hannemann u.a., MaRisk, TB 1, 2025, AT 3, Rn. 95

[14] Pressemitteilung der EZB vom 24.07.2024 (https://www.bundesbank.de/resource/blob/937238/bcdc155de32e6946d9cd2c2e386ba1b6/472B63F073F071307366337C94F8C870/2024-07-24-konsultationsverfahren-download.pdf)

[15] Dieser Artikel hat den Stand 20.01.2026.

[16] BVR-Roadshow 2026; https://intern.bvr.de/e.nsf/E21C0A31FAB9BA59C1258DB5004909BB/$FILE/BVR_Roadshow_Foliensatz.pdf

Chancenmanagement von KI-Technologien

Welche Chancen und Risiken liegen in der Anschaffung und Nutzung von KI-Technologien? Der folgende Beitrag zeigt auf, wie Sie sich einen schnellen Überblick verschaffen können. Dazu werden praxiserprobte Methoden zur strukturierten Chancen- und Risikoermittlung von KI-Technologien vorgestellt.

Mit der KI-VO (Künstliche Intelligenz – Verordnung (EU) 2024/1689) wird der Einsatz von KI-Technologien (KI-Systeme und KI-Modelle), im Weiteren KI-Anwendungen genannt, EU-weit reguliert. Die Regulatorik sollte jedoch nicht davon abhalten, sich für KI-Technologien zu entscheiden. Sie ist vielmehr eine Chance, KI sicher einzusetzen. Dennoch stellt sich die Frage, ob die Einhaltung der Regulatorik im Verhältnis zum Nutzen steht.

Zuerst empfiehlt es sich, in drei Schritten sich einen groben und schnellen Überblick zu verschaffen:

1. Zusammentragen von möglichen KI-Anwendungen, die bereits von Fachabteilungen angefragt/gefordert werden.
2. Anschließend kann eine Chancen-/Nutzen- und Aufwandsermittlung/-schätzung sowie Risikoklassifikation erfolgen.
3. Dem folgt ein Abwägungs- und Entscheidungsprozess, der sich an zuvor festgelegten Parametern aus der KI-Strategie orientiert.

Die drei genannten Schritte könnten tabellarisch festgehalten werden (siehe illustrative Abb. 1).

Abb. 1. **Chancen-Dashboard KI-Technologien (KI-Assets)**

Bezeichnung der KI-Technologie	Strategischer Zweck	Implementierungsaufwand	Dringlichkeit der Nutzung	KI-Risikoklasse	Anwendungsrolle
Musteranwendung TestGPT	KPI-Steigerung: Senkung Prozessdauer/ Kostenoptimierung	**mittel**	**hoch**	**mittel**	Betreiber
Ablagemanagement KI-plus	Automatisierungsgrad (Reduzierung MAK/ Umverteilung)	**niedrig**	**mittel**	**gering**	Betreiber
Chat-Plus Web	KPI-Steigerung: Kundenzufriedenheit/ Kundenerlebnis	**mittel**	**mittel**	**mittel**	Anwender
					Summe:

Schritt 1: **Potenzielle KI-Anwendungen zusammentragen/Bedarfsermittlung**

Um eine Priorisierung möglicher KI-Anwendungen im Unternehmen einzuführen, ist zunächst eine Bedarfsabfrage sinnvoll. Hierzu können Anfragen/Impulse aus den jeweiligen Fachbereichen zusammengetragen werden. Da jedoch die Einführung mehrerer KI-Anwendungen gleichzeitig oft durch begrenzte Ressourcen limitiert ist, sollte die Bedarfsabfrage in Form einer Liste zusammengetragen werden. In dieser Liste empfiehlt es sich, weitere Bewertungen hinsichtlich Chancen/Nutzen sowie Aufwand und Risiken vorzunehmen.

Schritt 2: **Chancen-/Nutzen- und Aufwandsermittlung/-schätzung sowie Risikoklassifikation**

I. Chancen und Nutzen ermitteln

Bevor eine KI-Anwendung eingeführt wird, sind hinsichtlich der möglichen Chancen und des Nutzens folgende Punkte zu klären:

a) Warum sollte die Anwendung eingesetzt werden?

Der strategische Zweck kann folgende Kategorisierungen umfassen:

- KPI-Steigerung: Umsatzsteigerung
- KPI-Steigerung: Senkung Prozessdauer/Kostenoptimierung
- KPI-Steigerung: Kundenzufriedenheit/Kundenerlebnis
- Automatisierungsgrad (Reduzierung MAK/Umverteilung)
- Skalierbarkeit (Standardisierung auf andere Bereiche)

Kosten p.a. für Bezug und Betrieb in EUR	geschätzter regulativer Aufwand p.a. in EUR	geschätzte Gewinnmaximierung/ Ersparnis p.a. in EUR	Status der Chancenbewertung	Verantwortlich	Entscheidung für Einführung/ Umsetzung
6.000 EUR	250 EUR	5.500 EUR	**erledigt**	Herr Mustermann	ja
3.500 EUR	220 EUR	1.200 EUR	**in Bearbeitung**	Frau Mustermann	ja
9.200 EUR	250 EUR	2.500 EUR	**offen**	Frau Mustermann	nein
18.700 EUR	720 EUR	**9.200 EUR**			

b) Wie dringlich wird die KI-Anwendung benötigt?
Hier kann eine Skalierung mit den Parametern niedrig, mittel und hoch verwendet werden. Die Beurteilung sollte mit den betroffenen Fachbereichen abstimmt werden.

c) Welche Kosten lassen sich einsparen?
Die Kostenpotenziale können beispielsweise aus Einsparung von Sachkosten oder auch von Arbeitszeitkosten (neue Freiräume können für andere Arbeiten geschaffen werden) resultieren. Die Kostenkalkulation sollte die Kosten pro Jahr normieren und kann für eine mehrjährige Vorschaurechnung verwendet werden.

d) Welcher Mehrertrag kann mit der KI-Anwendung erzielt werden?
Sofern eine KI-Anwendung zu zusätzlichen Erträgen führen kann oder soll (z. B. KI-basierte Auswertungen für vertriebliche Fragestellungen), sollte das Ergebnis der Kalkulation herangezogen werden. Analog zu den Kosten sollten die Erträge eine jährliche Betrachtung implizieren und ebenso für eine mehrjährige Vorschaurechnung verwendet werden.

II. Einführungs- und Betriebsaufwand identifizieren und Einordnung in Risikoklassifizierung

Bei der Einführung von KI-Anwendungen ist der Einführungsaufwand sowie der fortlaufende Betriebsaufwand zu berücksichtigen. Ferner sollte auch gleich eine Risikoklassifizierung vorgenommen werden: Sie schafft Transparenz hinsichtlich möglicher Regulierungsaufwände (Erfüllung von Pflichten gem. KI-VO, DSGVO etc.) und hinsichtlich möglicher Aufwände für erforderliche Maßnahmen zum sicheren Betrieb.

Dazu empfiehlt es sich, folgende Fragen zu bearbeiten:

a) Wie hoch ist der organisatorische und technische Implementierungsaufwand?
Um den Implementierungsaufwand zu ermitteln, sollten Arbeitszeit-, Lizenz- und Bezugskosten sowie Infrastrukturkosten (z. B. Serverressourcen) berücksichtigt werden.

b) Wie hoch sind die laufenden Kosten zum Betrieb der KI-Anwendung?
Wie jede IT-Anwendung führt der Betrieb von KI-Anwendungen auch zu laufenden Kosten. Dies können beispielsweise jährliche Lizenz-, Infrastruktur- sowie Betreuungskosten sein.

c) Welcher regulatorische Aufwand ist mit der KI-Anwendung verbunden?
Die Betreuungskosten können nicht nur technisch-administrativer Art sein, sondern auch Compliance-Aufwände (z. B. Inventarisierung im Informationsverbund im IKT-Risikomanagement/Informationssicherheit, Prüfung und Einhaltung der Pflichten der KI-VO, Prüfung und Einhaltung des Datenschutzes) beinhalten. Hier können Kosten in Form von Arbeitszeitaufwänden herangezogen werden.

Des Weiteren sollte insbesondere – basierend auf der KI-VO – die Risikoklassifizierung vorab vorgenommen sowie die Rolle geprüft werden, in der das Unternehmen die KI-Anwendung nutzt (z. B. Betreiber, Anbieter, Entwickler). Mit der jeweiligen Rolle sind auch unterschiedliche Pflichten gemäß der KI-VO und die damit einhergehenden regulatorischen Aufwände verbunden.

Vereinfacht lässt sich sagen:

- Die Rolle als Anbieter umfasst die meisten Pflichten – die Betreiberrolle die wenigsten Pflichten.
- Je höher die Risikoklasse ist, desto mehr Pflichten ergeben sich in der jeweiligen Rolle.

Die Risikoklassifizierung kann folgende Einstufungen umfassen:

- gering (vgl. Art 95 KI-VO)
- mittel (vgl. Art. 50 KI-VO)
- hoch (vgl. Art. 6 ff. KI-VO)
- verboten (vgl. Art. 5 KI-VO)

Schritt 3: **Abwägung der Chancen und Risiken / des Aufwands**

Wenn die Schritte 1 und 2 so weit abgeschlossen und die Ergebnisse in einem Dashboard zusammengetragen wurden, kann die Übersicht als Entscheidungsgrundlage dienen, welche KI-Anwendung möglicherweise zuerst und welche später implementiert werden sollte.

Die KI-Anwendungen mit einer geringen und mittleren Risikoklasse und mit der Rolle „Betreiber" bringen in der Regel den geringsten regulatorischen Aufwand hinsichtlich der KI-VO mit sich. Mit diesen KI-Anwendungen könnte die Implementierung im Unternehmen beginnen, sofern der Output zum Input verhältnismäßig ist.

Fazit

Mit dem beschriebenen Chancenmanagement in drei Schritten kann nachhaltig und fortlaufend KI-Innovation unternehmensindividuell betrachtet und die Wettbewerbsfähigkeit ausgebaut werden.

Ein weiterer Vorteil ist, dass die Übersicht zum Abgleich der eigenen unternehmensinternen KI-Strategie herangezogen werden kann. Schlussendlich kann sie auch rückwirkend zur Evaluation genutzt werden. ▬

Benjamin Wellnitz
Bereichsleiter IKT-Risikokontrolle, Informationssicherheit & Datenschutz,
E-Mail: benjamin.wellnitz@dz-cp.de

Herausforderungen bei Geschäftsbeziehungen mit internationalen Verflechtungen

Die globale Vernetzung nimmt stetig zu und mit ihr die Komplexität von Geschäftsbeziehungen zu Kunden mit grenzüberschreitenden oder interkontinentalen Beziehungen. Sowohl Privatkunden als auch Firmenkunden bedürfen in diesen Fällen erhöhter Aufmerksamkeit und ausführlicherer Dokumentation.

Die klassische Kundenstruktur von Volksbanken Raiffeisenbanken mit starkem Bezug zum Mittelstand steht nach wie vor im Fokus der Genossenschaftlichen FinanzGruppe. Allerdings hat sich die Geschäftswelt auch dieser Kundengruppe in den letzten Dekaden spürbar verändert. Selbst kleine Mittelstandsbetriebe erleben eine Überregionalisierung oder sogar Internationalisierung ihrer Geschäftsaktivitäten bzw. ihrer eigenen Kundenbeziehungen. Gleichzeitig ziehen Volksbanken Raiffeisenbanken auch Neukunden mit internationaler Verflechtung an. Dies hat Auswirkungen auf Risikobewertung, Know-Your-Customer und Dokumentationsaufwand in den Instituten.

Im Rahmen dieses Artikels sollen „Einfallstore“ für Geldwäsche, Betrug und organisierte Kriminalität insbesondere bei Kunden mit internationalen Beziehungen in Risikoländer und bei Kunden aus Risikoländern erörtert werden. Dabei sind „Risikoländer“ abstrakt zu verstehen und nicht gleichzusetzen mit den in der Delegierten Verordnung (EU) genannten Staaten. Denn das Risiko einer Geschäftsbeziehung oder Transaktion mit internationalem Bezug steigt u. a. mit der Entfernung zum Wohn-/Geschäftssitz des Kunden. Gerade auch in diesem Kontext sollte die genossenschaftliche Wertewelt Kompass und Richtschnur sein.

Firmenkunden mit Bezug in Risikoländer

Auch kleinere und mittelständische Firmenkunden importieren und exportieren Güter sowie Dienstleistungen, wodurch dem grenzüberschreitenden Warenverkehr – teils sogar über Kontinentalgrenzen hinweg – entsprechende internationale Finanzströme folgen. Um prüfungssicher und risikoadjustiert agieren zu können, ist das Verständnis der Grundgeschäfte von essentieller Bedeutung.

Die BaFin hatte im Frühjahr 2025 nochmals besonders auf Missbrauchsmöglichkeiten bei Außenhandelsgeschäften hingewiesen. Dem kann die einzelne Bank vor Ort nur durch erhöhte Sorgfalt bei der Plausibilisierung der jeweiligen Transaktionen und ein tiefes Verständnis für die Geschäftsprozesse der Firmenkunden entgegenwirken.

Erhöhte Wachsamkeit ist geboten, wenn Transaktionen nach Art und Umfang nicht zum Geschäftsmodell eines Firmenkunden passen oder Gelder erkennbar über Drittländer umgeleitet werden. Dies gilt auch für Fälle, in denen handelnde oder beteiligte Personen eines Firmenkunden oder der Firmenkunde selbst im (EU-)Ausland ansässig sind. Ist der Geschäftsführer oder Gesellschafter eines deutschen Firmenkunden Mehrfachgeschäftsführer – Stichwort: Strohmannkartelle – sollte die Geschäftsbeziehung tief hinterfragt werden.

Privatkunden mit Bezug in Risikoländer

Die deutsche Financial Intelligence Unit hat im vergangenen Jahr in einer Veröffentlichung an die geldwäscherechtlich Verpflichteten ausdrücklich auf die Risiken von Zahlungen aus Asien, konkret: Vietnam, aufmerksam gemacht. Hintergrund sind vermehrte Beobachtungen der Behörde von Zahlungseingängen im hohen sechsstelligen Bereich auf inländische Privatkonten, die angeblich aus Immobilien- oder Firmen- und Beteiligungsverkäufen im Ausland stammen.

Auch und gerade in diesen Fällen ist die finale Mittelherkunft kaum nachzuvollziehen. Selbst bei glaubwürdig erscheinenden Dokumenten ist höchste Vorsicht und Sorgfalt geboten. Keinesfalls sollten bankseitig „selbstbeglaubigte“ Dokumente akzeptiert werden, wie Immobilienkaufverträge, Schenkungsverträge oder Ähnliches.

Sowohl bei Privat- als auch bei Firmenkunden mit Bezug in Risikoländer ist bei Auslandstransaktionen zu beachten, dass länderspezifische Bescheinigungen/Beglaubigungen grundsätzlich nicht kongruent zum deutschen Recht sind und nicht automatisch den deutschen bzw. EU-Anforderungen genügen.

Privatkunden aus Risikoländern

Neben Firmen- und Privatkunden mit internationalen Zahlungsströmen können Geschäftsbeziehungen mit Privatkunden aus Nicht-EU-Ländern Risiken bergen. Dies ist ein höchst sensibles, aber unbedingt zu thematisierendes Risikofeld. Es betrifft Personen, die ggf. selbst Opfer krimineller Strukturen geworden sind und unter Umständen als Zwangsarbeiter oder in Verhältnissen ähnlicher Abhängigkeit leben und gezielt als „Strohmänner“ eingesetzt werden.

Insbesondere bei Kunden, die in Niedriglohnsektoren angestellt sind, bestehen mitunter – und durchaus unbemerkt – Abhängigkeiten zu Arbeitgebern, angeblichen Freunden oder Verwandten im In- und Ausland (Stichwort: Zwangsarbeit).

In diesem Kontext ist gerade bei niederschwelligen Zahlungsströmen besondere Aufmerksamkeit gefordert. Auf den Kundenkonten sind ggf. Transaktionen zu beobachten, die nicht der Vermögenssphäre des Kunden zuzurechnen sind und nicht den eigenen wirtschaftlichen Verhältnissen entsprechen. In solchen Fällen werden die Konten genutzt, um kriminelle Gelder einzuschleusen, ohne dass die eigentlichen Hintermänner in Erscheinung treten. Die Betroffenen handeln dabei oft nicht freiwillig – sie sind selbst Opfer. Diese Erkenntnis macht den Umgang mit solchen Fällen besonders anspruchsvoll.

Maßnahmen zur Risikominimierung

In allen drei genannten Fallkonstellationen ist in jedem Fall der Geldwäschebeauftragte zu kontaktieren und das weitere Vorgehen zu besprechen.

Damit die beschriebenen Risikoszenarien vermieden werden, sollten Verpflichtete Maßnahmen ergreifen, die für Nachvollziehbarkeit und Transparenz der kundenseitigen Geschäfte sorgen. Hierzu zählen unter anderem:

- gezielter Aufbau von Expertenwissen auf Bankseite in Markt- und Marktfolgebereichen, insbesondere bei der Erschließung neuer, bislang wenig vertrauter Märkte (Geografie, Kultur, Rechtsrahmen etc.)
- gelebtes Know-Your-Customer mit einer hohen Sensibilität für und bei ausländischen Zahlungsströmen und einer freundlichen, aber nachdrücklichen Hartnäckigkeit bezüglich nachvollziehbarer kundenseitiger Nachweise und Erläuterungen.

Zu beachten ist eine für Dritte nachvollziehbare und prüfungssichere Dokumentation. Dabei ist unbedingt zu berücksichtigen, dass die Anforderungen an die Dokumentation mit dem Risiko des Geschäftes steigen.

Fazit

Genossenschaftsbanken erleben auch in der für die FinanzGruppe zentralen mittelständischen Firmenkundschaft eine zunehmende Internationalisierung. Geschäftsbeziehungen zu Kunden mit internationalen geschäftlichen Verbindungen – insbesondere in Risikoländer – erhöhen die Anforderungen an Risikobewertung, Know-Your-Customer und Dokumentation.

Im Privatkundensegment bergen hohe Auslandseingänge mit schwer nachvollziehbarer Mittelherkunft besondere Risiken, zumal ausländische Dokumente nicht automatisch deutschen Standards entsprechen. Besonders sensibel sind Fälle, in denen Privatkunden aus Nicht-EU-Staaten als „Strohmänner“ missbraucht werden könnten.

Konsequentes Know-Your-Customer, vertieftes Marktverständnis, frühzeitige Einbindung des Geldwäschebeauftragten sowie eine risikoadäquate, prüfungssichere Dokumentation sind in diesem Kontext zentrale Maßnahmen zur Risikominimierung.

Zentraler Rahmen der obigen Überlegungen ist dabei natürlich die konsequente Beachtung der genossenschaftlichen Wertewelt. ▬

Thomas Schröder
Abteilungsleiter Geldwäsche- und Betrugsprävention,
E-Mail: thomas.schroeder@dz-cp.de

Genossenschaftliche FinanzGruppe
Volksbanken Raiffeisenbanken

Allein oder vertrauen

Ob Sie Ihrer Verantwortung im Beauftragtenwesen allein gerecht werden oder dabei einem Partner vertrauen – wir unterstützen Sie, Ihre Entscheidung erfolgreich umzusetzen: **www.dz-cp.de**

#freiraumsichern

DZ CompliancePartner

Interne Revision

Regelmäßig berichten wir an dieser Stelle über die Interne Revision der DZ CompliancePartner GmbH. Wir möchten Ihnen damit einen Überblick über die Qualität der unterschiedlichen Auslagerungsdienstleistungen geben und Sie in Ihrem Auslagerungscontrolling unterstützen. Die durchgeführte Revisionstätigkeit der DZ CompliancePartner GmbH steht im Einklang mit den Anforderungen gemäß MaRisk AT 4.4.3 und BT 2.

Seit der letzten Berichterstattung in der Point of Compliance (3/2025, S. 26) wurden aus der von der Geschäftsführung genehmigten Jahresprüfungsplanung 2025 die Prüfungen des Bereichs „IKT-Risikokontrolle, Informationssicherheit & Datenschutz", hier „Datenschutz" sowie „IKT-Risikokontrolle, Informationssicherheit" und der Bereiche „Geldwäsche- und Betrugsprävention / Compliance-Spezialisten" abgeschlossen und an die Mandanten der jeweiligen Auslagerungen versandt. Darüber hinaus wurden aus dem Bereich der Unternehmenssteuerung das „Rechnungswesen & Controlling" geprüft. Da diese Prüfung nicht dienstleistungsbezogen ist, wurde der Bericht nur intern veröffentlicht.

Außerdem wurde aus der von der Geschäftsführung genehmigten Jahresprüfungsplanung 2026 die Prüfung des Bereichs „Marketing & Vertrieb" abgeschlossen. Der Prüfungsbericht ist nicht dienstleistungsbezogen und wurde daher intern veröffentlicht.

Die externe Prüfung der Geschäftsbereiche Datenschutz, Geldwäsche- und Betrugsprävention, IKT-Risikokontrolle und Informationssicherheit, MaRisk-Compliance und WpHG-Compliance sowie Single Officer (WpHG) nach IDW PS 951 (Typ 2) wurde wiederum von der EY GmbH & Co. KG Wirtschaftsprüfungsgesellschaft vorgenommen. Für alle Bereiche wurde ein Testat uneingeschränkt erteilt. Die Endfassungen der Berichte zur externen Prüfung wurden an die Kunden der jeweiligen Dienstleistung versandt.

Die Quartalsberichte für das dritte und vierte Quartal 2025 der Internen Revision wurden fristgerecht erstellt und den Mandanten, die im Zeitraum zu unseren Kunden gehörten, zur Verfügung gestellt.

Weiterhin wurde turnusgemäß je ein Follow-up-Quartalsbericht für Q3 und Q4 2025 erstellt und der Geschäftsführung der DZ CompliancePartner GmbH vorgelegt. In den Follow-up-Berichten wird die Abarbeitung der von internen und externen Prüfern getroffenen Maßnahmen/Empfehlungen dokumentiert. Offene Punkte werden durch die Interne Revision konsequent nachgehalten.

Als weiterer Informationsaustausch finden zwischen dem Sprecher der Geschäftsführung der DZ CompliancePartner GmbH und der Internen Revision regelmäßige Jours Fixes statt. ▬

Ansprechpartner:
Lars Schinnerling, *Bereichsleiter Interne Revision,*
E-Mail: lars.schinnerling@dz-cp.de

Wirtschaftliche Lage

Die DZ CompliancePartner GmbH ist erwartungsgemäß in das neue Jahr gestartet. Nach einem wie erwartet schwachen Monat Januar lagen die operativen Erträge im Februar wieder 86 TEUR über Plan. Zwar lag auch der operative Aufwand im Februar 31 TEUR über Plan, diese Planüberschreitung ist jedoch im Wesentlichen auf unterjährige Rückstellungen von Urlaubsansprüchen zurückzuführen. Insgesamt liegt das kumulierte Ergebnis nunmehr mit -19 TEUR leicht unter dem Plan von -4 TEUR. Insoweit ist zum gegenwärtigen Zeitpunkt anzunehmen, dass das geplante Ergebnis 2026 erreicht werden wird. ▬

Ansprechpartner:
Jens Saenger, *Sprecher der Geschäftsführung,*
E-Mail: jens.saenger@dz-cp.de

3 Fragen an Björn Blechenberg

Herr Blechenberg, was ist für Sie persönlich der besondere Reiz, in einem genossenschaftlich geprägten Unternehmen tätig zu sein?

Björn Blechenberg: Das genossenschaftliche Prinzip der Subsidiarität: Verantwortung dort zu belassen, wo sie hingehört, und gezielt zu unterstützen, wo Entlastung nötig ist – das ist nicht nur sinnvoll, sondern hochaktuell. Ich sehe hier die Chance, meine Vertriebserfahrung mit einem klaren Wertefundament zu verbinden.

Was ist aus Ihrer Sicht die größte Herausforderung in der Compliance?

Björn Blechenberg: Die Kombination aus regulatorischer Dynamik und operativer Realität.

Die regulatorischen Anforderungen steigen stetig. Doch damit nicht genug, wir befinden uns in einer Zeit geopolitischer Umbrüche und fortschreitender Digitalisierung. Darauf müssen die Banken Antworten finden und gleichzeitig effizient, kundenorientiert und wirtschaftlich arbeiten.

Deshalb braucht es in Bezug auf die Compliance-Anforderungen Lösungen, die nicht nur fachlich exzellent, sondern auch praktikabel sind.

Was dürfen Kundinnen und Kunden konkret von Ihnen erwarten?

Björn Blechenberg: Einen offenen Dialog auf Augenhöhe. Mir ist wichtig, zuerst zuzuhören und die individuelle Situation eines Instituts zu verstehen. Ob Auslagerung, Beratung oder Schulung – entscheidend ist, dass die Lösungen passen, entlasten und Sicherheit schaffen. Partnerschaft ist für mich kein Schlagwort, sondern Arbeitsprinzip.

Lassen Sie uns darüber reden, wie wir Compliance partnerschaftlich gestalten können. Ich freue mich sehr auf den Austausch mit unseren Kunden. ▬

Mit Björn Blechenberg hat zum 1. Januar 2026 ein ausgewiesener Marketingexperte und Branchenkenner die Leitung des neu geschaffenen Bereichs Marketing und Vertrieb in der DZ CompliancePartner GmbH übernommen. Mit der Personalie unterstreicht die DZ CompliancePartner ihre Verantwortung als zentraler Partner in allen Compliance-Fragen innerhalb der Genossenschaftlichen FinanzGruppe und setzt ein klares Zeichen für eine noch stärkere Kundenorientierung.

Björn Blechenberg bringt eine langjährige Expertise als Direktor und Filialgebietsleiter der Deutsche Bank AG und ihren Tochtergesellschaften sowie eine ausgeprägte Leidenschaft für den persönlichen Kundenkontakt mit.

Freitag, 2. Oktober 2026
Schloss Montabaur

AVE THE DATE - SAVE THE DATE - SAVE THE

Der Compliance-Kongress 2026
Zur Zukunft der Compliance im Verbund

Bitte merken Sie sich diesen Termin schon jetzt vor.

Es erwarten Sie spannende Themen, interessante Keynote-Speaker und der direkte Austausch im **größten Compliance-Netzwerk der Genossenschaftlichen FinanzGruppe.**

HE DATE - SAVE THE DATE - SAVE THE DATE

Erfahren Sie mehr und melden Sie sich jetzt an:
www.dz-cp.de/compliance-kongress

ComplianceCollege

ComplianceCollege ist eine Marke der DZ CompliancePartner