Point of Compliance
Das Risikomanagement-Magazin

AUSGABE 2/2025

PoC

COMPLIANCE-KULTUR

DZ CompliancePartner

STARTPUNKT

Folgen Sie der DZ CompliancePartner GmbH auf Social Media.

IMPRESSUM

PoC – Point of Compliance
Das Risikomanagement-Magazin,
Ausgabe 36, 2/2025
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, Frank Lutter, Marcia Metzner, Giannis Petras, Jens Saenger, Jörg Scharditzky, Lars Schinnerling, Thomas Schröder, Christian Tipkemper, Benjamin Wellnitz

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

Redaktionsschluss: 7. Mai 2025
Auflage: 2.500 Exemplare

Spoofing, Scamming, Phishing – wir lernen heute ständig neue Wortschöpfungen, die für ebenso ständig neue Betrugsmaschen stehen. Was allen gemein ist: Sie bedienen sich technischer Lösungen, um menschliche Schwächen auszunutzen. Genau hier liegt denn auch unser Hebel im Kampf gegen Online-Betrug. Es geht vor allem darum, Bewusstsein und Aufmerksamkeit der Mitarbeitenden zu stärken (Seite 4).

Natürlich bringt die rasante Entwicklung der KI neben neuen Risiken auch neue Möglichkeiten: In der Wertpapier-Compliance könnte KI beispielsweise dazu beitragen, die komplexen regulatorischen Anforderungen im Wertpapiergeschäft automatisiert, effizient und fehlerarm zu erfüllen (Seite 10).

Diese und andere Entwicklungen machen die Zukunft der Compliance im Verbund so spannend wie nie zuvor. Aus diesem Grund haben wir uns bei der DZ CompliancePartner auch dazu entschlossen, den unterschiedlichen Perspektiven auf das komplexe Themenfeld eine neue Plattform zu geben: Am 25. September 2025 begrüßen wir beim Compliance-Kongress 2025 auf Schloss Montabaur externe und interne Entscheider und Experten – und gerne auch Sie. Mehr dazu finden Sie in dieser Ausgabe der PoC und auf unserer Website.

Für heute wünschen wir Ihnen inspirierende Lektüre und eine ebensolche Sommerzeit.

Herzlichst
Ihr Jens Saenger

Jens Saenger
Sprecher der Geschäftsführung

Spoofing, Scamming, Telefonbetrug – Betrugsmaschen 4.0 im modernen Bankalltag

Banken und ihre Kunden sind täglich einer Vielzahl von Betrugsversuchen ausgesetzt. Der folgende Beitrag stellt gängige Betrugsmaschen vor und geht auf mögliche Abwehrmaßnahmen ein.

Die Kriminalität oder besser: die Ausführung krimineller Handlungen hat sich in den letzten Jahren vor dem Hintergrund der zunehmenden Digitalisierung gewandelt.

In der „analogen" Welt werden Diebstahl, Raub, Einbruch und ähnliche Delikte – abhängig vom jeweiligen Zielobjekt – umfangreich und minutiös geplant. An der jeweiligen Tathandlung sind ggf. mehrere Personen (Spezialisten) mit unterschiedlichen Aufgaben beteiligt. Vorhandene Sicherungsmaßnahmen, wie z. B. Einbruchsschutz, Sicherheitspersonal oder Alarmsysteme, müssen überwunden werden. Vorbereitung, Durchführung und „Nachbereitung" folgen einem Plan, der unbedingt einzuhalten ist. Spuren müssen verwischt, Fluchtpläne entwickelt sein.

Gemeinsam ist den Delikten in der analogen Welt der konkrete räumliche Bezug oder Kontakt zwischen Täter und Opfer bzw. Zielobjekt. Geldbörsen müssen vor Ort entwendet, Handtaschen der Eigentümerin entrissen oder Gemälde aus einem Museum gestohlen werden.

In der „digitalen" Welt hingegen ist kein unmittelbarer Kontakt des Kriminellen mit potenziellen Opfern notwendig. Die „Kommunikation" kann ohne räumlichen Bezug und damit deutlich anonymer erfolgen. (Einzel-)Täter können praktisch von überall auf der Welt aktiv werden.

Ein weiterer wesentlicher Unterschied scheint der „Faktor Mensch als (vermeintliche) Schwachstelle" im digitalen System zu sein. Kriminelle müssen in der digitalen Welt nicht mehr stehlen oder rauben – es muss ihnen nur gelingen, andere dazu zu bringen, Geld oder Vermögenswerte „aus freien Stücken" zu übertragen. Hierbei spielen gute Kenntnisse und Informationen über das oder die Opfer (z. B. eine Privatperson oder auch eine Bank), eine „gute" Geschichte und das psychologische Geschick, die emotionale Schwachstelle des digitalen „Gegenübers" unmittelbar zu erfassen, eine bedeutsame Rolle.

Kriminellen gelingt es immer wieder, angeblich besonders dringende Zahlungen mittels telefonischer Überweisungen bei einer Bank auszulösen. Privatpersonen werden dazu gebracht, Geld für Flugtickets oder Arztrechnungen für eine angeblich in Not geratene Person zu zahlen. Ein Klassiker ist nach wie vor, Notarkosten für einen angeblichen Glücksspielgewinn oder eine absurde Nachlassabwicklung überweisen zu lassen.

In diesem Zusammenhang fallen häufig Begriffe wie Spoofing, Scamming, Phishing oder auch der so genannte CEO-Fraud.

Was verbirgt sich hinter diesen Begriffen?

- Beim **SPOOFING** handelt es sich schlicht um das Fälschen von Identitäten im Internet oder per Telefon.

  Täter geben sich als vertrauenswürdige Personen (z. B. Bankmitarbeiter) aus, um an sensible Daten oder Zugangsdaten zu gelangen. Bekannt geworden ist dieses Vorgehen insbesondere durch die Manipulation von Telefonnummern. Ein Krimineller ruft z. B. von außerhalb der EU an. Auf dem Zieltelefon wird die Telefonnummer der Hausbank angezeigt. Zu dieser Betrugsmasche zählt aber auch die so genannte Enkeltrick-Methode.

  Ziel des Spoofings ist es, Geld oder persönliche (Zahlungs-)Daten des Opfers zu erhalten.
- **PHISHING** geht mit dem Spoofing einher. Opfer werden durch gefälschte E-Mails oder Webseiten verleitet, vertrauliche Daten wie Kennwörter oder Kontodaten preiszugeben. Nicht selten enthalten offiziell erscheinende Phishing-E-Mails Dateianhänge, die – werden sie geöffnet – Malware auf dem PC oder Netzwerk installieren.
- **SCAMMING** ist ein Oberbegriff für Internetbetrug im Allgemeinen. Der Scamming-Mechanismus lautet vereinfacht: Zahle wenig, erhalte viel.

  Ziel ist es, Menschen dazu zu motivieren, Geld oder persönliche (Zahlungs-)Daten zu überlassen. Häufig tritt Scamming im Zusammenhang mit vorgetäuschter Liebe (Love-Scamming) oder Gewinn-/Erbschaftsversprechen auf.
- **CEO-FRAUD** ist eine gezielte Betrugsmasche in oder gegen Unternehmen und Banken.

  Dabei geben sich Kriminelle per E-Mail oder Telefon als z. B. Geschäftsführer des eigenen Unternehmens oder – wichtiger für die Bankbranche – eines guten Geschäftskunden aus.

  Mitarbeiter werden unter Zeit- und psychologischem Druck und mit schlüssiger Begründung dazu gebracht, beträchtliche Überweisungen (ins Ausland) zu tätigen.

  Ist erst mal Geld in Richtung Kriminelle geflossen, lässt es sich durch die modernen Zahlungssysteme in Sekundenschnelle an nahezu jeden beliebigen Ort der Welt weiterleiten.

Genaue Zahlen über die Höhe der Schäden, die durch Internetbetrug und CEO-Fraud entstehen, gibt es nicht. Dies liegt auch daran, dass es – wie z. B. beim Love-Scamming – einige Zeit dauern kann, bis Opfer die perfide Übervorteilung erkennen und realisieren. Zudem wird nicht jede Straftat zur Anzeige gebracht. Schätzungen gehen dennoch von Schäden in Milliardenhöhe aus (siehe hierzu auch: BKA-Forschungsbericht: Kosten und Schäden durch Cyber-Kriminalität in Deutschland 1/2024[1]).

Fazit

Die Kriminalität hat sich durch Nutzung digitaler Werkzeuge und moderner Technik verändert. Der in der analogen Welt notwendige räumliche Bezug zwischen Täter und Opfer ist im Internetzeitalter nicht mehr ausschlaggebend. Ganz wesentlich, insbesondere bei der Initiierung von Abwehrmaßnahmen gegen Internetbetrügereien, ist der Faktor Mensch.

Für die Bankenbranche ist es daher von besonderer Wichtigkeit, nicht nur konkrete Sicherungsmaßnahmen weiter zu pflegen und nachzujustieren. Vielmehr sind regelmäßige Mitarbeiter-Schulungen zu den Betrugsmaschen 4.0 und ein Klima von Vertrauen und Sicherheit essentiell, um Betrugsversuche zu entdecken und zu verhindern. Im tatsächlichen Schadensfall gilt es, einen kühlen Kopf zu bewahren und die notwendigen Schritte zur Schadensbegrenzung zügig, aber nicht hektisch, einzuleiten. ▬

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

[1] Quelle: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/2024KKAktuell_Kosten_Schaeden_Cyberkriminalitaet.html

Schwerwiegende IKT-Vorfälle unter DORA

Meldepflichten und Praxisanforderungen unter DORA: Wie DORA und die BaFin den Umgang mit IKT-Vorfällen neu definieren und welche neuen Anforderungen damit verbunden sind – insbesondere bei (Teil-)Ausfällen von IKT-Drittdienstleistern, Cyberangriffen, Systemausfällen oder internen Sicherheitsverletzungen.

Mit der DORA-Verordnung (Digital Operational Resilience Act – Verordnung (EU) 2022/2554) sowie den technischen Regulierungsstandards (RTS 2024/1774[1] und RTS 2025/301[2]) wird der Umgang mit sogenannten IKT-Vorfällen verbindlich geregelt. Gleichzeitig konkretisiert die BaFin mit ihren Leitlinien, welche Erwartungen sie an die Institute stellt. Dieser Beitrag beleuchtet die gesetzlichen Anforderungen, grenzt den Begriff des IKT-Vorfalls praxisnah ab und beschreibt, welche Schritte im Ereignisfall notwendig sind.

Gesetzliche Anforderungen

Der Art. 3 Abs. 8 DORA definiert IKT-Vorfälle als nicht geplante Ereignisse bzw. eine entsprechende Reihe von Ereignissen, die die Sicherheit der Netzwerk- und Informationssysteme beeinträchtigen und negative Auswirkungen auf die Sicherheitsziele von Daten oder Diensten haben.

Art. 17 bis 23 DORA regeln den detaillierten Umgang mit IKT-Vorfällen und verpflichtet, Institute, Verfahren zur Erkennung, Klassifizierung, Behandlung und Meldung vorzuhalten.

Die Klassifizierung von Wesentlichkeitsschwellen und der Einzelheiten von Meldungen schwerwiegender Vorfälle ist im RTS 2024/1772 vorgegeben.

Die Meldefristen für schwerwiegende IKT-Vorfälle hat die BaFin im September 2024 präzisiert (BaFin – Veranstaltungen – Präsentation 4 – IKT-Vorfallsmeldewesen)[3].

Was ist ein IKT-Vorfall und wie ist er zu bewerten?

Nicht jede Störung ist ein meldepflichtiger IKT-Vorfall. Entscheidend ist die Auswirkung auf Funktionen oder Informationen. Abb. 1. gibt eine Orientierungshilfe, wie ein (potenzieller) IKT-Vorfall bewertet werden kann.

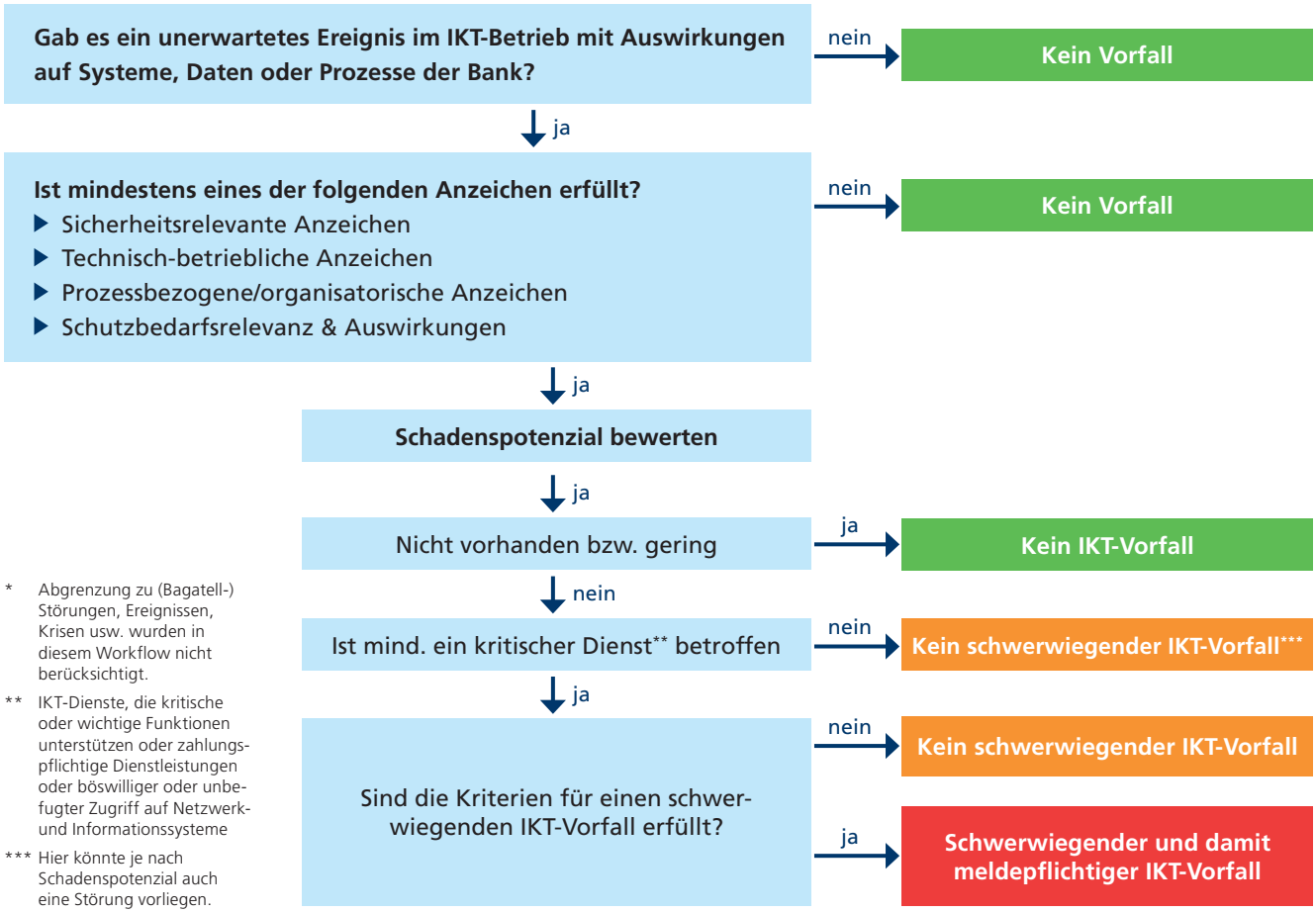
Sicherheitsrelevante Anzeichen

- Meldungen aus dem Security Information and Event Management (SIEM)
- Hinweise auf Malware, z. B. durch Virenscanner oder ungewöhnliche Prozesse
- Phishing-Angriffe oder kompromittierte Zugangsdaten
- Unautorisierter Datenabfluss (Data Leakage)
- Ungewöhnliche Anmeldezeiten oder -orte (z. B. Login aus Ländern, in denen keine Beschäftigten tätig sind)

Technisch-betriebliche Anzeichen

- Systemausfälle (z. B. relevante Anzahl an Clients, Server, Netzwerk, Storage) ohne erkennbare Ursache
- Unerwartet hohe Last auf Systemen oder Netzwerken
- Unerklärliche Veränderungen an Konfigurationen oder Datenbeständen
- Signifikanter Anstieg von Fehlermeldungen oder Support-Tickets

Abb. 1. **Einordnen von IKT-Vorfällen***



* Abgrenzung zu (Bagatell-) Störungen, Ereignissen, Krisen usw. wurden in diesem Workflow nicht berücksichtigt.

** IKT-Dienste, die kritische oder wichtige Funktionen unterstützen oder zahlungspflichtige Dienstleistungen oder böswilliger oder unbefugter Zugriff auf Netzwerk- und Informationssysteme

*** Hier könnte je nach Schadenspotenzial auch eine Störung vorliegen.

Prozessbezogene/organisatorische Anzeichen

- Schutzbedarf (Authentizität, Vertraulichkeit, Integrität, Nachvollziehbarkeit, kurz ACIN) von Geschäftsprozessen ist gestört oder kann nicht mehr gewährleistet werden.
- Kommunikation über zentrale Kanäle ist beeinträchtigt (z. B. E-Mail, Telefon).
- Mitarbeiter meldet Auffälligkeiten bei Systemnutzung oder IKT-Dienstleistungen.
- Verfügbarkeit von Funktionen ist eingeschränkt/nicht mehr vorhanden (z. B. Zahlungsverkehr, Ordersysteme, Limitsysteme, Onlinebanking etc.).

Schutzbedarfsrelevanz & Auswirkungen

- Reputationsschäden, rechtliche Konsequenzen oder finanzielle Verluste sind möglich.

Der IKT-Vorfall hat per Definition eine gewisse Reichweite, z. B. über mehrere Organisationseinheiten oder Institute hinweg. Die obige Aufzählung gibt eine Orientierung, was einen Vorfall ausmachen kann. Wesentlich ist die Frage, ob der Schutzbedarf (ACIN) der Prozesse eingehalten werden kann. Hier zeigt sich auch ein direkter Mehrwert aus der Einwertung der Funktionen im Informationsverbund durch die Prozessverantwortlichen.

Wir sehen, dass die Prozessverantwortlichen, die Beauftragten und der IT-Betrieb durch die Anforderungen immer enger und abgestimmter im Informationsverbund zusammenarbeiten.

Was ist zu tun, wenn ein IKT-Vorfall vorliegt?

Sobald ein IKT-Vorfall identifiziert ist, muss dessen Wesentlichkeit (RTS 2024/1772) eingestuft werden. Das Ergebnis zeigt auf, ob der IKT-Vorfall der BaFin gemeldet

werden muss (schwerwiegender IKT-Vorfall, vgl. Abb. 1). Die Klassifizierungskriterien werden in sieben Kategorien geclustert:

- Kunden, finanzielle Gegenparteien und Transaktionen
- Reputationsschaden
- Dauer und Ausfallzeit
- Geografische Ausbreitung
- Verlust von Daten
- Kritikalität der betroffenen Dienste
- wirtschaftliche Auswirkung

Im Rahmen der Anforderungen des RTS 2024/1772 haben wir als DZ CompliancePartner unseren Mandanten ein Tool bereitgestellt, mit dem sich die relevanten Kriterien systematisch abfragen lassen. Das Tool liefert eine klare Auswertung darüber, ob ein schwerwiegender und somit meldepflichtiger IKT-Vorfall vorliegt.

Im Falle einer Einstufung als schwerwiegender Vorfall leitet die Bank unverzüglich geeignete Gegenmaßnahmen ein, um die Auswirkungen einzugrenzen. Parallel dazu werden die vorgesehenen Kommunikationspläne aktiviert. Der Beauftragte IKT-Risikomanagement und Informationssicherheit bewertet gemeinsam mit dem zuständigen Fachverantwortlichen das Risiko für die Bank.

Die Erstmeldung eines schwerwiegenden IKT-Vorfalls an die BaFin erfolgt innerhalb der gesetzlich vorgegebenen Fristen über das Meldeportal der BaFin. Sollte sich der Sachstand der Erstmeldung wesentlich ändern oder sollten neue Erkenntnisse eine Neubewertung erfordern, wird eine Zwischenmeldung abgegeben. Zudem kann die BaFin jederzeit eine Zwischenmeldung anfordern. Nach Abschluss der Ursachenanalyse und der Ermittlung der tatsächlichen Auswirkungen wird eine Abschlussmeldung erstellt.

Grundsätzlich besteht die Möglichkeit, die Pflichten zur Meldung schwerwiegender IKT-Vorfälle auszulagern. Hierbei sind jedoch weitere aufsichtsrechtliche Anforderungen zu beachten. Kunden der ATRUVIA AG können diese Meldepflichten über das Produkt DORA-MIR auslagern. DORA-MIR umfasst eine 24/7-Überwachung von Störungen anhand der Kriterien gemäß Art. 18 und 23 DORA sowie die fristgerechte Übermittlung der erforderlichen Meldungen an die BaFin. Für Rückfragen der Aufsicht steht ebenfalls die ATRUVIA AG als primärer Ansprechpartner zur Verfügung.

Fazit

DORA regelt den Umgang mit IKT-Vorfällen neu. Ob tatsächlich ein meldepflichtiger IKT-Vorfall vorliegt entscheidet sich über die Frage nach den Auswirkungen der Störung. Wesentlich ist die Frage, ob der Schutzbedarf eingehalten werden kann oder eben nicht. Wenn es sich um einen schwerwiegenden Vorfall handelt, müssen einerseits unmittelbar Gegenmaßnahmen ergriffen werden und andererseits entsprechende Kommunikationspläne aktiviert werden.

Insgesamt ist mit DORA der Prozess um die Identifizierung schwerwiegender IKT-Vorfälle nachvollziehbarer und transparenter, leider aber auch aufwendiger geworden. ▬

[1] RTS 2024/1774 (https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401772, abgerufen am 25.04.2025)

[2] RTS 2025/301 (https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202500301, abgerufen am 25.04.2025)

[3] https://www.bafin.de/SharedDocs/Downloads/DE/Veranstaltung/dl_IT_Aufsicht_2024_4.html und https://www.bafin.de/DE/Aufsicht/DORA/Meldewesen_IKT_Vorfaelle/Meldung_schwerwiegender_IKT_bezogener_Vorfaelle_und_erheblicher_Cyberbedrohungen/Meldung_schwerwiegender_IKT_bezogener_Vorfaelle_und_erheblicher_Cyberbedrohungen_artikel.html

Frank Lutter
Beauftragter IKT-Risikokontrolle und Informationssicherheit,
E-Mail: frank-lutter@dz-cp.de

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

Herzlich willkommen, Yvonne Strunk

Bereits 29 Jahre ist Yvonne Strunk beruflich in der Genossenschaftlichen FinanzGruppe tätig und startete im März 2025 als Bereichsleiterin Compliance bei der DZ CompliancePartner. In den ersten Tagen ihrer neuen Tätigkeit konnte sie sich schnell im „neuen, alten" Themenfeld orientieren und erste Impulse für den Betrieb und den Ausbau des Bereichs Compliance einbringen.

Yvonne Strunk
Bereichsleiterin Compliance
E-Mail: yvonne.strunk@dz-cp.de

Frau Strunk, wie sind Sie beruflich zum Thema „Compliance" gekommen?
Wenn man das so sagen kann, über einen „direkten Umweg". Nach verschiedenen Stationen in der Westerwald Bank eG hatte ich bald auch erste Berührungspunkte mit der Compliance durch die Betreuung des Wertpapiergeschäfts. Und schon war ich infiziert: Seit 2021 habe ich schließlich das Thema als WpHG-Compliance-Beauftragte bzw. Single Officer in der Bank geführt.

Als Bereichsleiterin treiben Sie gemeinsam mit der Geschäftsleitung Compliance-Themen weiter voran. Wo sehen Sie Ihren Bereich in drei bis fünf Jahren?
Ich sehe meine Aufgabe vor allem darin, den Bereich Compliance im Sinne unserer Kunden weiter auszubauen. Dabei stehen Produktideen – sowohl in der MaRisk-Compliance als auch in der WpHG-Compliance – im Fokus, die die Kundenbedarfe bzw. die regulatorischen Anforderungen wirksam und zugleich effizient umsetzen. Egal, ob wir dabei den Kunden dauerhaft begleiten, punktuell beraten oder Wissen weitergeben, die DZ CompliancePartner hat nicht nur die Kraft der Mehrmandantentätigkeit, sondern auch das Potenzial, auf bankindividuelle Besonderheiten zu reagieren und über den Tellerrand hinausdenken zu können. Mein Ziel ist es, in drei Jahren die DZ CompliancePartner in den „Köpfen der Primärinstitute" als wichtigen strategischen Partner in den Compliance-Themen stärker verankert zu haben.

Was macht Sie als neue Bereichsleiterin Compliance besonders?
Ich bringe den Blick aus einem Primärinstitut mit. Die aktuellen Schmerzpunkte sind mir noch sehr präsent. Ich weiß, was die Banken „triggert". Das sind genau die Ansprüche und Wünsche, die ich bei der DZ CompliancePartner im Sinne von Services umsetzen möchte: Unter anderem ist es mir wichtig, unseren Kunden frühzeitig Umsetzungssicherheit zu vermitteln – auch wenn die BVR-Empfehlung vielleicht noch in der Ausarbeitung ist. Und natürlich ist es eines meiner wichtigsten Anliegen, Hilfestellungen und Unterstützung zu bieten angesichts der nicht enden wollenden Regulierungsflut. Meine Erfahrungen in Prozessen und Automatisierung sind dabei die Werkzeuge, die ich mitbringe, um die Compliance-Themen neu zu denken und nach vorne zu bringen. Übrigens: Meine Erfahrungen sind hier nur ein Werkzeug unter vielen: Ich bin hier auf ein sehr engagiertes Team gestoßen. Es macht schlicht Spaß, solch vermeintlich trockene regulatorische Themen mit so kompetenten und motivierten KollegInnen (neu) zu denken und auch gemeinsam Veränderungen herbeizuführen.

Zum Abschluss noch einige persönliche Fragen: Was essen Sie zum Frühstück?
Eher trinken: Zwei Tassen Kaffee und der Tag ist mein Freund.

Was ist Ihr größtes Talent?
Ich kann sehr gut organisieren und bin sehr strukturiert. Ich liebe es, viele Bälle in der Luft zu haben und sie dann aber auch nicht fallen zu lassen: Meine KollegInnen, aber auch meine Kunden können sich darauf verlassen, dass ihr Anliegen aufgefangen und bearbeitet wird.

Was ist Ihr bestes Smalltalk-Thema?
„Schönwetterthemen" sind nicht meine Sache. Ich gehe gerne direkt auf mein Gegenüber ein und komme auch gerne schnell auf den Punkt.

Frau Strunk, vielen Dank für Ihre Antworten.

Künstliche Intelligenz als Unterstützung in der Wertpapier-Compliance

Künstliche Intelligenz (KI) revolutioniert zunehmend unseren Alltag – auch im Finanzsektor. Doch kann KI auch in der Wertpapier-Compliance systemseitig unterstützen? Erste Versuche sind vielversprechend: Zukünftig könnte KI dazu beitragen, die komplexen regulatorischen Anforderungen im Wertpapiergeschäft automatisiert, effizient und fehlerarm zu erfüllen.

Vor einem möglichen Einsatz gilt es jedoch, die rechtlichen Rahmenbedingungen innerhalb der Wertpapierdienstleistungsunternehmen zu analysieren, relevante Hürden zu identifizieren und geeignete Maßnahmen zur Sicherstellung der rechtlichen Konformität zu entwickeln. Zielgerichtet eingesetzt, kann KI nicht nur die Einhaltung regulatorischer Vorgaben verbessern, sondern auch Kosten senken sowie die Präzision und Geschwindigkeit von Risikoanalysen deutlich steigern – etwa bei der Erkennung potenzieller Verstöße gegen das Marktmissbrauchsverbot.

Rechtliche und technische Einstiegshürden

Beim Einsatz von KI in der Wertpapier-Compliance sind insbesondere datenschutz- und aufsichtsrechtliche Anforderungen zwingend zu berücksichtigen. Eine der zentralen Herausforderungen stellt die Einhaltung der Datenschutz-Grundverordnung (DSGVO) dar. KI-Systeme verarbeiten häufig große Mengen personenbezogener Daten, was Herausforderungen in Bezug auf Datensicherheit, Transparenz und die Auswahl einer geeigneten Rechtsgrundlage für die Verarbeitung mit sich bringt. Besonders kritisch ist dabei die potenzielle Übermittlung von Daten in Drittstaaten ohne angemessenes Datenschutzniveau.

Hinzu kommt der regulatorische Rahmen durch die EU-Verordnung zur künstlichen Intelligenz (AI Act), die spezifische Anforderungen an KI-Systeme, insbesondere im sensiblen Bereich des Finanzwesens, formuliert. Der rechtskonforme Einsatz von KI erfordert daher eine sorgfältige Auswahl, Implementierung und Überwachung der Systeme, um Risiken zu minimieren und die aufsichtsrechtliche Konformität sicherzustellen.

Vor der praktischen Einführung ist zunächst zu prüfen, welche Prozesse innerhalb des Instituts grundsätzlich für einen KI-Einsatz geeignet sind. Darauf aufbauend sind die passenden KI-Modelle zu identifizieren und dem jeweiligen Anwendungsbereich zuzuordnen. Dabei ist gemäß Art. 4 KI-VO auch sicherzustellen, dass die erforderlichen KI-Kompetenzen im Institut vorhanden sind, um einen rechtskonformen Einsatz zu gewährleisten.

Nachfolgend ein Überblick über gängige Einsatzmodelle:

- Überwachungs- und Analysesysteme: Maschinelles Lernen ermöglicht die Echtzeitüberwachung von Handelsaktivitäten zur Identifikation auffälliger Muster oder Anomalien.
- Prognosemodelle: Aus historischen Daten werden zukünftige Trends oder Risiken abgeleitet.
- Berichterstattungssysteme: Automatisieren die Erstellung und Formatierung von Berichten.
- Natural Language Processing (NLP): Dient der Analyse umfangreicher Textdokumente und kann Prozessvorschläge generieren.
- Virtuelle Assistenten: Beantworten Fragen, erläutern Sachverhalte und liefern regulatorisch relevante Informationen in Echtzeit.
- Entscheidungssysteme: Unterstützen bei risikobasierten Bewertungen durch datengetriebene Entscheidungslogiken.

Grundlegend für das Verständnis ist auch die Unterscheidung der „Intelligenzgrade“:

- Schwache KI ist heute Stand der Technik. Sie löst klar definierte Aufgaben innerhalb enger Anwendungsgrenzen, ohne eigenständiges Bewusstsein.
- Starke KI ist bisher rein hypothetisch und zeichnet sich durch menschenähnliches Verständnis, Lernen und Denken aus. Ihr Einsatz wirft erhebliche ethische und regulatorische Fragen auf.

KI im Praxisalltag der Wertpapier-Compliance

Der potenzielle Nutzen von KI für die Wertpapier-Compliance ist vielfältig. Nachfolgend werden fünf exemplarische Anwendungsbereiche aufgezeigt:

1. Marktmissbrauch, Insiderhandel und Marktmanipulation

Durch den Einsatz von Analyse- und Überwachungssystemen können verdächtige Aktivitäten schneller erkannt werden. Auffälligkeiten wie ungewöhnliche Handelsvolumina, Transaktionen außerhalb üblicher Marktzeiten oder plötzliche Preisveränderungen lassen sich durch KI-basierte Systeme in Echtzeit analysieren. Durch kontinuierliches „Training“ der Algorithmen verbessert sich die Qualität der Erkennung fortlaufend, was eine präzisere und schnellere Reaktion auf potenzielle Verstöße ermöglicht.

2. Berichterstattung

Gemäß MaComp BT 1.2.2 sind regelmäßige schriftliche Compliance-Berichte an die Geschäftsleitung zu erstellen. Diese Berichte dokumentieren u. a. die Wirksamkeit des Kontrollsystems und identifizierte Risiken. KI kann in diesem Kontext Daten aggregieren, analysieren und in standardisierte Berichtsvorlagen überführen – was sowohl Zeit spart als auch potenzielle Fehlerquellen reduziert. Die abschließende inhaltliche Verantwortung verbleibt jedoch beim Compliance-Beauftragten, der für die Richtigkeit und Vollständigkeit der Berichte haftet. Die KI nimmt hier unterstützend eine Art „Sekretariatsfunktion“ ein.

3. Rechtsmonitoring

NLP-Technologien können regulatorische Texte analysieren, relevante Inhalte identifizieren und potenziellen Handlungsbedarf ableiten. Der Einsatz solcher Systeme bietet enormes Effizienzpotenzial: Bestehende Prozesse können automatisiert auf regulatorische Änderungen geprüft werden. Die institutsindividuelle Interpretation und Umsetzung verbleibt beim Compliance-Beauftragten, der die Ergebnisse der KI validiert. Dieses Zusammenspiel ermöglicht eine deutliche Arbeitserleichterung, ohne auf menschliche Expertise zu verzichten.

4. Virtuelle Assistenten

KI-basierte Chatbots können in Wertpapierdienstleistungsunternehmen wiederkehrende Anfragen beantworten, Richtlinien erläutern oder regulatorische Informationen bereitstellen. Auch in der Schulung von Mitarbeitenden könnten virtuelle Assistenten zum Einsatz kommen – etwa in interaktiven Lernumgebungen mit integriertem Feedbacksystem. Ein denkbares Zukunftsmodell wäre ein „KI-WpHG-Compliance-Chatbot", der Mitarbeitenden bei alltäglichen Fragestellungen autonom zur Verfügung steht. Besonders relevante oder sensible Themen könnten dabei automatisiert an die Compliance-Abteilung weitergeleitet werden.

5. Entscheidungsunterstützung

Entscheidungsunterstützungssysteme basieren auf der Analyse großer Datenmengen. Sie identifizieren Risiken, liefern strukturierte Empfehlungen und erleichtern fundierte Entscheidungen – etwa bei der Einstufung von Sachverhalten oder der Auswahl geeigneter Maßnahmen. Voraussetzung ist jedoch eine fachgerechte Einbindung unter Aufsicht des Compliance-Beauftragten. Richtig eingesetzt, erhöhen diese Systeme die Qualität von Entscheidungen und reduzieren die Fehleranfälligkeit komplexer Bewertungen.

Fazit

Künstliche Intelligenz bietet das Potenzial, die Wertpapier-Compliance effizienter, präziser und zukunftsfähiger zu gestalten. Ihre Fähigkeit, große Datenmengen zu verarbeiten, Risiken frühzeitig zu erkennen und Prozesse zu automatisieren, kann Compliance-Funktionen spürbar entlasten und optimieren.

Gleichzeitig ist der Einsatz mit hohen Anforderungen an Datenschutz, Transparenz und regulatorische Konformität verbunden. Diese Hürden müssen im Vorfeld einer Implementierung sorgfältig geprüft und adressiert werden, um rechtliche Risiken zu vermeiden.

KI wird die menschliche Expertise nicht ersetzen – insbesondere nicht die Rolle des Compliance-Beauftragten, der weiterhin gesetzlich verantwortlich bleibt. Vielmehr ist KI als unterstützendes Werkzeug zu verstehen, dessen Wirksamkeit letztlich von der Kompetenz und Steuerung durch den menschlichen Anwender abhängt. In diesem Zusammenspiel kann die Wertpapier-Compliance maßgeblich von den Möglichkeiten der KI profitieren – ohne dabei auf die notwendige menschliche Kontrolle zu verzichten. Und das ist auch gut so. ▬

Marcia Metzner
Beauftragte WpHG-Compliance,
E-Mail: marcia.metzner@dz-cp.de

Giannis Petras
Beauftragter WpHG-Compliance,
E-Mail: giannis.petras@dz-cp.de

Nachhaltigkeit in der Anlageberatung

Im nachfolgenden Beitrag werden die Anforderungen an die Nachhaltigkeit gemäß der Offenlegungsverordnung und deren praktische Umsetzung im Beratungsgeschäft vorgestellt.

Der Kapitalmarkt nimmt eine zentrale Rolle bei der Transformation hin zu einer nachhaltigen Wirtschaft ein. Im Rahmen des „EU Green Deal", der die Klimaneutralität bis 2050 zum Ziel hat, wurden umfassende regulatorische Maßnahmen ergriffen, um Kapitalströme gezielt in nachhaltige Aktivitäten zu lenken. Das Herzstück dieser Regulierungsarchitektur bildet die Verordnung (EU) 2019/2088 über nachhaltigkeitsbezogene Offenlegungspflichten im Finanzdienstleistungssektor (SFDR). Sie verpflichtet Finanzmarktteilnehmer dazu, sowohl auf Unternehmens- als auch auf Produktebene transparent über den Umgang mit Nachhaltigkeitsrisiken zu informieren. Ziel ist es, Greenwashing zu verhindern und fundierte Investitionsentscheidungen zu ermöglichen.

Ergänzt wird die SFDR durch die EU-Taxonomie-Verordnung (EU) 2020/852, die ein einheitliches Klassifikationssystem für ökologisch nachhaltige wirtschaftliche Aktivitäten etabliert. Demnach gelten Aktivitäten dann als nachhaltig, wenn sie

- wesentlich zu mindestens einem der sechs definierten Umweltziele beitragen,
- das DNSH-Prinzip (Do No Significant Harm, deutsch: Prinzip der Vermeidung erheblicher Beeinträchtigungen) wahren und
- soziale Mindeststandards einhalten.

Gemeinsam bilden SFDR und EU-Taxonomie die zentralen Säulen der Sustainable-Finance-Strategie der EU. Dieses kohärente Rahmenwerk zielt auf eine erhöhte Transparenz, bessere Vergleichbarkeit sowie auf die effektive Umlenkung von Kapital in eine klimaneutrale und ressourcenschonende Wirtschaft ab.

MiFID II und Nachhaltigkeitspräferenzen

Mit Wirkung zum 2. August 2022 sind die erweiterten europäischen Vorgaben zur Integration von Nachhaltigkeitspräferenzen in der Anlageberatung in Kraft getreten. Die Delegierte Verordnung (EU) 2021/1253 ergänzt MiFID II um verpflichtende Anforderungen zur Berücksichtigung individueller Nachhaltigkeitsziele. Seither sind Anlageberater verpflichtet zu erfassen, ob und in welchem Umfang Anleger nachhaltige Finanzprodukte bevorzugen. Diese Präferenzen sind als Teil der Anlageziele zu dokumentieren und bei der Produktauswahl zu berücksichtigen.

In der Praxis erfolgt eine Einteilung in drei Produktkategorien:

(a) Produkte mit einem Mindestanteil ökologisch nachhaltiger Investitionen gemäß Taxonomieverordnung,
(b) Produkte mit nachhaltigen Investitionen gemäß SFDR,
(c) Produkte, die wesentliche nachteilige Auswirkungen auf Nachhaltigkeitsfaktoren reduzieren.

Ein Abgleich zwischen Kundenpräferenz und Produktprofil ist obligatorisch – eine Empfehlung ohne Übereinstimmung ist unzulässig. Änderungen der Präferenzen sind ebenfalls zu dokumentieren.

Mit der Aktualisierung des Moduls BT 7.1 MaComp wurde die Abfragepflicht um eine quantitative Komponente erweitert. Neben dem „Ob" wird nun auch das „Wie viel" erhoben, also der gewünschte Mindestanteil nachhaltiger Investitionen in den Kategorien (a) und (b). Die Auswahl erfolgt über standardisierte Antwortoptionen

(1 %, 15 %, 50 % oder keine Festlegung). Die erfassten Mindestanteile sind in der Geeignetheitserklärung inkl. Begründung der Produktempfehlung zu dokumentieren. Etwaige Abweichungen zwischen Produktquoten und Präferenzen sind dem Kunden zu erläutern.

Anforderungen der Offenlegungspflichten in der Anlageberatung

Finanzberater sind verpflichtet, im Rahmen ihrer Beratung zentrale Informationen zu Nachhaltigkeitsrisiken offenzulegen. Dies umfasst u. a.:

- die Strategie zur Integration von Nachhaltigkeitsrisiken in die Anlagestrategie,
- deren Berücksichtigung in der Vergütungspolitik sowie
- konkrete Erläuterungen zur Einbindung dieser Risiken in den Beratungsprozess.

Darüber hinaus ist eine Bewertung der potenziellen Auswirkungen von ESG-Risiken (Umwelt/Environment, Soziales/Social, Unternehmensführung/Governance) auf die Rendite der empfohlenen Finanzprodukte vorzunehmen. Dabei ist offenzulegen, inwieweit nachteilige Auswirkungen auf Nachhaltigkeitsfaktoren berücksichtigt werden.

Die Offenlegungsverordnung verpflichtet zur Veröffentlichung dieser Informationen sowohl auf der Unternehmenswebsite als auch in den vorvertraglichen Informationen (VVI). Letztere müssen dem Kunden vor Erbringung einer Wertpapier(neben)dienstleistung zur Verfügung gestellt werden. Eine erneute Aushändigung wird erforderlich, wenn sich gemäß Art. 46 Abs. 4 der Delegierten Verordnung (EU) 2017/565 seit der letzten Beratung wesentliche Änderungen ergeben haben. Die Integration der vorvertraglichen Informationen in den Beratungsprozess ist daher dringend zu empfehlen.

Je nach Art der Anlageberatung erfolgt die Umsetzung der Offenlegungspflichten unterschiedlich. Für Produkte verbundener Unternehmen werden in der Regel standardisierte Anlagen des BVR verwendet. Diese beinhalten:

- die Veröffentlichung der Strategien zur Einbeziehung von Nachhaltigkeitsrisiken (Art. 3 Abs. 2 SFDR),
- Informationen zur Vergütungspolitik (Art. 5 SFDR),
- Erläuterungen zur Einbindung von Nachhaltigkeitsrisiken in den Beratungsprozess sowie
- Bewertungen der Auswirkungen auf die Rendite (Art. 6 SFDR).

Zudem wird eine Erklärung zur Berücksichtigung der wichtigsten nachteiligen Auswirkungen auf Nachhaltigkeitsfaktoren (Art. 4 Abs. 5 SFDR) bereitgestellt.
Die Dokumente sind sowohl auf der Unternehmenshomepage des jeweiligen Instituts als auch in den vorvertraglichen Kundeninformationen aktuell verfügbar. Eine nachvollziehbare Änderungshistorie und ein Versionsdatum im Dateinamen sind
sicherzustellen.

Bei der Beratung zu Produkten außerhalb der Verbund-Hausmeinung werden beide Anlagen inhaltlich ergänzt und angepasst, um eine konforme Offenlegung zu gewährleisten. Im Rahmen von Beratungsmandaten gegenüber Kapitalverwaltungsgesellschaften erfolgt zusätzlich eine spezifische Beschreibung der Produktauswahl für geeignete Gegenparteien.

Einfluss auf den Product-Governance-Prozess

Die Zielmarktüberprüfung stellt sicher, dass die Bank-Hausmeinung mit den Nachhaltigkeitsanforderungen der angebotenen Produkte übereinstimmt. Von besonderer Relevanz sind die definierten Mindestausschlüsse, die aktuell geächtete Waffen, Tabakproduktion, Kohle sowie schwere Verstöße gegen die Prinzipien des UN Global Compact umfassen. Der zuvor geltende Ausschluss von Rüstung wurde im Rahmen der jüngsten Überarbeitung der Mindeststandards zur Zielmarktbestimmung entfernt. Grundlage der Prüfung sind die standardisierten Formu-

lare des Verbändekonzepts zur Klassifikation nachhaltiger Finanzprodukte. Diese Verpflichtung gilt ausschließlich für explizit als nachhaltig deklarierte Produkte. Einzeltitel wie Aktien oder Anleihen sind nicht von der SFDR erfasst und unterliegen daher nicht der Offen-legungspflicht.

Ein zentrales Problem stellt die fehlende regulatorische Standardisierung der Nachhaltigkeitsquoten in der Produktgruppe „positiver Beitrag zur Nachhaltigkeit“ dar. Bislang wurden von der BaFin keine verbindlichen Vorgaben zur Ermittlung des Mindest- und Ist-Anteils nachhaltiger Investitionen veröffentlicht. Das birgt das Risiko zivilrechtlicher Beanstandungen bei zweifelhaften Berechnungsansätzen – mit der Gefahr, dem Vorwurf des Greenwashings ausgesetzt zu sein.

Um dieses Risiko zu minimieren, empfiehlt es sich für Banken, Produkte vom Beratungsvorschlag auszuschließen, wenn der Produkthersteller keine belastbaren und nachvollziehbaren Angaben zur ESG-Berechnung liefert. Für Produkte von DZ BANK, Union Investment und R+V liegt grundsätzlich eine transparente Methodik vor. Vor diesem Hintergrund ist ein Vorstandsbeschluss zum Umgang mit Ausschlusskennzeichen in der Produktgruppe (b) sinnvoll. Aktuell existieren verschiedene Ansätze, darunter der „activity-based“, „pass-fail-activity-based“, „entity-based“ sowie der „Best-in-Class“-Ansatz. Produkte, die keine taxonomiekonforme Methodik aufweisen oder deren Methodik nicht nachvollziehbar begründet ist, können mit einem Ausschlusskennzeichen versehen werden.

Christian Tipkemper
Beauftragter WpHG-Compliance,
E-Mail: christian.tipkemper@dz-cp.de

Fazit

Die Integration von Nachhaltigkeitskriterien in die Anlageberatung stellt eine zentrale Herausforderung, aber auch eine strategische Chance dar.

Obwohl laut BaFin die Nachhaltigkeitspräferenzen in der Praxis bislang eine untergeordnete Rolle spielen, sind sie dennoch ein verbindlicher Bestandteil der Anlageberatung nach MiFID II.

Ob und in welchem Umfang die regulatorisch geforderte Nachhaltigkeitspolitik tatsächlich gelebt und implementiert wird, bleibt fraglich. Oftmals stehen bei der Produktauswahl weiterhin Rendite und Diversifikation im Vordergrund. Es ist abzuwarten, ob der regulatorische Rahmen künftig zu einer vertieften Relevanz führt und umfassendere Anforderungen an die Finanzinstitute stellt, um noch transparenter und zielgerichteter vorzugehen.

Bereits jetzt leisten die EU-Regulierungen einen Beitrag zur Steigerung der Transparenz und zur gezielten Umlenkung von Kapital in nachhaltige Investitionen. Ob sie langfristig eine messbare Wirkung entfalten, wird maßgeblich von der konsequenten Umsetzung, der Entwicklung belastbarer ESG-Standards sowie dem Verhalten der Anleger abhängen. ▬

Finanzsanktionen & MaRisk-Compliance-Funktion

Hätte man vor wenigen Jahren gefragt, wer in einer Bank für Finanzsanktionen und Embargos zuständig ist, so hätten die meisten wohl auf den Geldwäsche-Beauftragten, vielleicht auch auf die Interne Revision verwiesen. Das hat sich mit dem Merkblatt der Deutschen Bundesbank zur Einhaltung von Finanzsanktionen vom Juli 2021 grundlegend geändert.

Merkblatt zur Einhaltung von Finanzsanktionen 2021

Finanzsanktionen werden ergriffen, um bestimmten Personen, Organisationen oder Staaten den Zugang zum globalen Finanzsystem zu beschränken. Mit dem Merkblatt vom Juli 2021 verband sich das Ziel, den Akteuren im Finanzsektor eine Orientierung zu geben, auf welche Art und Weise den in Deutschland geltenden Finanzsanktionen entsprochen werden kann.

Neben operativen Tätigkeiten zu Finanzsanktionen wie Verfügungs- und Bereitstellungsverboten, Beschränkungen des Zahlungsverkehrs, Verboten und Vorbehalten sowie Meldepflichten werden nun auch **„Vorbildliche Verfahren“** zur Einhaltung von Finanzsanktionen in dem Merkblatt beschrieben. Die „Vorbildlichen Verfahren“ oder auch Best-Practice-Verfahren betreffen die Geschäftsorganisation, das Interne Kontrollsystem und die Interne Revision.

- Interne Revision: Von der Internen Revision werden regelmäßige Prüfungen zum Thema Finanzsanktionen erwartet, wobei grundsätzlich ein Dreijahresrhythmus ausreichend ist, bei besonderen Risiken jedoch ein jährlicher Rhythmus einzuhalten ist. Auch ist die Risikoeinstufung der Aktivitäten und Prozesse regelmäßig zu überprüfen und zu dokumentieren.
- Geschäftsorganisation: Hinsichtlich der Geschäftsorganisation hat die Geschäftsleitung sicherzustellen, dass aktuelle schriftliche Organisationsrichtlinien vorliegen und den betroffenen Beschäftigten in geeigneter Weise bekannt gemacht werden. Auch sind die Dokumente aktuell zu halten und auf geänderte Aktivitäten und Prozesse anzupassen.

Neu waren in dem Rundschreiben die Ausführungen zur Verantwortlichkeit der **(MaRisk-)Compliance-Funktion.** Sie hat auf die Implementierung wirksamer Verfahren zur Einhaltung der Finanzsanktionen und entsprechender Kontrollen hinzuwirken und diese Kontrollen zu überwachen.

Ferner wird der Compliance-Funktion eine Unterstützungs- und Beratungsfunktion gegenüber der Geschäftsleitung zugewiesen. Schlussendlich hat sie auch eine Berichterstattungspflicht, die üblicherweise durch den Kontrollbericht sowie im Rahmen des Jahresberichtes erfüllt wird.

Der BVR hat mit der Musterbestandsaufnahme April 2023 eine Zuständigkeit der MaRisk-Compliance-Funktion für Finanzsanktionen postuliert.

Eigenständige Arbeitsanweisung Finanzsanktion?

Vor dem Hintergrund des Merkblattes und von dessen Zielen stellt sich die Frage nach einer eigenständigen Arbeitsanweisung zu Finanzsanktionen. Zumindest in der Genossenschaftlichen FinanzGruppe gibt es derzeit eine solche Muster-Arbeitsanweisung zu Finanzsanktionen nicht. Die Regelungen sind bislang in anderen Dokumenten enthalten (insbesondere Auslandszahlungsverkehr, Kundenanlage, -änderung und -löschung oder Kontoanlage, -änderung und -auflösung bzw. Prävention von Geldwäsche, Terrorismusfinanzierung und strafbaren Handlungen).
Aus Gesprächen mit der Aufsicht ist der DZ CompliancePartner allerdings bekannt, dass eine eigenständige Arbeitsanweisung zu Finanzsanktionen (und Embargos) gewünscht ist.

Inhalte einer Arbeitsanweisung Finanzsanktionen könnten sein:

- Zielsetzung/Vorgaben
- Zuständigkeiten
- Begriffsbestimmungen
- Datenversorgung
- Prozessablauf/Umgang mit Verdachtsmomenten/ Verdachtsfällen
- Auswertung Kundenbestand/Überwachung und Bearbeitung sanktionierter Kunden
- Finanzsanktionen Russland/Ukraine: Kontrollen bezüglich Einlagen von russischen/belarussischen Staatsangehörigen
- Datenkontrollen Kundenbestand
- Wertpapiergeschäft
- Schulungen

Eine solche eigenständige Arbeitsanweisung hätte den ganz praktischen Vorteil, dass sie von den Mitarbeitern sofort gefunden wird, dass die Regelungen in einem Dokument zusammengefasst sind und inhaltlich in der Gesamtheit erschlossen werden können. Gerne unterstützen wir Sie bei der Implementierung einer Arbeitsanweisung zu Finanzsanktionen.

Fachlicher Hinweis des IDW vom 24. November 2022 zur Compliance-Funktion

Aufgrund des Russland-Ukraine Krieges hat der Bankenfachausschuss des Institutes der Wirtschaftsprüfer am 24. November 2022 einen fachlichen Hinweis zu den Auswirkungen des Krieges auf die Geldwäscheprüfung nach § 29 Abs. 2 KWG und die Beurteilung der MaRisk-Compliance-Funktion veröffentlicht. In der Verlautbarung werden die Anforderungen an die MaRisk-Compliance-Funktion in Bezug auf Finanzsanktionen dargestellt, insbesondere die aus dem Russland-Ukraine-Krieg resultie-renden Finanzsanktionen gegen Russland und Belarus[1].
Inhaltlich stellt das IDW folgende Anforderungen an die MaRisk-Compliance-Funktion:

- Mit-Verantwortung der MaRisk-Compliance-Funktion bezüglich der Identifikation, Einwertung und Überwachung von Finanzsanktionen
- Mit-Verantwortung der MaRisk-Compliance-Funktion imProzess zur Identifikation von Neuerungen
- Einbindung in die Betroffenheitsanalyse zu Sanktionsregimen
- Einbindung in die Erhebung und Beurteilung der Wesentlichkeitsbetrachtung gemäß AT 4.2.2. MaRisk
- Implementierung von Kontrollen nebst Berichterstattung
- Identifikation von Umsetzungsbedarfen
- Berichterstattung mit Aussagen zur Angemessenheit und Wirksamkeit von Maßnahmen

Merkblatt zur Einhaltung von Finanzsanktionen 2024

Im Juni 2024 hat die Deutsche Bundesbank dann eine aktualisierte Version des Merkblattes zur Einhaltung von Finanzsanktionen veröffentlicht (RS 46/2024). Die Überarbeitung war notwendig, da im vorherigen Merkblatt neue Sanktionsmaßnahmen, die maßgeblich mit den EU-Sanktionen gegen Russland und Belarus eingeführt wurden, nicht enthalten waren, z. B. der SEPA-Ausschluss

russischer Banken, neue Meldepflichten sowie neue Themen, wie beispielsweise Sanktionen mit Bezug zu Kryptowerten.

Hinsichtlich der „Vorbildlichen Verfahren“ wird nun darauf hingewiesen, dass sie keinen gesetzlichen Charakter haben, sie aber gleichwohl die Empfehlungen der RAG RELEX[2] und der FATF[3] aufgreifen und sich auf Maßstäbe beziehen, die sich aus dem KWG, den MaRisk oder dem VAG ergeben können.

Hinsichtlich der MaRisk-Compliance-Funktion und des Berichtswesens werden keine neuen Anforderungen postuliert, die Formulierungen sind in beiden Merkblättern gleich.

Überblick über die Neuerungen

Die Neuerungen aus dem Merkblatt 2024 lassen sich wie folgt zusammenfassen:

- Die bei der Grenzzolldirektion angesiedelte Zentralstelle für Sanktionsdurchsetzung wird erwähnt.
- Eine Übersicht über verschiedene finanz- und kapitalmarktbezogene Verbote, die über die schon bestehenden Verfügungs- und Bereitstellungsverbote hinausgehen, wurde aufgelistet, auch wurden Wertpapierhandels- und Dienstleistungsverbote ergänzt.
- Bereitstellungsverbote von Finanzhilfen betreffen nun auch Versicherungen und Investitionsverbote.
- Sanktionen mit Bezug zu Kryptowerten und Versicherungen werden behandelt.
- Es gibt nun einen allgemeinen Teil für alle Unternehmen im Finanzsektor und einen speziellen Teil für Finanzinstitute und (Rück-)Versicherungen.
- Im allgemeinen Teil werden Ausführungen zum Erkennen indirekt sanktionierter Personen, der Umgehung von Sanktionsvorschriften sowie zum Umgang mit Neu-, Bestandskunden und Entlistungen gemacht.
- Im speziellen Teil werden die Anforderungen an die Kreditinstitute betreffend die Einrichtung kunden- oder kontobezogener Sperren konkretisiert, Kryptowerte und Echtzeitüberweisungen werden erfasst.
- Im speziellen Teil werden in Bezug auf (Rück-)Versicherungen neue Anforderungen für Versicherungsprämien und Leistungsauszahlungen aufgestellt.

Zusammenfassung

Die Anforderungen an die Bearbeitung und Einhaltung von Finanzsanktionen sind grundsätzlich nicht neu. Mit dem Bundesbank-Merkblatt zur Einhaltung von Finanzsanktionen aus dem Jahr 2021 wurde jedoch der Aufgabenkreis der MaRisk-Compliance-Funktion neu gestaltet und erweitert. Sie ist nun mitverantwortlich für die Einhaltung von Finanzsanktionen im Institut.

Die MaRisk-Compliance-Funktion und deren Bedeutung im Institut wird hierdurch aufgewertet. Dies zeigt deren generalistischen Ansatz, der in den letzten Jahren immer stärker zum Tragen kam. Als Stichworte seien hier nur die Themen „Nachhaltigkeit“, „Immobilien“ oder „Produkt-Governance“ genannt.

Um die Erwartungen der Aufsicht zu erfüllen und den Mitarbeitern die Arbeit zu erleichtern, empfiehlt es sich, eine eigenständige Arbeitsanweisung für Finanzsanktionen (und Embargos) im Institut zu implementieren (siehe Infokasten oben).

Benötigen Sie Unterstützung bei der Implementierung einer Arbeitsanweisung zu Finanzsanktionen oder haben Fragen, so sprechen Sie uns gerne an. ▬

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

[1] Im Jahr 2024 betrafen 19 von 84 Sanktionsrundschreiben den Russland-Ukraine-Krieg und im Jahr 2025 sind es bislang vier von 15 (Stand 15.04.2025). Daraus lässt sich die Wichtigkeit der Überwachung ableiten.

[2] Europäischer Rat: Gruppe der Referenten für Außenbeziehungen (RELEX), https://www.consilium.europa.eu/de/council-eu/preparatory-bodies/working-party-foreign-relations-counsellors/

[3] Financial Action Task Force, https://www.fatf-gafi.org/

Donnerstag, 25. September 2025
Schloss Montabaur

Der Compliance-Kongress 2025
Zur Zukunft der Compliance im Verbund

Regulatorik
Was die Aufsicht jetzt von Banken erwartet

Compliance-Radar
Was Sie aus 1.200 Auslagerungsmandaten für Ihre Bank lernen können

Verbund
Wie Gemeinschaft Compliance stärkt

Compliance-Forecast
Womit Sie 2026+ im Beauftragtenwesen rechnen sollten

Psychologie
Warum Regelbrüche menschlicher sind, als wir meist denken

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

ComplianceCollege

Umsetzungspflicht für KI-Verordnung und KI-Kompetenz

Die Umsetzungsverpflichtungen aus der KI-Verordnung (KI-VO) und hier insbesondere zur Schulung von KI-Kompetenz gemäß Art. 4 KI-VO betreffen alle Unternehmen und Banken, die KI-Systeme oder KI-Modelle verwenden – und das trifft fast ausnahmslos auf alle Volksbanken Raiffeisenbanken zu.

Viele meinen, dass Ihre Bank nicht Adressat der KI-VO sei, da sie in der Regel ihre Umsetzungslösungen vom Rechenzentrum bucht und somit das Rechenzentrum in der alleinigen Verantwortung zur Umsetzung der KI-VO stehe. Das stimmt so nicht. Die KI-VO unterscheidet unterschiedliche Rollen, welche mit entsprechend unterschiedlichen Pflichten verbunden sind. Somit fällt auch eine Bank, die lediglich ein Produkt des Rechenzentrums oder eines anderen Dienstleisters mit KI-Bezug gebucht hat, in den Anwendungsbereich der KI-VO und steht folglich auch in der Umsetzungspflicht gemäß KI-VO[1].

Schulung von KI-Kompetenz

Eine erste Anforderung ergibt sich aus Art. 4 KI-VO i.V.m. Art. 113 KI-VO: Alle Mitarbeiterinnen und Mitarbeiter, „die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI Systemen befasst sind“, müssen über „ein ausreichendes Maß an KI-Kompetenz verfügen“. Die Erfüllung dieser Pflicht ist bereits seit Februar 2025 erforderlich.

Dabei ist es nicht ausreichend, wenn ein Unternehmen bzw. eine Bank einige auserwählte Mitarbeiter, wie bspw. HR-Abteilungsleitungen oder Marketingabteilungsleitungen, hinsichtlich der KI-Kompetenz gemäß Art. 4 KI-VO schult. Der Nachweis einer geeigneten KI-Kompetenz (vgl. auch PoC-Ausgabe 1/2025[2]) bezieht sich auf alle Mitarbeiter, die KI (potenziell) nutzen können – unabhängig von deren Tätigkeitsschwerpunkten, Kompetenz oder Rolle im Unternehmen. Dieser Tatbestand wird in der Praxis häufig nicht berücksichtigt, was zu einer unzureichenden Umsetzung der KI-VO führt.

Damit fällt auch der Sachbearbeiter bei der Kreditvergabe durch bspw. VR-Rating oder der Kundenberater mit der Möglichkeit der Nutzung des Edge-Browsers Copilot oder M365 unter den Anwendungsbereich.

Abb. 1. **Kompetenzen für die Umsetzung**

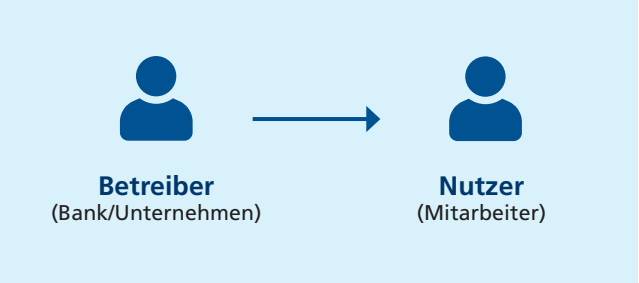
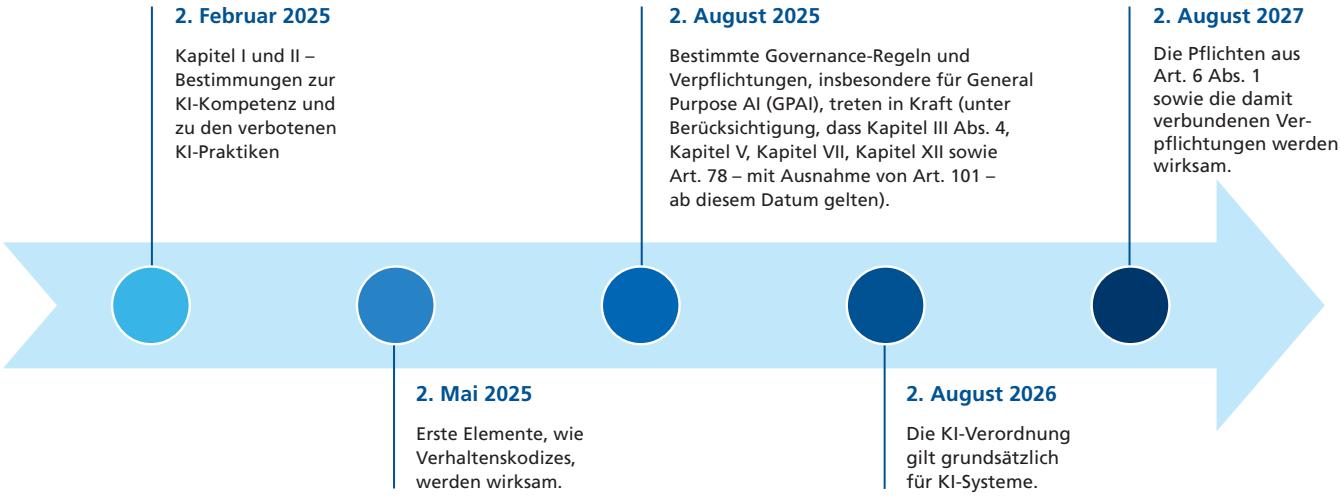


Abb. 2. **Zeitstrahl zur KI-Verordnung (KI-VO)**



Sensibilisierung

Das heißt nicht, dass nun alle Mitarbeiter zu KI-Managern oder KI-Experten werden müssen. Es ist gemäß Art. 4 KI-VO ausreichend, dass Mitarbeiter durch entsprechende Schulungen bestmöglich sensibilisiert sind.

Alle Mitarbeiter sollen erkennen können, was eine KI im Sinne der KI-VO ist und wie KI-Systeme sicher und sachkundig eingesetzt werden. Ebenso ist ein wesentlicher Punkt, alle Mitarbeiter hinsichtlich der Chancen, Risiken und potenziellen Schäden der Nutzung von KI-Systemen oder -Modellen zu sensibilisieren.

Fazit

- Die Schulung hinsichtlich der KI-Kompetenz betrifft alle Mitarbeiter im Unternehmen und ist seit Februar 2025 verpflichtend, aber bis 2. August noch ohne Sanktionen belegt.
- Die KI-VO ist auch dann umzusetzen, wenn lediglich Produkte mit KI-Systemen vom Rechenzentrum gebucht werden und nicht selbst entwickelt wurde.
- Der Vorstand bzw. die Geschäftsleitung ist gemäß Art. 25a KWG verpflichtet, erforderliche Maßnahmen für die Ausarbeitung der entsprechenden institutsinternen Vorgaben zu ergreifen. Es ist sicherzustellen, dass die Bank bzw. das Unternehmen die gesetzlichen Vorschriften einhält.
- Der BVR hat bereits erste Leitfäden für den Umgang mit KI im Unternehmen herausgegeben. Darin sind die möglichen Rollen der Bank und deren Folgen erwähnt[3].
- Die BaFin fordert entsprechende organisatorische Maßnahmen und die Mindestanforderungen an ein Risikomanagementsystem umzusetzen[4]. ▬

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

[1] Als Einführung zur KI-Verordnung empfehle ich auch den Artikel: Isikli in PoC 01/2024, Seite 18 bis Seite 21: „Einführung in die KI-Verordnung“ oder abrufbar unter https://www.dz-cp.de/medien/pdf/point-of-compliance/2024/poc_1-2024_ki-verordnung_isikli.pdf

[2] Diamante/Isikli in PoC 01/2025, Seite 8 bis Seite 10: „KI-Kompetenz-Schulung gemäß KI-Verordnung“ oder abrufbar unter https://www.dz-cp.de/medien/pdf/point-of-compliance/2025/poc_1-2025-ki-kompetenzschulung.pdf/

[3] BVR: Leitfaden KI und Recht – Allgemeine Darstellung am Bsp. ChatGPT

[4] BaFin, Rundschreiben 06/2024 BA: BaFin – Rundschreiben – Rundschreiben 06/2024 (BA) – MaRisk (PDF-Version)

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 CP genügt den Anforderungen gemäß MaRisk AT 4.4.3 und BT 2.

Seit der letzten Berichterstattung in der Point of Compliance (1/2025, S. 26) wurden aus der von der Geschäftsführung genehmigten Jahresprüfungsplanung 2025 die Prüfungen der Bereiche „Hinweisgebersystem“ und „Kommunikation und Bildung“ abgeschlossen und ersterer an die Mandaten der jeweiligen Auslagerungen versandt. Der zweitgenannte Prüfungsbericht ist nicht dienstleistungsbezogen und wurde daher intern veröffentlicht.

Die externe Prüfung der Geschäftsbereiche Datenschutz, Geldwäsche- und Betrugsprävention, Informationssicherheit, MaRisk-Compliance und WpHG-Compliance nach IDW PS 951 (Typ 2) wurde wiederum von der Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft vorgenommen. Für alle Bereiche wurde jeweils ein Testat ohne wesentliche Einschränkung erteilt. Die Endfassungen der Berichte zur externen Prüfung wurden an die Kunden der jeweiligen Dienstleistung versandt.

Die externe Prüfung der Funktion Hinweisgebersystem nach IDW PS 331 erfolgte ebenfalls durch die Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft. Es wurde die Ordnungsmäßigkeit testiert und der Prüfungsbericht an die Mandantschaft versandt.

Der Quartalsbericht für das erste Quartal 2025 der Internen Revision wurde fristgerecht erstellt und den Mandanten, die im Zeitraum zu unseren Kunden gehörten, zur Verfügung gestellt.

Weiterhin wurde turnusgemäß ein Follow-Up Quartalsbericht für Q1 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

Das wirtschaftliche Ergebnis der DZ CompliancePartner lag im ersten Quartal 2025 mit +140 T€ leicht über Plan. Die Erträge überschritten im selben Zeitraum den Plan um 4 %. Die Personal- und Sachkosten zzgl. der Abschreibungen lagen 1 % über Planniveau.

Die DZ CompliancePartner wird die tarifliche Lohnsteigerung für ihre Beschäftigten analog umsetzen. Vor dem Hintergrund sehr enger Gewinnmargen verbunden mit der Preisstabilität der letzten Jahre ist eine entsprechende Preisanpassung zum 1. Juli 2025 vorgesehen. Geschäftsstrategisch verbindet sich mit der Gehalts- und mittelbar Preisanpassung eine Investition in die Qualität der Dienstleistung, um langfristig qualifiziertes Personal für die Beauftragtentätigkeit binden zu können.

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

Genossenschaftliche FinanzGruppe
Volksbanken Raiffeisenbanken