Point of Compliance
Das Risikomanagement-Magazin

AUSGABE 2 / 2023

PoC

DZ CompliancePartner

Folgen Sie DZ CompliancePartner auf Social Media.

IMPRESSUM

PoC – Point of Compliance
Das Risikomanagement-Magazin,
Ausgabe 31, 2/2023
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: Reinhold Gillich, Axel Hofmeister, Derya Isikli, Silke Lenhart, Kevin Lohmann, Michael Maier, Chantal Pfeffer, Jens Saenger, Jörg Schardtzky, Lars Schinnerling, Thomas Schröder, Gabriele Seifert, Sarah-Lena Tiburtius, Benjamin Wellnitz

Bildnachweise: DZ CompliancePartner GmbH, iStock.com/Nuthawut Somsuk
Gestaltung: Ralf Egenolf
Druck: Thoma Druck, Dreieich
Redaktioneller Hinweis: Nachdruck, auch auszugsweise, nur mit ausdrücklicher Genehmigung der Redaktion sowie mit Quellenangabe und gegen Belegexemplar. Die Beiträge sind urheberrechtlich geschützt. Zitate sind mit Quellenangabe zu versehen. Jede darüber hinausgehende Nutzung, wie die Vervielfältigung, Verbreitung, Veröffentlichung und Onlinezugänglichmachung des Magazins oder einzelner Beiträge aus dem Magazin, stellt eine zustimmungsbedürftige Nutzungshandlung dar. Namentlich gekennzeichnete Beiträge geben nicht in jedem Fall die Meinung des Herausgebers wieder. Die DZ CompliancePartner GmbH übernimmt keinerlei Haftung für die Richtigkeit des Inhalts.
Redaktionsschluss: 1. September 2023
Auflage: 2.400 Exemplare

MIX Papier | Fördert gute Waldnutzung FSC® C044135
Druckerzeugnis klimaneutral durch CO2-Ausgleich

„CHEF, NICHTS GEHT MEHR. WIR WURDEN GEHACKT.“

Jens Saenger
Sprecher der Geschäftsführung

Ich gebe es zu, vor diesem Anruf fürchte ich mich. Obwohl wir alles tun, um ein solches Szenario zu vermeiden und im Falle eines Falles handlungsfähig zu sein.

Spätestens mit Corona hat sich das Wirtschaftsleben weitgehend in den digitalen Raum verlagert. Neben den willkommenen Impulsen führte das aber auch dazu, dass wir noch angreifbarer für Cyber-Attacken geworden sind. Der Digitalverband Bitkom weist allein für das Jahr 2022 Cybercrime-Schäden in Höhe von 203 Mrd. Euro aus.

Angesichts dessen erscheint es höchst bedenklich, dass sich laut Bitkom fast jedes zweite Unternehmen nicht ausreichend gerüstet sieht. Gerade weil die Lage bedrohlich ist, gilt es, nicht in Resignation zu verfallen. Auch hier kann das Risiko gemanagt werden: Indem Informationssicherheit mit den notwendigen Ressourcen ausgestattet wird, die Mitarbeitenden sensibilisiert und Notfallpläne erarbeitet werden.

In dieser Ausgabe haben wir einen Schwerpunkt auf betrügerische Aktionen gelegt – und was man dagegen tun kann: aus Sicht der Betrugsprävention (S. 6), aus Sicht des Datenschutzes (S. 13) und vor allem aus der Perspektive der Informationssicherheit (S. 20). Hinter all dem steht die Erkenntnis: Informationssicherheit ist Chefsache, geht aber jeden etwas an.

In diesem Sinne wünsche ich eine anregende Lektüre.

Herzlichst
Ihr Jens Saenger

Strafbare Handlungen und Betrugsprävention – was für die Praxis wichtig ist

Nicht nur systemrelevante Banken, sondern gerade auch Genossenschaftsbanken mit ihrer gelebten Kundennähe und ihrem regionalen Filialnetz sind oft Ziel krimineller Energie. Der folgende Beitrag spiegelt unsere Erkenntnisse aus über 400 Auslagerungsmandaten und gibt praxisbezogen Hinweise zum wirksamen Risikomanagement.

Aufgrund der vielschichtigen mikro- und makroökonomischen Bedeutung wird häufig von der Systemrelevanz bestimmter Banken oder auch der Finanzbranche insgesamt gesprochen.

Angesichts dieser systemischen Bedeutung der Banken als Wohlstandsfaktor sind die gesetzlichen und regulatorischen Anforderungen für den Finanzsektor sehr hoch – insbesondere hinsichtlich der Vorkehrungen, die Banken treffen müssen, um sich vor strafbaren Handlungen zu ihren eigenen Lasten zu schützen.

Auch und gerade Genossenschaftsbanken mit ihrer gelebten Kundennähe und ihrem lokalen und regionalen Filialnetz sind Ziel krimineller Energie. Dies zeigen z. B. die jüngsten Anstiege von Geldautomatensprengungen.

Besondere Relevanz – besondere Anforderungen

Um nicht zu einem Risiko für das Gesamtsystem zu werden, müssen Kreditinstitute gem. § 25h Abs. 1 Kreditwesengesetz (KWG) über ein angemessenes Risikomanagement sowie über Verfahren und Grundsätze verfügen, um strafbare Handlungen abzuwenden, die zu einer Gefährdung ihres Vermögens führen können. Dafür haben sie angemessene geschäfts- und kundenbezogene Sicherungssysteme zu schaffen und zu aktualisieren sowie Kontrollen durchzuführen.

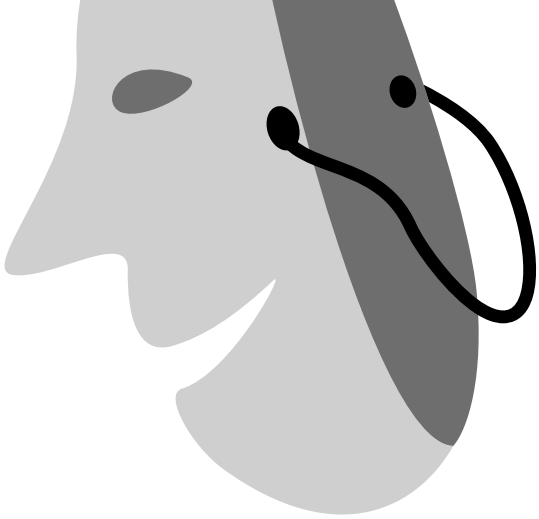
Der Begriff „strafbare Handlungen“, die zu einer (wesentlichen) Gefährdung des Vermögens des Instituts führen können, wurde vom Gesetzgeber bewusst nicht abschließend definiert.

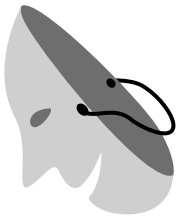
Eine Begriffsbestimmung wurde 2014 zwischen der Deutschen Kreditwirtschaft (DK), dem Bundesministerium der Finanzen und der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) in den damals geltenden Auslegungs- und Anwendungshinweisen vorgenommen.

Nach Sinn und Zweck der Gesetzesvorschrift umfasst der Begriff im Folgenden alle strafbaren Delikte, die zu einer Gefährdung des Vermögens des Instituts führen können. Dies kann durch vorsätzliche Handlungen externer und/oder interner Personen geschehen.

Zu den „strafbaren Handlungen“ im Sinne des § 25h Abs. 1 KWG zählen u. a.:

- Betrugs- und Untreuetatbestände
- Diebstahl
- Unterschlagung
- Raub und räuberische Erpressung
- Insolvenzstraftaten
- Ausspähen und Abfangen von Daten
- Identitätsdiebstahl





Zu einer wesentlichen Gefährdung der Vermögenslage zählen auch Reputationsschäden, die – ausgelöst z. B. durch negative Presseberichte oder (verfälschte) Nachrichten in den sozialen Medien – eine enorme Dynamik entfalten können.

Strafbare Handlung = Motivation + Möglichkeit

Die tatsächliche Ausführung hängt dabei nicht unbeträchtlich davon ab, welche (Gewinn-) Möglichkeiten – hier im Sinne von Erfolgsaussichten – das Ziel bzw. das potenzielle Opfer bietet.

Die Finanzbranche wird praktisch täglich mit strafbaren Handlungen konfrontiert. Das Augenmerk dieses Beitrags liegt – ausweislich der gesetzlichen Regelungen in § 25 KWG – auf den strafbaren Handlungen, die sich originär gegen die Bank richten. In diesen Fällen soll das betroffene Institut durch die strafbare Handlung bewusst und vorsätzlich geschädigt werden. Ein möglicher materieller oder immaterieller Schaden ginge zu Lasten der Bank.

Neben der Frage „Wer ist Ziel der strafbaren Handlung?“ ist im Rahmen der Präventionsmaßnahmen von wesentlicher Bedeutung, wer der Täter ist bzw. ob er oder sie außerhalb oder innerhalb des Unternehmens steht.

Zu den strafbaren Handlungen durch Dritte von außen, die sich gegen die Bank richten, zählen insbesondere:

- Einreichung gefälschter Überweisungsträger oder sonstiger Zahlungsaufforderungen per E-Mail oder Fax von vermeintlichen Kunden, Führungspersonen, Kollegen, Behörden etc.
- Einbruch/Diebstahl
- Konto-/Kartennutzung ohne Deckung
- Kreditbetrug
- Sachbeschädigung von Bankeigentum
- Sprengung/Aufbruch von Geldautomaten/Tresoren/Schließfächern

Strafbare Handlungen durch Dritte von innen (Mitarbeitende) sind häufig:

- Ungerechtfertigte Verfügungen von Konten
- Diebstahl (Wertgegenstände/Tresorinhalte)
- Eröffnung von „Fake-Konten“
- Gewährung von Darlehen ohne ersichtlichen Grund

Präventionsmaßnahmen

Je nachdem, ob strafbare Handlungen gegen eine Bank von internen oder externen Tätern ausgehen, werden verschiedene Abwehr- bzw. Sicherungsmaßnahmen in Kombination, aber mit unterschiedlichen Schwerpunkten eingesetzt.

Straftaten von außen begegnet ein Kreditinstitut insbesondere durch:

- Konsistente und intelligente Zugangsbeschränkungen für sensible Bereiche in der Bank
- Zuverlässige Alarm- und Videoüberwachungssysteme
- Moderne Schutzeinrichtungen für und Sichtprüfungen von Geldautomaten
- Gezielte Vorgaben und Regelungen in Form von Arbeitsanweisungen
- Stringente Kontrollprozesse hinsichtlich eingerichteter Systeme und eingereichter Dokumente
- Systemseitige Unterlegung des Vieraugenprinzips durch entsprechende (EDV-)Kompetenzregelungen
- Regelmäßige Schulung und Sensibilisierung der Mitarbeitenden

Um dolose Handlungen durch interne Täter zu verhindern, werden die meisten der oben aufgelisteten Maßnahmen ebenfalls – ggf. mit anderen Schwerpunkten – eingesetzt. Die besondere Schwierigkeit liegt dabei darin, dass Mitarbeitende die Sicherungssysteme kennen und unter Umständen auszuhebeln wissen.

Das bedeutet aber, dass neben „harten" Sicherungsmaßnahmen weiche Faktoren hinzutreten, die auf den Menschen bzw. die handelnde Person und ihr Verhalten gerichtet sind. Ganz allgemein lässt sich dieser Ansatz unter das Know-your-employee-/Know-your-colleague-Prinzip subsumieren. Dieses Prinzip setzt quasi vor der eigentlichen dolosen Handlung an und zielt auf die Zuverlässigkeit der Mitarbeitenden ab.

Dies beginnt praktisch schon vor der Einstellung von Mitarbeitenden. Die sorgfältige Prüfung eingereichter Bewerbungsunterlagen (Lebenslauf, Zeugnisse) sollte sich zu einem schlüssigen Bild einer Person zusammenfügen.

Die Einreichung und turnusmäßige Aktualisierung des polizeilichen Führungszeugnisses (z. B. nach drei Jahren) sollten im Bankalltag mittlerweile zum Standard gehören. Die Einrichtung eines internen Hinweisgebersystems ist seit 2. Juli 2023 nun ohnehin gesetzlich verpflichtend (hierzu auch unser entsprechender Fachbeitrag zum HinSchG in dieser PoC-Ausgabe).

Faktor Mensch

Von besonderer Bedeutung für die Verhinderung von dolosen Handlungen durch interne Täter ist allerdings das frühzeitige Erkennen von Warnsignalen. Im Einzelfall können diese als vorübergehend betrachtet werden, in regelmäßiger Kombination sollten sie jedoch unbedingt Beachtung und Würdigung finden und konkrete Maßnahmen auslösen.

Insbesondere folgende Typologien können Anzeichen für ein drohendes Fehlverhalten bzw. Gefahrenpotenzial sein.

- Bemerkenswerte Veränderungen im Wesen einer Person
- Grundlegende Veränderung im soziokulturellen Umfeld einer Person
- Häufige Nichteinhaltung von Vereinbarungen
- Vermeidung von (Urlaubs-)Abwesenheiten
- Kenntnis über finanzielle Probleme

Zahlen – Daten – Fakten

Wir haben in der DZ CompliancePartner GmbH als Mehrmandantendienstleister die im Vorjahr an uns gemeldeten Schadensfälle der Banken analysiert. Dabei wurden nur die Fälle berücksichtigt, die die jeweils bankspezifische Bagatellgrenze überschritten haben.

Die dolosen Handlungen lassen sich in folgender absteigender Reihenfolge sortieren.

- Überweisungsbetrügereien (inkl. Phishing)
- Automatensprengungen
- Einbruch
- Unterschlagung durch Mitarbeitende
- Sonstiges

An dieser Stelle besonders wichtig: Wird eine interne Straftat verhindert, wird nicht nur die Bank geschützt. Dem potenziellen Täter kann so auch Hilfe angeboten werden. Ein jähes Karriereende im Strafvollzug wäre nicht nur eine Belastung für den Täter, sondern auch für seine Familie und sein gesamtes persönliches Umfeld.

Unabhängig davon, ob strafbare Handlungen durch interne oder externe Täter verübt werden: Die eingerichteten Sicherungs- und Abwehrmaßnahmen greifen nur dann vollumfänglich, wenn sie durch alle Beteiligten gelebt und umgesetzt werden.

Insofern ist nicht nur die regelmäßige Sensibilisierung und Information der Mitarbeitenden von wesentlicher Bedeutung. Die Bank muss die entsprechende Compliance-Kultur über alle Hierarchiestufen vorleben.

Automatensprengungen

Wie bereits erwähnt, hat die Zahl der Automatensprengungen in den letzten Jahren stark zugenommen. Das Thema wird mittlerweile auch auf hoher politischer Ebene beobachtet und diskutiert. So gab es im Frühjahr dieses Jahres einen „Runden Tisch Geldautomatensprengungen" beim Bundesministerium des Innern. Ebenfalls im Frühjahr startete der BVR eine Umfrage unter den angeschlossenen Instituten. Die wichtigsten in diesen Gremien erarbeiteten Empfehlungen zur Verhinderung/Erschwerung von Automatensprengungen haben wir für Sie aufgelistet.

- Nachtverschluss bei SB-Foyers von 23:00 bis 06:00 Uhr
- Elektronische Überwachung durch qualifizierte Einbruchmeldetechnik
- Einsatz von Nebelsystemen (diese haben sich als besonders gute Schutzmaßnahme erwiesen)
- Einsatz von Einfärbe- und Klebesystemen
- Mechanische Schutzmaßnahmen
- Videoüberwachung
- Reduktion des Bargeldhöchstbestandes
- Standortwahl (Risikoanalyse der „Kommission Polizeiliche Kriminalprävention")

Technische Unterstützung durch Monitoring- und Fraud-Systeme

Die in bzw. für die Banken eingesetzten Monitoring- und Fraud-Systeme sind programmiert, um strafbare Handlungen – ob von intern oder extern – aufzudecken und zu verhindern. Diese technischen Unterstützungen sind flankierende Maßnahmen. Nicht jede Straftat kann im Vorfeld durch ein EDV-System oder Künstliche Intelligenz erkannt werden. Beispielhaft sei hier die nächtliche Automatensprengung genannt.

Dennoch runden Monitoring- und Fraud-Systeme das gesamte Maßnahmenpaket eines internen Kontrollsystems ab.

Fazit

Die Kreditwirtschaft hat in einer modernen Volkswirtschaft eine Schlüsselrolle. Daher wird häufig von der Systemrelevanz einzelner Banken bzw. der Branche an sich gesprochen.

Aufgrund dieser Sonderstellung sind die regulatorischen Anforderungen an die internen Sicherungsmaßnahmen in den Banken besonders hoch und auch gesetzlich verankert. Banken sind regelmäßig mit krimineller Energie von außen, aber auch von innen konfrontiert.

Basis für ein gut funktionierendes internes Kontrollsystem sind eine gelebte Compliance-Kultur und die schlüssige Kombination technischer und organisatorischer Sicherungsmaßnahmen. Nicht zuletzt haben die Sensibilisierung und Schulung der handelnden Personen besonderes Gewicht. ▬

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

Hinweisgeberschutzgesetz

Zum 2. Juli 2023 ist das lang erwartete Hinweisgeberschutzgesetz in Kraft getreten. Als Umsetzungsgesetz der entsprechenden EU-Richtlinie dient es dem Schutz von Personen, die Verstöße gegen das Unionsrecht melden. Wir geben eine Übersicht über die neuen Vorgaben und die damit verbundenen Pflichten und erläutern, was nun zu tun ist.

Um es vorwegzunehmen: Die aufsichtsrechtlichen Verpflichtungen zur Einrichtung einer Meldestelle z. B. nach KWG, GwG bleiben bestehen und gelten unverändert fort.

Das Hinweisgeberschutzgesetz (HinSchG) regelt den Schutz von Personen, die im Rahmen ihrer beruflichen Tätigkeit Informationen über Verstöße erlangt haben und diese an Meldestellen weitergeben möchten. Das Gesetz legt daher fest, welche Sachverhalte an Meldestellen gemeldet werden können, wie diese Meldestellen auszugestalten sind, welche Arten von Meldestellen künftig existieren und wie ein Verfahren abzulaufen hat.

Meldesachverhalte und Definitionen

Zu den wichtigsten Informationen, die gem. § 2 HinSchG an die Meldestellen gemeldet werden können, zählen

- Verstöße, die strafbewehrt sind,
- Verstöße, die bußgeldbewehrt sind, soweit die verletzte Vorschrift dem Schutz von Leben, Leib oder Gesundheit oder dem Schutz der Rechte von Beschäftigten oder ihrer Vertretungsorgane dient,
- sonstige Verstöße gegen Rechtsvorschriften des Bundes und der Länder sowie unmittelbar geltende Rechtsakte der Europäischen Union und der Europäischen Atomgemeinschaft (z. B. Bekämpfung von Geldwäsche und Terrorismusfinanzierung, Vorgaben zur Produktsicherheit, Vorgaben zur Sicherheit im Straßenverkehr, Umweltschutz, Regelung der Verbraucherrechte und des Verbraucherschutzes, Schutz personenbezogener Daten, Verstöße, die von § 4 Abs. 1 Satz 1 FinDAG erfasst sind, und viele mehr).

Verstöße sind jedoch gem. § 3 Abs. 2 HinSchG nur solche Handlungen oder Unterlassungen, die im Rahmen einer beruflichen, unternehmerischen oder dienstlichen Tätigkeit erfolgen und dabei rechtswidrig sind oder dem Ziel und Zweck der Regelungen zuwiderlaufen, die in den sachlichen Anwendungsbereich des Gesetzes fallen.

Beschäftigte sind nicht nur ArbeitnehmerInnen und arbeitnehmerähnliche Personen, sondern auch die zu ihrer Ausbildung Beschäftigten.

Für hinweisgebende Personen besteht ein Wahlrecht zwischen interner und externer Meldung. Wurde einer internen Meldung nicht abgeholfen, kann sich die hinweisgebende Person auch an eine externe Meldestelle wenden. Aus § 7 Abs. 3 HinSchG ergibt sich die Vorgabe, dass Anreize geschaffen werden sollen, damit sich hinweisgebende Personen zuerst an die interne Meldestelle wenden. Interne Meldestellen sind die selbst oder durch Dritte ausgestalteten Stellen. Externe Meldestellen hingegen sind beim Bund angesiedelt, z. B. beim Bundesamt der Justiz oder der BaFin.

Sowohl für hinweisgebende Personen als auch für Personen, die Gegenstand einer Meldung sind, sowie die sonstigen in der Meldung genannten Personen besteht gem. § 8 HinSchG das Vertraulichkeitsgebot. Die Meldestellen haben somit die Vertraulichkeit der Identität der gerade genannten Personen zu wahren. Das Gebot gilt im Übrigen unabhängig davon, ob die Meldestelle für die eingegangene Meldung überhaupt zuständig ist.

In § 4 HinSchG wird festgelegt, dass spezifische Regelungen über die Mitteilung von Informationen über Verstöße dem HinSchG vorgehen. Hierzu zählen z. B. die Meldeverfahren nach §§ 6 Abs. 5 und 53 GwG, § 25a Abs. 1 Satz 6 Nr. 3 KWG, § 13 Abs. 1 WpIG.

Dokumentation

Die Meldestellen dokumentieren alle eingehenden Meldungen in dauerhaft abrufbarer Weise unter Beachtung des Vertraulichkeitsgebots. Bei telefonischen Meldungen gilt es zu beachten, dass eine Tonaufzeichnung oder ein Wortprotokoll nur mit Einwilligung der hinweisgebenden Person erfolgen darf. Liegt eine solche Einwilligung nicht vor, ist die Meldung in Form eines Inhaltsprotokolls zu dokumentieren. Zusätzlich ist der hinweisgebenden Person Gelegenheit zu geben, das Protokoll zu prüfen, ggf. zu korrigieren und zu bestätigen.

Eine Löschung der Dokumentation erfolgt drei Jahre nach Abschluss des Verfahrens. Eine Abweichung hiervon ist nur gem. § 11 Abs. 5 HinSchG möglich.

Meldestellen

Private Beschäftigungsgeber müssen gem. § 16 Abs. 3 HinSchG interne Meldestellen einrichten, die es ermöglichen, Hinweise in mündlicher oder in Textform anzugeben. Zudem ist auf Wunsch der hinweisgebenden Person eine persönliche Zusammenkunft zu ermöglichen, die auch im Wege einer Bild- und Tonübertragung erfolgen kann. Wichtig ist zu beachten, dass anonyme Meldungen bearbeitet werden sollten. Es besteht jedoch keine Verpflichtung, die Meldekanäle so zu gestalten, dass sie die Abgabe anonymer Meldungen ermöglichen.

Die mit der Aufgabe der internen Meldestelle betrauten Personen sind bei der Ausübung der Tätigkeit unabhängig. Die Wahrnehmung anderer Aufgaben und Pflichten ist zulässig, es darf jedoch nicht zu Interessenskonflikten kommen. Zudem ist dafür Sorge zu tragen, dass die beauftragten Personen über die notwendige Fachkunde verfügen.

Verfahren nach Hinweiseingang

Geht bei einer internen Meldestelle ein Hinweis ein, beginnt ein Verfahren mit bestimmten Anforderungen nach § 17 HinSchG:

- Eingangsbestätigung an hinweisgebende Person spätestens nach sieben Tagen
- Überprüfung, ob gemeldeter Verstoß in den sachlichen Anwendungsbereich fällt
- Kontakthalten mit der hinweisgebenden Person
- Stichhaltigkeit der eingegangenen Meldung überprüfen
- Bei Bedarf weitere Informationen von hinweisgebender Person erfragen
- Folgemaßnahmen ergreifen

Zudem hat die interne Meldestelle der hinweisgebenden Person innerhalb von drei Monaten nach der Eingangsbestätigung eine Rückmeldung zu geben. Diese enthält die Mitteilung geplanter oder bereits ergriffener Folgemaßnahmen und die Gründe hierfür. Interne Nachforschungen oder Ermittlungen dürfen hierdurch nicht berührt werden. Auch dürfen die Rechte der betroffenen Personen nicht beeinträchtigt werden.

Als Folgemaßnahmen kommen gem. § 18 HinSchG insbesondere in Betracht:

- Interne Untersuchungen und Kontaktaufnahme mit betroffenen Personen
- Verweisung der hinweisgebenden Person an eine andere Stelle
- Abschluss des Verfahrens aus Mangel an Beweisen oder aus anderen Gründen
- Abgabe des Verfahrens zwecks weiterer Untersuchungen an eine für interne Ermittlungen zuständige Arbeitseinheit oder eine zuständige Behörde

Was ist zu tun?

Die gerade genannten Aspekte sind die aus unserer Sicht wichtigsten Anforderungen und Regelungen des neuen Gesetzes. Zusammenfassend ergeben sich somit folgende Pflichten zur Umsetzung der neuen Anforderungen.

Umsetzungspflichten
Die wichtigsten Vorgaben und Umsetzungspflichten sind:
- Einrichtung einer internen Meldestelle, entweder selbst oder durch Beauftragung eines Dritten
- Meldungen müssen in telefonischer oder Textform ermöglicht werden

Umsetzungsfristen
Die Vorgaben des Gesetzes sind von privaten Beschäftigungsgebern mit mehr als 249 Mitarbeitern und den in § 12 Abs. 3 HinSchG genannten Beschäftigungsgebern mit Inkrafttreten des Gesetzes umzusetzen.

Private Beschäftigungsgeber mit in der Regel 50 bis 249 Arbeitnehmern müssen ihre internen Meldestellen erst zum 17. Dezember 2023 einrichten.
Kreditinstitute sind von § 12 Abs. 3 Nr. 4 HinSchG erfasst und somit zur sofortigen Umsetzung verpflichtet.

Die Bußgeldvorschrift für die fehlende Einrichtung und den fehlenden Betrieb einer internen Meldestelle findet zum 1. Dezember 2023 Anwendung.

Jetzt handeln

Ein Hinweisgebersystem, das lange als notwendiges Übel galt, stellt in der heutigen Zeit eine Chance dar. Ein unabhängiges Hinweisgebersystem zeugt von einer transparenten und fairen Unternehmenskultur. Zudem ist der präventive Effekt hervorzuheben. Ein gut funktionierendes Hinweisgebersystem hat bei potenziellen Tätern eine abschreckende Wirkung.

Wir bieten Ihnen ein faires und zertifiziertes Hinweisgebersystem, das neben den Pflichten des KWG auch die Pflichten des Hinweisgeberschutzgesetzes abbildet. Informationen dazu finden Sie auf unserer Homepage (untenstehender QR-Code). ▬

https://www.dz-cp.de/geldwaesche-und-betrugspraevention/hinweisgebersystem

Sarah-Lena Tiburtius
Beauftragte Hinweisgebersystem,
E-Mail: sarah-lena.tiburtius@dz-cp.de

Datenschutz und KI – Wunschdenken?

Buzzwords wie ChatGPT, OpenAI, DALL-E 2 sorgten in den letzten Monaten für großes Aufsehen. Auch im Bankensektor ist Künstliche Intelligenz nicht mehr wegzudenken. Doch was ist Künstliche Intelligenz eigentlich? Und ist eine datenschutzkonforme Anwendung überhaupt möglich?

Die digitalen und physischen Bereiche der Industrie und Wirtschaft vernetzen sich immer weiter und intensiver aufgrund der rasanten Entwicklung der Technik und der unaufhaltsamen Dynamik der Digitalisierung. Dabei spielt der Einsatz der Künstlichen Intelligenz zunehmend eine signifikante Rolle in der Industrie 4.0, Wirtschaft und im Alltag eines jeden. Auch im Bankensektor hat Künstliche Intelligenz einen nicht mehr wegzudenkenden Platz eingenommen. Doch Künstliche Intelligenz ist weit vielschichtiger, als gemeinhin angenommen wird. Und – die Frage, ob eine datenschutzkonforme Anwendung möglich ist, muss differenziert beantwortet werden.

Prozesse werden immer mehr in autonome Systeme verlagert. Hierfür benötigen die Maschinen Daten und Information, auf die sie zurückgreifen können.

Gleichzeitig ist der Schutz der Daten in Deutschland und zumindest ganz Europa eine hochsensible Thematik.

Mit Hinblick auf die am 24. Mai 2016 in Kraft getretene und seit Mai 2018 wirksam anzuwendende europäische Datenschutzgrundverordnung und das neue Bundesdatenschutzgesetz stellt sich daher die Frage, inwieweit der Einsatz von Künstlicher Intelligenz rechtlich, unter Betrachtung der europäischen Datenschutzgrundverordnung und des Bundesdatenschutzgesetzes, möglich ist.

Durch die Komplexität der Systeme wird die Einhaltung der Ziele der Datenschutzgrundverordnung (DSGVO) jedoch schwierig. Kernprobleme sind u. a. die Einhaltung der Transparenzanforderungen der europäischen Datenschutzgrundverordnung sowie die Nachvollziehbarkeit, was konkret mit den persönlichen Daten im Netz und im System dahinter passiert. Doch was ist Künstliche Intelligenz?

Eine eindeutige Definition gibt es in der Wissenschaft nicht. Grund hierfür ist, dass sich der Begriff seit der Begriffsbildung Ende der 50er Jahre als interdisziplinäre Forschungsrichtung entwickelt. Dadurch passt sich die Begriffsdeutung an die immer weiter fortschreitenden technischen Möglichkeiten an.[1]

Künstliche Intelligenz (kurz KI) lässt sich als ein Teilgebiet der Informatik beschreiben, das sich mit der Erforschung von intelligentem menschlichem Verhalten befasst[2] und versucht, dieses zu adaptieren.[3]

Die Künstliche Intelligenz ist somit die „Erforschung eines intelligenten Problemlösungsverhaltens und die Erstellung von intelligenten Computersystemen".[4]

Welche Arten von Künstlicher Intelligenz gibt es?

Grundsätzlich kann man die Künstliche Intelligenz in vier Bereiche einteilen.[5] Die Einstufung bemisst sich dabei nach der Stärke der Künstlichen Intelligenz.

1. **Rein reaktive KI (reactive machine)[6]**
   Das System erkennt seine Umwelt und reagiert entsprechend darauf. Da es keinerlei Vorstellung von seiner Umwelt und auch keine Gedächtnisfunktion hat, um auf diese Erlebnisse in seiner Handlung zurückgreifen zu können, stellt es den Basis-Typ dar. In der Regel ist diese Form der KI darauf programmiert, eine ganz bestimmte Aufgabe zu erfüllen. Somit ist sie keine selbstlernende KI.

Beispiele hierfür sind IBMs Deep Blue, Schachcomputer, der lediglich mit Hilfe von Algorithmen bestmöglichst Schach spielen kann, oder auch das digitale Brettspiel AlphaGo von Google.[7]

2. Systeme mit begrenztem Gedächtnis (limited memory)

Wie bereits die Bezeichnung beschreibt, hat diese Form der Künstlichen Intelligenz ein Gedächtnis, das jedoch begrenzt ist. Sie kann Erfahrungen der Vergangenheit in die vorprogrammierte Darstellung ihrer Umwelt integrieren und ist nicht nur auf eine Aufgabe begrenzt.

Jedoch werden trotz begrenzter Speicherkapazität große Mengen von Daten verarbeitet. Bei dieser Art wird über Machine Learning die KI mit Daten gefüttert. Über neuronale Netze und durch überwachtes Lernen kann sie dann eine große Menge an Daten und Vorgehensweisen entwickeln. Jedoch kann sie nur auf begrenzte Informationen zurückgreifen.

Beispiele hierfür sind Sprachassistenten wie Siri oder OK-Google. Diese Sprachassistenten können aufgrund eines Sprachbefehls Informationen aus dem Internet suchen, Kalender verwalten oder einfach Handlungen ausführen wie die Telefonwahl. Auch beim autonomen Fahren handelt es sich um eine KI der zweiten Art, da sie neben den Verkehrsregeln auch auf unerwartete Situationen im Straßenverkehr reagieren kann. Auch Chat-GPT gehört in diese Kategorie, da sie im Vergleich zur dritten Art keine Emotionen verstehen und verarbeiten, geschweige denn etwas fühlen kann.

3. Systeme mit eigenem Bewusstsein (theory of mind)

In dieser Kategorie handelt es sich bereits um die nächste Stufe der Künstlichen Intelligenz. Diese Form der KI kann Emotionen, Absichten und Gedanken verstehen, sich ein eigenes Bild der Umwelt machen und entsprechend interagieren.

Diese Art von KI existiert derzeit noch nicht. Jedoch wären Beispiele für diese Kategorie der KI der knuffige Roboter R2-D2 oder sein goldener Freund C-3PO aus dem Filmklassiker Star Wars.

4. Sich „ihrer selbst" bewusste Systeme (self-aware)

Diese Art der selbstbewussten KI hat ein umfassendes Verständnis von sich selbst und kann über das hinausgehen, wofür sie ursprünglich entwickelt wurde. Sie verfügt über eine Superintelligenz, Empathie und Bewusstsein. Ihr äußeres Erscheinungsbild ist vom Menschen nicht mehr zu unterscheiden. Auch diese Form der KI existiert derzeit lediglich in Science-Fiction-Filmen wie M3GAN oder Ex Machina.

Ist KI nun mit geltendem Datenschutz vereinbar?

Eine KI benötigt, um effizient eingesetzt werden zu können, Daten. Dies teilweise in nicht geringen Mengen. (Wie eine Künstliche Intelligenz im Grundsatz funktioniert, wird in einem gesonderten Artikel in einer der nächsten PoC-Ausgaben ausführlich erörtert.)

Um der Angst entgegenzuwirken, ein sogenannter gläserner Kunde zu sein und durch die vermeintliche Datensammelwut die Kontrolle über die eigenen Daten zu verlieren, bedarf es eines klaren rechtlichen Rahmens und der Transparenz gegenüber der betroffenen Person.[8]

Aufgrund des hohen Stellenwerts der DSGVO und der steigenden Relevanz von Künstlicher Intelligenz, insbesondere für Wirtschaftsunternehmen, ist deren Zusammenspiel und die gesetzeskonforme Begutachtung der überschneidenden Themenbereiche von signifikanter Bedeutung.

Dabei ist zwischen zwei Phasen der datenschutzrechtlichen Begutachtung der Künstlichen Intelligenz zu unterscheiden. In der ersten Phase geht es um die Generierung von Künstlicher Intelligenz auf Grundlage von automatisierten Big-Data-Analysen (Analysen von großen Datamengen). Die zweite Phase beinhaltet die tatsächliche Implementierung von Künstlicher Intelligenz im Alltag, wie beispielsweise durch digitale Assistenten und automatisierte Entscheidungssysteme (vgl. Abb. 1[9]).

Beim Einsatz von KI, bei der personenbezogene Daten verarbeitet werden, handelt es sich um den Einsatz einer neuen Technologien. Daher bestehen kaum gerichtliche Entscheidungen oder Leitlinien. Es ist daher auch zu beachten, dass der Einsatz solcher Systeme stets mit einem Risiko verbunden ist.

Beispielsweise stellt sich die Frage, wer als Verantwortlicher eines eingesetzten KI-Systems gilt. Dies ist in der Regel derjenige, der das System in die unternehmensinternen Prozesse integriert und daher über den Zweck und die Mittel der Datenverarbeitung gem. Art. 4 Nr. 7 DSGVO entscheidet. Doch was ist mit dem Anbieter des KI-Systems? In den meisten Fällen erfolgt die Datenverarbeitung auf den Servern des Anbieters. Daher liegt es nahe, dass es

Abb. 1. **Zwei Phasen der KI bzw. automatisierten Entscheidung im Einzelfall**

Quelle: eigene Darstellung

sich hierbei um eine Auftragsdatenverarbeitung gem. Art. 28 DSGVO handelt. Dabei sollte durch den Verantwortlichen vor Abschluss geprüft werden, ob der Auftragsdatenverarbeiter die zugesicherten technisch-organisatorischen Maßnahmen auch tatsächlich einhalten kann. Das ist wichtig, da auch die Anbieter einen bestimmten Teil des KI-Sytems nicht selbst beherrschen können – Stichwort Blackbox.

Werden jedoch die durch die KI-Systeme erhobenen Daten für die Weiterentwicklung des Systems genutzt, könnte dies die Grenzen der Auftragsdatenverarbeitung verlassen und der Anbieter selbst, je nach Fallkonstellation, als Verantwortlicher oder aber auch als gemeinsam mit dem Anwender Verantwortlicher einzuordnen sein. Hieran sind weitere rechtliche Probleme gekoppelt, weshalb bei einer Vertragsanbahnung die datenschutzrechtliche Fachexpertise des Datenschutzbeauftragten unentbehrlich ist.

Für eine datenschutzkonforme Verarbeitung von personenbezogenen Daten durch KI-Systeme kommt in der Regel die Rechtsgrundlage der Einwilligung gem. Art 6 Abs. 1 lit. a DSGVO in Betracht.

Eine Begründung der Verarbeitung auf der Rechtsgrundlage des berechtigten Interesses gem. Art 6 Abs. 1 lit. f DSGVO ist aufgrund des sehr hohen Risikos der Verarbeitung durch KI-Systeme und der überwiegenden Interessen der Betroffenen häufig nicht gegeben.

Ein weiterer Punkt ist die Informationspflicht gem. Art. 13 DSGVO. Hierbei ist neben den bekannten Informationspflichten aber auch die Informationen über automatisierte Entscheidungsfindung gem. Art 22 DSGVO einzuhalten.

Gleichzeitig besteht die Pflicht, geeignete Prozesse zu haben, um als Betroffener die Ansprüche gem. der DSGVO auch ausführen zu können. In Anbetracht der Komplexität der KI wird es beispielsweise schwer sein, eine vollständige Löschung der Daten durchsetzen zu können, ohne dabei das Modell zu beeinträchtigen: Die Daten sind direkt in das KI-Modell eingeflossen und haben dieses verändert.[10]

Fraglich ist auch, inwieweit der Grundsatz des Transparenzgebotes gem. Art 5 DSGVO eingehalten und gelebt werden kann.

Transparenz i.S.v. Art. 5 DSGVO setzt nach dem Erwägungsgrund 58 der DSGVO grundsätzlich voraus, dass eine Information präzise, leicht zugänglich und verständlich ist und ggf. zusätzliche und verständliche visuelle Elemente eingesetzt werden.[11]

Der Grundsatz der Transparenz wird hinsichtlich der Gestaltung und des Verfahrens der Informationspflicht durch Art. 12 Abs. 1 DSGVO konkretisiert.[12] Damit werden durch Art. 12 DSGVO formale Anforderungen an die Informationspflichten aus Art. 13 ff. DSGVO normativ festgelegt.

Dies bedeutet für die Anwendung von KI-Systemen, dass nicht nur die Datenverarbeitungsprozesse und die Logik der datenbasierten Entscheidungen für die betroffene Person nachvollziehbar[13], sondern auch die Trainingsdaten leicht zugänglich und stringent im Sinne des Art. 12 Abs. 1 Satz 1 DSGVO sein müssen.[14] Somit muss der Betroffene beim Einsatz von personenbezogenen Daten für KI-Systeme auch darüber informiert werden: Erst durch diese Mitteilung kann der Betroffene selbst entscheiden, ob er einen solchen Dienst nutzen möchte oder nicht.

Dabei gilt für die Beschreibung der Verarbeitung nicht, dass tiefgreifende und ausführliche Informationen über den Verarbeitungsprozess erfolgen müssen.[15] Es sind viel-

mehr wesentliche, prägnante und beschränkte Erläuterungen gefordert, ohne den objektiven Empfänger zu überfordern.[16]

Hinsichtlich der auf Künstlicher Intelligenz basierenden Entscheidungen wird eine Datenschutzfolgeabschätzung jedoch nicht unproblematisch sein, da insbesondere bei selbstlernenden Prozessen die Risikoreichweite kaum bis überhaupt nicht abschätzbar ist.[17] Es wird jedoch grundsätzlich immer eine Datenschutzfolgeabschätzung erfolgen müssen.

Fazit

Zusammenfassend ist festzuhalten, dass eine datenschutzrechtskonforme Anwendung von sogenannten „schwachen" KI-Systemen (siehe oben „reactive machine" und „limited memory") nicht ausgeschlossen ist. Jedoch stellt sie Unternehmen gleichzeitig vor große Herausforderungen, die durch die DSGVO derzeit nicht völlig gelöst sind. Es bleibt daher offen, inwiefern eine KI-Verordnung dem Einsatz von KI-Systemen eine rechtliche Sicherheit geben kann.

Auch angesichts der wirtschaftlichen und gesellschaftlichen Bedeutung von algorithmenbasierten Entscheidungen und der rasanten Entwicklung der technischen Möglichkeiten, wird die Bedeutung von automatisierten Entscheidungen auch in Zukunft immer stärker zunehmen. So wird auch die DSGVO, in Anbetracht der fortschreitenden Technik, sich weiterentwickeln und weiter auslegen lassen müssen.

Dies ist ein Zeichen dafür, dass mit Blick in die Zukunft und angesichts der Entwicklungsprognose der Technik der Künstlichen Intelligenz mehr Raum eingeräumt werden muss. ▬

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

[1] Bitkom, Künstliche Intelligenz – Wirtschaftliche Bedeutung, gesellschaftliche Herausforderung, menschliche Verantwortung, 2017, S. 28 ff.

[2] Gruhn, Volker, Künstliche Intelligenz verleiht Cyber Physical Systems Flügel, in: Industrie 4.0 Management 34, Jg. 2018, S. 45-48 (45)

[3] Söbbing, Thomas, Fundamentale Rechtsfragen zur künstlichen Intelligenz (AI Law), Frankfurt am Main, dfv Mediengruppe 2019, S. 3

[4] Andresen, Maja (21. Oktober 2019), Wie funktioniert Künstliche Intelligenz, abgerufen am 25.08.2023 von https://www.zeitakademie.de/elearning/wie-funktioniert-kuenstliche-intelligenz/

[5] Möhring, Cornelia, Diese vier Arten von KI gibt es, auf Heise.de, abgerufen am 25.08.2023 von https://www.heise.de/tipps-tricks/Diese-vier-Arten-von-KI-gibt-es-9076579.html

[6] Dusold, Julia (10. Dezember 2019), Künstliche Intelligenz verständlich erklärt, abgerufen am 25.08.2023 von https://www.produktion.de/technik/kuenstliche-intelligenz-verstaendlich-erklaert-243.html#wiefunktioniert-kuenstliche-intelligenz

[7] Leichsenring, Dr. Hansjörg, Vier unterschiedliche Arten Künstlicher Intelligenz – Infografik, auf Der Bank Blog, abgerufen am 25.08.2023 auf https://www.der-bank-blog.de/typologie-kuenstliche-intelligenz/technologie/29269/

[8] Bitkom, Künstliche Intelligenz – Wirtschaftliche Bedeutung, gesellschaftliche Herausforderung, menschliche Verantwortung, 2017, S. 35.

[9] Gausling, Tina, Künstliche Intelligenz und DSGVO, in: DSRITB 2018, S. 519-545 (526)

[10] Globocnik in: ActiveMind.AG: Künstliche Intelligenz (KI) und Datenschutz, abgerufen am 21.08.2023 von https://www.activemind.de/magazin/kuenstliche-intelligenz/

[11] BeckOK DatenschutzR/ Spoerr, 32. Ed. 01.05.2020, DS-GVO Art. 26, RN 28,29

[12] Strassemeyer, Laurenz, Datenschutzrechtliche Transparenz von Algorithmischen Entscheidungen und Verarbeitungen mittels Gamification, Ablaufdiagramme und Piktogramme, in: Taeger, Jürgen (Hrsg.), Die Macht der Daten und Algorithmen – Regulierung von IT, IoT und KI, DSRI, Deutsche Stiftung für Recht und Informatik, München, Oldenbourg Verlag, 2019, S. 34

[13] DSGVO Fluch oder Segen für Europas Wettrennen um Künstliche Intelligenz? Erschienen Algorithmenethik 18.Oktober 2019 / Pierre Adrien Hanania, Dr. Nikolai Horn, Dr. Tobias Knobloch, abgerufen am 25.08.2023 von https://algorithmenethik.de/2019/10/18/datenschutzgrundverordnung-fluch-oder-segen-fuereuropas-wettrennen-um-kuenstliche-intelligenz/

[14] Hambacher Erklärung zur Künstlichen Intelligenz, Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörde des Bundes und der Länder, Hambacher Schloss 3. April 2019// So auch Erwägungsgrund 39 zur DSGVO

[15] Eßer in: Eßer/ Kramer/ von Lewinski, DSGVO/ BDSG, Köln, Carl Heymann Verlag, 6. Auflage, 2018, Art. 12 Rn. 6

[16] Strassemeyer, Laurenz, Datenschutzrechtliche Transparenz von Algorithmischen Entscheidungen und Verarbeitungen mittels Gamification, Ablaufdiagramme und Piktogramme, in: Taeger, Jürgen (Hrsg.), Die Macht der Daten und Algorithmen – Regulierung von IT, IoT und KI, DSRI, Deutsche Stiftung für Recht und Informatik, München, Oldenbourg Verlag, 2019, S. 36

[17] Conrad, C.S., Künstliche Intelligenz – Die Risiken für den Datenschutz, DuD 2017, S. 744

Schadensersatzansprüche

Kann bei Datenschutzverletzungen ein Schadensersatzanspruch bestehen? Wie ist der Schadensersatz gem. Art. 82 DSGVO zu verstehen – insbesondere bzgl. des immateriellen Schadensersatzanspruches? Und kann neben dem Schadensersatz gem. Art. 82 DSGVO auch zivilrechtlicher Schadensersatzanspruch bestehen?

Bei Datenschutzrechtsverstößen können neben Bußgeldern auch Schadensersatzansprüche drohen. Dieser Anspruch auf Schadensersatz ist in Art. 82 DSGVO geregelt.

Schadensbegriff

Der Schadensbegriff ist in der DSGVO nicht legaldefiniert. Die Vorschriften des internationalen Privatrechts sind hierbei zu beachten (siehe Art. 40 ff. EGBGB).

Der zivilrechtliche Schadensersatzanspruch gem. § 280 Abs. 1 BGB, § 823 Abs. 1 und 2 BGB i.V.m. der DSGVO nach Art. 82 DSGVO ist getrennt zu betrachten.[1]

Im öffentlichen Dienst wäre u.a. auch ein zivilrechtlicher Schadensersatzanspruch aus Art. 34 GG i.V.m. § 839 BGB nicht auszuschließen, dürfte jedoch in der Praxis Privatunternehmen (Banken, Versicherungsunternehmen etc.) nicht tangieren.

Im Gegensatz zum zivilrechtlichen Verfahren, bei dem das Verschulden durch den, der den Sachverhalt vorträgt, zu beweisen ist, gilt hinsichtlich der DSGVO eine Beweislastumkehr. Das bedeutet, dass der Verantwortliche bzw. Auftragsverarbeiter i.S.d. DSGVO beweisen muss, dass er einen Datenschutzverstoß nicht begangen hat (siehe hierzu Art. 82 Abs. 3 DSGVO). Dies resultiert u.a. aus der Rechenschaftspflicht gem. Art. 5 Abs. 2 DSGVO.

Anwendbarkeit des Art. 82 DSGVO

Ein Schadensersatzanspruch kann gem. Art. 82 Abs. 1 DSGVO für materielle und immaterielle Schäden, die durch einen Datenschutzrechtsverstoß entstanden sind, bestehen. Voraussetzung für die Anwendbarkeit des Art. 82 DSGVO ist, dass

1. ein Datenschutzverstoß gem. Art. 4 Nr. 2 DSGVO gegenüber der natürlichen Person vorliegt,
2. ein Verschulden seitens des Verursachers (Verantwortlicher oder Auftragsverarbeiter) vorliegt,
3. gem. Art. 82 Abs. 1 DSGVO ein Schaden entstanden ist (vgl. hierzu Erwägungsgrund 75 und 85 der DSGVO) und
4. der Schaden ursächlich (kausal) auf die/den Datenschutzverletzung/-verstoß zurückzuführen ist.

Gemäß Erwägungsgrund 146 Satz 6 der DSGVO „sollten die betroffenen Personen einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhalten". Materielle Schäden sind durch die objektiv feststellbare Schadenshöhe gem. Erwägungsgrund 146 Satz 6 der DSGVO leicht herleitbar.

Fraglich ist, ob jede Datenschutzverletzung – unabhängig von der Schwere – den Ersatz immaterieller Schäden zur Folge haben kann.

Immaterielle Schäden

Bezüglich immaterieller Schäden kann der Erwägungsgrund 143 Satz 6 der DSGVO die Frage nicht klären. Dies liegt daran, dass die „Vollständigkeit" der Schadenshöhe sich in diesem Kontext nicht objektivieren lässt. Damit vor dem Hintergrund des Effektivitätsgebots („effet utile") ein wirksamer und abschreckender Schadensersatz gewährleistet ist, steht den Mitgliedsstaaten ein weiterer Ermessensspielraum zu. Dabei ist das Gewicht der Rechtsverletzung sowie der objektive Umfang angemessen zu beachten. Von Bedeutung ist die Offenlegung personenbezogener Daten gegenüber Dritten ohne Einverständnis der betroffenen Person. In diesem Zusammenhang wird die materielle Entschädigung der öffentlichen „Bloßstellung" herangezogen.[2]

Das Landesgericht Feldkirch in Österreich beschäftigte sich mit einem möglichen Datenschutzverstoß hinsichtlich der Sammlung und Auswertung von Daten (u. a. Adressen und demografische Daten) von Bürgern in Österreich seitens der Österreichischen Post. Die Auswertung mittels eines Algorithmus hatte zum Ziel, eine Präferenz für politische Parteien zu ermitteln.

Das Landesgericht Feldkirch in Österreich stellte in seinem Urteil v. 7.8.2019 (Az.: 57 Cg 30/19b - 15) fest, dass der Art. 82 Abs. 1 DSGVO keine Erheblichkeitsschwelle für immaterielle Schäden definiert. Unter Erheblichkeitsschwelle versteht man eine Überschreitung von einzelfallbewerteten „Schadens-Grenzen", die lediglich bedeutsame Schäden berücksichtigen sollen. Weiterhin sind laut der Urteilsbegründung „nicht alle Unlustgefühle, die mit einer Rechtsverletzung verbunden sind, ersatzfähig, sondern muss der Interessenbeeinträchtigung ein Gewicht zukommen, weil dem österreichischen Schadenersatzrecht eine solche Erheblichkeitsschwelle immanent ist."[3]

Gerichtsurteile innerhalb der EU auf mitgliedsstaatlicher Ebene sind gleichrangig zu betrachten. Folglich hatte das Urteil des Landesgerichts Feldkirch eine gewisse Signalwirkung.

Zu einer ähnlichen Auffassung kommt das OLG Frankfurt/M. (Urteil v. 2.2.2022 – 13 U /206/20, Falschversand einer E-Mail an unbeteiligte Dritte im Rahmen eines Bewerbungsprozesses): Es muss bei der Datenschutzverletzung zu einem „tatsächlich erlittenen" Schaden für die betroffene Person gekommen sein, der entsprechend nachweisbar ist. Ferner sieht das OLG einen weiteren Hinweis im Erwägungsgrund 148 Satz 2 DSGVO, dass bei geringfügigen Verstößen eine Verwarnung ausgesprochen werden kann.[4]

Sehr weit hat jüngst das Arbeitsgericht Oldenburg in seinem Teilurteil vom 9.2.2023, Az. 3 Ca 150/21, ausgelegt, in dem u. a. ein immaterieller Schadensersatzanspruch einer verspäteten Auskunftserteilung auf ein Auskunftsersuchen gem. Art. 15 Abs. 3 DSGVO eines ehemaligen Mitarbeiters Gegenstand der Prüfung war. Das Arbeitsgericht Oldenburg sieht den Schadensersatzanspruch gem. Art. 82 Abs. 1 DSGVO als Präventivnorm: „Bereits die Verletzung der DS-GVO selbst führe zu einem auszugleichenden immateriellen Schaden. Denn der Schadenersatzanspruch nach Art. 82 Abs. 1 DS-GVO habe präventiven Charakter und diene der Abschreckung, so das ArbG unter Berufung auf das Bundesarbeitsgericht."[5]

Wenn man diverse Urteile vergleicht, zeigt sich, dass nicht jeder Datenschutzverstoß – unabhängig von seiner Schwere – den Ersatz immaterieller Schäden zur Folge gehabt hat. Häufig wurden mögliche erlittene Schäden dahingehend geprüft, ob „sogenannte Bagatellschäden" vorliegen „bzw. eine Erheblichkeitsschwelle nicht überschritten ist". Bisher war die Rechtsprechung jedoch nicht einheitlich, so dass mehr Klarheit erst durch eine Prüfung des Europäischen Gerichtshofes (EuGH) herbeigeführt werden konnte.[6]

Jüngst hat der EuGH zu dem Fall des Landesgerichts Feldkirch in Österreich (Sachverhalt siehe oben, Urteil v. 7.8.2019, Az.: 57 Cg 30/19b – 15) Stellung genommen.

Laut dem Urteil des EuGHs (Dritte Kammer) vom 4.5.2023 (Az.: C-300/21) sind hinsichtlich der Anwendung des Art. 82 Abs. 1 DSGVO entsprechende Voraussetzungen erfüllt (siehe oben). Des Weiteren sieht bei Vorliegen aller Voraussetzungen hinsichtlich der Anwendbarkeit des Art. 82 Abs. 1 DSGVO der EuGH keine Erheblichkeitsschwelle.[7] Folglich besteht keine Bagatellgrenze.

In der Praxis stellt diese Feststellung des EuGHs zum immateriellen Schadensersatz eine weiter gefasste Anwendung dar. Weitere Urteile des EuGHs sind u. a. durch vorliegende Vorlageverfahren C-590/22[8] und C-456/22[9] zu erwarten.

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

Fazit

Zusammenfassend lässt sich feststellen, dass bei Vorliegen von Datenschutzverletzungen gem. Art. 4 Nr. 12 DSGVO i.V.m. Art. 33, 34 DSGVO sowie anderweitiger Datenschutzverstöße (z. B. verspätete Auskunftserteilung auf ein Auskunftsersuchen gem. Art. 15 Abs. 3 DSGVO) nicht nur Bußgelder gem. Art. 83 DSGVO drohen, sondern – neben dem zivilrechtlichen Schadensersatz – auch ein separater materieller sowie immaterieller Schadensersatzanspruch gem. Art. 82 DSGVO bestehen kann. Der EuGH hat den immateriellen Schadensersatzanspruch bisher weit ausgelegt, so dass keine Bagatellgrenzen bestehen. ▬

[1] Isfen/Kreße/Wick, Rechte der betroffenen Personen I und Datenschutzbeauftragte/r, Fernuniversität Hagen, Hagen 2022, S. 67 f

[2] hIsfen/Kreße/Wick, Rechte der betroffenen Personen I und Datenschutzbeauftragte/r, Fernuniversität Hagen, Hagen 2022, S. 71 f

[3] https://www.datenschutz.eu/urteile/800-EUR-Schadensersatz-wegen-unerlaubter-DSGVO-Verarbeitung-Landgericht-Feldkirch-20190807/, abgerufen am 25.03.2023

[4] OLG Frankfurt/M., Urteil v. 02.02.2022 – 13 U /206/20

[5] https://rsw.beck.de/aktuell/daily/meldung/detail/arbg-oldenburg-immaterieller-schadensersatz-wegen-verletzung-des-ds-gvo-auskunftsanspruchs, abgerufen am 12.08.2023

[6] A. Galius in: Datenschutzpraxis 03/2023, S. 1 ff

[7] EuGH, Urteil v. 04.05.2023 - Az.: C-300/21 https://curia.europa.eu/juris/document/document.jsf?text=&docid=273284&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1, abgerufen am 12.08.2023

[8] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:62022CN0590&from=EN, abgerufen am 12.08.2023

[9] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:62022CN0456, abgerufen am 12.08.2023

Awareness gegen Cyber-Attacken

Jeden Tag erreichen uns über die verschiedensten Medien Mitteilungen und unterschiedlichste Nachrichten (Xing, LinkedIn usw.) über Cyber-Attacken. Neben monetären und Reputationsschäden kommt es dabei vor allem zu Daten- und Informationsverlusten. Die Frage ist: Wie kann es sein, dass Dritte die an sich hohen Sicherheitsvorkehrungen einer Bank überwinden?

Bei den Daten- und Informationsverlusten kann es sich sowohl um vertrauliches unternehmensbezogenes Datenmaterial als auch um Daten von Mitarbeitern und dritten Personen handeln. Begründeter Weise drängt sich die Frage auf, wie so etwas denn überhaupt passieren kann. Schließlich sind komplexe Sicherheitsvorkehrungen mittlerweile gelebte Praxis. So gehören in Organisationshandbüchern umfangreiche Passwortrichtlinien und Schulungskonzepte ebenso zum Standard wie technisch hoch entwickelte Firewalls und ein kontinuierliches Patchmanagement.

Hinter all den technischen Sicherheitsvorkehrungen gibt es eine weitere Verteidigungslinie, die durch die Mitarbeitenden selbst gebildet wird. So schützt jeder Mitarbeiter seinen Arbeitsplatz beispielsweise mit seinem individuellen Passwort, das kein anderer kennt und das auch niemandem gegenüber kommuniziert werden darf. Doch der Alltag sieht anders aus: Der Administrator möchte Ihre Benutzerdaten; Sie geben diese weiter. Doch tatsächlich war der „Administrator“ nicht „Ihr“ Administrator von Ihrer Bank. Und: Der wahre Administrator würde auch niemals nach Ihrem Passwort fragen. Bereits diese kleine Unachtsamkeit reicht aus, um den Datenhaushalt einem unkalkulierbaren Risiko auszusetzen. Dass so etwas nur „jemand anderem“ passieren kann, ist leider ein weit verbreiteter Irrtum.

Der unerwartete Moment, die kleine Unaufmerksamkeit

Die hoch technologisierten und entwickelten Sicherheitsvorkehrungen können nicht alle Einfallstore für Kriminelle absichern. Das ist diesen sehr bewusst und sie nutzen diese Tatsache zu ihrem Vorteil. So wie technische Schwachstellen direkt angegriffen werden, wird auch der kleinste Moment der menschlichen Unachtsamkeit direkt ausgenutzt. Ein greifbares Beispiel ist der Straßenverkehr. Hier wissen wir, wie oft und wie schnell man sich ablenken lässt und kurz unachtsam wird. Auch hier kann ein kleiner Moment entscheidend sein.

Dieser kleine, kurze und unerwartete Moment macht uns angreifbar. Damit repräsentiert er den Hauptaktionsbereich der Awareness. Awareness bedeutet in diesem Sinne, dass sich Banken und insbesondere die Mitarbeitenden ein Bewusstsein für diesen kurzen Moment der Unachtsamkeit und die damit verbundenen Risiken erarbeiten und nachhaltig etablieren. Awareness heißt damit nichts anderes als die Schärfung des Bewusstseins für betrügerische Handlungen.

Dieses Bewusstsein ist durch entsprechende Maßnahmen aktiv zu schaffen und einzuüben. Im BSI Standard 200-4, der sich mit dem Business Continuity Management (BCM) befasst, welches sich mit Notfall- und Krisensituationen beschäftigt, heißt es dazu: „Zudem erhalten sie In-

formationen direkt von Führungskräften sowie im Rahmen von Schulungen und Awareness-Maßnahmen."

Eine Frage der Unternehmenskultur

In der Folge wird ersichtlich, wie eng Awareness-Maßnahmen und Notfallmanagement zusammenhängen und wie wichtig es ist, dass beide Bereiche fester Bestandteil der Unternehmenskultur werden:

Sowohl BCM als auch Awareness betreffen grundsätzlich das gesamte Institut und haben in Konsequenz Auswirkungen auf jeden Mitarbeiter. Auch thematisch sind die bestehenden Notfallprozesse mit den Notfallübungen und den daraus resultierenden nachhaltigen Awareness-Maßnahmen und -Prozessen eng zu verzahnen. So sollte auch die Personalabteilung bei allen Entscheidungen und Maßnahmen im Kontext BCM involviert werden, die wesentlichen Einfluss auf die Rechte und Pflichten der Mitarbeiter haben. Daneben kann das Personalmanagement bei der Planung von Schulungen und Awareness-Maßnahmen unterstützen, um die Integration in die Kultur der Institution zu erhöhen.

Auch in einem anderen Informationssicherheitsstandard, der ISO/IEC 27001, Maßnahme A 7.2.2, ist Folgendes niedergeschrieben:

„Alle Beschäftigten der Organisation und, wenn relevant, Auftragnehmer, bekommen ein angemessenes Bewusstsein durch Ausbildung und Schulung sowie regelmäßige Aktualisierungen zu den Richtlinien und Verfahren der Organisation, die für ihr berufliches Arbeitsgebiet relevant sind."

Regelmäßige Übungen, Schulungen und insbesondere regelmäßige Informationen an die Mitarbeitenden sind also unerlässliche Maßnahmen, die in der Bank verankert sein müssen.

Im Rahmen einer Dreijahresplanung ist ein jährlicher Übungsplan aus unserer Sicht unerlässlich.

Schlussendlich sind in der BAIT II Tz. 4.9 folgende Regelungen und Maßnahmen dokumentiert:

„Weiterhin ist innerhalb der Bank durch ein kontinuierliches und zielgruppenorientiertes Sensibilisierungs- und Schulungsprogramm das Bewusstsein der Beschäftigten für Informationssicherheit zu schärfen und dabei insbesondere auf die Eigenverantwortung sowie auf die grundsätzlichen Vorkehrungen und Regelungen der Bank einzugehen."

Über alle Regelungen, Vorschriften und Empfehlungen ist zusammenfassend zu sagen, dass es in Zukunft eine ganzheitliche, prozessuale und individuelle Planung der Awareness-Maßnahmen benötigt. Diese Maßnahmen sind zentral zu installieren, durchzuführen, zu messen und schlussendlich zu überwachen.

Eine Bank benötigt demnach ein ganzheitliches Maßnahmenprogramm, das alle Themeninhalte berücksichtigt und dabei insbesondere den Menschen in den Fokus setzt. Denn tatsächlich sind 95 % aller Cybersicherheitsvorfälle auf menschliche Unachtsamkeit zurückzuführen (Quelle: World Economic Forum – The Global Risks Report 2022).

AwarenessCircle

Die Aufgabe ist also, technologisierte Prozesse in Einklang mit den Anwendern und deren Aufmerksamkeit zu bringen – und zwar dauerhaft bzw. wiederkehrend. Diese Anforderungen aufnehmend haben wir – basierend auf unseren Erfahrungen bei 180 Mandaten im Bereich Informationssicherheit/Notfallmanagement – eine ganzheitliche und nachhaltig wirkende Lösung aufgebaut, den AwarenessCircle. Unsere Herangehensweise sieht kurz erläutert wie folgt aus:

1. Security-Awareness-Plattform:

- Inbetriebnahme der Plattform in Absprache mit dem Kunden
- Durchführung der individuellen Maßnahmen durch individuelle Schulungspakete
- Auswertung nach definierbaren Gruppen in der Bank und Vergleich mit Benchmark-Gruppen
- Einbeziehung ISB und Berichtserstellung für die Quartalsberichte unserer Kunden
- Laufende Unterstützung und Nachhalten der Maßnahmen in der Bank

2. Awareness-Paket Mitarbeiter

- Halbtages Workshop in der Bank
- Schulung der Mitarbeitenden oder individueller Abteilungen
- Bei Bedarf Abgleich der Notfallplanung mit den abgeleiteten Awareness-Maßnahmen
- Erstellung einer dreijährigen Awareness-Planung
- Sensibilisierungsmaßnahmen von bestimmten Bereichen nach Absprache mit der Bank. Es ist zu beachten, dass knapp 30 % der Angriffe über E-Mails erfolgen; weitere knapp 40 % erfolgen über das Telefon.

Bleibt noch anzumerken, dass alle hier aufgeführten Awareness-Maßnahmen ergänzende bzw. weiterführende Maßnahmen sind, die zusätzlich zu den bisherigen Aufgaben der Informationssicherheit umzusetzen sind.

Zusammenfassend liegt das Thema Awareness im ureigenen Schutzinteresse der Bank, ist spätestens mit den neuen BAIT aber auch verpflichtend umzusetzen. Es gilt, nachhaltige Prozesse für Awareness in der Bank zu schaffen. Damit verbindet sich das Ziel, das Risiko für Cyber-Attacken deutlich zu minimieren – und zwar indem die notwendige Bewusstheit und Aufmerksamkeit zum Alltag aller Mitarbeitenden gemacht wird. ▬

Chantal Pfeffer
Abteilungsleiterin
Informationssicherheit & Datenschutz,
E-Mail: chantal.pfeffer@dz-cp.de

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

MaRisk-Novelle 2023

Die BaFin hat Ende Juni 2023 das Rundschreiben 05/2023 (BA) – Mindestanforderungen an das Risikomanagement veröffentlicht und damit die 7. Novellierung der MaRisk abgeschlossen. Im folgenden Artikel geben wir Ihnen einen Überblick zu den Schwerpunkten und Änderungen.

Schwerpunkte

Folgende Schwerpunkte setzt die 7. MaRisk-Novelle:

- Überführung der EBA-Leitlinien für Kreditvergabe und überwachung in die MaRisk
- Umfassende Integration von ESG-Risiken
- Das „Immobiliengeschäft“ als neues Modul BTO 3

Verweistechnik

In den MaRisk werden nun auch weitere Vorgaben zur Kreditvergabe und -überwachung aus den EBA/GL/2020/06 übernommen. Aufgrund der Detailtiefe der EBA/GL/2020/06 hat die Aufsicht auf eine vollständige Integration derselben in die MaRisk verzichtet. Bei der Implementierung der EBA/GL hat die Aufsicht vielmehr einen differenzierten Weg gewählt: zum einen Verweise auf die EBA/GL, zum anderen Ergänzungen des Textes der MaRisk.

Verweise kommen in der Regel dann zum Einsatz, wenn der jeweilige Abschnitt neben Klarstellungen auch neue Anforderungen enthält. Ergänzungen werden hingegen gewählt, wenn der bisherige Regelungstext die wesentlichen Vorgaben aus den Leitlinien bereits enthält. Bei den Ergänzungen wird der Text der MaRisk hinsichtlich der Anforderungen oder Klarstellungen lediglich ergänzt mit der Folge, dass die Vorgaben der EBA/GL danach vollständig implementiert sind.

Durch diese differenzierte Vorgehensweise bei der Implementierung der EBA/GL konnte die Aufsicht die Komplexität in der Umsetzung etwas verringern.

Inhalte aus den BA/GL/2020/06

Hinsichtlich einzelner Abschnitte der EBA/GL und deren Übernahme in die MaRisk verhält es sich wie folgt:

- Abschnitt 4 betreffend interne Governance zur Kreditvergabe und -überwachung wird durch Übernahme einzelner Formulierungen in die MaRisk integriert.
- Abschnitt 5 betreffend Verfahren zur Kreditvergabe unterscheidet konkret nach einzelnen Kreditnehmerarten, Art der Besicherung und Finanzierung unter Berücksichtigung von Verbraucherschutzzielen. Die Einbindung in die MaRisk erfolgt mittels Verweistechnik.
- Abschnitt 6 beschäftigt sich mit der risikoorientierten Bepreisung. Da schon in den MaRisk entsprechende Vorgaben vorhanden waren, wird das Modul BTO 1.2 Tz. 9 lediglich ergänzt.
- Abschnitt 7 macht Vorgaben für die Bewertung von Sicherheiten zum Zeitpunkt der Kreditaufnahme sowie zur Überwachung und Neubewertung. In BTO 1.2 Tz. 2 und BTO 1.2.2 Tz. 3 Erl. erfolgt eine Verweisung auf die EBA/GL/2020/06.
- Der 8. Abschnitt enthält Vorgaben an die laufende Überwachung des Kreditrisikos. Neuerungen sind nur in einzelnen Abschnitten enthalten, u.a. in BTO 1.2.2 Tz. 2 mit Verweis auf die EBA-Leitlinien für die Kreditvergabe und Überwachung des Abschnittes 8.3 (Regelmäßige Überprüfung der Kreditnehmer).

Die BaFin stellt klar, dass, wenn in den EBA-Leitlinien von „sollte“ die Rede ist, ist, diese Formulierung so auszulegen, dass die zugrundeliegende Anforderung verbindlich einzuhalten ist („es ist sicherzustellen“). Ebenso sind die Begriffe „Kreditgewährung“ (KWG) und „Kreditvergabe“ (EBA) inhaltsgleich.

Verwendung von Modellen – AT 4.3.5

Das neue Modul AT 4.3.5 regelt die Anwendung, Datenqualität, Validierung und Erklärbarkeit der Modelle, die im Risikomanagement der Säule II verwendet werden, einschließlich der Künstlichen Intelligenz. Klarstellungen im Vergleich zum Konsultationsentwurf betreffen die Aussage, dass Modelle, die in den CRR-Anwendungsbereich fallen, nicht Gegenstand des AT 4.3.5 sind, und Hinweise zur Proportionalität in AT 4.3.5 Tz. 1 und Tz. 6.

Immobiliengeschäft – BTO 3

Mit dem neuen Modul reagiert die BaFin auf die Investitionen von Banken in Immobilien, um dem noch im letzten Jahr herrschenden Niedrigzinsumfeld sowie dem Ertrags- und Konkurrenzdruck zu begegnen. Im Vergleich zur Konsultation wurde der Schwellenwert von 10 Mio. Euro aller Immobiliengeschäfte auf 30 Mio. Euro der Buchwerte bzw. 2 % der Bilanzsumme der Bank hochgesetzt. Als Immobiliengeschäfte werden Geschäfte auf eigene Rechnung definiert, mit denen die Bank das Ziel der Ertragsgenerierung durch späteren Verkauf oder Vermietung erreichen will. Es werden Vorgaben zur Aufbau- und Ablauforganisation gemacht, die ähnlich denen des Kreditgeschäftes sind (z. B. Trennung Markt und Marktfolge, Kompetenzordnung, Wirtschaftliche Analysen).

Umfasst von der Regelung des BTO 3 sind Direkterwerbe, bei denen das Institut die Objekte im eigenen Namen erwirbt, Investitionen über Tochtergesellschaften, die vom Institut als Beteiligung gehalten werden, sowie Rettungserwerbe. Ausgenommen vom Anwendungsbereich des BTO 3 sind eigengenutzte Immobilien, die überwiegend dem eigenen Geschäftsbetrieb dienen, und Immobilienfonds, die im Depot A gehalten werden.

Geschäftsmodellanalyse

An verschiedenen Stellen in den neuen MaRisk finden sich Ausführungen zur Geschäftsmodellanalyse, so u.a. in AT 4.1 Tz. 1, Tz. 11. Im Gegensatz zu den SREP-Leitlinien der EBA existiert diesbezüglich kein eigenes Modul, sondern es werden Ausführungen an verschiedenen Stellen der MaRisk gemacht. Neu ist u. a. die Aussage, dass die Kapitalplanung des Instituts sowohl mit seiner operativen Geschäftsplanung und deren strategischen Grundlagen als auch mit dem Geschäftsmodell im Einklang stehen muss.

Homeoffice

Homeoffice bzw. häusliches Arbeiten bei Handelsaktivitäten ist mit den neuen MaRisk dauerhaft zugelassen. Der häusliche Arbeitsplatz wird in BTO 2.2.1 Tz. 3 Erl. definiert. Um im Homeoffice arbeiten zu können, muss das Institut die Vertraulichkeit der den Geschäftsabschlüssen zugrundeliegenden Daten anhand geeigneter Richtlinien sicherstellen. Auch müssen die Vorgaben bzgl. der Stabilität der Abwicklungs- und Bestätigungssysteme und die Anforderungen an die IT grundsätzlich den vergleichbaren Anforderungen wie dem Handel in den Geschäftsräumen entsprechen. Auch muss eine ausreichende Präsenz der Händler in den Geschäftsräumen sichergestellt sein.

Für Geschäftsabschlüsse im Homeoffice gilt, dass diese unverzüglich in geeigneter Form dem eigenen Institut anzuzeigen und dem für den Handel zuständigen Geschäftsleiter bzw. einer von ihm autorisierten Organisationseinheit zur Kenntnis zu bringen sind, sofern die Handelsgeschäfte nicht direkt in einem Abwicklungssystem der Bank erfasst werden. Neu ist auch, dass sämtliche Geschäftsabschlüsse außerhalb der Geschäftsräume einem handelsunabhängigen Bereich zur Kenntnis zu bringen

sind und nicht mehr dem zuständigen Geschäftsleiter. Auch wurde für kleine Institute mit nur einem oder zwei Händlern eine Erleichterung aufgenommen: sie müssen hier zumindest für angemessene Vertretungsregeln sorgen oder Regelungen für den Wechsel vom häuslichen Arbeitsplatz in die Geschäftsräume treffen.

ESG-Risiken

ESG-Risiken sind spätestens seit dem Jahr 2019 aus dem BaFin-Merkblatt zum Umgang mit Nachhaltigkeitsrisiken bekannt. Nun haben ESG-Risiken auch formal Eingang in die MaRisk gefunden, wobei der Fokus auf den Umweltrisiken liegt.

In AT 2.2 Tz. 1 Erl. werden Nachhaltigkeitsrisiken ausführlich im Sinne von Environment-, Social- und Governance-Risiken beschrieben. Institute sollen Szenarien nutzen, die im Einklang mit wissenschaftlichen Erkenntnissen stehen. Hierzu können Szenarien von allgemein anerkannten Institutionen bzw. Netzwerken (die beispielhaft aufgeführt werden) genutzt und auf das eigene Geschäftsmodell adaptiert werden. Aus Sicht der Aufsicht ist es nicht zielführend, wenn Institute selbst Annahmen zum Klimawandel bzw. zur Transition hin zu einer nachhaltigen Wirtschaft treffen würden, die sich außerhalb der Bandbreite seriöser wissenschaftlicher Forschung bewegen.

ESG-Risiken wirken sich auf alle wesentlichen Risiken einer Bank aus. Dementsprechend geht die BaFin von einer Einbeziehung der ESG-Risiken in das gesamte Risikomanagement der Bank aus und erwartet eine Analyse und Dokumentation der potenziell negativen Auswirkungen. Betroffen von den ESG-Risiken sind u. a. die Risikoinventur, Stresstests und Szenarioanalysen, das Risikotragfähigkeitskonzept, die Strategie, das Limitsystem sowie das Risikoklassifizierungsverfahren bis hin zum Berichtswesen.

Proportionalität

An verschiedenen Stellen der MaRisk spiegelt sich die Proportionalität wider. Es beginnt bei der Implementierung der EBA/GL in die MaRisk. In dem in AT 1 Tz. 3 MaRisk verankerten Proportionalitätsprinzip wird ausdrücklich auf die Verhältnismäßigkeitskriterien in Tz. 16 lit. a-d der EBA/GL/2020/06 verwiesen. Demnach kommt es nicht allein auf die Eigenschaften eines Instituts wie Art, Größe und Komplexität an, sondern zukünftig werden auch Kriterien wie Art, Umfang und Komplexität der Kreditfazilität berücksichtigt. Bei den Verfahren zur Kreditvergabe (Abschnitt 5) und hier speziell bei der Finanzierungsart kommt es nur noch eingeschränkt auf die Größe des Instituts an.

Bei den Anforderungen an die Modelle, AT 4.3.5 MaRisk, finden sich in Tz. 1 und 6 Ausführungen zur Proportionalität. Dementsprechend haben die Institute die Anforderungen des Moduls proportional zu der Bedeutung des jeweiligen Modells im Risikomanagement, seiner Komplexität und etwaigen Risiken anzuwenden.

Bei den ESG-Risiken – und hier speziell bei der Wahl von Szenarien und der Festlegung des Betrachtungszeitraums – kommt dem Proportionalitätsprinzip eine hervorgehobene Rolle zu.
Je nachdem, wie kleinere Institute ESG-Risiken ausgesetzt sind, können sie die Anzahl der verschiedenen Szenarien beschränken, hinsichtlich der Komplexität ein reduziertes

Szenario wählen oder vereinfachte Folgewirkungen anwenden, die Bandbreite an Folgewirkungen vereinfachen bzw. für langfristige Betrachtungen einen ausschließlich qualitativen Ansatz wählen.

Trotz dieser wiederholten Proportionalitätserwägungen haben die neuen MaRisk nun eine Komplexität erreicht, die insbesondere für kleinere Institute nur schwer zu erfüllen ist. Es bleibt abzuwarten, ob und wie die MaRisk zukünftig ausgestaltet werden.

Bedeutende Förderbanken

Die für bedeutende Institute geltenden Vorgaben aus AT 4.4.1 Tz. 5 zur Risikocontrolling-Funktion und aus AT 4.4.2 Tz. 4 zur Compliance-Funktion gelten nun auch für große Förderbanken. Eine Förderbank ist groß, wenn ihre Bilanzsumme zu den jeweiligen Stichtagen der letzten vier Geschäftsjahre 70 Mrd. Euro überschritten hat, § 2 Abs. 9i Satz 2 KWG.

Übergangsfristen: Klarstellung und Neuerung

Wie in der Vergangenheit auch, gilt bei der aktuellen Novelle, dass Klarstellungen mit der Veröffentlichung (29.06.2023) in Kraft treten. Neuerungen sind ab dem 1. Januar 2024 umzusetzen. Nach Mitteilung der BaFin sind Vorgaben, die erst durch den Regelungstext der EBA-Leitlinien eingeführt werden, Neuerungen.

Folgende Neuerungen sind in den MaRisk vorhanden:

- Modul 4.3.5 – Verwendung von Modellen
- Modul BTO 3 – Immobilien
- AT 2.2 Tz. 1 Erl. – Berücksichtigung von ESG-Risiken
- AT 4.1 Tz. 1 sowie Tz. 2 Erl. – Risikotragfähigkeit: Berücksichtigung von ESG-Risiken und ESG-Risiken in der normativen und ökonomischen Perspektive
- AT 4.3.3. Tz. 1 – Stresstest und Berücksichtigung von ESG-Risiken
- AT 4.5 Tz. 5 – Risikomanagement auf Gruppenebene: Identifikation wesentlicher Risikoträger und explizite Berücksichtigung von ESG-Risiken
- BTO 1.2 Tz. 4 – Anforderungen an das Kreditgeschäft: Beurteilung des Adressenausfallrisikos – die Auswirkungen von ESG-Risiken sind zu berücksichtigen, es ist ein angemessen langer Zeitraum zugrunde zu legen.
- BT 3.1 Tz. 1 – Berücksichtigung von ESG-Risiken in den Risikoberichten
- BT 3.2 Tz. 1 Erl. – Berücksichtigung von ESG-Risiken über einen angemessen langen Zeitraum im Gesamtrisikobericht der Risikocontrolling-Funktion

Die Ergänzungen der Anforderungen an die Geschäftsmodellanalyse enthalten nur Klarstellungen, die ohne Übergangsfrist zu beachten sind. Die Regelungen zum Homeoffice sind zwar neu, bringen für die Institute aber Erleichterungen, so dass die neuen Homeoffice-Regelungen ohne Übergangsfrist gelten.

Die BaFin betrachtet den überwiegenden Teil der Anforderungen an das Risikomanagement von ESG-Risiken als Klarstellung (!) mit der Folge, dass sie ohne Übergangsfrist eingehalten werden müssen. Hintergrund ist, dass seit dem BaFin-Merkblatt zum Umgang mit Nachhaltigkeitsrisiken aus dem Jahr 2019 die ESG-Risiken grundsätzlich schon bekannt sind. Auch aufgrund der MaRisk 2021 waren die Banken verpflichtet, sich einen Überblick über die Risiken zu verschaffen und diese in das Risikomanagement einzubinden, einschließlich der damals schon bekannten ESG-Risiken.

Neue Anforderungen sieht die Aufsicht in den Regelungsbereichen der Risikoquantifizierung für ICAAP und Stresstesting. Hintergrund ist, dass sich ESG- bzw. Klima-Risiken über einen sehr langfristigen Zeithorizont materialisieren können. Daher ist eine Betrachtung über den bisher üblichen Risikobetrachtungszeitraum hinaus erforderlich. Auch neu ist der Einsatz von wissenschaftsbasierten Szenarien, s.o. ESG-Risiken.

Quick-Check zur MaRisk

Anders als bei der letzten Veröffentlichung der MaRisk im Jahr 2021 hat die BaFin dieses Jahr keine detaillierte und vollständige Übersicht veröffentlicht, bei welchen Änderungen der MaRisk es sich um Klarstellungen oder Neuerungen handelt.

Insoweit verweisen wir auf den vom Bereich MaRisk-Compliance der DZ CompliancePartner GmbH veröffentlichten Quick-Check zur MaRisk, in dem wir für jede einzelne Änderung in den neuen MaRisk Ausführungen dazu gemacht haben, ob es sich um eine Aktualisierung oder Neuerung handelt. Gleichzeitig geben wir in dem Quick-Check auch Umsetzungshinweise bzw. Handlungsempfehlungen. Diesen Quick-Check haben wir unseren Mandanten im Rahmen der Auslagerung zur Verfügung gestellt. ▬

Axel Hofmeister
Beauftragter MaRisk-Compliance,
E-Mail: axel.hofmeister@dz-cp.de

Silke Lenhart
Beauftragte MaRisk-Compliance,
E-Mail: silke.lenhart@dz-cp.de

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

Beauftragtenwesen – Mensch im Mittelpunkt

> ***„Ich mache meinen Job dann gut, wenn Menschen IT-Sicherheit wirklich (er)leben, wenn sie dem Angriff standhalten können, wenn sie wissen, wie sie sich richtig verhalten."***
> *Reinhold Gillich, Beauftragter Informationssicherheit und Datenschutz*

Wir in der DZ CompliancePartner GmbH wollen unsere Kunden im regulatorischen Beauftragtenwesen entlasten. Wir treten an, das Risiko eines Geldwäsche-, Betrugs- oder Datenschutzvorfalles zu minimieren, Informationssicherheit, MaRisk- und WpHG-Compliance zu gestalten.

Das macht keine Maschine, keine Anwendung und auch keine KI. Das kann nur der Mensch mit seinem fachlichen Wissen, seinen Tools, seinen Erfahrungen, seiner Intuition und vor allem auch seinem Netzwerk leisten. Der Mensch steht deshalb im Mittelpunkt – bei allem, was wir tun.

Mitarbeitende stärken

Jeder Mitarbeitende in der DZ CompliancePartner GmbH ist Experte auf seinem Gebiet und bringt nicht nur die erforderliche Sachkunde, sondern auch die notwendige Persönlichkeit mit. In meiner Verantwortung als Bereichsleiter Unternehmenssteuerung/Personal schaffe ich den passenden Rahmen. Dabei setze ich vor allem auf einen regelmäßigen, bidirektionalen Austausch. Spezielle Weiterbildungs- und Coaching-Angebote – z. B. bei den Bildungseinrichtungen der genossenschaftlichen Regionalverbände oder auch bei der Frankfurt School of Finance – sind obligatorisch. Darüber hinaus arbeiten wir mit flexiblen Arbeits(zeit)regelungen, die ebenfalls eine Grundvoraussetzung für individuelle – den jeweiligen Stärken entsprechende – Personalentwicklung sind.

Es ist unglaublich spannend, Menschen, die für ihren Fachbereich brennen, zu begleiten: Das heißt für mich, dass sich auch die personalpolitischen Maßnahmen kontinuierlich und vor allem mitarbeiterorientiert weiterentwickeln müssen. Welche Bedürfnisse, Erwartungen und auch persönliche Ziele haben die KollegInnen und wie können diese bei unternehmerischen Prozessen einfließen?

Der mitarbeiterorientierte Ansatz hilft uns, sowohl die fach- und sachbezogenen als auch die biographischen Anforderungen frühzeitig zu identifizieren und mit entsprechenden Maßnahmen darauf zu reagieren. Ein gutes Beispiel sind die o. g. Arbeitszeitmodelle, aber auch dass wir heute den Mitarbeitenden vom ersten Tag an die Möglichkeit anbieten, in ihrer Expertise Verantwortung zu übernehmen und eigene Ideen einzubringen.

Teams stärken

Die DZ CompliancePartner GmbH will der Bank vor Ort – mit Blick auf die enormen regulatorischen Herausforderungen – den Rücken freihalten, damit sie sich ihrem Markt zuwenden kann. Das kann einer alleine kaum erreichen, das kann nur gemeinsam funktionieren.

Wir arbeiten deshalb in kleinen Teams mit flachen Hierarchien. Damit wird der direkte Austausch untereinander, das dynamisches Arbeiten und auch das schnelle Handeln – wo immer es erforderlich ist – möglich. Uns hilft dabei die feste Verwurzelung in der Genossenschaftlichen FinanzGruppe: Die genossenschaftlichen Werte bestimmen unser Handeln und geben Orientierung. Sie bilden den Rahmen, in dem sich Mitarbeitende frei bewegen können.

Gleichzeitig können die Mitarbeitenden aus einen wirklich einzigartigen Wissensfundus schöpfen und auf ein starkes Netzwerk zurückgreifen: Wir bündeln immerhin die Erfahrung von knapp 100 Compliance-Beauftragten in 650 Auslagerungsmandaten.

„Ich spüre hier bei der DZ-CP, dass man mir als Werkstudentin etwas zutraut und mir verantwortungsvolle Aufgaben anvertraut. Ich selbst wiederum sehe, dass es hier Entwicklungspotenzial gibt. Beides lässt mich tatsächlich mit Zuversicht hier arbeiten."

Ayse Altintas, Werkstudentin

„Als Beauftragte arbeiten wir sehr nah und tief vernetzt mit unseren Auftraggebern und das oft über viele Jahre hinweg. Was unsere Kunden dabei wenig wahrnehmen: unser eigenes Netz innerhalb der DZ-CP, das uns den Rücken freihält und für saubere Abläufe im Hintergrund sorgt."

Jörg Scharditzky, Abteilungsleiter MaRisk-Compliance

„Wir sind ausgewiesene Spezialisten für Compliance. Dazu gehört, die komplexe Regulatorik einfach zu machen. Für mich ist das zunächst eine kommunikative Aufgabe, eine Übersetzungsleistung."

Gabriele Seifert, Bereichsleiterin Kommunikation und Bildung

Und noch eine Besonderheit zeichnet uns aus: Wir legen sehr großen Wert darauf, dass die Produktbereiche und die Betriebsbereiche – vom Vertrieb über die IT-Entwicklung bis hin zur Unternehmenssteuerung – eng zusammenarbeiten. Am Ende stehen wir immer gemeinsam in der Verantwortung, „gute" Lösungen für den Kunden zu schaffen. Die Erfahrung zeigt: Nur wenn Produkt- und Betriebsbereiche gleichermaßen begeistert sind, können wir auch den Kunden begeistern.

Schlussendlich stehen wir mit den Banken, mit den Verbänden und auch mit den Behörden in einem kontinuierlichen Austausch.

Damit sind wir nicht nur der Experte im Beauftragtenwesen – deutschlandweit. Wir sind auch Think-Tank und Place to Be für das Beauftragtenwesen: Wem Compliance am Herzen liegt, wird bei uns die Möglichkeit finden, sich einzubringen, sich zu vernetzen und zu wirken.

Wichtig ist mir dabei, ein kollaboratives, partnerschaftliches Umfeld anzubieten. Das heißt zunächst einmal, einen wertschätzenden Dialog zu etablieren und ein Arbeiten auf Augenhöhe zu ermöglichen. Auf Augenhöhe heißt auch, dass wir regelmäßig den fach- bzw. projekt-bezogenen persönlichen Austausch befördern. Das ist auch deshalb wichtig, weil wir im Arbeitsalltag überwiegend dezentral und mobil arbeiten. Mindestens zweimal im Jahr treffen wir uns bereichsübergreifend in ein- bis zweitägigen Offsites. Bei denen schauen wir gerne auch mal gemeinsam über den Tellerrand und nehmen uns Zeit und Raum für persönliche Begegnungen.

Letztlich ist Compliance ein People's Business, deren Voraussetzung ein gegenseitiges Vertrauen ist. Dieses Vertrauen aber müssen wir uns immer wieder gemeinsam erarbeiten.

Wenn Sie Fragen zu unserem Arbeitsmodell haben, kommen Sie gerne auf mich zu. ▬

Kevin Lohmann
Bereichsleiter Unternehmenssteuerung,
E-Mail: kevin.lohmann@dz-cp.de

Aktualisierung der MaComp

Die BaFin hat kürzlich das Rundschreiben 05/2018 (WA) – Mindestanforderungen an die Compliance-Funktion und weitere Verhaltens-, Organisations- und Transparenzpflichten für Wertpapierdienstleistungsunternehmen (MaComp) aktualisiert.

Mit Veröffentlichung der aktualisierten Fassung am 30. Juni 2023 auf der Webseite der BaFin traten wichtige Änderungen in Kraft:

Die BaFin hat die von der ESMA am 12. April 2022 veröffentlichten „Leitlinien zu einigen Aspekten der MiFID-II-Anforderungen an die Angemessenheit und das reine Ausführungsgeschäft" inhaltlich unverändert in den BT 6 der MaComp überführt. Die neuen Vorgaben enthalten klare Anforderungen an die Wertpapierdienstleistungsunternehmen, welche Daten über die Kenntnisse und Erfahrungen der Kunden zu erheben sind und wie die Kunden über die Angemessenheitsprüfung informiert werden müssen. Ziel der neuen Anforderungen ist es, dass die Institute ein besseres Verständnis für die individuellen Bedürfnisse und Risikoprofile ihrer Kunden bekommen und in der Folge geeignete Anlageprodukte und -dienstleistungen anbieten können.

Die bisher in BT 6 aufgeführten Vorgaben zur Geeignetheitserklärung wurden ohne inhaltliche Änderungen in BT 7 überführt.

Mit dem Rundschreiben S2307118 teilte der BVR mit, die neuen Vorgaben der MaComp im zuständigen Arbeitskreis auszuwerten und die Mitgliedsinstitute zeitnah in einem weiteren Rundschreiben über das Ergebnis inklusive etwaiger Handlungsnotwendigkeiten durch die Mitgliedsinstitute sowie verbundseitiger Unterstützung zu informieren. ▬

Michael Maier
Bereichsleiter Compliance,
E-Mail: michael.maier@dz-cp.de

DZ-CP nun auch auf LinkedIn

Point of Compliance – kurz PoC – steht für Compliance auf den Punkt gebracht, für die Konzentration auf das Wesentliche und auch für unseren Standpunkt als Experten.

Seit dem letzten Quartal sind wir nun auch auf LinkedIn aktiv und informieren Sie dort zu den neuesten regulatorischen Entwicklungen. Wir geben Hinweise zu den zwingend erforderlichen und auch zu den weniger notwendigen Maßnahmen, um die aufsichtsrechtlichen Anforderungen vollumfänglich umzusetzen und die eigenen Schutzinteressen zu wahren. Darüber hinaus geben wir auf dem LinkedIn-Kanal Einblicke in unsere Arbeitsweise. Wir möchten uns dort Ihnen auch ganz persönlich vorstellen, Ihrer Compliance ein Gesicht geben.

Wenn Sie unserer Seite folgen, bleiben Sie automatisch immer auf dem Laufenden – und können liken, teilen, kommentieren oder einfach nur beobachten. ▬

Folgen Sie DZ CompliancePartner auf Social Media

Gabriele Seifert
Bereichsleiterin Kommunikation & Bildung,
E-Mail: gabriele.seifert@dz-cp.de

Interne Revision

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

Seit der letzten Berichterstattung in der Point of Compliance (1/2023, S. 27) wurden aus der Jahresprüfungsplanung 2023 die Prüfungen der Bereiche „MaRisk-Compliance“ und „WpHG-Compliance“ abgeschlossen und an die Mandanten, die diese Dienstleistung von uns beziehen, versandt. Darüber hinaus wurde die Prüfung des Bereichs „Risikomanagement“ durchgeführt und der Bericht, da nicht dienstleistungsbezogen, intern veröffentlicht.

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

Weiterhin wurde turnusgemäß ein Follow-up-Quartalsbericht für das erste und zweite Quartal 2023 erstellt und der Geschäftsführung der DZ CompliancePartner GmbH vorgelegt. In den Follow-up-Berichten wird die Abarbeitung der von internen und externen Prüfern getroffenen Maßnahmen/Empfehlungen dokumentiert. Offene Punkte werden durch die Interne Revision konsequent nachgehalten.

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

Die externe Prüfung der Funktion Hinweisgebersystem nach IDW PS 331 erfolgte durch die Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft. Da die Prüfung erst nach Redaktionsschluss der PoC 1/2023 abgeschlossen wurde, kann erst an dieser Stelle darüber abschließend berichtet werden. Es wurde die Ordnungsmäßigkeit testiert und der Prüfungsbericht an die Mandantschaft versandt. ▬

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

Genossenschaftliche FinanzGruppe
Volksbanken Raiffeisenbanken