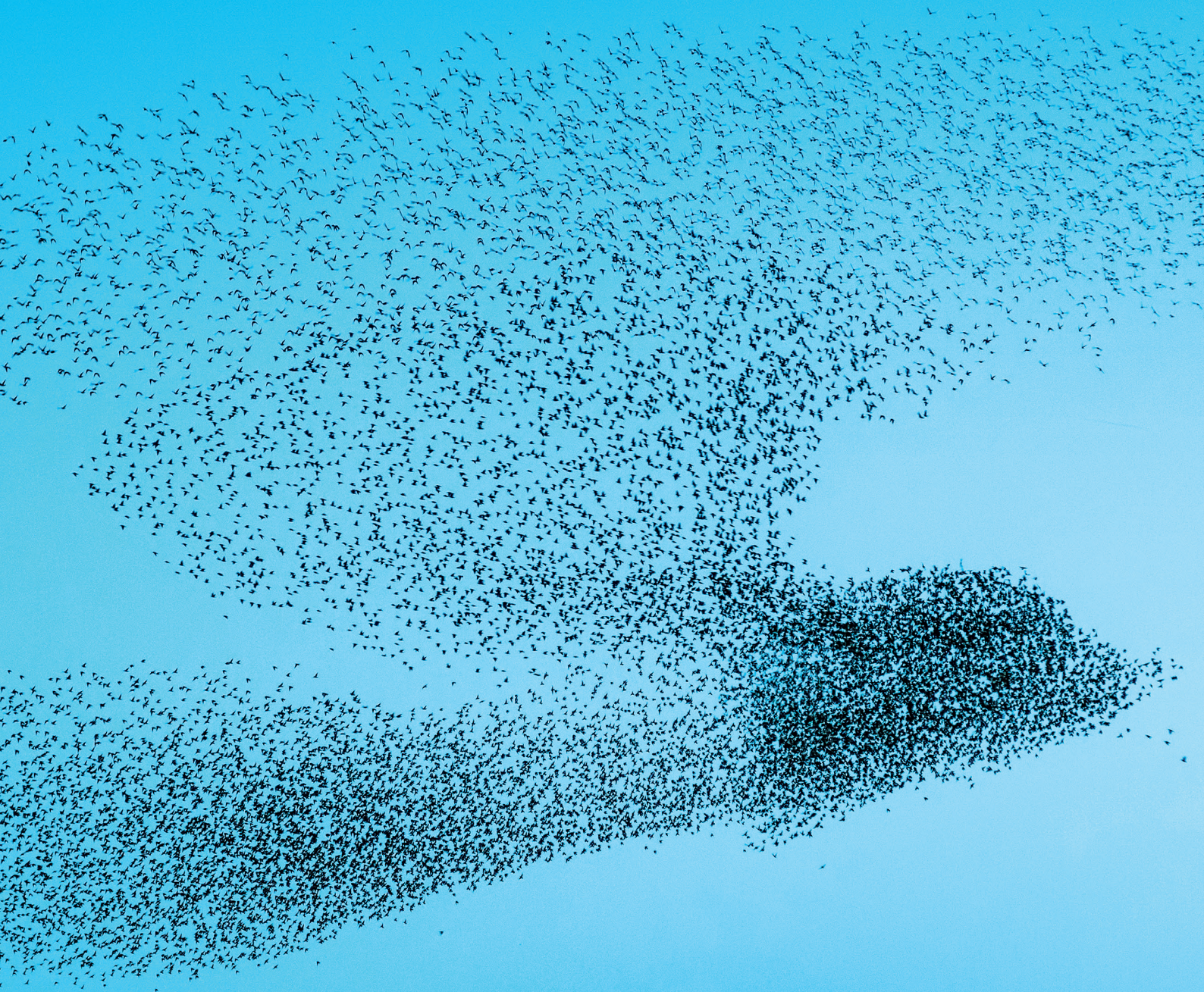
Point of Compliance
Das Risikomanagement-Magazin

AUSGABE 1 / 2024

PoC



Seite 4 **Gastbeitrag Ulrike Brouzi** Compliance ist ein Verbundthema
Seite 9 **WpHG-Compliance** Single Officer und WpHG-Compliance
Seite 17 **Informationssicherheit** Atruvia@AwarenessCircle

DZ CompliancePartner

GENOSSENSCHAFTLICHER FINANZVERBUND
Compliance ist ein Verbundthema 4

GELDWÄSCHEPRÄVENTION UND BETRUGSPRÄVENTION
Das geplante Finanzkriminalitäts-bekämpfungsgesetz 6

WPHG-COMPLIANCE
Single Officer und WpHG-Compliance – ein gutes Team? 9

INFORMATIONSSICHERHEIT
Business Continuity Management – praxisnahe Lösungen 11
Atruvia@AwarenessCircle 17

DATENSCHUTZ
Einführung in die KI-Verordnung 18

IN EIGENER SACHE
Datenschutz-Audit 22
Interne Revision 23

Folgen Sie DZ CompliancePartner auf Social Media.

IMPRESSUM

PoC – Point of Compliance
Das Risikomanagement-Magazin,
Ausgabe 32, 1/2024
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:
Marco Becker, Ulrike Brouzi,
Michaela Eckmann, Reinhold Gillich,
Derya Isikli, Jens Saenger, Lars Schinnerling,
Thomas Schröder, Marina Waidelich,
Benjamin Wellnitz

Bildnachweise: DZ CompliancePartner GmbH, iStock.com/georgeclerk
Gestaltung: Ralf Egenolf
Druck: Thoma Druck, Dreieich

Redaktionsschluss: 28. Dezember 2023
Auflage: 2.400 Exemplare

GEMEINSAM WIRKEN

Jens Saenger
Sprecher der Geschäftsführung

Seit 160 Jahren zeigt die genossenschaftliche Gruppe eindrucksvoll, wie positive Veränderungen aus einer gemeinsamen Kraft entstehen.

Wir kooperieren – und können durch das Teilen von Wissen und Ressourcen besser, effektiver und günstiger handeln.

Wir schließen uns zusammen – und werden auf gesellschaftspolitischer Ebene mit unseren Interessen wahrnehmbarer.

Wir integrieren bewusst ganz unterschiedliche Perspektiven und Fähigkeiten – und bleiben über Jahrhunderte auf Unternehmensebene, aber auch als Gruppe insgesamt, flexibel und anpassungsfähig.

Gemeinsam wirken – das ist auch ein Thema im regulatorischen Beauftragtenwesen, wie **Ulrike Brouzi** in dem Gastbeitrag **„Compliance ist ein Verbundthema“** (S. 4) ausführt oder wie sich – ganz operativ – an der Zusammenarbeit mit der **Atruvia** beim Thema **„Awareness“** (S. 17) zeigt.

Ich schätze mich glücklich und auch stolz, ein Teil all dessen zu sein, und freue mich – auch im Namen des gesamten Teams – auf die Zusammenarbeit in 2024.

Ihnen eine anregende Lektüre.

Herzlichst
Ihr Jens Saenger

Compliance ist ein Ver

Der Verbund ist immer dann besonders stark, wenn er seinen Mitgliedern den Rahmen bietet, gemeinsam wirtschaftlich erfolgreich zu sein. Um den Herausforderungen des Marktes zu begegnen, werden nach innen die Ressourcen und nach außen die Interessenvertretung gebündelt.

Wie erwartet sind die Anforderungen an die Compliance sowohl hinsichtlich der Qualität als auch des Umfanges weiter erheblich gestiegen. Der Gesetzgeber und die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) haben die Relevanz aller Beauftragtenfunktionen – von der Geldwäsche- und Betrugsprävention über den Datenschutz und die Informationssicherheit bis hin zur MaRisk- und WpHG-Compliance – unterstrichen und die Aufgaben erheblich ausgeweitet. Mit Nachdruck und unter Androhung von Sanktionen wird die Implementierung wirksamer Präventionsmaßnahmen eingefordert.

Um die regulatorischen Risiken abzuwehren, haben wir bereits 2018 mit der DZ CompliancePartner einen zentralen Anbieter für alle Compliance-Dienstleistungen geschaffen.

Heute sehen wir, dass die Anforderungen nochmals gestiegen sind. Die (gesamtwirtschaftliche) Risikosituation hat die Aufsicht und den Gesetzgeber nachvollziehbar zu einer kontinuierlichen Verschärfung der regulativen Vorgaben für die gesamte Branche getrieben. So sehen wir, dass die Anforderungen auch für unsere Genossenschaftliche FinanzGruppe nochmals spürbar gestiegen sind und weiter steigen werden. Gleichzeitig gewinnt das Thema „Prävention“ in den Banken aus einem eigenen Schutzinteresse an Bedeutung. Greifbar wird das beispielsweise in der Informationssicherheit: Cyber-Attacken beschäftigen uns schlicht mehr als noch vor fünf Jahren. Ein anderes Beispiel ist die Geldwäsche- und Betrugsprävention, wenn es gilt, sich gegen strafbare Handlungen – sei es von internen oder externen Tätern – zu wappnen.

Damit die Compliance-Aufgaben auch zukünftig sachlich richtig, schützend für die Bank und dabei betriebswirtschaftlich angemessen umgesetzt werden können, ist ein zentraler Lösungsanbieter, in dem sich Wissen und Umsetzungskompetenz konzentrieren, ein richtiger Weg.

Auslagerung von Compliance-Funktionen

Die Auslagerung einer oder mehrerer Compliance-Funktionen sollte risikoorientiert abgewogen werden.

Denn bei jeder Auslagerung einer Compliance-Funktion verbleibt die letztendliche Verantwortung und damit auch ein Teil der Aufgaben immer in der Bank. Kommt es zu Prüfungsfeststellungen beim Auslagerungsunternehmen, wirken sie sich in der Regel auf das auslagernde Unternehmen aus. In diesem Fall sind dann alle Beteiligten, auch das auslagernde Unternehmen, gefordert, entsprechende Maßnahmen zu identifizieren und umzusetzen.

In der Regel überwiegen die Vorteile jedoch: Mit der Bündelung der Aufgabenstellung in einem spezialisierten Auslagerungsunternehmen werden Erkenntnispotenziale gehoben, über die eine einzelne Bank nicht verfügen kann. Hohe Investitionen in Prozesse und Systeme können auf viele Schultern verteilt werden. Mit der Zusammenführung der Erkenntnisse aller Kunden auf Basis abgestimm-

Ulrike Brouzi ist seit dem 1. April 2023 Aufsichtsratsvorsitzende der DZ CompliancePartner GmbH. Die DZ CompliancePartner GmbH ist eine 100-prozentige Tochtergesellschaft der DZ BANK AG Deutsche Zentral-Genossenschaftsbank.

bundthema

ter und standardisierter Prozesse geht ein erheblicher Qualitätszugewinn einher – hinsichtlich der Transparenz, der Nachvollziehbarkeit und auch der Sicherheit.

Ergänzend drängen wir als Gesellschafter der DZ CompliancePartner darauf, dass mit der Aufgabenerfüllung für mehrere Kunden synergetische Effekte erreicht werden. So sind die Kosten im Vergleich zur Eigenfertigung signifikant niedriger. Wichtig ist uns auch ein weiterer Punkt: Mit der Bündelung der Kräfte, wie in der DZ CompliancePartner geschehen, gewinnt die Stimme der Genossenschaftlichen FinanzGruppe Volksbanken Raiffeisenbanken im aufsichtsrechtlichen Diskurs an Gewicht. Die Bündelung der Kräfte stärkt die Position der Primärinstitute und hilft damit, die proportionale Umsetzung der aufsichtsrechtlichen Anforderungen zu gewährleisten.

Alles in allem ist eine positive Bilanz zu ziehen: Nach fünf Jahren DZ CompliancePartner GmbH wird deutlich, dass die Konzentration auf einen zentralen Lösungsanbieter im Verbund die Leistungs-, Wertschöpfungs- und auch Wettbewerbsfähigkeit der Primärgenossenschaften befördert. Die Bündelung der Kräfte dient der Sicherheit und Reputation der einzelnen Bank und darüber hinaus dem Vertrauen des Kunden in unsere Gruppe insgesamt. Dies werden wir als Gesellschafter auch zukünftig tatkräftig unterstützen: Es ist gut, Compliance als eine zentrale Verbundaufgabe zu verstehen. ▬

Ulrike Brouzi
Vorsitzende des Aufsichtsrats
DZ CompliancePartner GmbH,
Neu-Isenburg

Mitglied des Vorstands
DZ BANK AG Deutsche
Zentral-Genossenschaftsbank,
Frankfurt am Main

Das geplante Finanzkriminalitätsbekämpfungsgesetz

Die Bundesregierung will die Bekämpfung von Geldwäsche und Finanzkriminalität nochmals verstärken. Dabei ist eine weitere Bündelung der Kompetenzen geplant. Ermittlungen sollen zukünftig nach dem „Follow the money"-Ansatz geführt werden.

Das Bundeskabinett hat am 11. Oktober 2023 den Entwurf des Gesetzes zur Verbesserung der Bekämpfung von Finanzkriminalität, kurz Finanzkriminalitätsbekämpfungsgesetz (FKBG), beschlossen. Mit dem FKBG soll die Bekämpfung von Finanzkriminalität und insbesondere von Geldwäsche nochmals einen neuen Impuls erhalten.

Zudem sollen mit dem FKBG die von der Financial Action Task Force (FATF) am 25. August 2022 in ihrem Abschlussbericht veröffentlichten Mängel beseitigt werden.

Der seinerzeitige Abschlussbericht der FATF hatte insbesondere

- die zersplitterte Zuständigkeit bei der Bekämpfung der Finanzkriminalität infolge einer Vielzahl von Behörden auf Bundes- und Landesebene,
- die strafrechtliche Ermittlungsarbeit bei der Strafverfolgung der Geldwäsche und
- die große Anzahl an Aufsichtsinstanzen im Nichtfinanzsektor bemängelt.

Bundesamt zur Bekämpfung von Finanzkriminalität

Kernziel des neuen Gesetzesentwurfs ist daher zum einen die Neuausrichtung der Geldwäschebekämpfung durch Bündelung von Kompetenzen in einer neuen Bundesoberbehörde, dem Bundesamt zur Bekämpfung von Finanzkriminalität (BBF). Zum anderen soll die Ermittlungsarbeit bei der Aufdeckung von Geldwäsche und Finanzkriminalität unter dem Dach des BBF konsequent dem „Follow the money"-Ansatz folgen.

Das BBF wird dabei – vereinfacht ausgedrückt – aus drei Säulen bestehen.

- Strafrechtliche Ermittlung
- Strategische und operative Analyse
- Koordinierung der Geldwäscheaufsicht

(siehe hierzu Grafik auf Seite 7)

Die strafrechtliche Ermittlungsarbeit entsprechend dem „Follow the money"- Ansatz **übernimmt das Ermittlungszentrum Geldwäsche (EZG).** Das EZG soll polizeiliche Ermittlungsbefugnisse erhalten und insbesondere Fälle internationaler Geldwäsche mit Deutschlandbezug verfolgen. Dabei setzt die Ermittlungsarbeit des EZG bereits bei verdächtigen Finanzströmen an - nicht an möglichen Vortaten.

Die **strategische und operative Analyse von Geldwäscheverdachtsmeldungen** unter Berücksichtigung des risikobasierten Ansatzes ist Aufgabe der **Financial Intelligence Unit (FIU),** die ab 1. Januar 2025 unter dem Dach des BBF arbeiten soll.

Die Zuständigkeit für die Koordinierung der Geldwäscheaufsicht und der administrativen Ermittlung liegt einerseits bei der **Zentralstelle für Geldwäscheaufsicht (ZfG).** Sie wird die geldwäscherechtlichen Aufsichtsmaßnahmen bundesweit koordinieren und auf die Vereinheitlichung und Stärkung der Aufsicht über den Nichtfinanzsektor hinwirken.

Quelle: Bundesministerium der Finanzen

Daneben ist die **Zentralstelle für Sanktionsdurchsetzung (ZfS)** verantwortlich für die Vermögensermittlung und -sicherstellung sowie die Koordinierung der Sanktionsdurchsetzung.

Mit einem separaten Gesetzesvorhaben soll zukünftig auch noch die Funktion einer **administrativen Vermögensermittlung** unter dem Dach des BBF implementiert werden. Die administrative Vermögensermittlung hat eine verfassungsrechtliche Dimension. Ihre Aufgabe soll nicht nur die Aufklärung der Besitzrechte verdächtiger Vermögensgegenstände und ihrer Herkunft sein, sondern auch ein eventueller Eigentumsentzug, sofern Besitz oder Berechtigung nicht nachgewiesen werden können.

Auswirkungen des FKBG für die Geldwäscheprävention

Das FKBG wurde als sogenanntes Artikelgesetz entworfen. Das bedeutet, dass die einzelnen Artikel des FKGB Änderungen diverser anderer Gesetze nach sich ziehen. Auch das Geldwäschegesetz (GwG) wird geändert.

Nachfolgend haben wir wichtige Änderungen für Sie zusammengefasst.

Geldwäschegesetz (GwG)

- Durch eine Änderung von § 8 Abs. 2 GwG (Aufzeichnungs- und Aufbewahrungspflicht) soll klargestellt werden, dass auch Personalausweise, die nicht die ausstellende Behörde, sondern nur den ausländischen Staat erkennen lassen, zur Identifizierung geeignet sind.
- Die Identifizierungspflicht für Immobilienmakler wird noch etwas weiter gefasst, indem sich weite Teile des § 12 GwG (Überprüfung von Angaben zum Zweck der Identifizierung) künftig auch auf die Fälle des § 11 Abs. 2 GwG (Identifizierung und Erhebung von Angaben zum Zweck der Identifizierung bei Immobilienmaklergeschäften) beziehen.
- Durch § 51 Abs. 11 E sollen die Aufsichtsbehörden im Wege einer Allgemeinverfügung bestimmen können, welche Meldungen, Anzeigen, Berichte, Anträge oder sonstige Informationen elektronisch in welchem Datenformat, Umfang bzw. Zeitpunkt vorzulegen bzw. welche elektronischen Kommunikationsverfahren hierfür zu verwenden sind.
- Ferner soll die BaFin nach § 52 Abs. 7 durch Allgemeinverfügung festlegen können, welche für die Bankenaufsicht notwendigen Information ihr regelmäßig zu welchen Zeitpunkten zu übermitteln sind.

„Das geplante Finanzkriminalitätsbekämpfungsgesetz bietet Vorteile, indem es dazu beiträgt, die Integrität des Finanzsystems zu schützen. Es hilft, die Bekämpfung von Geldwäsche, Betrug und anderen finanziellen Straftaten zu verbessern. Unserer Funktion und Aufgabe als Geldwäschebeauftragte verleiht es zudem einen noch höheren Stellenwert. Durch strengere Regulierungen und verstärkte Überwachung können Risiken minimiert und das Vertrauen in die Finanzmärkte gestärkt werden.“

Marco Becker
Bereichsleiter Geldwäsche- und Betrugsprävention

Hier bleibt insbesondere abzuwarten, welche Informationen die BaFin bei den Kreditinstituten anfordern wird.

Transparenzregister

- Die registerführende Stelle des Transparenzregisters soll von mitteilenden Personen geeignete Nachweise über die Vertretungsberechtigung anfordern dürfen.
- Zudem soll die registerführende Stelle die im Transparenzregister einzutragenden Daten auch durch Abrufe nach § 24c KWG bei den Melderegistern, dem Grundbuchamt oder dem Stiftungsregister abfragen dürfen.
- Außerdem soll im Transparenzregister mit Wirkung ab 1. Januar 2027 nicht nur das Geburtsdatum des wirtschaftlich Berechtigten von transparenzregisterpflichtigen Vereinigungen, sondern auch der entsprechende Geburtsort eingetragen werden.
- Können im Zusammenhang mit Unstimmigkeitsmeldungen Angaben nicht überprüft werden, weil das betroffene Unternehmen nicht fristgerecht mitwirkt, wird dies auf dem Registerauszug vermerkt.

Immobilientransaktionsregister

- Beim BBF soll ein Immobilientransaktionsregister eingerichtet werden, das Meldedaten nach § 18 Grunderwerbsteuergesetz (GrEStG) von Gerichten, Behörden und Notaren bei Erwerben ab einem Kaufpreis von 20.000 Euro betrifft.

  Das BBF soll über eine Schnittstelle entsprechende Datensätze erhalten können.
- Abrufe sollen auf Ersuchen durch die FIU, die ZfS, dass EZG sowie Strafverfolgungsbehörden und Gerichte erfolgen können.

Ausblick

Mit welchen Anpassungen das FKBG letztlich in Kraft treten wird, kann zum Zeitpunkt der Drucklegung dieses Artikels noch nicht abschließend beurteilt werden. Zahlreiche Interessenverbände (u. a. auch die Deutsche Kreditwirtschaft) haben zum Teil umfangreiche Stellungnahmen zum Gesetzesentwurf eingereicht.

Über wesentliche materielle Änderungen gegenüber der in diesem Artikel beschriebenen Entwurfsfassung des FKBG werden wir informieren. ▬

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

Single Officer und WpHG-Compliance – ein gutes Team?

Mit der Schaffung des Single Officer hat der Gesetzgeber Banken weitere Verpflichtungen und Tätigkeiten auferlegt. Doch bedeutet dies unweigerlich einen starken, zusätzlichen Aufwand? Die Antwort lautet: Nicht zwingend.

Die Funktion des Beauftragten zum Schutz von Kundenfinanzinstrumenten – auch genannt „Single Officer" – ist eigentlich gar nicht so neu. Sie wurde bereits mit MiFID II ab 2018 eingeführt. Klarheit erhielt die Position dann durch die Mindestanforderungen an die ordnungsgemäße Erbringung des Depotgeschäfts und den Schutz von Kundenfinanzinstrumenten für Wertpapierdienstleistungsunternehmen – oder kurz: MaDepot.

Gemäß § 81 Abs. 5 WpHG trägt der Single Officer die Verantwortung dafür, „dass das Wertpapierdienstleistungsunternehmen seine Verpflichtungen in Bezug auf den Schutz von Finanzinstrumenten und Geldern von Kunden einhält". Diese knappe Definition im WpHG lässt allerdings viele Fragen zu den konkreten Tätigkeiten offen.

Ein Blick in die MaDepot sorgt für etwas mehr Klarheit. So sollen u.a. organisatorische Vorkehrungen geschaffen werden, um die Eigentumsrechte von Kunden an den für sie verwahrten Finanzinstrumenten zu schützen. Dies umfasst beispielsweise die ordnungsgemäße Verwahrung und Depotbuchführung von Kunden- und Eigenbeständen sowie besondere Sorgfalts- und Überwachungspflichten bei Drittverwahrern.

Bündelung der Funktionen – möglich, aber nicht verpflichtend

Für die Beurteilung der Art, des Umfangs und der Komplexität der Tätigkeiten des Single Officer ist zunächst eine Bestandsaufnahme der konkreten Geschäftstätigkeiten mit anschließender Risikoanalyse erforderlich. Hieraus abgeleitet ergeben sich dann Kontrolltätigkeiten in Abhängigkeit vom institutsspezifischen Risiko. Über alle Tätigkeiten des Single Officer ist mindestens jährlich und ggf. anlassbezogen ein Bericht zu erstellen und der Geschäftsleitung vorzulegen.

Diese Systematik kommt Ihnen bekannt vor? Richtig. Ein kurzer Vergleich des WpHG-Beauftragten und des Single Officer zeigt vergleichbare Anforderungen des Aufsichtsrechts und eine gewisse Analogie (siehe Tabelle Seite 10).

Die MaDepot lassen Wertpapierdienstleistungsunternehmen explizit die Wahl, ob die Aufgaben des Single Officer durch den Beauftragten WpHG-Compliance wahrgenommen werden oder nicht. Im Falle einer Trennung der beiden Funktionen wäre hier jedoch organisatorisch eine klare Abgrenzung der Zuständigkeitsbereiche zu schaffen.

Tätigkeiten	WpHG-Beauftragter	Single Officer
Zentrale Rechtsgrundlagen des Beauftragten	§ 80 Abs. 1 WpHG, Art. 22 DV 2017/565 und BT 1 MaComp	§ 81 Abs. 5 WpHG und MaDepot
Notwendigkeit einer Risikoanalyse	ja	ja
Durchführung von Kontrollen	ja	ja
Berichterstattung (Jahresbericht bzw. Ad-hoc-Bericht)	ja	ja
Überwachungsfunktion	ja	ja
Beratungsfunktion	ja	ja
Auswertung von internen und externen Prüfungsberichten	ja	ja
Vorhandensein notwendiger Befugnisse, Fachkenntnisse und Ressourcen	ja	ja
Verbot der Beteiligung an zu überwachenden Tätigkeiten	ja	ja
Unabhängigkeit und Weisungsfreiheit bei der Aufgabenwahrnehmung	ja	ja

Unser Angebot

Sie nutzen bereits unser Auslagerungsangebot der WpHG-Compliance und möchten zusätzlich Entlastung durch die Übernahme des Single Officer durch uns? Gerne lassen wir Ihnen hierzu weitere Informationen sowie ein unverbindliches Angebot zukommen.

Sie nutzen unser Auslagerungsangebot der WpHG-Compliance noch nicht? Kein Problem. Wir bieten die Übernahme der Funktion des Single Officer auch separat an.

Fazit

Der WpHG-Compliance-Beauftragte und der Single Officer sind zwei unterschiedliche Funktionen mit verschiedenen Aufgabenbereichen und Rechtsgrundlagen, die aber gewisse Schnittstellen in ihren Tätigkeiten zueinander und eine vergleichbare systematische Vorgehensweise haben. Beide Funktionen müssen aufsichtsrechtlich vorhanden sein, wenn Wertpapierdienstleistungsunternehmen das Depotgeschäft betreiben.

In der Praxis hat sich aus Effizienzgründen bei vielen Banken etabliert, beide Positionen einer Person zuzuordnen. Auch innerhalb der DZ CompliancePartner handhaben wir dies so, was zusätzlich den Vorteil eines einheitlichen Ansprechpartners für unsere Banken beinhaltet. ▬

Marina Waidelich
Abteilungsleiterin WpHG-Compliance,
E-Mail: marina.waidelich@dz-cp.de

Business Continuity Management – praxisnahe Lösungen

Notfallmanagement macht Sinn. Auf den Punkt gebracht, sichert es im Krisenfall die Aufrechterhaltung des Geschäftsbetriebs. Mit der „Bankenaufsichtliche Anforderungen an die IT (BAIT)“ - Novelle wurden die Anforderungen an das Notfallmanagement konkretisiert. Doch – wie sollte es aufgebaut sein und worauf ist zu achten?

Das Notfallmanagement oder auch Business Continuity Management (BCM) folgt vor allem dem Zweck, den Geschäftsbetrieb im Krisenfall fortführen zu können. Es soll gewährleisten, dass auch unter erschwerten Voraussetzungen, trotz eines kritischen Vorfalls, der Geschäftsbetrieb auf einem akzeptablen, vordefinierten Level fortgeführt werden kann. Dazu werden im BCM geeignete Strategien und Maßnahmen definiert, um – beispielsweise bei technischen Störungen, den Geschäftsbetrieb „lähmenden“ Personalausfällen oder auch bei Hackerangriffen – handlungsfähig zu bleiben.

Als Teil des Wirtschafts- und Finanzsystems hat das BCM für Banken darüber hinaus eine formale Bedeutung. Mit dem Notfallmanagement sind bestimmte aufsichtsrechtliche Pflichten und gesetzliche Bestimmungen verbunden, die die Bank erfüllen muss.

Notfallmanagement nun auch für IT-Systeme

Die gesetzliche Grundlage zur Festlegung eines angemessenen BCM, insbesondere der Einbindung von IT-Systemen, ist in § 25a Abs. 1 Nr. 5 KWG geregelt. Daran anknüpfend greifen die Mindestanforderungen an das Risikomanagement (MaRisk) das Notfallmanagement (MaRisk AT 7.3) auf.

Gemäß MaRisk AT 7.3 sind im Notfallmanagement

- zeitkritische Aktivitäten und Prozesse,
- Auswirkungsanalysen,
- Risikoanalysen (MaRisk AT 7.3 Tz. 1) sowie
- das Notfallkonzept und Notfallszenarien (MaRisk AT 7.3 Tz. 2) und
- die Überprüfung des Notfallkonzepts (MaRisk AT 7.3 Tz. 3) zu berücksichtigen.

Ein wesentlicher Bestandteil und Basis eines BCM ist die Business-Impact-Analyse (BIA). In ihr werden zunächst Prozesse und Funktionen in der Organisation identifiziert, um dann die Auswirkungen möglicher Störungen oder Ausfälle zu beschreiben. In der sogenannten Auswirkungsanalyse wird die Zeitkritikalität der jeweiligen Geschäftsprozesse ermittelt und werden geeignete Vorsorgemaßnahmen ausgearbeitet.

Ergänzend sind nun in den BAIT die Anforderungen an das IT-Notfallmanagement konkretisiert worden (Kapitel 10 „IT-Notfallmanagement“). Insbesondere die Differenzierung der Verfügbarkeitsanalyse (Business Impact)

- in der Wiederanlaufzeit (Recovery Time Objective – RTO) und
- in dem maximal tolerierbaren Zeitraum eines Datenverlustes (Recovery Point Objective – RPO)

ist dabei zu beachten.

Es reicht nicht mehr aus, nur die zeitkritischen Prozesse im Notfallkonzept zu berücksichtigen. Vielmehr müssen auch „IT-Systeme, welche zeitkritische Aktivitäten und Prozesse unterstützen“ sowie die „Abhängigkeiten zwischen den IT-Systemen“ (BAIT Tz. 10.4) eingebunden werden.

Schlankes BCM?

Fakt ist, dass sowohl die technischen als auch die organisatorischen Konstellationen – samt den personellen Zuständigkeiten – einem steten Wandel unterworfen sind. Um dem Rechnung zu tragen und die Handlungsfähigkeit auch dann in einem Notfall zu gewährleisten, sind die aufsichtsrechtlichen Anforderungen an die Aktualität gestiegen.

Die Business-Impact-Analyse (BIA) ist mindestens einmal jährlich durchzuführen. Wenn vorab ein anlassbezogener Grund vorliegt, wird zudem eine unterjährige Analyse erforderlich. Dies gilt übrigens auch für Objekte aus dem Informationsverbund, die zeitkritische Auswirkung bei einem Ausfall haben können. Darüber hinaus sind für „alle speziell relevanten Szenarien zu den zeitkritischen Aktivitäten und Prozessen“ jährlich Notfalltests und Übungen durchzuführen.

Die aufgeführten Konkretisierungen können bei bestehenden Lösungen zu einer – signifikanten – Ausweitung des BCM und damit des Gesamtaufwands führen. Zu fragen ist, wie angesichts dessen noch ein praxisnahes und effizientes Notfallmanagement aufgestellt werden kann.

Umsetzung

In der Praxis sind längst noch nicht alle Umsetzungsfragen abschließend beantwortet. Es erscheint deshalb zweckmäßig, sich bis auf Weiteres an dem bewährten Umsetzungsrahmen – dem Standard 200-4 des Bundesamts für Sicherheit in der Informationstechnik (BSI) – zu orientieren. Für die Bank selbst ist es zunächst wichtig, einen internen Mitarbeiter als Notfallbeauftragten zu benennen und zu qualifizieren.

Folgende weitere Schritte sind zu empfehlen und zu beachten:

1

Business-Impact-Analyse (BIA) durchführen

Mit Hilfe der Business-Impact-Analyse wird in Zusammenarbeit mit den Informationseigentümern (i.d.R. der jeweilige Fachbereich) die Zeitkritikalität der Prozesse ermittelt.

Bezeichnung	Besondere Zeit	MaRisk	MTA
Interne Prozesse			
Betriebliche Grundfunktionen			
Bereitstellung Informations- und Kommunikationstechnologie		Nein	
Entsorgung von Datenträgern/Belege		Nein	
Meldewesen		Nein	< 7 Tage
Rechnungswesen		Nein	
Ver-/Entsorgung, Überwachung, Störungsmanagement		Nein	< 7 Tage
Kunde			
Kontokorrent / Kontoführung		Nein	< 7 Tage
Managementprozesse			

Beispielhafte Darstellung der Geschäftsprozess-Übersicht der BIA

2

Szenarien festlegen

Des Weiteren sind Szenarien nach Relevanz festzulegen, die einen Notfall auslösen können. An dieser Stelle wird mit Pflicht-Szenarien und Kann-Szenarien gearbeitet. Die sogenannten Pflicht-Szenarien sind grundsätzlich durch die Bank zu berücksichtigen.

Bezeichnung	Gefährdungen	Direkt relevant
Gebäudeausfall	G 0.001 Feuer,G 0.002 Ungünstige klimatische Bedingungen,G 0.003 Wasser,G 0.004 Verschmutzung, Staub, Korrosion	IT-Systeme,Netze/Kommunikationsverbindungen,Räume und Lokationen
Infrastrukturkomponentenausfall	G 0.008 Ausfall oder Störung der Stromversorgung,G 0.009 Ausfall oder Störung von Kommunikationsnetzen,G 0.010 Ausfall oder Störung von Versorgungsnetzen	IT-Systeme,Netze/Kommunikationsverbindungen,Räume und Lokationen

Beispielhafte Darstellung der Übersicht der Szenarien der BIA

WAZ	RPO	Status
	tägliche Sicherung	Aktiv
	tägliche Sicherung	Aktiv
160	tägliche Sicherung	Aktiv
	tägliche Sicherung	Aktiv
160	tägliche Sicherung	Aktiv
160	tägliche Sicherung	Aktiv

3

Festlegung organisatorischer Rahmenbedingungen/Einheiten

Im Folgenden sollte überprüft werden, ob im bisherigen Notfallkonzept die Angaben zu den

- Filialen/Geschäftsstellen,
- Abteilungen,
- Räumungsbereichen,
- BCM-Rollen der Mitarbeiter (z. B. Brandschutzhelfer, Ersthelfer, Krisenmanagement-Leitung, Krisenmanagement-Team etc.) und
- externen Stellen (z. B. Kontaktdaten Dienstleister, Versorgungsunternehmen, Hilfsdienste wie Polizeidienststellen, Krankenhaus, Ärzte etc.) aktuell sind.

Ressource	Szenario	Maßnahmenart
agree21AZV		
Cyber-Angriff		
agree21AZV	Cyber-Angriff	Korrektive Maßnahme
agree21AZV	Cyber-Angriff	Präventive Maßnahme
Dienstleisterausfall		
agree21AZV	Dienstleisterausfall	Korrektive Maßnahme
agree21AZV	Dienstleisterausfall	Präventive Maßnahme
agree21Banking (CBS)		
Cyber-Angriff		
agree21Banking (CBS)	Cyber-Angriff	Korrektive Maßnahme

Beispielhafte Darstellung der Übersicht der Soll-Übungen

4

Überprüfung der Anweisungen zu den Objekten und den zeitkritischen Geschäftsprozessen

Ferner sind die Objekte (IT-Systeme, IT-Anwendungen etc.), die zeitkritische Auswirkungen auf den Geschäftsbetrieb haben, hinsichtlich der Wiederanlauf-, Notbetriebs- und Wiederherstellungsplanung sowie auf Geschäftsprozessebene die Geschäftsfortführungs- und Wiederherstellungsplanung zu prüfen und zu aktualisieren.

Objekt	Wa	N/G	Wh	A	Status
Objekt					
agree21AZV	✔	✔	✔		abgeschlossen
agree21Banking (CBS)	✔	✔	✔		abgeschlossen
agree21Client	✔	✔	✔		abgeschlossen
agree21Client 'Mobil'	✔	✔	✔		abgeschlossen
agree21Debitkarten	✔	✔	✔		abgeschlossen
agree21eBanking-ZV	✔	✔	✔		abgeschlossen
Prozess					
Basis-Zahlungsverkehr					
agree21AZV	✔	✔			abgeschlossen
agree21ZV	✔	✔			abgeschlossen
agree21ZV-unbar	✔	✔			abgeschlossen
ipsYdion ZV	✔	✔			abgeschlossen

Beispielhafte Darstellung der Übersicht der Anweisungen

5

Aktualisierung der Notfalldokumente

Die Aktualität der neben den o.g. Notfallanweisungen auch benötigten Dokumente ist ebenfalls regelmäßig zu überprüfen

Die Verfügbarkeit der vollständigen Notfalldokumente muss jederzeit gewährleistet sein. Dies kann in ausgedruckter Form, als PDF auf einem gesonderten Laptop oder in einem sicheren Cloud-basierten Datenraum erfolgen.

Titel	Bearb.datum
Handbuch Krisenstab	30.10.2023 14:06:17
Leitlinie Business Continuity Management	17.10.2023 16:37:29
Notfallhandbuch Krisenstab	30.10.2023 14:08:07
Notfallplan Sofortmaßnahmen	30.10.2023 14:09:19

Beispielhafte Darstellung der Übersicht der Notfallhandbücher und Notfall-Rahmendokumente

6

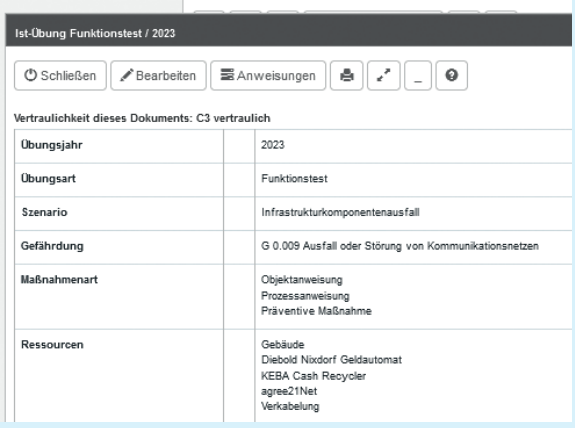
Festlegung der Soll-Übungen

Die Soll-Übungen, die unterschiedliche Szenarien und Maßnahmenarten berücksichtigen, werden durch das System generiert/festgelegt.

8

Durchführung und Dokumentation der Ist-Übungen

Nach Festlegung der Übungsplanung sind die Ist-Übungen durchzuführen. Ein Abgleich zwischen Soll- und Ist-Übungen kann vorgenommen werden.



Beispielhafte Darstellung der Dokumentation zu den Ist-Übungen (Alle Screenshots stammen aus dem Tool BCM kompakt der DZ CompliancePartner.)

7

Festlegung der Übungsplanung

Anschließend ist die jährliche Übungsplanung aufzustellen.

Beispielhafte Darstellung der Übersicht Übungsplanung

Fazit

Um im Krisenfall handlungsfähig zu sein, sind die kritischen Geschäftsprozesse und -ressourcen in einem zentralen Notfallmanagement zu identifizieren und mit entsprechenden Gegenmaßnahmen zu hinterlegen. Dabei sind insbesondere die Auswirkungen von Störungen und Ausfällen zu analysieren. Mit der Business-Impact-Analyse steht und fällt das Notfallmanagement.

Abschließend ist festzuhalten, dass die Anforderungen insgesamt gestiegen sind. Um den Aufwand einzugrenzen, sollte eine intelligente Softwarelösung in Betracht gezogen werden. Sie sorgt für die erforderliche Transparenz und Nachvollziehbarkeit bei der Dokumentation – und stellt vor allem im Notfall sicher, dass wichtige Informationen griffbereit sind. ▬

Weiterführende Infos zu den BAIT:
https://www.bundesbank.de/de/aufgaben/bankenaufsicht/einzelaspekte/risikomanagement/bait/bankaufsichtliche-anforderungen-an-die-it-598580, abgerufen am 31.10.2023

Notfallmanagement der DZ CompliancePartner

Ein Finanzinstitut muss seine Kernprozesse und die Auswirkungen von Ausfällen genau kennen, um angemessen auf kritische Situationen reagieren zu können: Mit dem Beratungskonzept der DZ CompliancePartner in Verbindung mit der digitalen Lösung „BCM kompakt“ haben Sie Ihre – bankindividuellen – zeitkritischen Geschäftsprozesse und Ressourcen im Blick und können im Ernstfall die erforderlichen Maßnahmen ergreifen.

Michaela Eckmann
Beauftragte Informationssicherheit & Datenschutz,
E-Mail: michaela.eckmann@dz-cp.de

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

Atruvia@AwarenessCircle

Awareness bedeutet, ein Bewusstsein der Bankmitarbeiter für Cyber-Angriffe jeglicher Art zu schaffen. Wir setzen dabei auf eine Verbundlösung.

Die bekannten Cybercrime-Schäden belaufen sich allein in Deutschland auf 223,5 Miiliarden Euro jährlich. Es gibt kaum mehr ein Unternehmen, das noch nicht Ziel eines Angriffs war. Die Frage ist längst nicht mehr ob, sondern wann man Ziel eines Angriffs wird. Deshalb ist es so wichtig, sich hier stark aufzustellen.

Um die Banken bestmöglich zu unterstützen, setzen wir auf einen Verbundansatz: Im Sinne der „Bündelung der Kräfte“ ist es gelungen, eine Kooperation mit der Atruvia zu initiieren.

Atruvia stellt mit dem Produkt „PhishingSimulation“ den Banken eine Plattform für die Simulation von mail-basierten Cyber-Angriffen zur Verfügung. Diese Leistung integrieren wir in unser Awareness-Angebot „AwarenessCircle“.

Informationssicherheit (er)leben

Der AwarenessCircle steht für nachhaltige Sicherheit, um sich langfristig gegen Cyber-Angriffe zu wappnen, aber auch, um den aufsichtsrechtlichen Anforderungen nachzukommen.

Je nach Anforderungen kann zwischen einer Comfort- und einer Premiumvariante gewählt werden. Der Unterschied liegt in der Intensität der Sensibilisierungsmaßnahmen und der Integration in das Notfallmanagement. Beide Varianten umfassen eine

- umfangreiche Kampagnenbegleitung,
- die Erstellung eines Zweijahresplans zur Sensibilisierung in Ihrem Haus und
- eine über zwei Jahre ausgelegte Phishing-Kampagne.
  - Atruvia-Banken haben dabei die Möglichkeit, auf das Produkt „PhishingSimulation“ zurückzugreifen.
  - Für Kunden und Institute, die nicht an Atruvia angeschlossen sind, ist weiterhin die Phishing-Simulation von Hornetsecurity Bestandteil der Leistung.

Fazit

Warten ist kein guter Ratgeber beim Thema „Cyber-Security“. Neueste Fälle zeigen, wie anfällig Systeme sind und in welchem Ausmaß die Unternehmen mit Einbußen jeglicher Art zu kämpfen haben, wenn „das Kind erst einmal im Brunnen liegt“. Die Kooperation zwischen Atruvia und DZ CompliancePartner GmbH – genauer noch die Integration der „PhishingSimulation“ in den „AwarenessCircle“ – ist Garant für ein hohes, an die spezifischen Bedürfnisse der genossenschaftlichen Banken optimiertes Sicherheitsniveau. ▬

Reinhold Gillich
Beauftragter
Informationssicherheit & Datenschutz,
E-Mail: reinhold.gillich@dz-cp.de

Einführung in die KI-Verordnung

Was beinhaltet die KI-Verordnung? Welchen Sinn und Zweck verfolgt sie und welche Sanktionen sind bei Verstoß vorgesehen? Welche Zuständigkeiten bzgl. der Einhaltung und Weiterentwicklung der KI-Verordnung ergeben sich auf europäischer und nationaler Ebene?

DALL-E2 oder ChatGPT sind die Schlagzeilen, die unausweichlich unsere Aufmerksamkeit in den letzten Monaten auf sich gezogen haben.

Auch wenn zunächst große Skepsis gegenüber den neuen Tools bestand, kann man beobachten, dass die ersten Hemmschwellen bereits überwunden werden. Selbst die ersten Kultusministerien befürworten mittlerweile den Einsatz von KI an unseren Schulen.[1] Doch ist KI nicht ohne Risiken und Nebenwirkungen. Daher soll die neue europäische KI-Verordnung oder auch bekannt als AI-Act, Abhilfe schaffen.

Was ist die KI-Verordnung?

Dass mit dem Einsatz von KI-Systemen durchaus Risiken und Gefahren einher gehen können, hat auch die Europäische Union erkannt und ist daher derzeit dabei, eine erste europäische Rechtsnorm, die KI-Verordnung oder auch AI ACT (kurz KI-VO) genannt, zu erlassen.[2]

Diese KI-Verordnung stellt die erste Regulierung hinsichtlich der Entwicklung, Bereitstellung und Nutzung von KI-Systemen dar.

Das Gesetz, das im April 2021 durch die Europäische Kommission vorgestellt wurde, beinhaltet neben Regulierungen auch einheitliche Bestimmungen für den Einsatz der künstlichen Intelligenz in der EU[3] sowie die Festlegung einer einheitlichen Definition des Begriffs der künstlichen Intelligenz[4]. Jedoch haben sich die Vertreter der europäischen Fraktionen erst dieses Jahr zu einer einheitlichen Definition im Art. 3 Nr. 1 KI-VO geeinigt.

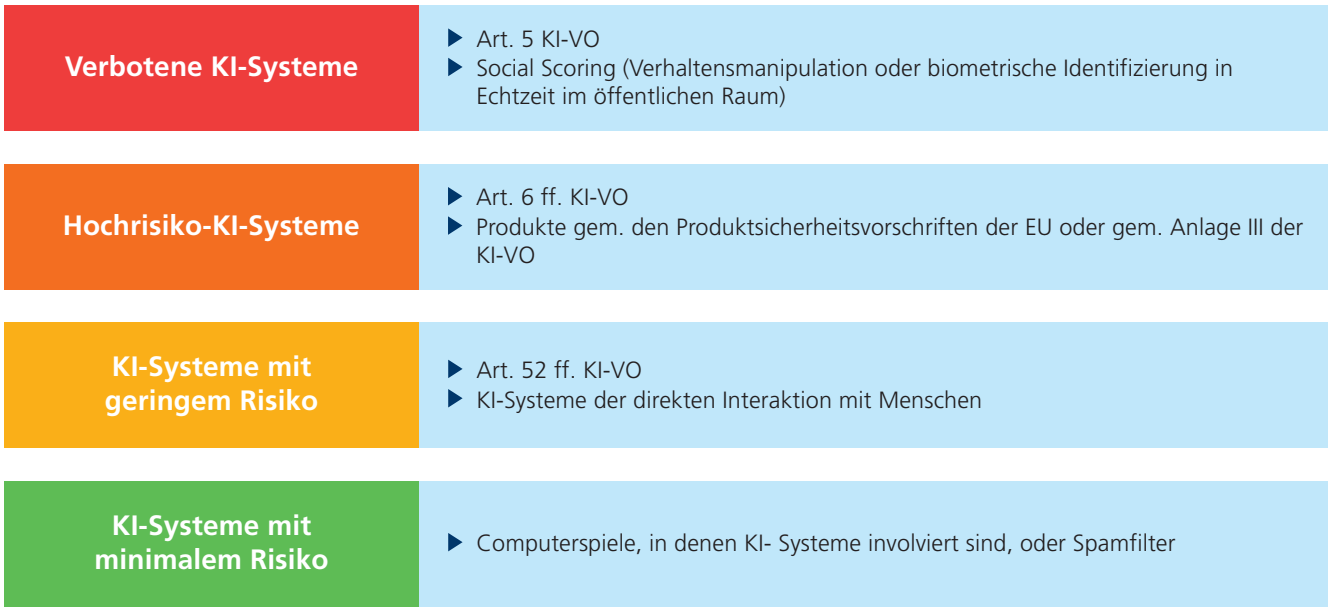
Danach ist gem. Art. 3 Nr. 1 KI-VO ein „System der künstlichen Intelligenz“ (KI-System) „eine Software, die mit einer oder mehreren der in Anhang I aufgeführten Techniken und Konzepte entwickelt worden ist und im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren“.

Dies ist eine sehr erfreuliche Entwicklung, da es bisher in der Literatur keine klare einheitliche Definition gab[5] und erst recht keine, die in einer Regulatorik verankert war.

Sinn und Zweck der KI-Verordnung

Sinn und Zweck der KI-Verordnung ist es zunächst, einem unkontrollierten Einsatz von KI-Systemen entgegenzuwirken und Diskriminierung, Überwachung und andere mögliche Nachteile insbesondere mit einschneidenden Auswirkungen im Bereich der Grundrechte zu verhindern.[6] Hierbei orientiert sich die Gesetzgebung an einer risikobasierten Herangehensweise (siehe Abbildung 1). Jedes KI-System, auch wenn es nur ein minimales Risiko darstellt, ist danach zu bewerten. So werden gem. Nr. 2.3 in der Begründung der KI-Verordnung auch

Abb. 1. **Eigene Darstellung der Risikoklassen von KI-Systemen orientiert an TÜV AI LAB[7]**



die Transparenzpflichten im Verhältnis zur Risikobewertung entsprechend unterschiedlich weit eingestuft.[8]

Aber die KI-Verordnung soll nicht nur eine Einschränkung sein, sondern auch eine regulatorische Möglichkeit, die Potenziale für Wirtschaft und Gesellschaft voranzubringen. Hierbei soll der Wettbewerb innerhalb der Europäischen Union, aber auch weltweit gestärkt werden.[9]

Zusammenfassend kann festgehalten werden, dass die Verordnung verschiedene Gesichtspunkte der KI-Systeme regelt. Diese sind in Abbildung 2 auf Seite 20 skizziert.

Adressaten der KI-Verordnung

Adressaten der KI-Verordnung sind gem. Art. 2 Abs. 1 lit. a bis c KI-VO

- Anbieter von KI-Systemen,
- Nutzer von KI-Systemen in der EuropäischenUnion aber auch
- Anbieter und Nutzer mit einer Niederlassung in einem Drittland, sofern das Ergebnis durch das KI-System in der Europäischen Union seine Anwendung findet.

Dies kommt dem einen oder anderen vermutlich an dieser Stelle sehr bekannt vor und erinnert an Art. 3 DSGVO. Gemäß Art. 3 KI-VO wird der persönliche Anwendungsbereich noch einmal detaillierter ausgeführt. Danach sind auch

- Händler,
- Einführer von KI-Systemen,
- Anbieter, Bevollmächtigte und Hersteller wie auch
- Betroffene, deren Gesundheit, Sicherheit oder Grundrechte durch die Nutzung eines KI-Systems beeinträchtigt sind, erfasst.[10]

Sanktionen bei Verstoß gegen die KI-Verordnung

Die KI-Verordnung sieht entsprechende Sanktionen und Bußgelder bei einem Verstoß vor. So regelt Art. 71 KI-Verordnung die verschiedenen Bußgeldhöhen, abhängig von der Schwere des Verstoßes.

Hierbei sind drei Bußgeldhöhen bzw. drei Stufen der Sanktionierung definiert:

1. Stufe: In der ersten Stufe gem. Art. 71 Abs. 3 KI-VO liegt der Bußgeldrahmen in Höhe von bis zu 30 Millionen Euro oder bei einem Verstoß durch ein Unternehmen von bis zu 6 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahrs.

2. Stufe: In der zweiten Stufe gem. Art. 71 Abs. 4 KI-VO liegt der Bußgeldrahmen in Höhe von bis zu 20 Millionen Euro oder bei einem Verstoß durch ein Unternehmen von bis zu 4 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahrs.

Abb. 2. **Verschiedene Gesichtspunkte, welche die KI-Verordnung reguliert**

3. Stufe: In der dritten Stufe gem. Art. 71 Abs. 5 KI-VO liegt der Bußgeldrahmen in Höhe von bis zu 10 Millionen Euro oder bei einem Verstoß durch ein Unternehmen von bis zu 2 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahrs.

Welche Verstöße unter welche Stufe fallen, stellt Abbildung 3 auf Seite 21 dar.

Zuständigkeit

Zu unterscheiden ist zwischen Unionsebene und nationaler Ebene.

Auf Unionsebene ist gem. Art. 56 KI-VO i.V.m. ErwGr. 76 der KI-VO angedacht, dass ein europäischer Ausschuss für künstliche Intelligenz errichtet werden soll, der durch Vertreter der Mitgliedstaaten und der Kommission besetzt wird.

So wie im Bereich des Datenschutzes die EDSA[11] soll auch hier der Ausschuss dazu beitragen, dass die Kommission und die nationalen Aufsichtsbehörden zusammenarbeiten und eine wirksame und harmonisierte Durchführung der Verordnung sichergestellt wird.

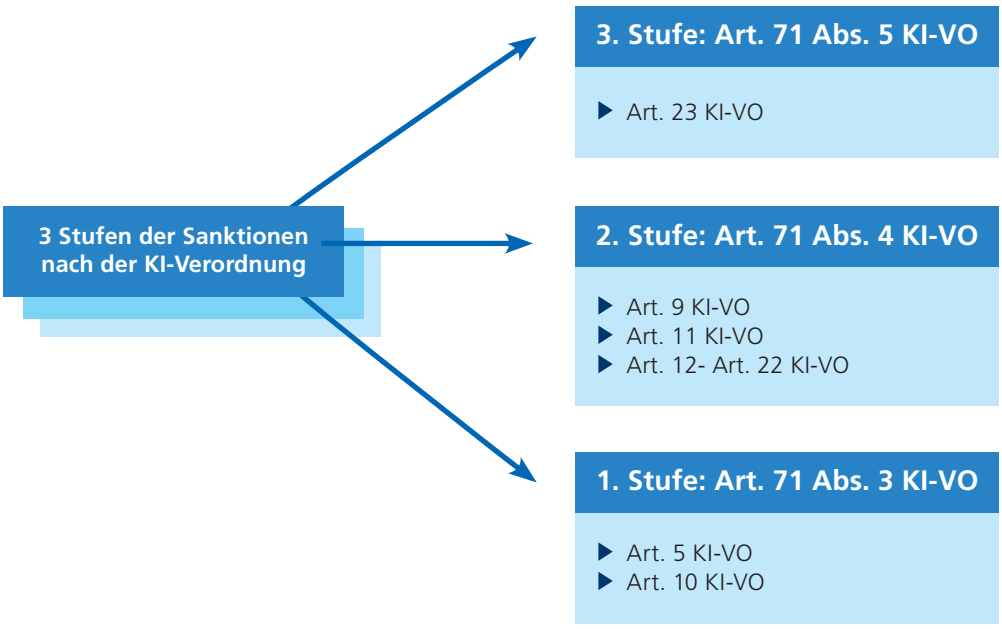
Auf nationaler Ebene sollen gem. Art 59 KI-VO i.V.m. ErwGr. 77 ein oder mehrere nationale zuständige Behörden als sogenannte Aufsichtsbehörden benannt werden, welche zur Aufgabe haben, die Anwendung und Durchführung der Verordnung zu überwachen.

Da der europäische Datenschutzbeauftragte die zuständige Aufsichtsbehörde für die Organe und Einrichtungen der Union ist, stellt sich die Frage, ob auf nationaler Ebene die nationalen Datenschutzaufsichtsbehörden zuständig sein werden. Dies hätte logischerweise zur Folge, dass wir auch in diesem sehr komplexen Gebiet 16 Aufsichtsbehörden mit gegebenenfalls unterschiedlichen Ansichten hätten, was eine Rechtssicherheit erschweren würde.

Eine Besonderheit besteht hinsichtlich des Bankensektors. Hier soll gem. Art. 63 Abs. 4 KI-VO bei KI-Systemen, „die von auf der Grundlage des Finanzdienst-

Derya Isikli
Beauftragte Informationssicherheit & Datenschutz,
E-Mail: derya.isikli@dz-cp.de

Abb. 3. **Drei Stufen der Sanktionen gem. Art. 71 KI-VO**



leistungsrechts der Union regulierten Finanzinstituten in Verkehr gebracht, in Betrieb genommen oder eingesetzt werden, als Marktüberwachungsbehörde für die Zwecke der KI-VO die in jenen Rechtsvorschriften für die Finanzaufsicht über diese Institute benannte Behörde“ gelten.

Auf Deutschland bezogen würde in diesem Fall die BaFin zuständig sein.

Fazit

Die KI-Verordnung stellt einen der ersten fundamentalen Grundsteine für die Regulierung der künstlichen Intelligenz in der EU dar und wird erhebliche Auswirkungen auf die digitalen Geschäfte haben. Nicht nur in der Vertragsgestaltung wird dies zu berücksichtigen sein, sondern auch in der Informationssicherheit und im Datenschutz, bspw. hinsichtlich des Transparenzgrundsatzes (Art 5 DSGVO), der Informationspflichten (Art. 13 ff. DSGVO) oder der technisch-organisatorischen Maßnahmen (Art. 25 DSGVO, Art. 32 DSGVO). Es werden entsprechende interne Kontrollsysteme eingerichtet werden müssen , um zu gewährleisten, dass die KI-Systeme auch rechtskonform mit der KI- Verordnung sind. Ebenso sind Mitarbeiter im Bereich der KI und KI Verordnung zu schulen, damit ein Verständnis und eine Sensibilisierung der Mitarbeiter gegeben ist.

Wann die KI-Verordnung in Kraft tritt, ist noch nicht konkret definiert. Derzeit werden noch Änderungen im Gesetzesentwurf vorgenommen. ▬

[1] Handreichung „Künstliche Intelligenz (KI) in Schule und Unterricht“ | Digitale Schule Hessen (abgerufen am 21.11.2023)

[2] EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu), AI steht für Artificial Intelligence, was mit künstlicher Intelligenz übersetzt werden kann

[3] Kretschmann/ Meutzner (Mai 2023), EU Artificial Intelligence Act: was wird relevant beim Einsatz von KI in Unternehmen?, abgerufen am 21.11.2023 von https://www.elevait.de/blog/eu-ai-act

[4] Contzen / Gresbrand (Juni 2023), „Ein Meilenstein für die KI-Verordnung: Europäisches Parlament stimmt dem neuen Rechtsrahmen für Künstliche Intelligenz zu“, abgerufen am 21.11.2023 von https://www2.deloitte.com/dl/de/pages/legal/articles/ki-verordnung-eu.html

[5] Siehe auch PoC-Artikel, Ausgabe 02/2023, Datenschutzrecht und KI, abrufbar unter: https://www.dz-cp.de/medien/pdf/point-of-compliance/2023/poc_2-2023_gesamtausgabe.pdf

[6] Kaulartz/ Hirzle (August 2023), KI-Verordnung – Die Regulierung generativer KI, abgerufen am 21.11.2023 von https://www.cmshs-bloggt.de/rechtsthemen/kuenstliche-intelligenz/ki-verordnung-die-regulierung-generativer-ki/

[7] Dörfel/Fliehe/Kolf/Komorowski/Schimanko/Schlesinger/Steinbach/Walter, (August 2021), Vorschlag für eine Risikoklassifizierung von KI Systemen, abgerufen am 21.11.2023 von https://www.tuev-verband.de/?tx_epxelo_file[id]=850772&cHash=f1c6c52b992bbfd2b3dd7598fa5477e3

[8] EUR-Lex – 52021PC0206 – DE – EUR-Lex (europa.eu)

[9, 10] Kaulartz/ Hirzle (August 2023), KI-Verordnung – Die Regulierung generativer KI, abgerufen am 21.11.2023 von https://www.cmshs-bloggt.de/rechtsthemen/kuenstliche-intelligenz/ki-verordnung-die-regulierung-generativer-ki/

[11] Europäischer Datenschutzausschuss

Datenschutz-Audit

In einem Datenschutz-Audit wird systematisch überprüft, wie wirksam die Datenschutz-Maßnahmen in einer Bank sind. Alle datenschutzrelevanten Prozesse werden beurteilt, die Stärken, aber auch die Schwächen der Bank identifiziert. In einem zweiten Schritt werden geeignete Maßnahmen herausgearbeitet, um letztlich eine datenschutzrechtliche Konformität zu erlangen.

Zu den Tätigkeiten eines Datenschutz-Auditors gehört neben der Beurteilung des bestehenden Datenschutzniveaus die Bewertung, ob die technischen und organisatorischen Maßnahmen angemessen sind.

Darüber hinaus fällt es in die Zuständigkeit eines Datenschutz-Auditors, das Audit-Programm bzw. die Audit-Methoden zu entwickeln, anhand derer Stichprobenprüfungen und Interviews durchgeführt werden.

Schlussendlich muss er die Kriterien definieren, anhand derer der Betrieb und die fortlaufende Verbesserung des eigenen Datenschutzmanagementsystems sichergestellt werden können.

Das ist eine anspruchsvolle Tätigkeit. Neben der Fachkompetenz, der tiefen Branchenkenntnis und einem breiten Erfahrungshintergrund sollte bei der Wahl des Datenschutz-Auditors immer auch darauf geachtet werden, dass er auf dem aktuellen Stand ist. Wir bilden deshalb alle unsere MitarbeiterInnen beständig weiter. Wir sind stolz auf das Engagement unserer MitarbeiterInnen und fördern es, wo wir können. Diesmal gratulieren wir Derya Isikli und Najat Lissner zum bestandenen Zerifizierungslehrgang „Datenschutz-Auditor“. ▬ (red.)

Von rechtlichen Nuancen bis zu praxisnahen Strategien hat die Schulung meinen Horizont erweitert, stärkt mein Verständnis und befähigt mich, Datenschutz auf eine fundierte Weise zu gestalten. Dies ist für mich als Datenschutzbeauftragte und Auditor eine wertvolle Bereicherung, um meine Mandanten optimal beraten zu können.

Najat Lissner

Durch die DGI-Schulung habe ich weitere nützliche Methoden an die Hand bekommen, um die Sicht eines Prüfers noch besser nachvollziehen zu können. Dies ist im Rahmen der Betreuung meiner Mandantschaft von großem Vorteil, um die entsprechenden Weichen präventiv zu stellen und Überraschungen zu vermeiden.

Derya Isikli

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 genügt den Anforderungen gemäß MaRisk AT 4.4.3 und BT 2.

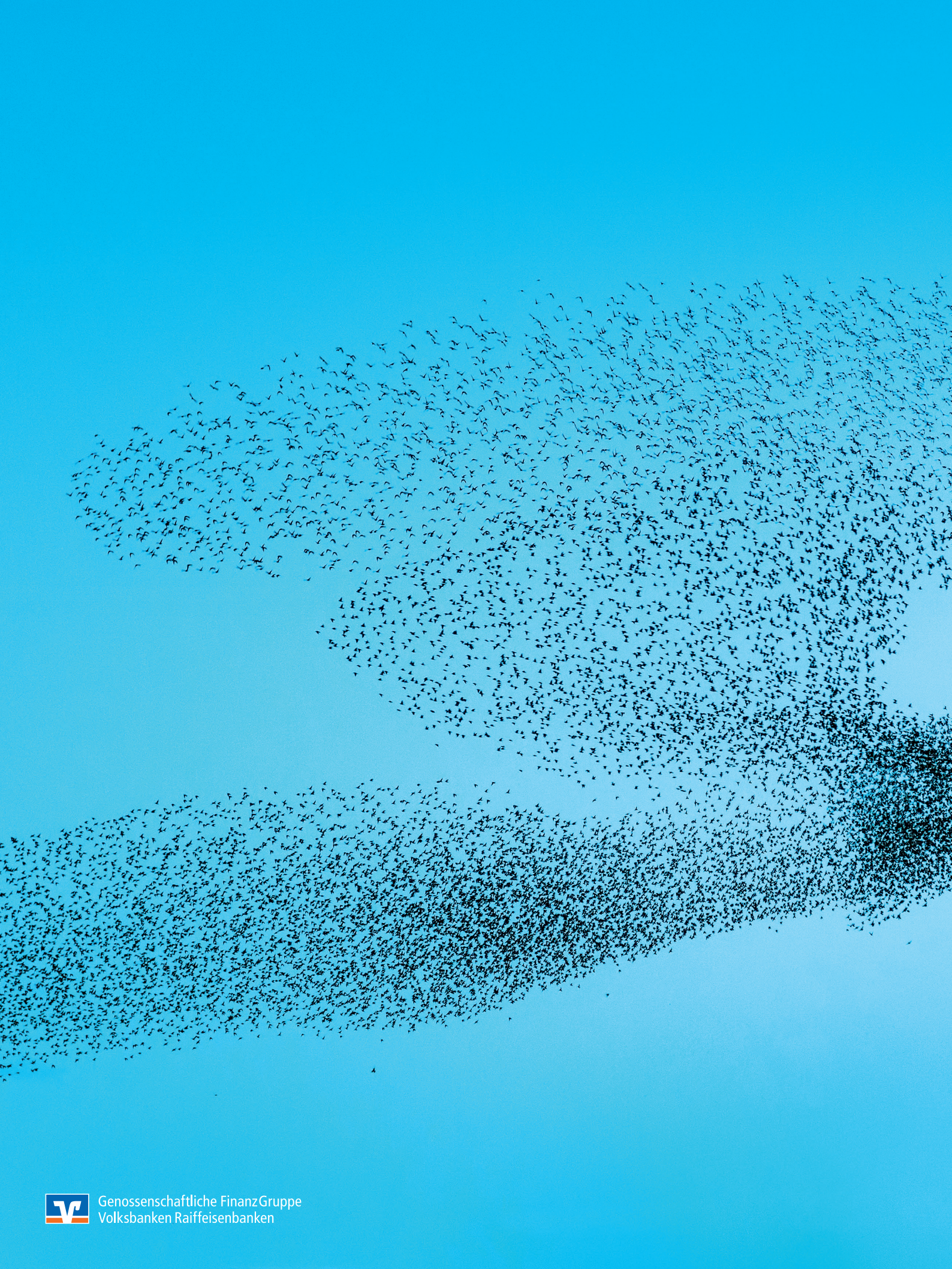
Seit der letzten Berichterstattung in der Point of Compliance (2/2023, S. 31) wurde aus der Jahresprüfungsplanung 2023 die Prüfung des Bereichs „IT & Projekte / IT-Systeme“ abgeschlossen und an alle Kunden versandt. Darüber hinaus wurden die Prüfungen der Bereiche „IT & Projekte – Allgemeine Betriebsorganisation/Dienstleistersteuerung“ und „Unternehmenssteuerung – Rechnungswesen & Controlling“ durchgeführt sowie die Berichte, da nicht dienstleistungsbezogen, intern veröffentlicht.

Der Quartalsbericht zum dritten Quartal 2023 der Internen Revision wurde fristgerecht erstellt und unserer Mandantschaft zur Verfügung gestellt.

Weiterhin wurde turnusgemäß ein Follow-up-Quartalsbericht für das dritte Quartal 2023 erstellt und der Geschäftsführung 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 und der Internen Revision regelmäßige Jours Fixes statt. ▬

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



Genossenschaftliche FinanzGruppe
Volksbanken Raiffeisenbanken