Point of Compliance
Das Risikomanagement-Magazin

AUSGABE 1/2025

PoC

DZ CompliancePartner

Folgen Sie der DZ CompliancePartner GmbH auf Social Media.

IMPRESSUM

PoC – Point of Compliance
Das Risikomanagement-Magazin,
Ausgabe 35, 1/2025
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:
Najat Diamante, Felix Fröhlich, Derya Isikli, Marcia Metzner, Giannis Petras, Jens Saenger, Jörg Scharditzky, Björn Scherer, Lars Schinnerling, Thomas Schröder

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

Redaktionsschluss: 31. Januar 2025
Auflage: 2.400 Exemplare

„KI IST wahrscheinlich das Beste oder das Schlimmste, was der Menschheit passieren kann“, so Stephen Hawking, lange bevor „künstliche Intelligenz“ in aller Munde war. Heute fragen wir uns: „Wie machen wir das Beste aus KI?“

Meiner Ansicht nach indem wir uns klare Regeln geben. Insofern befürworte ich sehr, dass KI nun einen ersten regulativen Rahmen bekommt. Ob DORA, DSGVO oder nun auch ganz explizit die KI-Verordnung: Gemeinsam ist diesen Initiativen, dass sie uns die Chance bieten, sinnvoll, strukturiert und risikobewusst mit KI umzugehen.

Wir machen das Beste aus KI, wenn wir darauf achten, dass der Einsatz von KI immer unseren Grundwerten entspricht. Deshalb macht die – ab diesem Monat verpflichtende – KI-Schulung gemäß KI-Verordnung auch Sinn: Sie fördert den systematischen KI-Kompetenzaufbau und sensibilisiert für die Chancen und Risiken (S. 8). In der Anwendung und Umsetzung wird uns das Zusammenspiel technischer und organisatorischer Maßnahmen helfen, eventuelle Bedrohungsrisiken verlässlich zu erkennen und ihnen zu begegnen (S. 4).

Ich bin überzeugt, dass wir die strukturellen, die kulturellen und auch die ethischen Fragen lösen werden, um unternehmerischen Freiraum zu sichern und auch auszubauen. Wir unterstützen Sie dabei als die Compliance-Experten und Partner in der Genossenschaftlichen FinanzGruppe.

Ich wünsche Ihnen eine spannende Lektüre.

Herzlichst
Ihr Jens Saenger

Jens Saenger
Sprecher der Geschäftsführung

KI – ein IKT-Risiko?

KI hat zwischenzeitlich Einzug in den Bankenalltag gefunden. Grund genug, sich dem Themenfeld KI aus der Perspektive des IKT-Risikos und der Informationssicherheit anzunähern.

Die großen Sprachmodelle („large language models", LLM) wie ChatGPT haben künstliche Intelligenz (KI) nicht nur der breiten Öffentlichkeit zugänglich gemacht, sondern auch in der Genossenschaftlichen FinanzGruppe zu einem festen Bestandteil der täglichen Arbeit werden lassen. Sei es beim Erstellen von Präsentationen, Übersetzen von Texten oder zur Generierung ansprechender Grafiken: KI-Systeme zu nutzen, ist in zahlreichen Prozessen der Bank inzwischen etabliert. Deshalb soll hier das Themenfeld „KI" aus dem Blickwinkel des IKT-Risikomanagements und der Informationssicherheit betrachtet werden. Der Fokus liegt auf potenziellen und realen Bedrohungen, aber auch auf den Chancen, Ihre IKT- und Informationssicherheitsprozesse auszubauen.

Für uns gilt grundsätzlich, dass KI-gestützte Systeme weder als Universallösung für alle Anforderungen zu preisen, noch als generelle Bedrohung anzusehen sind.Sie sind Werkzeuge wie viele andere und können daher sowohl konstruktiven als auch destruktiven Verwendungszwecken dienen (sog. Dual-Use-Güter). Ein Beispiel hierzu wären Penetrationstests, die sowohl beim Red Teaming einen Angriff auf ein Zielnetzwerk simulieren können als auch bei der Durchführung tatsächlicher Angriffe Verwendung finden. Oder Sprachmodelle, die den Anwender anhand seiner Stimme – nahezu einwandfrei – identifizieren können und ihm so eine einfache Anmeldung an einem System ermöglichen. Andererseits wird mithilfe derselben Modelle auch Identitätsdiebstahl vereinfacht.

Einfluss von KI am Beispiel von Sprachmodellen

Der Start von ChatGPT im November 2022 führte zu einem intensiven Wettbewerb auf dem Markt für Chatbots. Seitdem sind zahlreiche weitere Sprachmodelle auf den Markt gekommen mit teilweise erheblichen Leistungssprüngen. Die allgegenwärtige Verfügbarkeit leistungsstarker Sprachmodelle beeinflusst seitdem nicht nur zahlreiche Branchen in ihren Kernprozessen, sondern wird aller Voraussicht nach auch den Cybersicherheitssektor nachhaltig beeinflussen.

Wir bei der DZ CompliancePartner setzen uns daher bereits seit geraumer Zeit mit Sprachmodellen auseinander. Auch ohne Kenntnisse der Sprache generieren Angreifer beispielsweise mittels Sprachmodellen qualitativ hochwertige Phishing-Nachrichten. Textbausteine können hierbei mit zusätzlichem Inhalt ergänzt werden, um die Nachrichten zu personalisieren oder einen bestimmten Schreibstil zu verwenden – was zu überzeugenden Nachrichten führt. Bisher etablierte Ansätze zur Identifizierung von betrügerischen Nachrichten, wie z. B. die Prüfung auf Rechtschreibfehler und unkonventionellen Sprachgebrauch, reichen heute nicht mehr aus. Dies sollte im Rahmen der Sensibilisierung und des Awareness-Trainings Ihrer Mitarbeitenden thematisiert werden.

Die Kombination von Sprachmodellen mit weiteren generativen KI-Techniken, wie z. B. Deepfakes (realistisch wirkende verfälschte Medieninhalte) in Webmeetings, ermöglicht es, Angriffe von zuvor unerreichter Qualität durchzuführen. So wurde vor circa einem Jahr bereits ein Mitarbeiter eines internationalen Konzerns in Hongkong im Rahmen einer Videokonferenz mittels KI-generierten Teilnehmern dazu verleitet, rund 24 Mio. Euro an Betrüger zu transferieren.[1] Sämtliche Teilnehmer des Meetings mit Ausnahme des betreffenden Angestellten bestanden aus KI generierten „Personen", die allesamt von den tatsächlich existierenden Personen nicht zu unterscheiden waren.

Weiterhin werden ChatGPT und seine Ableger auch bei der Schadcode-Generierung vermehrt genutzt. Die Einstiegshürden für Personen, die bösartige Aktivitäten durchführen wollen, sind stark gesunken, da die Generierung und Verbreitung von hochpotentem Schadcode keine besonderen Anforderungen mehr an die technische Qualifikation der Angreifer stellt.[2] Die Maßnahmen zur Verhinderung von Missbrauch erstrecken sich dagegen bisher allenfalls auf rudimentäre Filtersysteme, die allzu böswillige Prompts wie „Erstelle mir ein Script für Denial-of-Service-Angriffe" abwehren. Mit ein wenig Experimentierfreude sind derartige Maßnahmen jedoch leicht zu umgehen.

So existieren heute KI-Systeme, die Teilschritte von Cyberangriffen durchführen können: Mithilfe von ChatGPT sowie der Assistants API von OpenAI können Entwickler beispielsweise Anwendungen mit anspruchsvollem Copilot-ähnlichem Verhalten erstellen, die Daten durchsuchen, Lösungen vorschlagen und Aufgaben automatisieren. Angreifer wie auch Pentester verwenden diese Verfahren, um beispielsweise in der Aufklärungsphase eines Cyberangriffs Serverantworten automatisiert zu analysieren. Weiterhin können hiermit auch SQL Injections (Ausnutzen von Schwachstellen im Quelltext von Anwendungen, um beispielsweise Schadcode einzubinden) oder Brute-Force-Angriffe (Erraten von Passwörtern oder anderer Codes durch massenhaftes Ausprobieren) äußerst effizient durchgeführt werden.[3]

Grenzen aktueller KI-Systeme

Für umfangreiche, breite Angriffsszenarien durch technisch kaum oder wenig versierte Täter ist eine KI erforderlich, die alle sechs Schritte einer Cyberattacke autonom durchführen kann:

- Aufklärung,
- Rüstung und Bereitstellung,
- Ausnutzung,
- Installation,
- Erlangung von Befehls- und Kontrollgewalt sowie
- Ausführung (des Schadcodes, des Datendiebstahls etc.).

Aus der Sicht eines Penetrationstesters könnten derartige Werkzeuge selbstverständlich auch effizient dazu genutzt werden, um die Widerstandsfähigkeit von IT-Systemen zu verifizieren und somit den Zeit- und Kostenaufwand für die Durchführung von Penetrationstests zu optimieren. Obschon die Leistungsfähigkeit sowie auch die Abstraktionsfähigkeit der aktuellen KI-Systeme auf einem beeindrucken Niveau angekommen sind und fortlaufend weiter geforscht wird, existieren aktuell zumindest – noch – keine Tools für tatsächliche vollautonome Angriffsszenarien.[4]

Vor dem Hintergrund sich stetig verändernder Bedrohungslagen und damit einhergehender aufsichtsrechtlicher Anforderungen, wie z. B. DORA, ist es bedeutsam, dem Thema Cybersicherheit eine erhöhte Aufmerksamkeit einzuräumen. Ihre Fähigkeit, auf neue Bedrohungsszenarien schnell und wirksam zu reagieren bzw. diese im besten Fall vorherzusehen, wird zukünftig maßgeblich für ein hinreichendes IKT- und Informationssicherheitsniveau sein. Nur **technische und organisatorische Maßnahmen im Zusammenspiel** können dies gewährleisten. Da KI häufig klassische Angriffe verstärkt, fallen die nachfolgend dargestellten Maßnahmen weitgehend auch in den Bereich der klassischen IKT-Risikokontrolle und Informationssicherheit.

Technische Maßnahmen

- **Detektion und Reaktion auf Angriffe:**
  Mittels KI-gestützter Tools können Cyberattacken in sehr kurzer Zeit und mit hohem Präzisionsgrad lanciert werden. Eine resiliente Infrastruktur enthält Mechanismen zur zeitnahen Detektion und Reaktion (Intrusion Prevention/Detection sowie Data Loss Prevention/Detection) auf solche Angriffe, sodass Angriffe rasch erkannt und Risiken hieraus minimiert werden können. Durch die Implementierung von Automatisierungen und intelligenten (KI-gestützten) Sicherheitssystemen kann die Reaktionszeit erheblich verkürzt werden. KI-Systeme sind beispielsweise in der Lage, bei DDoS-Angriffen verdächtige **Datenströme** (beispielsweise mit einem gemeinsamen Verhaltensprofil oder aus einem ähnlichen IP-Bereich) in Echtzeit zu **analysieren,** um diese gar nicht erst zu den eigentlichen Serversystemen durchzuleiten.
- **Einsatz von Sicherheitszonen:**
  Durch die Implementierung einer **mehrschichtigen Sicherheitsarchitektur,** die sowohl physische als auch logische Sicherheitsvorkehrungen umfasst, wird die Infrastruktur besser gegen Angriffe abgesichert. Selbst wenn eine Ebene überwunden wird, bleibt der Schutz durch andere Sicherheitsmaßnahmen bestehen. Angreiferbewegungen innerhalb eines Netzwerks können mittels **Zero-Trust-Modellen** (und einer hieraus resultierenden kontinuierlichen Überprüfung und Authenti-

Angebliche E-Mails von PayPal und der Volksbanken Raiffeisenbanken. Quelle: www.verbraucherzentrale.de

fizierung aller Benutzer und Geräte, unabhängig von ihrem Standort oder ihrer Herkunft) oder **Segmentierung** eingegrenzt werden. Sehr hoch schutzbedürftige Informationen wie z. B. sensible Mitarbeiterdaten oder Geschäftsgeheimnisse können hierdurch selbst bei einer Kompromittierung eines Teilnetzes geschützt bleiben.

- **Implementierung redundanter Strukturen zur Ausfallsicherheit:**
  Der **Einsatz redundanter Strukturen** sorgt dafür, dass KI-basierte Angriffe Ihre IT-Services nicht dauerhaft außer Betrieb setzen können, wodurch die Auswirkungen des Angriffs verringert werden.
- **Einsatz von Multi-Faktor-Authentifizierung (MFA):**
  Auch mittels MFA können Social-Engineering-Angriffe in der Praxis oft wirksam abgewendet werden; insbesondere trifft dies auf **Phishing-Angriffe** zu. Selbst wenn ein Angreifer an die Zugangsdaten eines Mitarbeiters gelangt, verhindert eine MFA, dass er sich ohne den zusätzlichen Authentifizierungsfaktor Zugang verschaffen kann. Sichern Sie daher sehr hoch schutzbedürftige respektive kritische Bestandteile Ihres Informationsverbundes stets mittels MFA ab.
- **Einsatz von Anti-Viren-Software und Firewalls:**
  Der Einsatz von E-Mail-Sicherheitslösungen, die Phishing-Versuche und schadhafte Links erkennen und blockieren, ist ein weiterer wichtiger Baustein zum Schutz. Hierdurch werden E-Mails mit dolosen Inhalten schon häufig herausgefiltert, bevor sie den Posteingang des Mitarbeitenden erreichen. Der Einsatz von Firewall-Systemen und Anti-Viren-Software erscheint bei von der Atruvia AG betriebenen IT-Systemen zwar wirksam umgesetzt, jedoch offenbart sich bei der Verwendung von (ggf. GFG-fremden) Drittanbietern hier noch Optimierungspotenzial. Dem **IKT-Dienstleistermanagement** kommt somit eine besonders wichtige Rolle zu.

Organisatorische Maßnahmen

- **Wirksames Patchmanagement:**
  Ein effektives und effizientes Patchmanagement ist entscheidend, um sich vor KI-gesteuerten Angriffen zu schützen. Es trägt dazu bei, Sicherheitslücken in der Software und in IT-Systemen zeitnah zu schließen. KI-Technologien, insbesondere maschinelles Lernen und automatisierte Angriffsstrategien, können Schwachstellen in IT-Systemen schneller und gezielter ausnutzen als traditionelle Angriffsmethoden. Durch die regelmäßige Aktualisierung von Software und das Schließen von Sicherheitslücken können potenzielle Einstiegspunkte für diese Angriffe minimiert werden. Daher ist das Patchmanagement, auch von nicht durch Atruvia AG gemanagten Bestandteilen Ihres Informationsverbundes, ein zentraler Bestandteil einer umfassenden Cybersicherheitsstrategie.
- **Anpassungsfähigkeit:**
  KI und maschinelles Lernen entwickeln sich rasant weiter, sodass sich auch Angriffstechniken ständig ändern. Eine resiliente IT-Infrastruktur ist darauf ausgelegt, kontinuierlich an neue Bedrohungen und Technologien angepasst zu werden. Dies bedeutet, dass im Rahmen von **Soll-Soll-Abgleichen die Maßnahmenkataloge** an die jeweils aktuellen Bedrohungen anzupassen sind.

- **Schulung und Sensibilisierung der Mitarbeitenden/ User:**
  Regelmäßig sowie anlassbezogen sollten alle Mitarbeitenden in den gängigen **Techniken des Social Engineering geschult** werden, um verdächtige Aktivitäten sicher erkennen zu können. Hierzu zählen Verfahren wie
  - Phishing,
  - Spear-Phishing,
  - Vishing (Voice-Phishing),
  - Pretexting oder Baiting.

  Darüber hinaus sollte mittels **simulierter Angriffe** (z. B. durch Phishing-Tests) regelmäßig überprüft werden, wie Ihre Mitarbeitenden auf solche Attacken reagieren. Scheinangriffe helfen hierbei unserer Erfahrung nach maßgeblich, die Awareness zu schärfen und auch unter Stress richtig zu reagieren.
- **Klare Kommunikationsrichtlinien:**
  Risikobehaftete Geschäftsvorfälle wie beispielsweise das Ausführen von **Überweisungen** oder der **Handel von Wertpapieren** bedürfen stets einer **Verifizierung** des Berechtigten und der **Autorisierung** durch einen Berechtigten (Kunden/Bevollmächtigten). Hierzu ist es ratsam, für derartige Geschäftsvorfälle ausschließlich als **sicher geltende Kommunikationskanäle** zu verwenden. Auch unklare oder verdächtige Anfragen beispielsweise per Telefon oder E-Mail sollten stets über einen sicheren, bekannten Kanal vor Ausführung abgeklärt werden.
- **Identitäts- und Rechtemanagement:**
  Der Zugang zu kritischen IT-Systemen und sowie der Zugriff auf hoch schutzbedürftige Informationen ist zwingend auf ein Minimum zu beschränken. Dies gilt **auch für Drittsysteme** und **Webanwendungen,** die bei Dienstleistern außerhalb des Atruvia-Umfeldes betrieben werden. Mitarbeitende (eigene und die ggf. verwendeter Dienstleister) sollten nur auf die Informationen zugreifen können, die sie für die Erledigung ihrer Aufgaben tatsächlich benötigen.[5] Weiterhin sind die so definierten Sollkonzepte regelmäßigen sowie anlassbezogenen Überprüfungen zu unterziehen.

Fazit

Sowohl Cybersicherheit als auch künstliche Intelligenz unterliegen einem ständigen Wandel. Als Verantwortliche für Informationssicherheit sind wir gut beraten, die kommenden Entwicklungen eng zu beobachten: Fakt ist, dass sich die KI-Modelle und damit auch ihre Anwendbarkeit für Cyberangriffe rasant weiter entwickeln werden. Entsprechend sind auch die Abwehrmöglichkeiten massiv zu erweitern. Die Implementierung sowie der Betrieb der hierzu erforderlichen technischen Maßnahmen obliegt, bei ausschließlicher Nutzung von Atruvia-Services, in der Regel dem Rechenzentrum. Banken unserer Gruppe fällt intern insbesondere die Aufgabe zu, die zuvor dargestellten organisatorischen Maßnahmen zu implementieren und die Mitarbeitenden zu schulen. ▬

Björn Scherer
Beauftragter IKT-Risikokontrolle und Informationssicherheit
E-Mail: bjoern.scherer@dz-cp.de

[1] https://www.heise.de/news/Videokonferenz-voller-KI-Klone-Angestellter-schickt-Betruegern-24-Millionen-Euro-9618064.html, abgerufen am 28.12.2024
[2] Vgl. Van Eeten, Michel, et al. An Attacker's Dream? Exploring the Capabilities of ChatGPT for Developing Malware, Delft University of Technology, 2023.
[3] Vgl. Fang, Richard, et al. LLM Agents can Autonomously Hack Websites: https://openreview.net/pdf?id=6xubl2J2VP , abgerufen am 04.01.2024
[4] Vgl. Wenig, Lilian. LLM Powered Autonomous Agents: https://lilianweng.github.io/posts/2023-06-23-agent/, abgerufen am 04.01.2024
[5] Vgl. AT 4.3.1 Tz. 2 der MaRisk

KI-Kompetenz-Schulung gemäß KI-Verordnung

KI-Systeme werden bereits in vielen Bereichen der Banken eingesetzt. PlainGPT, Microsoft Copilot oder auch agree21 Fraud Detection in der Betrugsprävention sind bereits alltägliche Begleiter. Damit gilt die KI-Verordnung auch für Sie als Bank bzw. Unternehmen. Das heißt (u. a.) auch, dass Sie die KI-Kompetenz aktiv schulen müssen.

Wer KI-Systeme einsetzen möchte, muss sicherstellen, dass das Personal, das mit KI-Systemen potenziell in Berührung kommt, entsprechend geschult ist. Die regulatorische Vorgabe ergibt sich direkt aus der KI-Verordnung (KI-VO).

Gemäß Art. 4 KI-VO i. V. m. Art. 113 lit. a KI-VO müssen Unternehmen ab dem 2. Februar 2025 sicherstellen, dass ein ausreichendes Maß an KI-Kompetenz geschult wird. Die Erforderlichkeit der KI-Kompetenz-Schulung findet auch in anderen bereits angewendeten Verordnungen und Gesetzen ihren Ausdruck. So ist die erforderliche Kompetenz des Personals im Umgang mit KI-Systemen beispielsweise ein zwingender Bestandteil der geeigneten technischen und organisatorischen Maßnahmen im Sinne des Art. 24 Abs. 1 DSGVO oder Art. 29 DSGVO.

Was ist unter einer KI-Kompetenz zu verstehen?

Konkrete Anweisungen zur KI-Kompetenz sind in der KI-Verordnung nicht enthalten. Art. 3 Nr. 56 KI-VO gibt jedoch einen Rahmen vor, was darunter zu verstehen ist. Danach bezeichnet man als KI-Kompetenz „die Fähigkeiten, die Kenntnisse und das Verständnis, die es Anbietern, Betreibern und Betroffenen ermöglichen, KI-Systeme unter Berücksichtigung ihrer jeweiligen Rechte und Pflichten im Rahmen dieser Verordnung“ sachkundig einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden.

Hieraus abgeleitet kann somit festgehalten werden, dass Unternehmen gem. Art. 4 KI-VO bestmöglich sicherstellen müssen, dass das Personal und andere Personen, die mit KI-Systemen arbeiten, über ein ausreichendes Maß an KI-Kompetenz verfügen.

Es ist wichtig, an dieser Stelle den Begriff der KI-Kompetenz von dem Begriff des KI-Beauftragten, auch AI Officer genannt, klar abzugrenzen.

Ähnlich wie ein Datenschutzbeauftragter hat der KI-Beauftragte zu gewährleisten, dass alle relevanten Fachbereiche der KI-Wertschöpfungskette eingebunden sind. Der KI-Beauftragte nimmt folglich eine vermittelnde Position zwischen den Fachbereichen ein und hat die Aufgabe, sicherzustellen, dass die KI-Verordnung eingehalten wird.

Ob ein Unternehmen einen KI-Beauftragten benötigt, kann nicht pauschal beantwortet werden, sondern hängt von bestimmten Faktoren ab.[1] Man kann jedoch festhalten, dass je intensiver und umfangreicher ein Unternehmen KI-Systeme einsetzt oder anbietet, desto eher die Notwendigkeit eines KI-Beauftragten gegeben ist.

Ziele der KI-Kompetenz-Schulung

Das Ziel der KI-Kompetenz-Schulung ist nicht nur die Einhaltung und Erfüllung der gesetzlichen Pflicht gem. Art. 4 KI-VO. Darüber hinaus sollen sowohl Vorstände als auch Mitarbeiter einen regulatorischen Überblick über die KI-Verordnung erhalten und die Schnittstellen zu weiteren Regularien wie beispielsweise DORA, DSGVO etc. kennen, die im Finanzsektor einen hohen Stellenwert haben.

Beispielsweise gelten bei automatisierten Entscheidungsfindungen gem. Art. 22 DSGVO die besonderen Pflichten der Information gem. Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g und Art. 15.Abs. 1 lit. h DSGVO. Diese Transparenzpflicht ist auch bei KI-Systemen zu berücksichtigen.[2]

Mit der KI-Kompetenz-Schulung sollen indessen auch die Chancen von KI-Systemen gewahrt und zugleich die Risiken für Gesundheit, Sicherheit und Grundrechte der Grundrechtscharta minimiert werden, indem eine hinreichende Kompetenz in der Wertschöpfungskette entwickelt wird.[3]

Mit dieser Kompetenz ist es dann möglich, dass KI-Systeme den vom Menschen definierten Werten entsprechen.

> **„Künstliche Intelligenz** beschreibt die Fähigkeit von Maschinen, basierend auf Algorithmen Aufgaben autonom auszuführen und dabei die Problemlösungs- und Entscheidungsfähigkeiten des menschlichen Verstandes nachzuahmen."
>
> Quelle: EU verabschiedet erstes KI-Gesetz weltweit | Bundesregierung/ https://www.bundesregierung.de/breg-de/aktuelles/ai-act-2285944

Chancen der KI-Kompetenz-Schulung

Wer nicht sensibilisiert, darf keine KI-Systeme einsetzen. Dabei bringt die Mitarbeiter-Sensibilisierung viele Vorteile mit sich:

1. Risikominimierung:
Die Sensibilisierung minimiert Risiken auf unterschiedlichen Ebenen. Zunächst reduziert sie die Gefahr, dass Mitarbeiter „heimlich" KI-Systeme einsetzen und dabei personenbezogene Daten und/oder Geschäftsgeheimnisse eingeben, die später durch unbefugte Dritte offengelegt werden könnten.

Weiterhin wird vermieden, dass unrechtmäßige Datenverarbeitungen stattfinden und daraus Schäden und damit einhergehend Bußgelder drohen.

2. Synergieeffekte zu anderen anwendbaren Verordnungen schaffen:
Durch die KI-Kompetenz können Mitarbeiter Synergien zu anderen Verordnungen schaffen, indem beispielsweise Dokumentationsanforderungen miteinander synchronisiert werden.

3. **Einhaltung der Umsetzungsfrist aus der KI-Verordnung:**
   Mit der KI-Kompetenz-Schulung wird die gesetzliche Verpflichtung zur Mitarbeiter-Schulung eingehalten.

4. **Digitales und innovatives Arbeiten im sicheren bzw. gesetzes- und aufsichtskonformen Umfeld:**
   Der Einsatz von KI-Systemen kann Freiraum für effizienteres und qualitatives Arbeiten schaffen. Mitarbeiter müssen sich nicht mehr mit administrativen Themen auseinandersetzen und können ihre Arbeitszeit bewusst für fachliche und persönliche Entwicklungen und Projekte nutzen. Daher sollte die Mitarbeiter-Schulung zur KI-Kompetenz als Chance für zufriedene Mitarbeiter sowie als Chance für eine betriebliche und wirtschaftliche Weiterentwicklung betrachtet werden.

Weitere Informationen zur KI-Verordnung

Wenn Sie mehr darüber erfahren möchten, was Sie als Vorstand oder was Ihre Mitarbeiter beim Einsatz von KI-Systemen im Unternehmen beachten müssen, dann sind Sie herzlich eingeladen, gemeinsam mit uns und Herrn Ben Hansen, LL.M.[4] und Herrn Andreas Sachs[5] an einem unserer regelmäßig stattfindenden Webinare zur KI-Verordnung teil-zunehmen.[6] ▬

Najat Diamante
Beauftragte Datenschutz, zertifizierte Datenschutzauditorin und KI-Expertin,
E-Mail: najat.diamante@dz-cp.de

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

[1] https://haerting.de/wissen/ki-kompetenz-ki-beauftragter-ai-officer/
[2] Martini/Wendehorst/Wendehorst, 1. Aufl. 2024, KI-VO Art. 4 Rn. 8
[3] Martini/Wendehorst/Wendehorst, 1. Aufl. 2024, KI-VO Art. 4 Rn. 1, 2
[4] Ben R. Hansen, Tech Lawyer | Data Scientist | AI Officer
[5] Andreas Sachs, Vizepräsident des Bayerischen Landesamts für Datenschutzaufsicht
[6] Nähere Informationen unter: https://www.dz-cp.de/ueber-uns/newsroom/news/

RM kompakt

Ein Rechtsmonitoring-Tool von Compliance-Beauftragten für Compliance-Beauftragte

In einem früheren Beitrag hatten wir über die **Herausforderungen beim Rechtsmonitoring** (PoC 2/2022, S. 22) berichtet. Während in dem früheren Beitrag regulatorische Vorgaben, die begriffliche Definition und Inhalte eines Rechtsmonitorings näher betrachtet wurden, werden im folgenden Artikel die technischen Umsetzungsmöglichkeiten und Erleichterungen dargestellt.

Jedes Institut muss fortlaufend über die wesentlichen rechtlichen Regelungen und Vorgaben informiert sein und diese aufsichtskonform umsetzen. Das ergibt sich aus § 25a KWG i.V.m. AT 4.4.2 MaRisk und der Verantwortung der Geschäftsleitung für eine ordnungsgemäße Geschäftsorganisation, die auch die Einhaltung der zu beachtenden Regelungen umfasst.

Die sich daran anschließende Frage lautet: Wie kann am effektivsten die Umsetzung eines aufsichtskonformen Rechtsmonitorings innerhalb des Institutes erfolgen?

Grundsätzlich steht es den Instituten frei, wie sie Rechtsmonitoring umsetzen. In unserer täglichen Praxis als MaRisk-Compliance-Beauftragte erleben wir unterschiedliche Umsetzungsarten.

Eigenerstelltes Rechtsmonitoring

So kann das Institut das Rechtsmonitoring selbst erstellen. Dazu müssen die einschlägigen Rechtsquellen, seien es nun Rundschreiben, Urteile, Gesetze oder Vorgaben der Aufsicht, durch Bankmitarbeiter gemonitort, ausgewertet und adressatengerecht für die Umsetzungsverantwortlichen vorbereitet und diesen zur Verfügung gestellt werden.

Vorteil eines solchen eigenerstellten Rechtsmonitorings sind die auf das jeweilige Haus zugeschnittenen individuellen Rechtsmonitoring-Einträge sowie die Kosteneinsparung für den nicht erfolgten Fremdbezug.

Die Eigenerstellung ist aber auch mit Nachteilen verbunden. So müssen Mitarbeiter abgestellt werden, die die Arbeit der Erstellung des Rechtsmonitorings erledigen. Dies relativiert die Kosteneinsparung. Die Mitarbeiter müssen auch entsprechende Kapazitäten haben und fachlich qualifiziert sein, um aus den vielfältigen Quellen für Rechtsmonitoring-Einträge, seien es Gesetze, gerichtliche Entscheidungen, Vorgaben der Aufsicht oder Informationen der Verbände etc., die richtigen Informationen herauszufiltern und institutsgerecht aufzubereiten.

Da ein kontinuierliches Rechtsmonitoring zu erfolgen hat, muss bei der Eigenerstellung auch personeller Ersatz bei Abwesenheit des eigentlich verantwortlichen Mitarbeiters eingeplant werden.

Nicht jede Bank verfügt über eine eigene Rechtsabteilung, die das Rechtsmonitoring erstellen kann, sodass auch entschieden werden muss, wo das Rechtsmonitoring organisatorisch angesiedelt wird, möglicherweise beim Vorstandsstab oder der Compliance-Funktion.

Auch stellt sich die Frage, wie bei einem eigenerstellten Rechtsmonitoring sichergestellt ist, dass alle wesentlichen Quellen berücksichtigt werden. Im Hinblick auf den Geno-Sektor fragt sich beispielsweise, ob auch Rundschreiben von anderen Verbänden berücksichtigt werden oder nur die des Verbandes, dem die Bank angehört.

Schlussendlich sollte das Rechtsmonitoring revisionssicher bearbeitet und dokumentiert werden. Es muss also über die Bearbeitung in einer Datenbank etc. entschieden werden.

Rechtsmonitoring im Fremdbezug

Neben dem eigenerstellten Rechtsmonitoring gibt es auch die Möglichkeit, ein Rechtsmonitoring einzukaufen (Make or buy). Dadurch vermeidet die Bank die Fragestellungen und potenziellen Risiken, die mit der Eigenerstellung eines Rechtsmonitorings einhergehen.

Vorteil eines Rechtsmonitorings im Fremdbezug ist, dass bei der Erstellung auf ein Expertenteam von unterschiedlichen Autoren mit unterschiedlicher Profession zurückgegriffen werden kann: Bankkaufleute, Compliance-Beauftragte, Juristen etc. Der Mix aus unterschiedlichen Professionen hat den Vorteil einer Vielfalt von Expertisen und des Erfahrungsaustausches bzw. der fachlichen Diskussion bei der Erstellung des Rechtsmonitorings.

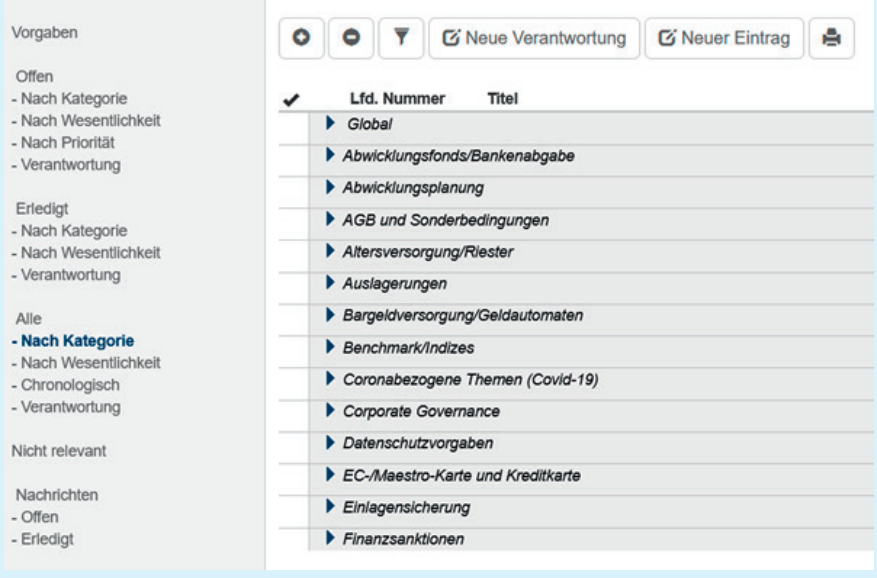
Es gibt ganz unterschiedliche Anbieter für Rechtsmonitoring im Fremdbezug: aus dem öffentlichen Bankensektor, von Beratungsgesellschaften und auch aus dem Geno-Sektor.

Im Folgenden stellen wir Ihnen unser Produkt RM kompakt vor: Das Produkt wurde vor dem Hintergrund und dem Wissen unserer Erfahrungen als MaRisk-Compliance-Beauftragte bei einer Vielzahl von Banken entwickelt. Ansatzpunkt ist denn auch: Was für ein Rechtsmonitoring-Tool wünsche ich mir als MaRisk-Compliance-Beauftragter?

RM kompakt

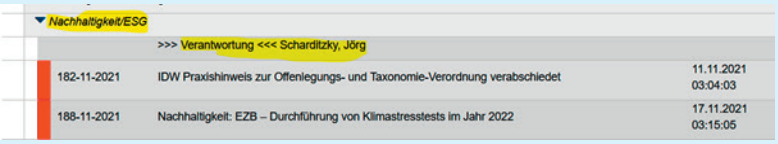
RM kompakt ist eine browserbasierte Anwendung und erfordert von der technischen Seite nur einen Internetzugang und einen Browser.

Kategorien der BVR-Musterbestandsaufnahme
RM kompakt orientiert sich streng an der BVR-Musterbestandsaufnahme, d. h., die Kategorien der BVR-Musterbestandsaufnahme – beginnend mit Steuerrecht bis hin zum Zwangsvollstreckungsrecht – werden ebenfalls als Kategorien in RM kompakt geführt, wobei sie in der nachfolgend gewählten Ansicht „Kategorie“ alphabetisch geordnet sind:

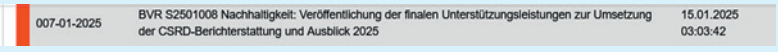


Der Screenshot bildet nur einen Teil der Kategorien ab. Aus Archivgründen wird die Kategorie „Coronabezogene Themen (Covid-19)“ weiterhin dargestellt, in der aktuellen BVR-Musterbestandsaufnahme wird sie bereits nicht mehr aufgeführt.

Unter die einzelnen Kategorien sind dann die entsprechenden Rechtsmonitoring-Einträge aufsteigend gruppiert: Nachfolgend am Beispiel Nachhaltigkeit/ESG:



Bis hin zu:



Der erste Eintrag in der Kategorie Nachhaltigkeit/ESG datiert aus dem Jahr 2021 und der letzte Eintrag vom 15.01.2025.

Verantwortungen: Person oder Funktion

Ziel jeden Rechtsmonitorings ist es, bestimmte Personen oder Funktionen mit Informationen zu versorgen, d. h., einzelne Rechtsmonitoring-Einträge müssen zu bestimmten Personen oder Funktionen gelangen. Dies geschieht in RM kompakt über die Einrichtung von Verantwortungen.

Jede Kategorie muss einer Person oder Funktion zugeordnet werden. Den so benannten Verantwortlichen werden dann die jeweiligen Rechtsmonitoring-Einträge unmittelbar zugeordnet, und der Verantwortliche erhält eine Information über einen neuen, von ihm zu bearbeitenden Rechtsmonitoring-Eintrag. Unser Rechtsmonitoring-Tool ist so gestaltet, dass jede Bank selbst die Verantwortungen für ihre Mitarbeiter, aber auch Dritte vergeben kann. Dritte können z. B. ausgelagerte Funktionen sein.

Es kann sowohl einzelnen oder mehreren Personen als auch einzelnen oder mehreren Funktionen die Verantwortung für eine Kategorie zugeordnet werden. Wir haben die Unterscheidung zwischen Personen und Funktionen bei der Verantwortung getroffen, um für die nutzenden Institute möglichst flexibel zu sein. Im obigen Beispiel ist der Autor dieses Artikels als verantwortliche Person für die Kategorie Nachhaltigkeit/ESG hinterlegt. Die entsprechende Verantwortung wird im Tool angezeigt.

Der Vollständigkeit halber sei erwähnt, dass Rechtsmonitoring-Einträge einschließlich Handlungsempfehlungen vom eigentlich Verantwortlichen an Dritte weiterdelegiert werden können.

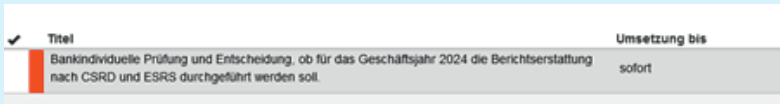
Möglicherweise fragen Sie sich, was es mit der Kategorie „Global“ auf sich hat, die in der ersten Abbildung bei den Kategorien ganz oben steht: Durch diese Kategorie und die damit verbundene Verantwortung ist sichergestellt, dass neue Kategorien in der BVR-Musterbestandsaufnahme nicht ins Leere laufen und keine weißen Flecken entstehen. Ein Beispiel hierfür ist die Kategorie Nachhaltigkeit/ESG, die mit der BVR-Musterbestandsaufnahme April 2020 erstmals als sonstige Regelung eingeführt wurde. Da es diese Kategorie bis dahin nicht gab, konnte auch noch keine Verantwortlichkeit in RM kompakt definiert sein. Eine Bearbeitung wäre mangels Verantwortlichkeit nicht erfolgt.

Diese bis dahin nicht vorhandene Kategorie wurde von RM kompakt automatisch der Kategorie „Global“ zugeordnet und somit sichergestellt, dass sie nicht übersehen wurde. Die Person oder Funktion, die für die Kategorie „Global“ verantwortlich war, konnte dann entscheiden, welche Person oder Funktion für die neue Kategorie Nachhaltigkeit zukünftig verantwortlich ist.

Rechtsmonitoring-Eintrag: Beschreibung und Handlungsempfehlung

Ein Rechtsmonitoring-Eintrag setzt sich aus einer Beschreibung und einer Handlungsempfehlung zusammen. In der Beschreibung fassen wir den Sachverhalt oder das Rundschreiben, das Thema des Rechtsmonitoring-Eintrages ist, kurz zusammen.

Daran schließt sich eine Handlungsempfehlung an, in der konkrete Handlungsempfehlungen für den Verantwortlichen vorgegeben sind.



Relevanz und Wesentlichkeit
Bestandteil jeden Rechtsmonitoring-Eintrages sind Ausführungen zur Relevanz und die Bestimmung der Wesentlichkeit. Die Relevanz gibt an, ob der Eintrag für das Institut einschlägig/relevant ist. Für Institute, die beispielsweise kein Verbrauchergeschäft betreiben, sind Rechtsmonitoring-Einträge, die auf Verbraucherthemen abstellen, nicht relevant. Durch diese Einstellung werden dem Institut nur die Rechtsmonitoring-Einträge eingespielt, die für das Institut bedeutsam sind. Das heißt, unser Rechtsmonitoring ist auch institutsindividuell.
Die Bestimmung der Wesentlichkeit richtet sich nach den bekannten Kriterien des Risikos von Sanktionen, eines Vermögensschadens oder eines Reputationsrisikos. Ergänzend wird auch die Einschätzung des BVR zur Wesentlichkeit mit aufgeführt.

Verlinkung von Quellen
Durch die Verlinkung der Quelle im Rechtsmonitoring-Eintrag gelangt der Verantwortliche unmittelbar auf das dem Rechtsmonitoring-Eintrag zugrundeliegende Gesetz, Urteil, Rundschreiben oder die Information der Aufsicht, um sich ggf. vertieft zu informieren.

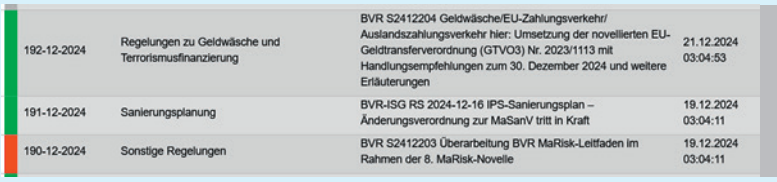
Die Bank hat auch die Möglichkeit, eigene Quellen oder Dateien mit dem Rechtsmonitoring-Eintrag zu verlinken, z. B. eigene Vorstandsbeschlüsse, Arbeitsanweisungen, erstrittene Urteile etc.

Gab es zu dem aktuellen Rechtsmonitoring-Eintrag in der Vergangenheit schon einmal einen oder mehrere Einträge in unserem Tool, so sind auch diese verlinkt, um sich einen vollständigen Überblick zur Thematik zu verschaffen.

Eigene Einträge
Unser Tool ist offen konzipiert und nicht auf die Kategorien der BVR-Musterbestandsaufnahme beschränkt. Das heißt, jede Bank kann eigene Kategorien oder Themen in ihr Rechtsmonitoring-Tool einbringen und es so bankindividuell gestalten.

Ist z. B. Leasing Teil des Geschäftsmodells der Bank, so findet sich dazu nichts in der BVR-Musterbestandsaufnahme. Für die Bank besteht aber die Möglichkeit, durch eigene Einträge in RM kompakt eine Urteilssammlung aufzubauen oder Rundscheiben des BDL zu archivieren.

Ampelsystem
Durch das in RM kompakt enthaltene Ampelsystem kann man sich schnell einen Überblick verschaffen, welche Rechtsmonitoring-Einträge bzw. Handlungsempfehlungen abgeschlossen sind und welche nicht.



192-12-2024	Regelungen zu Geldwäsche und Terrorismusfinanzierung	BVR S2412204 Geldwäsche/EU-Zahlungsverkehr/ Auslandszahlungsverkehr hier: Umsetzung der novellierten EU-Geldtransferverordnung (GTVO3) Nr. 2023/1113 mit Handlungsempfehlungen zum 30. Dezember 2024 und weitere Erläuterungen	21.12.2024 03:04:53
191-12-2024	Sanierungsplanung	BVR-ISG RS 2024-12-16 IPS-Sanierungsplan – Änderungsverordnung zur MaSanV tritt in Kraft	19.12.2024 03:04:11
190-12-2024	Sonstige Regelungen	BVR S2412203 Überarbeitung BVR MaRisk-Leitfaden im Rahmen der 8. MaRisk-Novelle	19.12.2024 03:04:11

Wurde die Handlungsempfehlung durch den Verantwortlichen final bearbeitet, so muss er sie abschließen. Dies erfolgt durch eine schriftliche Notiz, wie die Handlungsempfehlung institutsintern umgesetzt wurde. Danach wechselt der Rechtsmonitoring-Eintrag die Farbe von Rot auf Grün.

Ansichts-/Filtermöglichkeiten
Für den Nutzer bzw. Verantwortlichen für RM kompakt bestehen verschiedene Ansichts-/Filtermöglichkeiten. So kann eine Filterung nach „offenen“ oder „erledigten“ Einträgen jeweils nach den Kriterien Kategorie, Wesentlichkeit und Verantwortung erfolgen. Auch besteht die Möglichkeit, sich alle Rechtsmonitoring-Einträge chronologisch darstellen zu lassen; hierdurch erhält man eine gute Übersicht zum Sachstand der Abarbeitung insgesamt. Details zu den Filtermöglichkeiten können Sie der linken Bildhälfte der ersten Abbildung entnehmen.

Rechtsmonitoring & KI

Künstliche Intelligenz wird wesentlich dazu beitragen, Rechtsmonitoring-Tools zu unterstützen und die Arbeit der Rechtsmonitoring-Ersteller zu erleichtern. Rechtsmonitoring ist ein typisches Produkt, bei dem KI eingesetzt werden kann.

Als Vorstufe der KI gibt es aktuell schon Suchagenten und elektronische Alerts, mit deren Hilfe der Nutzer über Neuigkeiten zu einem bestimmten Thema informiert wird. Dann ist es auch konsequent, den nächsten Schritt zu gehen und die so gewonnenen Informationen durch KI auswerten und einen Rechtsmonitoring-Eintrag daraus erstellen zu lassen.

Vorgaben/Auswertungen/Eskalationen
Über die ebenfalls enthaltene Funktion zu den Vorgaben bestehen diverse Einstell- und Auswertmöglichkeiten. So gibt es u.a. die Möglichkeit, dass bestimmte Personen oder Funktionen informiert werden, wenn Rechtsmonitoring-Einträge den Status Grün erhalten bzw. wenn vorgegebene Bearbeitungsfristen nicht eingehalten werden. Empfänger solcher Eskalationsmails könnten beispielsweise die Interne Revision oder die Compliance-Funktion sein, um auf ein zeitnahes Abarbeiten hinzuwirken.

Print- und Suchfunktionen
In unserem Tool ist natürlich auch eine Print- und Suchfunktion integriert.

Fazit

Was auf den ersten Blick sehr komplex ausschaut, stellt sich bei näherer Betrachtung und im täglichen Doing als effektives Tool dar, um Rechtsmonitoring aufsichtskonform abzubilden und so die Vorgaben des § 25a KWG i.V.m. AT 4.4.2 MaRisk zu erfüllen.

Dieser Artikel kann Ihnen naturgemäß nur einen groben Überblick über unser Rechtsmonitoring-Tool geben und nicht alle Facetten beleuchten. Gerne stellen wir Ihnen das Tool live vor. ▬

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

Retail Investment Package stärkt Interessen von Privatanlegern

Das geplante Retail Investment Package (RIP) stellt eine wichtige aufsichtsrechtliche Neuerung dar, die wesentliche Auswirkungen auf die Finanzmärkte in der Europäischen Union ab dem Jahr 2026 haben wird. Insbesondere für Volksbanken Raiffeisenbanken in Deutschland, die eine wichtige Rolle im Finanzsystem spielen, sind die Änderungen durch das RIP von großer Bedeutung.

Das Retail Investment Package beruht auf einer Initiative der Europäischen Union (8. Punkt: „Building retail investors' trust in capital markets") im Rahmen des am 23. September 2020 veröffentlichten, neuen Aktionsplans für eine Kapitalmarktunion („Capital markets union 2020 action plan"). Die Intention ist, den Schutz von Kleinanlegern zu erhöhen und die Transparenz auf den Finanzmärkten zu verbessern.

Hintergrund sind u. a. folgende Probleme, die die Europäische Union identifiziert hat:

- Kleinanleger haben Schwierigkeiten, an relevante, vergleichbare und leicht verständliche Informationen heranzukommen, um fundierte Investitionsentscheidungen zu treffen.
- Kleinanleger laufen zunehmend Gefahr, durch Marketing in den sozialen Medien und über neue Marketingkanäle unangemessen beeinflusst zu werden.
- Finanzberatung erfolgt ggf. nicht immer im besten Interesse der Kleinanleger.
- Einige Anlageprodukte bieten Kleinanlegern nicht immer ein gutes Preis-Leistungs-Verhältnis.

Darüber hinaus sollen diese Probleme mitunter die Ursache für folgende Erkenntnisse sein:

- Nur 17 % des Vermögens der privaten Haushalte in der EU waren 2021 in Finanztiteln (wie Aktien oder Anleihen) angelegt, deutlich weniger als der entsprechene Vermögensanteil der Haushalte in den USA.
- Kleinanleger zahlen 40 % höhere Gebühren als institutionelle Anleger (z. B. bei Pensionsfonds).
- 45 % der Europäer sind nicht davon überzeugt, dass die Anlageberatung, die sie von Finanzvermittlern erhalten, in ihrem besten Interesse ist.

Die Konsequenz ist, dass weitere Regelungen geschaffen werden sollen, die eine Reihe von Maßnahmen festlegen. Dadurch werden die Offenlegungspflichten und die Beratungsstandards für Finanzdienstleister verschärft. Auch wenn das RIP noch finale politische Entscheidungsprozesse durchlaufen muss, ist es kurzsichtig, sich nicht vorzubereiten und dann im Institut einen Mehraufwand oder sogar Prüfungsfeststellungen zu riskieren.

Nach derzeitigem Kenntnisstand ist mit einer Anwendungspflicht für deutsche Wertpapierinstitute im Jahr 2026 zu rechnen. Das RIP hat die Rechtsnatur eines EU-Gesetzgebungspakets, das aus mehreren Maßnahmen besteht. Es umfasst sowohl wesentliche Neuerungen an bestehenden Richtlinien als auch eine neue Änderungsverordnung. Konkret beinhaltet das RIP die sog. Omnibus-Richtlinie und die PRIIPs-Änderungsverordnung.

Europarechtlich sind Richtlinien Rechtsakte der Europäischen Union und als solche Teil des sekundären Unionsrechts. Der wesentliche Unterschied zu Verordnungen besteht darin, dass Richtlinien gemäß Art. 288 Abs. 3 des AEUV nicht unmittelbar gelten. Richtlinien müssen daher von den jeweiligen Mitgliedstaaten in nationales Recht umgewandelt werden.

Merken kann man sich: Verordnungen gelten unmittelbar, Richtlinien erst nach Tätigwerden des nationalen (z. B. deutschen) Gesetzgebers. Wenn, wie in diesem Fall,

ein Maßnahmenpaket bestehend aus Richtlinien und Verordnungen erlassen wird, ist der gesetzgeberische Wille erkennbar, tiefergehende Änderungen im Regelungsbereich – in diesem Fall dem Finanzmarkt – herbeizuführen.

Wesentliche Änderungen

Die Omnibus-Richtlinie soll bestehende EU-Richtlinien wie MiFID II, IDD, Solvency II, UCITS und AIFMD ändern.

Da eine Darstellung aller angestrebter Änderungen zu umfangreich wäre, wird an dieser Stelle nur auf einen Teil der wesentlichen Änderungen zu MiFID II eingegangen:

Bezogen auf Zuwendungen sollen sog. „general overarching principles", also allgemein-übergreifende Prinzipien, eingeführt werden, die durchgängig zu beachten sind. Weiterhin soll ein standardisierter Zuwendungstest eingeführt werden. Im Zuge des Tests soll jedoch berücksichtigt werden, dass nicht alle Kriterien gleichermaßen Anwendung finden können. Dennoch werden Wertpapierfirmen dazu angehalten, abweichende Beurteilungen zu begründen.

Ebenso neu eingeführt wird der „value for money"-Ansatz. Investitionen sollen demnach nicht nur auf Kosten, sondern auch auf den erzielten Nutzen ausgerichtet sein. Im RIP wird daher Wert darauf gelegt, dass Investitionen für den Verbraucher den Ertrag liefern, der den finanziellen Aufwand auch tatsächlich rechtfertigt. Eine transparente Mittelverwendung und eine bessere Entscheidungsfindung sollen hierdurch ermöglicht werden. Durch die Fokussierung auf den Ertrag wird zudem sichergestellt, dass die eingesetzten Mittel zur Verbesserung der konkreten Anlageentscheidung des Verbrauchers beitragen. Letztlich zielt der „value for money"-Gedanke darauf ab, nachhaltige und positive Veränderungen zu bewirken, die über kurzfristige finanzielle Einsparungen hinausgehen.

Ferner sollen Ergänzungen rund um das Marketing und dessen digitale Verbreitungskanäle Einzug finden. So sollen Begriffe wie Marketingkommunikation (marketing communication), Marketingverfahren (marketing practice) und Online-Benutzeroberfläche (online interface) bereits in MiFID II legaldefiniert werden und eine neue jährliche Berichterstattung an das Leitungsorgan über das Marketing eingeführt werden. Im Rahmen dessen soll an Kunden gerichtetes Marketing die Kriterien Eindeutigkeit, Klarheit und Deutlichkeit noch stärker berücksichtigen. Darüber hinaus sollen auch die Aufzeichnungspflichten in Bezug auf Dritte, die an der Verbreitung der Marketinginformationen beteiligt sind, erweitert werden.

Daneben werden Banken gegenüber ihren Kunden höhere Informationspflichten treffen. Es sollen z. B. standardisierte Formate für Kosteninformationen eingeführt werden, und Risikowarnhinweise für risikoreiche Produkte sollen nach dem Willen des Gesetzgebers angemessen sein, sprich die Risiken, die der jeweilige Kunde eingeht, auch tatsächlich abbilden.

Abb. 1. **Entwicklung des RIP**

24. September 2020	Veröffentlichung des „Capital markets union 2020 action plan" durch die EU-Kommission
11. Mai bis 3. August 2021	Öffentliche Konsultationen zur „Retail investment strategy"
27. Juli 2021	Aufruf zur Stellungnahme der EU-Kommission an die EIOPA
3. August 2021	Aufruf zur Stellungnahme der EU-Kommission an den Gemeinsamen Ausschuss der ESA
22. April 2022	Veröffentlichung des „Technical advice on retail investor protection" durch die ESMA
29. April 2022	Veröffentlichung des „Technical advice on retail investor protection" durch die EIOPA
3. bis 31. Mai 2022	Sondierung des RIP
24. Mai 2023	Annahme und Veröffentlichung des RIP durch die EU-Kommission
25. Mai bis 28. August 2023	Feedback-Zeitraum für des RIP
12. Juni 2024	EU-Rat vereinbarte sein Verhandlungsmandat für die beiden Vorschläge des RIP
Q4 2024	Zu erwartende Verhandlungen zwischen EU-Kommission, -Parlament und -Rat
2026	Mögliches Inkrafttreten

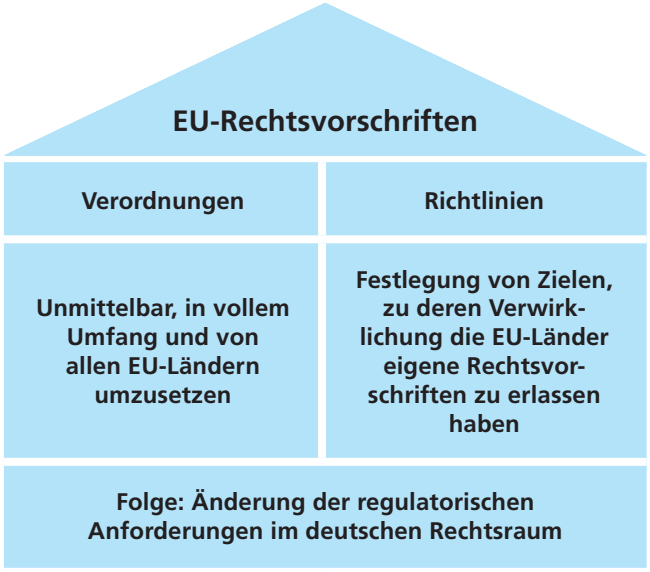
Quelle: eigene Darstellung

Dies geht einher mit verschärften Eignungsanforderungen an die Kunden für die jeweiligen beabsichtigten Finanzinstrumente. Diese finden sich dann in einer modifizierten Angemessenheits- und Geeignetheitsprüfung wieder. Es kommt nach dem Willen der EU-Gesetzgebung zu einer Ausweitung der einzuholenden und zu betrachtenden Informationen gegenüber Kunden. Hierbei ist eine Erweiterung der Hintergrundanalyse zur Verlusttragfähigkeit der Kunden vorgesehen. Außerdem soll bei der Geeignetheitserklärung der Wunsch des Kunden nach Diversifizierung im Portfolio miteinbezogen werden. Bei negativer Angemessenheitsprüfung ist zudem eine implementierte Kundenaufforderung zur Fortführung der Transaktion vorgesehen. Zur Gewährleistung dieser neuen Anforderungen sollen die Sachkundeanforderungen der Anlageberater erhöht werden. Die Opt-in-Kriterien für eine Einstufung als professioneller Kunde sollen verringert werden. Vorgesehen ist, das derzeitige Vermögenslimit von 500.000 Euro auf 250.000 Euro zu reduzieren. Bei der Kundenklassifizierung hingegen soll zukünftig ein weiteres Kriterium (Kenntnisse/Ausbildung) berücksichtigt werden. Zudem besteht im Rahmen der Omnibus-Richtlinie der generelle Ansatz des EU-Gesetzgebers, einen Teil der neuen regulatorischen Anforderungen fünf Jahre nach Inkrafttreten erneut zu evaluieren.

Durch die Änderung der PRIIPs-Verordnung soll der Anlegerschutz wiederum dadurch verbessert werden, dass die Transparenz für „Packaged Retail and Insurance-based Investment Products“ weiter erhöht wird und die Datenbereitstellung digitaler und attraktiver für den Kleinanleger wird. Im Näheren bedeutet dies, dass die Größenbeschränkung der Basisinformationsblätter (BIB) unangetastet bleibt, aber zwei weitere Abschnitte hinzukommen sollen: „Product at a glance“ und „How sustainable is this product?“. Letzterer soll zur Konsolidierung von Nachhaltigkeitsinformationen beitragen, gleichzeitig sollen die Nachhaltigkeitsinformationen zu PRIIPs aus anderen Nachhaltigkeitsveröffentlichungen wegfallen. Mithin sollen die BIB vorrangig, sofern vom Kunden nicht explizit Gegenteiliges artikuliert wurde, digital zur Verfügung gestellt werden.

Inhaltlich haben die oben genannten Änderungen zusammengefasst für Institute vier Kernfolgen:

1. Höhere Informationspflichten
2. Verschärfte Eignungsanforderungen
3. Erweiterte Transparenzvorschriften
4. Höherer Umsetzungsaufwand



Quelle: eigene Darstellung

Abb. 2. **Unterscheidung von EU-Rechtsvorschriften**

Auswirkungen der Änderungen in der Praxis

Die Auswirkungen werden wiederum vielfältig sein und können noch nicht in Gänze erfasst werden. Jedoch ist es möglich, aus den Änderungsentwürfen entsprechende Auswirkungen abzuleiten. Anbei eine erste Übersicht möglicher Auswirkungen:

Zuwendungen

Die neuen allgemein-übergreifenden Prinzipien müssten in das Anweisungswesen der Bank überführt, neue Prozesse zur Beachtung und Anwendung des Zuwendungstests müssten in das Produktfreigabeverfahren implementiert und bestehende Zuwendungen müssten erneut auf den Prüfstand gestellt werden.

„value for money“-Ansatz

Das Produktfreigabeverfahren dürfte um ein entsprechendes „value for money assessment“ ergänzt werden müssen. Dies träfe Produktkonzepteure und -vertreiber, die weitere Kosten und Gebühren, welche sich erst aus dem Vertrieb des Produktes ergeben, erfassen werden müssen, gleichermaßen. Im Zuge dessen müssten wiederum Kosteninformationen bzw. -ausweise inhaltlich angepasst werden.

Marketingmitteilungen

Für Mehraufwand wird voraussichtlich die Implementierung und Umsetzung der neuen Berichtspflicht an das Leitungsorgan sorgen. Unklar bleibt hingegen, wie umfangreich Marketingverfahren dokumentiert werden müssten, ebenso dürfte die erweiterte Aufzeichnungspflicht eine gewisse Herausforderung darstellen.

Qualifikationsanforderungen

In Anbetracht des bereits sehr ausgeprägten Anforderungsprofils im deutschen Rechtsraum und der bereits imple-

mentierten Prozesse der Institute dürfte sich prozessual nur bedingt etwas ändern. Gegebenenfalls kommen neue Qualifikationen/Zertifizierungen hinzu, wohingegen andere abgeändert werden oder wegfallen.

Kosteninformationen

Die Umstellung auf einen standardisierten Kostenausweis würde zu Beginn einen großen Umsetzungsaufwand, vor allem in der informationstechnischen Implementierung, mit sich bringen. Es ist davon auszugehen, dass zumindest bei den entsprechenden Dienstleistern für die Institute eine Effizienzsteigerung und evtl. Kostensenkung einträte. Gleichzeitig dürfte mehr Rechtssicherheit einkehren.

Angemessenheits- und Geeignetheitsprüfung

Die Änderungen der Angemessenheits- und Geeignetheitsprüfung dürften sehr umfangreich ausfallen, angefangen mit der Integration und Überarbeitung der entsprechenden Unterlagen/Fragebögen bis hin zu den Prozessstrecken. Es ist auch anzunehmen, dass zukünftig mehr Zeit für eine entsprechende Beratung eingeplant werden muss, was sich auf die Mitarbeiterkapazitäten auswirken kann. Folglich dürften auch Anlageberater entsprechend nachgeschult werden müssen.

Basisinformationsblätter/Nachhaltigkeitsinformationen

Wenngleich die Basisinformationsblätter zumeist nicht von den Wertpapierfirmen, die diese verwenden, erstellt werden, so wird eine Prüfung aller neuen BIB mit Inkrafttreten der geänderten PRIIPs-Verordnung erfolgen müssen. Die verwendende Wertpapierfirma muss schlussendlich in eigener Verantwortung sicherstellen, dass diese gesetzeskonform sind.

Dies wird einen erhöhten Kontrollaufwand für die Compliance-Funktion, zumindest bis von einer reibungslosen Umstellung ausgegangen werden kann, bedeuten. Des Weiteren werden Nachhaltigkeitsveröffentlichungen zumindest einmalig auf Basis der oben aufgeführten Änderungen vorgenommen werden müssen.

Fazit

Das „Retail Investment Package“ beabsichtigt, den Schutz der Kleinanleger zu verbessern und die Transparenz auf dem Finanzmarkt zu erhöhen. Welcher Umsetzungsaufwand für die Volksbanken Raiffeisenbanken damit einhergeht, ist noch nicht in Gänze abzusehen.

Nichtsdestotrotz ist davon auszugehen, dass ein gewisser Umsetzungsaufwand bestehen wird. Entsprechend sollten Banken die weitere Entwicklung des Retail Investment Package genau im Blick behalten, um mit der beabsichtigten Finalisierung rechtzeitig auf die Neuerungen reagieren zu können. Verzögerungen könnten schließlich zu Feststellungen in der externen Prüfung führen.

Über Konkretisierungen im Zeitablauf und notwendige konkrete Umsetzungsschritte werden wir rechtzeitig informieren. ▬

Felix Fröhlich
Beauftragter WpHG-Compliance,
E-Mail: felix.froehlich@dz-cp.de

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

Redlich, eindeutig und nicht irreführend – BT 3 MaComp

Der besondere Teil (BT) 3 der MaComp ist ein zentraler Bestandteil der regulatorischen Anforderungen, der gewährleistet, dass Informationen, die von Wertpapierdienstleistungsunternehmen an ihre Kunden weitergegeben werden, redlich, eindeutig und nicht irreführend sind. Diese Anforderungen beruhen auf § 63 Abs. 6 des Wertpapierhandelsgesetzes (WpHG) und sind darauf ausgelegt, das Vertrauen der Anleger zu stärken und die Transparenz auf den Finanzmärkten zu erhöhen.

Anwendungsbereich

Der BT 3 der MaComp, ausführlich Mindestanforderungen an die Compliance-Funktion und die weiteren Verhaltens-, Organisations- und Transparenzpflichten für Wertpapierdienstleistungsunternehmen, gilt unterschiedslos für alle Informationen betreffend Finanzinstrumente oder Wertpapier(neben)dienstleistungen, die Wertpapierdienstleistungsunternehmen an Privatkunden und professionelle Kunden richten. Die Vorschriften gelten sowohl für bestehende als auch für potenzielle Kunden, die noch keine Geschäftsbeziehung mit dem Unternehmen haben.

Gemäß § 63 Abs. 6 S. 2 WpHG sind Marketingmitteilungen eindeutig als solche erkennbar zu machen. Dies kann sich aus der Art und der Form der Darstellung der werblichen Information oder aus dem Inhalt ergeben. Eine Marketingmitteilung ist eine Information, die die Adressaten zum Erwerb eines Finanzinstruments oder zur Beauftragung einer Wertpapierdienstleistung bewegen will und ferner eine absatzfördernde Zielrichtung aufweist.

Als klassische Beispiele gelten Broschüren und Kundenflyer, die in den Geschäftsräumen zu Werbezwecken ausgelegt werden. Um die Anforderungen zu verdeutlichen, führen wir beispielhaft zwei Marketingmitteilungen auf, die ebenfalls unter den Begriff mit definiert werden.

- Marketingmitteilungen, die dem Anschein nach objektive Beiträge in Kundenzeitschriften eines Wertpapierdienstleistungsunternehmens darstellen, aber primär eine absatzfördernde Zielrichtung verfolgen, sind als werbliche Informationen anzusehen.

Ausnahmen bei den Anwendungsbereichen

Von dieser Regelung ausgenommen sind Informationen, die sich ausschließlich an geeignete Gegenparteien richten. Unter den Begriff fallen darüber hinaus auch keine neutralen Produktinformationen, die im Rahmen der anlage- und anlegergerechten Beratung zugänglich gemacht werden, da diese nicht als Werbung gelten. Produktinformationen der DZ BANK, von Union Investment und attrax fallen demnach nicht unter die Regelung.

- Kundenanschreiben, die den Erwerb bestimmter Wertpapiere nahelegen, insbesondere wenn es sich um persönlich adressierte Schreiben handelt, sind ebenfalls als werbliche Informationen anzusehen.

Gemäß § 63 Abs. 6 S. 2 WpHG müssen Marketingmitteilungen ausnahmslos (d. h. ohne eigenen Ermessensspielraum) eindeutig als solche erkennbar sein.

Zugänglichmachung

Laut BT 3.2 Tz 1 MaComp fallen gem. § 63 Abs. 6 S. 1 WpHG und Art. 44 DV sämtliche Informationen, die Wertpapierdienstleistungsunternehmen Privatkunden und professionellen Kunden zugänglich machen, in den Anwendungsbereich der Vorschriften. Nach BT 3.2 Tz. 2 MaComp sind auch jene Informationen davon betroffen, die in einer Weise verbreitet werden, dass Privatkunden und professionelle Kunden wahrscheinlich davon Kenntnis erlangen können.

Wichtig ist hierbei zu verstehen, dass es nicht darauf ankommt, ob die Information vom Wertpapierdienstleistungsunternehmen stammt. Es wird rein auf die Zugänglichmachung abgestellt, nicht auf die Herkunft der jeweiligen Information. Daher ist man auch im Anwendungsbereich der Vorschrift, wenn Informationen von Dritten (außerhalb der Verbundpartner) verwendet werden.

Darstellung gegenüber den Kunden

Weiteres zentrales Element des BT 3 MaComp sind die Darstellungsvorschriften. Grundsätzlich ergibt sich die Erkennbarkeit der Werbung aus der Art und Darstellung der Marketingmitteilung. Sofern dies nicht der Fall ist, ergibt sich aus dem Gesetz die Pflicht, die Marketingmitteilung explizit als solche zu kennzeichnen. Dies soll sicherstellen, dass die verwendeten Informationen klar und verständlich sind. Informationen sind daher so zu formulieren, dass sie für den durchschnittlichen Kunden verständlich sind. Dies umfasst klare und präzise Formulierungen sowie eine einheitliche Darstellung im Hinblick auf vorhandene Risiken, Bedingungen sowie Chancen. Gemäß § 63 Abs. 6 S. 1 WpHG müssen Marketingmitteilungen redlich, eindeutig und nicht irreführend sein.

Werden beispielsweise in einer Marketingmitteilung Garantieaussagen getätigt, ist zu benennen, von wem die Garantie stammt und welche Bedingungen oder Einschränkungen damit verbunden sind.

Sofern sich bei bereits veröffentlichten Marketingmitteilungen wesentliche Änderungen ergeben haben, müssen die Informationen überarbeitet und neu veröffentlicht oder ggf. aus dem Rechtsverkehr zurückgezogen werden. Ein Beispiel ist die Finanzkrise 2008, die das Risiko von Zertifikatemittenten verdeutlichte.

Wesentliche Vorteile einer Wertpapierdienstleistung oder eines Finanzinstruments dürfen nur dann ins Feld geführt werden, wenn auch auf die jeweiligen Risiken aufmerksam gemacht wird. Die Darstellung muss ausgewogen sein, wobei die Anzahl der Vorteile und Risiken nicht gleich sein muss. Wichtig ist, dass alle wesentlichen Vorteile und Risiken genannt werden. Auch auf die Formalitäten bei der Darstellung ist hierbei zu achten. So darf die Darstellung wichtige Punkte nicht kaschieren oder abschwächen. Risiken sind daher in derselben Schriftgröße wie die Vorteile aufzuführen. Sie müssen für den jeweiligen Kunden leicht erkennbar sein. Bei gedruckten Informationen müssen die Risikohinweise im selben Dokument wie die Vorteilsdarstellung stehen. Ein Verweis auf andere Dokumente oder Webseiten ist nicht ausreichend und daher als unzulässig zu erachten. Dies folgt aus Art. 44 Abs. 2 c) DV. Die graphische Gestaltung hat sicherzustellen, dass die maßgeblichen Risiken leicht erkennbar, also auf den ersten Blick zu verstehen sind.

Darstellung von Wertentwicklungen

BT 3.3.4 MaComp beschreibt die Anforderungen an die Darstellung von Wertentwicklungen. Hierdurch soll unterbunden werden, dass Kunden anhand missverständlicher Darstellung in die Irre geführt werden. Somit muss klar auf den Bezugszeitraum hingewiesen werden. Es ist auch verständlich hervorzuheben, dass frühere Wertentwicklungen kein verlässlicher Indikator für die Zukunft sind. Weil ein Wertpapier von 2010 bis 2020 rund 10 % Rendite generiert hat, kann hieraus nicht den Kunden suggeriert werden, dies werde sich in der Zukunft derart fortsetzen. Bei Angaben in anderen Währungen als Euro ist eine Warnung vor Währungsschwankungen für Privatkunden erforderlich. Vergangenheitsbezogene Angaben dürfen nicht hervorgehoben werden. Die Vorschriften betreffend Wertentwicklungsangaben unterscheiden zum Teil zwischen vergangenheitsbezogenen (Art. 44 Abs. 4 und Abs. 5 DV) und zukunftsbezogenen (Art. 44 Abs. 6 DV) Angaben. In BT 3.3.4 MaComp führt die BaFin anhand des Art. 44 DV anschaulich dazu aus, wann geeignete Angaben vorliegen:

- Vergangenheitsbezogene Angaben müssen sich auf die letzten fünf Jahre beziehen, wobei „Jahre“ Zwölfmonatszeiträume sind. Die Informationen müssen so aktuell wie möglich sein. Wenn nur Daten für einen kürzeren Zeitraum vorliegen, müssen diese vollständig angegeben werden. Angaben für weniger als zwölf Monate sind grundsätzlich nicht erlaubt, außer bei nicht-werblichen, nachgefragten Informationen.
- Zukunftsbezogene Angaben zur künftigen Wertentwicklung dürfen nicht auf simulierten früheren Daten basieren. Sie müssen auf objektiven Annahmen beruhen und klar angeben, wie sich Gebühren und Entgelte auswirken. Die Informationen sollen positive und negative Szenarien unter verschiedenen Marktbedingungen darstellen und die Risiken der analysierten Instrumente widerspiegeln. Eine deutliche Warnung, dass Prognosen kein verlässlicher Indikator für die Zukunft sind, ist erforderlich.

Sonstige Vorgaben

- **Steuerliche Behandlung:**
  BT 3.4 MaComp verlangt zudem den Hinweis, dass die steuerliche Behandlung von den jeweiligen persönlichen Verhältnissen des einzelnen Kunden abhängt und Änderungen unterworfen sein kann. Diese liegen in der eigenen persönlichen Risikosphäre. Es ist erforderlich, dass sich die Kunden bzgl. der steuerlichen Behandlung von ihrem Steuerberater aufklären lassen.
- **Übereinstimmung mit Produktinformationen:**
  BT 3.5 MaComp beschreibt, dass Marketinginformationen mit den Produktinformationen übereinstimmen müssen.
- **Keine Benennung der Finanzaufsicht:**
  Aus BT 3.6 MaComp folgt das Verbot, den Namen einer Aufsichtsbehörde so zu verwenden, dass der Eindruck entsteht, sie habe das Produkt genehmigt. Bei Verstößen drohen Maßnahmen seitens der Aufsicht. Beispielsweise darf nicht suggeriert werden, dass die Bundesanstalt ein Finanzinstrument ausdrücklich gebilligt hat.
- **Pflicht zur Dokumentation:**
  BT 3.7 MaComp legt fest, dass Marketingmitteilungen dokumentiert werden müssen. Es reicht aus, ein Beispiel-Exemplar aufzubewahren, wenn die Erstellung der einzelnen Dokumente nachvollziehbar ist. Diese Regelungen sollen Transparenz und Klarheit in der Kommunikation mit Kunden gewährleisten und verhindern, dass irreführende Informationen verbreitet werden.
- **Vergleichende Werbung:**
  Sofern bei Marketingmitteilungen Vergleiche gezogen werden, ist das „Gesetz gegen den unlauteren Wettbewerb“ zu beachten.

Fazit

Wertpapierdienstleistungsunternehmen müssen sicherstellen, dass alle Informationen, die sie ihren Kunden zugänglich machen, den gesetzlichen Anforderungen entsprechen. Dies betrifft sowohl die Marketingmitteilungen in Printform als auch digital. Informationen auf der Homepage, auf Social Media und in Apps fallen ebenfalls unter die Anforderung des BT 3 MaComp.

Eine sorgfältige Prüfung und ggf. Anpassung der Informationsmaterialien ist zwingend anzuraten.
Dadurch wird das Vertrauen der Anleger gestärkt und die Transparenz auf den Finanzmärkten erhöht. Auch wenn die praktische Umsetzung dieser Anforderungen im Geschäftsbetrieb eine Herausforderung darstellt, kann nicht auf die notwendige Sorgfältigkeit verzichtet werden. Durch die Verwendung von klaren und präzisen Formulierungen sowie die Bereitstellung zusätzlicher Erklärungen und Hinweise können Institute sicherstellen, dass ihre Informationen den gesetzlichen Anforderungen entsprechen. Transparenz und Sorgfalt schaffen hier Vertrauen.

Bedeutung in der Praxis der Volksbanken Raiffeisenbanken

Bei der Verwendung von Marketingmitteilungen/Informationen aus dem genossenschaftlichen Finanzsektor (DZ BANK AG, Union Investment, attrax) werden diese bereits durch die Verbundpartner unter Beachtung der gesetzlichen Vorschriften erstellt und überprüft. Die bankinterne Kontrolle kann sich hierbei auf die sog. „Prüfung auf offensichtliche Fehler“ beschränken.

Sofern Marketingmitteilungen/Informationen von verbundfremden Anbietern bezogen werden, sind diese vollumfänglich zu prüfen. Andernfalls ist eine sog. Konformitätsbescheinigung vom Fremdanbieter anzufordern, die zusichert, dass die Marketingmitteilungen den gesetzlichen Anforderungen entsprechen. Dann genügt die Prüfung auf offensichtliche Fehler.

Wenn die Bank eigene Informationen erstellt, sind die dargestellten gesetzlichen Anforderungen zwingend einzuhalten und entsprechend vollumfänglich zu überprüfen. ▬

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

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

Know-Your-Customer-Prinzip in der Bankpraxis

Die eigenen Kunden zu kennen ist gesetzlicher Auftrag – und betriebswirtschaftliche Notwendigkeit

Eine große deutsche Versicherungsgesellschaft warb eine Zeitlang mit dem Slogan „Versichern heißt verstehen". Natürlich ist dies vor allem eine eingängige Marketingbotschaft. Dennoch drückt sie mit wenigen Worten den Zusammenhang aus zwischen geschäftlichem Erfolg und dem, was ein Unternehmen über seine Kunden weiß. Seine Kunden zu kennen liegt im Urinteresse eines jeden Produkt- und Dienstleistungsanbieters. Das Verständnis für die Bedürfnisse und Präferenzen der eigenen bzw. potenziellen Kunden bildet die Grundlage für den Erfolg am Markt.

Die klassischen betriebswirtschaftlichen Begriffe wie Kundenbindung, Kundenzufriedenheit und Wettbewerbsvorteile gehen mit dem Know-Your-Customer-Prinzip einher.

Gesetzliche Anforderungen

Innerhalb der Finanzbranche allgemein und im Bankensektor speziell ist das Know-Your-Customer-Prinzip fester regulatorischer und gesetzlicher Bestandteil des Tagesgeschäfts. Es spiegelt sich insbesondere in den allgemeinen und verstärkten Sorgfaltspflichten der §§ 10 und 15 des Geldwäschegesetzes zur Verhinderung von Geldwäsche- und Terrorismusfinanzierung wider. Gesetzgeber und Aufsicht verlangen und erwarten, dass Verpflichtete – hierzu zählen allerdings nicht nur Banken und Versicherer – ihre Kunden kennen und dieses Wissen „up to date" halten. In diesem regulatorischen Kontext bezieht sich das Know-Your-Customer-Prinzip vor allem auf die Anforderung, Informationen über Kunden zu erheben, zu überprüfen und zu speichern. Hinzu treten kundenbezogene Risikomanagementmaßnahmen wie das Monitoring oder die turnusmäßige Risikoanalyse.

Ebenso wichtig ist die intensive Auseinandersetzung mit potenziellen Kunden bereits im frühen Stadium der Geschäftsanbahnung bzw. des Kundenannahmeprozesses. Schon in dieser Phase ist die Entwicklung eines tiefen Verständnisses der geschäftlichen Aktivitäten und Ziele des (neuen) Kunden für die Risiko- und Ertragsbeurteilung von Relevanz.

Dass die BaFin insbesondere auch der Aktualität der Kundendaten eine hohe Bedeutung beimisst, zeigt der Blick auf die jüngste Anpassung ihrer Auslegungs- und Anwendungshinweise zum Geldwäschegesetz. Mit ihrer Veröffentlichung im November 2024 hat die Aufsicht die Aktualisierungszeiträume der Kundendaten auf ein Jahr (hohes Risiko) bzw. fünf Jahre (normales Risiko) verkürzt. Verpflichteten bleibt bis 2027 Zeit für die finale Umsetzung.

Vor dem Hintergrund der tendenziell zunehmenden Regulatorik verwundert es nicht, dass das Know-Your-Customer-Prinzip manchmal als lästig, häufig als zeitraubend und nicht immer hilfreich für das eigentliche (Bank-) Geschäft empfunden wird.

Dennoch ist die gesetzliche und regulatorische Anforderung simpel: Nur wer seine Kunden kennt, kann die Rechtmäßigkeit und Plausibilität von Transaktionen und Geschäftsmodellen ausreichend würdigen und beurteilen.

Wirtschaftlicher Nutzen

Gelebtes Know Your Customer sollte jedoch nicht auf den gesetzlichen Auftrag verkürzt werden. Daten und Informationen werden oft und gerne als Treibstoffe für die digitale Welt und das Informationszeitalter an sich bezeichnet. Dabei wird nicht selten in großen „Machine Learning" und KI-Ansätzen gedacht. Dabei ist Know Your Customer vor allem ein sehr menschlicher Prozess von Kennen- und Schätzenlernen. Wobei „schätzen" durchaus auch „abschätzen" heißen darf.

Denn es geht nicht nur um die geldwäscherechtlichen Fragen nach Namen, Alter, Wohnort und Geschäftszweck des Kunden. Für die im lokalen und regionalen Markt stark verwurzelten Volksbanken und Raiffeisenbanken sind insbesondere die Kunden von Wert, die das genossenschaftliche Prinzip verstehen und gemeinsam mit der Bank vor Ort leben und mit Leben füllen wollen. Diese Kunden liefern erwartungsgemäß auch einen entsprechenden Deckungsbeitrag für die Bank.

Insofern kann ein breit verstandenes und gelebtes Know-Your-Customer-Prinzip mit entsprechend umfangreichen Daten und Informationen über den Kunden eine wesentliche Entscheidungshilfe im Tagesgeschäft der Banken sein, um sowohl regulatorisch einwandfreie als auch ertragsmäßig interessante Kundenbeziehungen zu gewinnen, zu halten und auszubauen.

Die regelmäßige Prüfung und ggf. Aktualisierung der Informationen zum Kunden sichert und erhöht zudem die Qualität der vorhandenen Daten. Dies erleichtert wiederum die Beurteilung von Sachverhalten im Hinblick auf ein erhöhtes betriebswirtschaftliches oder regulatorisches Risiko.

Weit über die reine Regulatorik hinaus unterstützt das gelebte Know-Your-Customer-Prinzip dabei, die richtigen Geschäfte mit den richtigen Kunden zu machen. Im Umkehrschluss bedeutet das aber auch, sich perspektivisch von Kunden zu trennen, deren Geschäftsmodelle nicht zur Wertewelt der Genossenschaftlichen FinanzGruppe passen. Gibt es sogar einen geldwäscherechtlichen Verdachtsfall, sollte die Kündigung einer solchen Geschäftsbeziehung Regel und nicht Ausnahme sein.

Fazit

Das Know-Your-Customer-Prinzip ist fester gesetzlicher und regulatorischer Bestandteil, insbesondere in der Finanzbranche. Aus betriebswirtschaftlicher Sicht ist die Einschätzung eines Kunden für den geschäftlichen Erfolg essenziell. Über die gesetzlich geforderten Daten zum Kunden hinaus kann mit tiefen Kenntnissen der Kundenbeziehung beurteilt werden, ob die Geschäftsbeziehung zur genossenschaftlichen Wertewelt passt und sich Ansatzpunkte für eine Vertiefung der Geschäftsbeziehung ergeben. ▬

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

Interne Revision

Regelmäßig berichten wir an dieser Stelle über die Interne Revision der DZ CompliancePartner. 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 genügt den Anforderungen gemäß MaRisk AT 4.4.3 und BT 2.

Seit der letzten Berichterstattung in der Point of Compliance (3/2024, S. 27) wurden aus der von der Geschäftsführung genehmigten Jahresprüfungsplanung 2024 die Prüfungen der Bereiche „Datenschutz", „Informationssicherheit", „IT & Projekte/IT-Systeme sowie Produkte und Prozesse" und „Geldwäsche- und Betrugsprävention/Compliance Spezialisten" abgeschlossen und die Prüfungsberichte an die Mandanten mit den jeweiligen Auslagerungen versandt. Darüber hinaus wurden aus dem Geschäftsbereich Unternehmenssteuerung die Bereiche „Rechnungswesen & Controlling" sowie „Risikomanagement" geprüft und die Berichte, da diese nicht dienstleistungsbezogen sind, intern veröffentlicht. Der Jahresprüfungsplan wurde auch 2024 vollständig und fristgerecht erfüllt.

Die Quartalsberichte für das dritte und vierte Quartal 2024 der Internen Revision wurden fristgerecht erstellt und den Mandanten, die im Zeitraum zu unseren Kunden gehörten, zur Verfügung gestellt.

Weiterhin wurde turnusgemäß ein Follow-up-Quartalsbericht für das dritte und vierte Quartal 2024 erstellt und der Geschäftsführung der DZ CompliancePartner 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 und der Internen Revision regelmäßige Jours Fixes statt. ▬

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

Wirtschaftliche Lage

Mit einem Jahresergebnis von 1.810 T€ konnte die DZ CompliancePartner GmbH ihr Ergebnisziel von 1.745 T€ leicht überschreiten (+4 %). Auf der Ertragsseite lag die Gesellschaft mit 23.531 T€ mit 7 % über Plan (21.983 T€), wohingegen der Aufwand mit 21.784 T€ knapp 8 % über Plan lag. Saldiert um Zinserträge und -aufwendungen ergab sich das ausgewiesene Ergebnis.

Die besondere Belastung in der DORA-Umsetzung sowie eine Vielzahl neuer regulativer Vorgaben, die in die Dienstleistungserbringung eingepreist werden mussten, haben den Aufwand der Gesellschaft im Wesentlichen geprägt. Ergänzt wurde dies durch eine Abschreibung auf einen 2020 erworbenen Firmenwert.

Das Ergebnis bestätigt die Positionierung der Gesellschaft: Mit einer Umsatzrendite von knapp 8 % steht auch weiterhin der qualitative Verbundnutzen im Rahmen des Förderauftrags insbesondere der DZ BANK Gruppe im Vordergrund, nicht die Gewinnmaximierung der Gesellschaft. Die Erwirtschaftung einer positiven Umsatzrendite im Sinne eines „cost+"-Systems bleibt aber gerade in Zeiten sich stark verändernder Regulatorik und grundlegender technologischer Änderungen wie KI von Bedeutung.

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

Genossenschaftliche FinanzGruppe
Volksbanken Raiffeisenbanken