Point of Compliance
Das Risikomanagement-Magazin

AUSGABE 1 / 2023

PoC

DZ CompliancePartner

Folgen Sie DZ CompliancePartner auf Social Media.

IMPRESSUM

PoC – Point of Compliance
Das Risikomanagement-Magazin,
Ausgabe 30, 1/2023
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, Norbert Schäfer

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:
Christina Fiedler, Martin Hierlemann,
Silke Lenhart, Chantal Pfeffer,
Jens Saenger, Jörg Scharditzky,
Lars Schinnerling, Maximilian Schmidt,
Thomas Schröder, Michael Switalla,
Justus Aron Tychek

Bildnachweise: DZ CompliancePartner GmbH, iStockphoto
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: 27. März 2023
Auflage: 2.600 Exemplare

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

DER TREND IST UNGEBROCHEN:

Seit Jahren wachsen die regulatorischen Aufgaben sowohl quantitativ als auch qualitativ.

Jens Saenger
Sprecher der Geschäftsführung

Aktuell sehen wir, dass weitere Risiken wie z. B. Kryptowährungen (S. 7) in den aufsichtsrechtlichen Fokus genommen werden. Gleichzeitig steigen – beispielsweise im Zuge des Ukrainekrieges (S.4), mit der voranschreitenden Digitalisierung (S. 16) oder auch mit Blick auf das Auslagerungsmanagement (S. 18) – erneut die Umsetzungsanforderungen. Die Hoffnung auf eine baldige Entspannung im Beauftragtenwesen ist dabei spätestens mit dem jüngsten Bankenbeben auf einem Nullpunkt. Die Sorge vor einer reflexartigen Ausweitung der Regulierung ist daher nicht unbegründet.

Auf der anderen Seite erschweren Faktoren wie der demographische Wandel, der deutlich spürbare Fachkräftemangel und auch die Inflation die Umsetzung und engen den unternehmerischen Spielraum weiter ein. Die Wahrheit ist, Banken müssen, um den komplexen Anforderungen zu genügen, immer mehr in ihr aufsichtsrechtliches Risikomanagement investieren: in das Personal, das Know-how, die Prozesse und auch in die IT.

Wir, als Ihr Auslagerungspartner, sehen es als unseren Auftrag, Sie in dieser Lage zu entlasten. Auch wir werden auf die gestiegenen Anforderungen und den Fachkräftemangel reagieren müssen. Aber als Mehrmandantenanbieter können wir die aufsichtsrechtlich notwendige Sicherheit effizienter gewährleisten, als eine Bank es alleine könnte (S.23).

Ich wünsche Ihnen eine anregende Lektüre.

Herzlichst
Ihr Jens Saenger

Das Sanktionsdurchsetzungsgesetz – Auswirkungen für die GwG-Verpflichteten

Mit dem Sanktionsdurchsetzungsgesetz wird die Sanktionsdurchsetzung in Deutschland strukturell neu aufgestellt. Die Umsetzung von Sanktionen soll noch effektiver werden. Durch das Artikelgesetz werden zugleich weitere Maßnahmen zur Geldwäschebekämpfung auf den Weg gebracht.

Als Reaktion auf den russischen Angriffskrieg gegenüber der Ukraine wurden unmittelbar nach Beginn der Kriegshandlungen am 24. Februar 2022 umfangreiche Sanktionen und Embargos gegen russische und belarussische Personen und Einrichtungen verhängt. Hierzu zählen insbesondere das Einfrieren von Vermögenswerten und Reisebeschränkungen, Beschränkungen der wirtschaftlichen Zusammenarbeit und Import- und Exportrestriktionen.

Um Regelungslücken auf der Vollzugsebene zur Sanktionsdurchsetzung kurzfristig zu schließen, wurde im Mai 2022 das Sanktionsdurchsetzungsgesetz I (SanktDG I) verabschiedet. Das Gesetz trat am 28. Mai 2022 in Kraft. Sowohl das SanktDG I als auch das im Dezember 2022 in Kraft getretene SanktDG II sind sogenannte Artikelgesetze. Das heißt, mit diesen Einzelgesetzen werden andere Gesetze, z. B. auch das Geldwäschegesetz (GwG), geändert.

SanktDG I

Ausweislich der Gesetzesbegründung war es Ziel des SanktDG I, bestehende rechtliche Regelungen zielgenauer auf die Sanktionsdurchsetzung auszurichten und einen speziell auf die Sanktionsdurchsetzung abgestimmten Rechtsrahmen zu schaffen.

Mit dem SanktDG I wurden u. a. die Befugnisse zuständiger Behörden erweitert, Zeugen vorzuladen und zu vernehmen, Beweismittel sicherzustellen und Wohnungen und Geschäftsräume zu durchsuchen.

Zudem wurde es Behörden erleichtert, Einsicht in Grundbücher und andere öffentliche Register zu nehmen, Konten zu ermitteln und abzufragen und Schließfächer sowie Wertpapierdepots von sanktionierten Personen zu ermitteln.

Ergänzend wurde die strafbewehrte Anzeigepflicht über Gelder und andere wirtschaftliche Ressourcen eingeführt. Sanktionierte Personen sind seither verpflichtet, ihr Eigentum der Deutschen Bundesbank beziehungsweise dem Bundesamt für Wirtschaft und Ausfuhrkontrolle unverzüglich anzuzeigen. Diese Anzeigepflicht gilt in abgeschwächter Form auch für Logistikdienstleister, die etwa Beförderungsdienstleistungen für sanktionierte Personen übernehmen.

Auch dürfen Behörden künftig Gelder und wirtschaftliche Ressourcen, bei denen mindestens die begründete Vermutung besteht, dass sie einer Verfügungsbeschränkung unterfallen, (vorläufig) sicherstellen und in Ausnahmefällen sogar verwerten.

Schließlich wurde der Informationsaustausch zu sanktionsrelevanten Informationen zwischen Behörden erleichtert. Hierzu zählt sowohl der behördliche Zugriff auf Daten aus dem Transparenzregister als auch die Abfrage von Kontodaten bei der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin).

Nicht zuletzt soll die Zentralstelle für Finanztransaktionsuntersuchungen (FIU) durch die entsprechenden Änderungen im GwG u. a. bei der Vermögensfeststellung mitwirken. Die FIU erhält zudem die Befugnis, Transaktionen mit Sanktions- oder Embargobezug zu untersagen.

Auch darf die BaFin nun gegenüber jedermann Handelsverbote bei Sanktionsbezug anordnen.

SanktDG II

Das zweite Gesetz zur effektiveren Durchsetzung von Sanktionen (SanktDG II) trat am 28. Dezember 2022 in Kraft. Mit ihm werden ergänzend zu den kurzfristigen Maßnahmen des SanktDG I strukturelle Verbesserungen für die Sanktionsdurchsetzung in Deutschland initiiert.

Auf behördlicher Seite sind dabei die Schaffung der Zentralstelle für Sanktionsdurchsetzung bei der Generalzolldirektion, die damit verbundenen Befugnisse für die sanktionsbezogene Vermögensermittlung und die Schaffung eines Registers für Vermögenswerte sanktionierter Personen und Personengesellschaften hervorzuheben.

Für GwG-Verpflichtete sind die durch das SanktDG II ausgelösten Änderungen des Geldwäschegesetzes von Bedeutung. Hierzu zählen insbesondere das neue Barzahlungsverbot bei Immobilientransaktionen (§ 16a GwG) sowie diverse Regelungen zur Erhöhung der Transparenz im Immobilienbereich.

Barzahlungsverbot

Das Barzahlungsverbot bewirkt, dass eine geschuldete Gegenleistung (damit ist regelmäßig die Zahlung des Kaufpreises der Immobilie gemeint) nicht durch Bargeld, Kryptowerte, Gold, Platin oder Edelsteine erfolgen darf.

Besonders wichtig: Die Vorschrift umfasst sowohl alle Kauf- und Tauschverträge, die auf den Erwerb von Immobilien gerichtet sind, als auch Kauf- und Tauschverträge von Anteilen an Gesellschaften mit direktem oder indirektem Immobilienbesitz. Gleichgültig ist es dabei auch, ob es sich bei den Vertragsparteien um natürliche oder juristische Personen handelt. Auch gewerbliches Handeln ist nicht erforderlich. Die Regelung findet auf Rechtsgeschäfte, die vor dem 1. April 2023 geschlossen wurden, keine Anwendung.

Das neue GwG verbietet aber nicht nur die Barabwicklung. § 16a Abs. 2 GwG verlangt von den am Immobilienkauf Beteiligten den Nachweis, dass die erbrachte Gegenleistung mit anderen Mitteln als den genannten Barwerten erfolgt ist.

Nachweispflicht

Die Beteiligten, also typischerweise Käufer bzw. Verkäufer der Immobilie, haben dem an der Abwicklung des Immobiliengeschäfts beteiligten Notar die entsprechenden Nachweise zur Verfügung zu stellen. Die vorgelegten Nachweise sind durch den Notar auf Schlüssigkeit zu prüfen.

Geeignete Nachweise sind insbesondere Zahlungsbestätigungen von auf Veräußerer- oder Erwerberseite an der Transaktion beteiligten Kreditinstituten oder elektronische Kontoauszüge bzw. elektronische Zahlungseingangsbestätigungen des kontoführenden Kreditinstitutes des Veräußerers.

Die Nachweispflichten der Beteiligten und die Pflicht zur Schlüssigkeitsprüfung durch den Notar entfallen, wenn die geschuldete Gegenleistung einen Betrag von 10.000 Euro nicht übersteigt oder sofern sie über ein Anderkonto des mit der Einreichung des Eintragungsantrags beauftragten Notars erbracht wird.

Weitere relevante Regelungen

Durch das SanktDG II wurden noch weitere geldwäscherechtliche Änderungen auf den Weg gebracht, die – wie auch das Barzahlungsverbot bei Immobilientransaktionen – in ihrer Bedeutung und Tragweite für die Bekämpfung der Finanzkriminalität nicht unterschätzt werden dürfen.

So verpflichtet das neue GwG die nach § 20 GwG transparenzregisterpflichtigen Rechtsvereinigungen, bei der Eintragung von fiktiven wirtschaftlich Berechtigten in das Transparenzregister künftig auch den Grund anzugeben, der zur Meldung eines fiktiven wirtschaftlich Berechtigten führt.

Zudem sieht das neue GwG nun vor, dass im Transparenzregister im Hinblick auf die transparenzregisterpflichtigen Vereinigungen künftig auch Angaben zu Immobilien zugänglich sind. Verkürzt gesagt werden Basisdaten aus den Grundbüchern zu Eigentümer, Flurstück und Grundbuchblatt künftig in das Transparenzregister übernommen und den dort verzeichneten Vereinigungen zugeordnet.

Eine nachhaltige Wirkung im Hinblick auf deutlich mehr Transparenz bei der Zuordnung von Immobilienvermögen erzeugt auch die Änderung von § 20 Abs. 1 Satz 2 GwG.

Künftig müssen sich auch alle juristischen Personen des Privatrechts und eingetragene Personengesellschaften mit Sitz im Ausland ins Transparenzregister eintragen, wenn sie Immobilieneigentum in der Bundesrepublik Deutschland halten oder sich zu dessen Erwerb verpflichtet haben.

Zusätzlich besteht zukünftig die Pflicht zur Abgabe einer Unstimmigkeitsmeldung, wenn die zur Einsichtnahme in die Immobiliendaten berechtigten Behörden und Verpflichteten Abweichungen zwischen den im Transparenzregister gespeicherten Angaben und eigenen Erkenntnissen über Immobilien feststellen.

Die transparenzregisterführende Stelle wird auf der Internetseite des Transparenzregisters eine technische Möglichkeit einrichten, um solche Unstimmigkeitsmeldungen abzugeben.

Die entsprechenden Regelungen wurden im neuen § 23b GwG kodifiziert. Sie treten am 1. Januar 2026 in Kraft.

Fazit

Die Gesetze zur effektiveren Durchsetzung von Sanktionen (SanktDG) sind ein wesentlicher Baustein bei der sanktionsspezifischen Vermögensermittlung und -sicherstellung und verbessern die operative Umsetzung von Sanktionen. Gleichzeitig stärken die Gesetze die Bekämpfung von Geldwäsche und Finanzkriminalität, insbesondere im Hinblick auf das Bargeldverbot bei Immobiliengeschäften und die Verzahnung der Informationen aus öffentlichen Registern mit dem Transparenzregister. ▬

Kontakt
Geldwäsche- und Betrugsprävention
E-Mail: poc@dz-cp.de

Risiko Kryptogeschäft

Warum die Forderungen nach einer strengeren Krypto-Regulierung lauter werden und welche Maßnahmen hier aktuell geplant sind

Der Skandal um die Kryptoplattform FTX brachte die gesamte Branche zuletzt in schwere Turbulenzen. Immer häufiger werden Kryptowerte auch mit finanzkriminellen Aktivitäten wie Geldwäsche und Terrorismusfinanzierung oder Sanktionsumgehungen in Zusammenhang gebracht.

Die nun geforderten Nachschärfungen in der Regulierung von Kryptogeschäften sollen den bisher bestehenden Risiken entgegenwirken. Auch der traditionelle Bankensektor könnte hier zukünftig stärker in die Pflicht genommen werden.

Die Kryptobranche hat eines der turbulentesten Jahre in ihrer Geschichte hinter sich. Der Bitcoin musste 2022 einen Kursverlust von etwa 60 % hinnehmen. Die rückläufige Entwicklung der bekanntesten und größten Digitalwährung (nach Marktkapitalisierung) steht dabei sinnbildlich für die Gesamtlage, in der sich die Branche derzeit befindet. Durch Skandale wie die Zusammenbrüche von Celsius, Three Arrows Capital oder FTX werden Kryptowerte bzw. Kryptoassets (siehe Glossar) vermehrt mit betrügerischen Handlungen in Verbindung gebracht. Auch der Verdacht, Kryptobörsen würden zur Wäsche von inkriminierten Geldern, Terrorismusfinanzierung oder der Umgehung von Sanktionsmaßnahmen genutzt, reißt nach den Skandalen um die Plattformen Garantex und Bitzlato nicht ab.

Anhaltende Zunahme von internationalen Geldwäscheaktivitäten durch Kryptowerte

In ausführlichen Crypto-Crime-Reporten analysiert die Blockchain-Datenplattform Chainalysis (siehe Glossar) jährlich die Entwicklung von Kriminalität und Geldwäsche im Zusammenhang mit Kryptowerten. Der aktuelle Report zeigt auch für das Jahr 2022 eine weitere Zunahme von Geldwäscheaktivitäten mittels Digitalwährungen (siehe Abb. 1).

Aktuellen Schätzungen zufolge umfasste die über Kryptowerte abgewickelte Geldwäsche im Jahr 2022 circa 23,8 Mrd. US-Dollar und erreicht mit einem Zuwachs von 68 % gegenüber dem Vorjahr einen neuen Rekordwert.

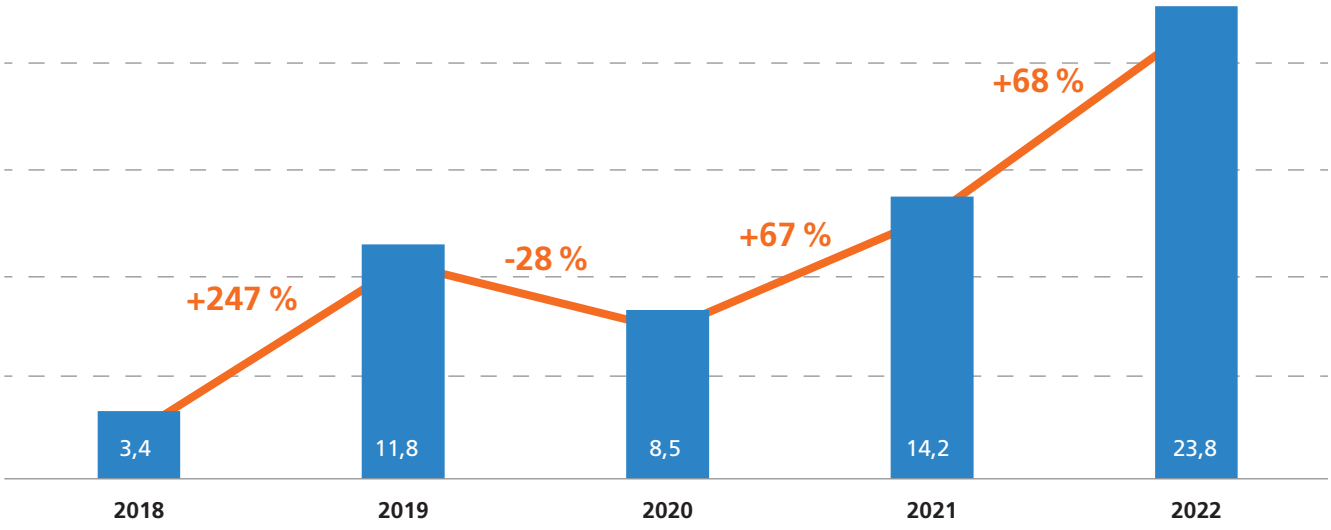
Wie bereits in den vergangenen Jahren waren vor allem Mainstream-Kryptobörsen die größten Empfänger von inkriminierten Kryptowerten. Knapp die Hälfte aller von illegalen Adressen gesendeten Kryptoassets wurde von ihnen abgewickelt. Insbesondere aufgrund ihrer Funktion als Tauschbörsen für Fiat-Währungen (siehe Glossar), auf denen die inkriminierten Digitalgelder in Giral- oder Bargeld umgewandelt werden können, ist diese Entwicklung als kritisch zu bewerten. Die von den großen Börsen vorgehaltenen Compliance-Strukturen scheinen demnach nicht konsequent umgesetzt zu werden und stellen somit ein erhebliches Geldwäscherisiko auch für die Integrität des traditionellen Bankensektors dar.

Auch national nehmen Geldwäschemeldungen im Zusammenhang mit Kryptowerten weiter zu.

Nicht nur auf internationaler Ebene zeichnen sich vermehrt Geldwäscheaktivitäten ab, die im Zusammenhang mit Kryptogeschäften stehen. Auch national ist hier ein konstantes Wachstum zu beobachten (siehe Abb. 2).

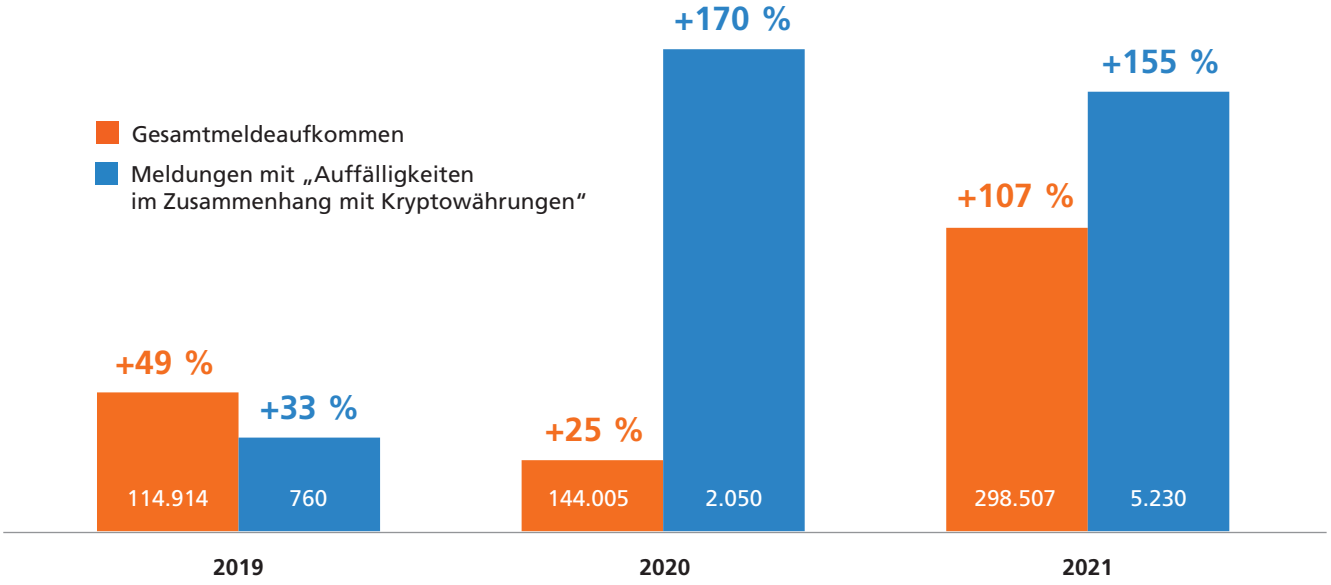
Im Jahr 2022 gingen bei der Financial Intelligence Unit (FIU) Deutschland 5.230 Geldwäsche-Verdachtsmeldungen mit „Auffälligkeiten im Zusammenhang mit Kryptowährungen“ ein. Dieser hohe Wert reiht sich damit in die seit 2018 fortlaufende Entwicklung ein und markiert mit einem Zuwachs von 155 % gegenüber dem Vorjahr ein neues Allzeithoch. Das Aufkommen von

Abb. 1. **Über Kryptowerte abgewickelte Geldwäsche in Mrd. US-Dollar**



Quelle: In Anlehnung an den Crypto-Crime-Report 2023 von Chainalysis, S. 43

Abb. 2. **Entwicklungen der eingegangenen Verdachtsmeldungen bei der FIU Deutschland gegenüber dem Vorjahr in Prozent (%)**



Quelle: In Anlehnung an den Jahresberichte der Financial Intelligence Unit Deutschland

Meldungen, die in Verbindung mit Kryptowerten stehen, ist damit das zweite Jahr in Folge gegenüber dem Gesamtmeldeaufkommen überproportional gestiegen.

Vor diesem Hintergrund hat auch das Bundesministerium der Finanzen dieses Thema stärker fokussiert. In der Ersten Nationalen Risikoanalyse (NRA) wird die Geldwäschebedrohung durch Kryptowerte in den Jahren 2018/2019 zwar noch mit mittel-niedrig bewertet, eine Zunahme der Geldwäscheaktivitäten in diesem Bereich wird jedoch schon zum damaligen Zeitpunkt erwartet (vgl. Bundesministerium der Finanzen: Erste Nationale Risikoanalyse 2018/2019, S. 114 f.). Insbesondere die folgenden Punkte werden dabei als besonders kritisch gesehen:

- bereits vorliegende inkriminierte Kryptowerte, die durch strafbare Handlungen im Darknet oder durch Kryptotrojaner (siehe Glossar) erwirtschaftet wurden,
- Verschleierung der illegalen Herkunft von Kryptoassets durch vorgeblich eigenes Mining oder Nutzung sogenannter „Mixer"- oder „Tumbler"-Dienste (siehe Glossar),
- feststellbarer Einsatz von Digitalwährungen im Zusammenhang mit Online-Betrugstaten (z. B. sogenannten Fakeshops).

Eine allgemeine Sensibilisierung der Regulierungs- und Aufsichtsbehörden für die mit Kryptogeschäften einhergehenden Risiken wird auch mit Blick auf die Ergebnisse der Evaluation Deutschlands durch die Financial Action Task Force (FATF) im vergangenen Jahr deutlich. Demnach wird das Risikoverständnis der BaFin gegenüber der Einschätzung der NRA als „weiter entwickelt" eingestuft (vgl. FATF: Anti-money laundering and counter-terrorist financing measures in Germany 2022, S. 17). Da die BaFin Kryptogeschäfte als einen aufstrebenden Bereich mit potenziell höherem Risiko bewertet und bereits 2020 als Schwerpunktbereich identifiziert hat, ist davon auszugehen, dass sich diese Einschätzung auch in der geplanten Aktualisierung der NRA des Bundesministeriums der Finanzen wiederfinden wird.

Kleines Kryptoglossar

Chainalysis ist eine Blockchain-Datenplattform, die Daten, Software, Dienstleistungen und Recherchen für Regierungsbehörden, Börsen, Finanzinstitutionen sowie Versicherungs- und Cybersicherheitsunternehmen in über 70 Ländern anbietet.

Fiat-Währungen sind nationale Währungen, die nicht an den Preis eines Rohstoffes wie Gold oder Silber gebunden sind. Sie dienen als Tauschmittel, besitzen dabei jedoch keinen inneren Wert. Herausgegeben werden Fiat-Währungen von Regierungen oder den Zentralbanken der jeweiligen Länder.

Kryptotrojaner oder auch Verschlüsselungstrojaner bzw. Erpressungstrojaner sind Schadprogramme für Computer, die dafür sorgen, dass der Rechner für den Nutzer gesperrt und nur gegen ein Lösegeld wieder freigeschaltet werden kann.

Kryptowerte bzw. Kryptoassets werden seit 2020 durch das KWG im Rahmen des §1 Abs. 11 Satz 4 KWG definiert. Demnach sind Kryptowerte bzw. Kryptoassets digitale Darstellungen eines Wertes, der von keiner Zentralbank oder öffentlichen Stelle emittiert wurde oder garantiert wird. Die Begriffe „Kryptowerte" und „Kryptoassets" werden im weitesten Sinne synonym verwendet.

Mixer- oder Tumbler-Dienste: Bei der Verwendung sogenannter Mixer- oder Tumbler-Dienste können Kryptowerte verschiedener Herkunft gemixt werden. Bei den „gemixten" Beträgen ist dann nur noch mit erheblichem Analyseaufwand nachvollziehbar, woher diese Assets kommen. Zudem steigt das Geldwäschepotenzial beim Umtausch verschiedener Kryptowerte untereinander weiter an.

Bestrebungen der EU-Kommission nach einer strengeren Regulierung von Kryptogeschäften werden sich mittelfristig auch in den nationalen Vorgaben wiederfinden.

Die Risikoeinschätzungen der nationalen Regulierungs- und Aufsichtsbehörden lassen sich längst in den Bestrebungen der Normgeber in Brüssel wiederfinden. Demnach sollen erstmals Kryptowerte, Emittenten von Kryptoassets und Anbieter von Kryptodienstleistungen einem strengen Regelungsrahmen unterworfen werden. Die aufgezeigten Entwicklungen zeigen, dass eine EU-weite Regulierung dringend erforderlich ist. Durch das AML/CTF-Paket der EU-Kommission vom 7. Mai 2020 (AML: Anti-Money Laundering; CTF: Counter-Terrorist Financing) soll ein einheitliches EU-Regelwerk zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung sowie zur Einführung einer auf EU-Ebene angesiedelten Aufsichtsbehörde geschaffen und damit auch eine strengere Krypto-Regulierung erzielt werden.

Das geplante „AML Package" enthält vier wesentliche Elemente:

1. **Einführung einer „AML-Verordnung"**
   Die AML-Verordnung bildet das Kernstück des Pakets. Sie regelt die wesentlichen Sorgfaltspflichten der Verpflichteten, wie sie in Deutschland bislang in den §§ 4-17 GwG geregelt waren, sowie die wichtigsten Definitionen. Darüber hinaus soll eine Erweiterung des Verpflichtetenkatalogs um die Kryptowertedienstleister erfolgen.

   Während die Geldwäschegesetzgebung der EU bisher vorsah, Richtlinien zu erlassen, die die Mitgliedstaaten umzusetzen hatten, würde mit Einführung der AML-Verordnung unmittelbar anwendbares Recht geschaffen werden, das keiner Umsetzung mehr bedarf.

2. **Ausdehnung der Geldtransferverordnung auf Kryptowerte**
   Die Geldtransferverordnung regelt bisher die Angaben, die von Kredit- oder Zahlungsinstituten bei Geldtransfers zu übermitteln bzw. zu kontrollieren sind. Diese Pflichten sollen nun auf Kryptowertedienstleister, sogenannte „crypto-asset service provider" (auch CASPs), ausgedehnt werden. Transfers von Kryptowerten sollen grundsätzlich grenzüberschreitenden Zahlungen gleichgestellt werden, sodass die Verpflichteten die Namen von Sender und Empfänger der Transaktion erheben und übermitteln müssen. Hiermit sollen anonyme Transaktionen mit Kryptowerten unterbunden werden.

   Eine detaillierte Definition von CASPs findet sich wiederum in der MiCA-Verordnung (Regulation on Markets in Crypto-Assets). Da Verbraucher zurzeit insbesondere bei Transaktionen außerhalb der EU nur ein sehr begrenztes Recht auf Schutz oder auf Wiedergutmachung haben, zielt die MiCA-Verordnung auch darauf ab, einen einheitlichen EU-weiten Regulierungsrahmen für Kryptoassets, deren Emittenten und bestimmte Dienstleister zu schaffen und auch Maßnahmen zum Anlegerschutz sowie zur Verhinderung von Marktmissbrauch zu definieren.

3. **Verabschiedung einer „6. Geldwäscherichtlinie"**
   Die Richtlinie soll Vorgaben enthalten, deren Ausgestaltung den Mitgliedstaaten überlassen wird. Dies gilt beispielsweise für die Gestaltung der Transparenzregister, die nationale Risikoanalyse oder die Struktur der FIUs. Die Aufsichtsbehörden über die Kundenprüfungs- und Transparenzregisterpflichten sollen weiterhin auf nationaler Ebene angesiedelt sein.

4. Gründung einer EU Anti-Money Laundering Authority

Die AMLA (Anti-Money Laundering Authority) soll sich vor allem zwei Aufgaben widmen: Einerseits soll sie die Arbeit der nationalen Aufsichtsbehörden koordinieren und einheitliche Vorgaben zur Konkretisierung des europäischen Primärrechts entwickeln. Andererseits gilt es für die Institution, bestimmte Verpflichtete aus dem Finanzsektor unmittelbar zu beaufsichtigen.

Die geplanten Maßnahmen der EU-Kommission stellen einen ersten Schritt hin zu einer strengeren Regulierung von Kryptogeschäften dar. Die Umsetzung der einzelnen Bestandteile auf nationaler Ebene steht hier jedoch noch am Anfang.

Fazit & Ausblick

Zukünftige Auswirkungen für den traditionellen Bankensektor heute konkret zu formulieren, gleicht einem Blick in die Glaskugel. Allerdings sollten Banken aufgrund der aufgezeigten Entwicklungen mehr Sensibilität im Umgang mit Kryptogeschäften entwickeln und damit einhergehende Risiken differenziert betrachten. Vor dem Hintergrund der politischen/aufsichtsrechtlichen Bestrebungen in diesem Bereich sollten die aktuellen Entwicklungen hier verstärkt beobachtet und verfolgt werden. Denn sicher ist, dass die Anforderungen an ein effizientes Risikomanagement weiter zunehmen werden und sich auch in der Regulierung und Aufsicht des traditionellen Bankensektors wiederfinden werden. ▬

Christina Fiedler
Compliance-Spezialistin,
E-Mail: christina.fiedler@dz-cp.de

Justus Aron Tychek
Compliance-Spezialist,
E-Mail: justus.tychek@dz-cp.de

Die dunkle Seite der Cloud: Datenschutzrisiken beim Einsatz von Microsoft 365?

In der öffentlichen Diskussion werden widersprüchliche Standpunkte hinsichtlich des Datenschutzes bei Microsoft 365 (siehe Infokasten) diskutiert. Während einige Experten die Plattform loben und als sichere Lösung empfehlen, gibt es andere Stimmen, die Risiken für den Datenschutz befürchten. Der vorliegende Artikel informiert über den aktuellen Stand und zeigt grundlegende Anforderungen auf, die bei der Implementierung zu beachten sind.

Cloud Technology: Elevating efficiency and teamwork

In Anbetracht der sich stetig wandelnden Anforderungen der modernen Arbeitswelt müssen sich Unternehmen frühzeitig mit neuen Technologien auseinandersetzen. In diesem Kontext hat sich Microsoft 365 als eine der führenden Lösungen für Unternehmen etabliert, die bestrebt sind, ihren Mitarbeitenden moderne Arbeitsmittel zur Verfügung zu stellen, um Arbeitsabläufe effizient und sicher zu gestalten und die Kollaboration zu optimieren. Dabei bietet Microsoft 365 innovative Technologien (wie etwa die Integration von KI-Funktionen für Office-Anwendungen), die es Unternehmen ermöglichen sollen, den Herausforderungen einer sich schnell verändernden Geschäftswelt standzuhalten und zugleich die Produktivität und Effizienz ihrer Arbeitsprozesse zu steigern.

Durch die Adaption innovativer Technologien können sich jedoch auch neue Gefahrenpotenziale manifestieren. Risiken aus den Bereichen Datenschutz und Informationssicherheit sind daher frühzeitig zu identifizieren, zu bewerten und mittels geeigneter Maßnahmen zu minimieren oder zu beseitigen.

Was die Datenschutzkonferenz kritisiert

Im Rahmen der Risikoermittlung wird man sich vernünftigerweise auch mit den Verlautbarungen der zuständigen Aufsichtsbehörden auseinandersetzen.

Die Datenschutzkonferenz (DSK), das gemeinsame Gremium der Aufsichtsbehörden, hat hierzu im November des vergangenen Jahres einstimmig beschlossen, dass der Nachweis von Verantwortlichen, Microsoft 365 datenschutzkonform zu betreiben, auf der Grundlage des von Microsoft bereitgestellten Data Protection Addendum (DPA) nicht geführt werden kann.

Prüfungsgegenstand waren weder das Unternehmen Microsoft noch dessen Produkte oder Dienstleistungen. Vielmehr wurde lediglich das für die zahlreichen Services zugrundeliegende DPA (der Auftragsverarbeitungsvertrag) begutachtet. Die Beanstandungen betreffen im Einzelnen:

- die unzureichende Festlegung von Arten und Zwecken der verarbeiteten Daten,
- Intransparenz in Bezug auf die Datenverarbeitungen, die Microsoft für eigene Geschäftszwecke vornimmt,
- Ausnahmen bei der Weisungsbindung aufgrund des Cloud Act und FISA 702,
- Sicherheitsmaßnahmen, die nur eine Teilmenge der vertragsgegenständlichen personenbezogenen Daten erfassen,
- Intransparenz und Ausnahmen bei der Löschung und Rückgabe von Daten,
- unzureichende Informationen bei der Einschaltung von Unterauftragnehmern und schließlich
- Datenübermittlungen in Drittstaaten (hier die USA).

Obwohl die genannten Kritikpunkte auf den ersten Blick gültig erscheinen, sollte nicht übersehen werden, dass es sich bei Microsoft 365 um hochkomplexe Dienste und Services eines global agierenden Hyperscale-Anbieters handelt. Es ist anzuerkennen, dass Verträge für komplexe Services nicht den gleichen Detaillierungsgrad aufweisen können wie beispielsweise ein trivialer Auftrag zum Druck von Visitenkarten.

Microsoft bietet ergänzend unzählige Produktinformationen, die zwar nicht Vertragsbestandteil sind, aber für weitreichende Transparenz sorgen. Unter Berücksichtigung dieser Umstände sowie der Tatsache, dass keine perfekten Verträge existieren, kann die Auffassung vertreten werden, dass die meisten der oben genannten Beanstandungen nicht angemessen sind und damit auch die Schlussfolgerung der Datenschutzkonferenz überzogen ist.

Wie Microsoft reagiert

Eine ausführliche Stellungnahme von Microsoft auf den DSK-Beschluss, in der die Kritik zurückgewiesen wurde, ließ nicht lange auf sich warten. Dem Verfasser der Stellungnahme ist es jedoch nicht gelungen, die Zweifel vollständig auszuräumen. Vermutlich wurden aus diesem Grund auch die vertraglichen Grundlagen ein weiteres Mal überarbeitet. Im Januar 2023 wurde eine angepasste Fassung des Data Protection Addendum veröffentlicht. Es handelt sich hierbei bereits um die 7. Anpassung in den zurückliegenden 36 Monaten. Ein Blick in den neuen Vertrag zeigt zwar einige Änderungen im Vergleich zur Vorversion aus September 2022, die von der DSK monierten Klauseln des Vertrags wurden jedoch entweder gar nicht oder nur unwesentlich abgeändert.

Daher ist das gelegentlich vorgebrachte Argument, der DSK-Beschluss sei allein aufgrund des neuen DPA hinfällig, als unhaltbar anzusehen. Bei vernünftiger Betrachtung bleiben die (überzogenen) Beanstandungen im Wesentlichen aktuell.

Quick Info: Microsoft 365

Microsoft 365 ist ein Abonnementdienst, der eine Vielzahl von Anwendungen (z. B. Word, Excel, PowerPoint, Outlook) und Diensten (u. a. OneDrive, SharePoint und Teams) umfasst. Es ist als Software-as-a-Service (SaaS) konzipiert, was bedeutet, dass die Programme, Anwendungen und Daten nicht auf unternehmenseigenen Geräten installiert und verarbeitet werden müssen. Stattdessen werden sie auf weltweit verteilten Microsoft-Servern gehostet, die über das Internet zugänglich sind. Dadurch können Benutzer von verschiedenen Geräten aus auf dieselben Anwendungen und Daten zugreifen, ohne dass sie physisch auf ihrem Computer installiert sein müssen.

Bedenkenlose Datentransfers in die USA bald möglich?

Trotz aller Entwicklungen und Maßnahmen werden im Rahmen der Nutzung von Microsoft 365 auch zukünftig bestimmte personenbezogene Daten in die USA übermittelt werden. Dies gilt selbst für den Fall der vollständigen Implementierung der EU Data Boundary (dazu sogleich).

Dies ist jedoch nur unter der Voraussetzung zulässig, dass das durch die DSGVO gewährleistete Schutzniveau in den USA nicht untergraben wird. Gegenwärtig versucht man dies im Wege der Nutzung sogenannter Standard Contractual Clauses (SCC) zu erreichen. Dabei besteht jedoch die Herausforderung, dass dieses Übermittlungsinstrument nur in Verbindung mit ergänzenden Maßnahmen wirksam ist, mit deren Hilfe die Rechtsschutzlücken im Drittland geschlossen werden können und die Einhaltung des unionsrechtlichen Schutzniveaus gewährleistet werden kann.

Entsprechende Maßnahmen sind nach Ansicht der DSK beim Einsatz von Microsoft 365 jedoch nicht verfügbar. Zwar bestehen hier verschiedene Möglichkeiten der Verschlüsselung, dabei ist jedoch Microsoft entweder selbst im Besitz des Verschlüsselungsschlüssels oder die Verschlüsselung ist (wie beispielsweise bei Nutzung des „Customer Key“) auf „Data at rest“ beschränkt. Viele der in Microsoft 365 enthaltenen Dienste erfordern zudem einen Zugriff von Microsoft auf die unverschlüsselten, nicht pseudonymisierten Daten, beispielsweise wenn die Daten im Browser angezeigt werden müssen. Microsoft hat somit regelmäßig und letztlich schon zur Erfüllung vertraglicher Leistungspflichten die Möglichkeit, Daten im Klartext zu lesen.

Abhilfe soll hier ein neuer Angemessenheitsbeschluss der EU-Kommission schaffen. Dabei handelt es sich um ein weiteres Instrument, welches die Bewertung und Anerkennung des Datenschutzniveaus in Drittstaaten ermöglicht. Durch einen Angemessenheitsbeschluss wird bestätigt, dass ein Nicht-EU-Land einen adäquaten Schutz von personenbezogenen Daten gewährleistet, wodurch Datenübermittlungen ohne ergänzende Schutzmechanismen erfolgen können. Dies trägt zur Vereinfachung und rechtlichen Absicherung des grenzüberschreitenden Datenaustauschs zwischen der EU und den betreffenden Ländern bei.

Angemessenheitsbeschlüsse bestehen für mehrere Länder (u. a. für Kanada, die Schweiz und Südkorea). Für die Übermittlung in die USA existierten in der Vergangenheit ebenfalls bereits Angemessenheitsbeschlüsse. Von 2000 bis 2015 durften Datenübermittlungen auf der Grundlage des Safe-Harbor-Abkommens erfolgen. Nachdem der Europäische Gerichtshof (EuGH) dieses für ungültig erklärte, wurde Mitte 2016 ein Nachfolger, das EU-US Privacy Shield, erlassen. Jedoch wurde auch dieser Angemessenheitsbeschluss vom EuGH für ungültig erklärt. Er begründete dies in seinem Urteil vom 16. Juli 2020 u. a. mit einer unverhältnismäßigen Überwachung durch US-Geheimdienste und einem unzureichenden Rechtschutzfür EU-Bürger gegenüber US-Geheimdiensten.

Im März 2022 gab die EU-Kommission schließlich bekannt, dass man sich mit den USA auf ein neues Abkommen geeinigt habe. Ein halbes Jahr später, am 7. Oktober, wurde diese grundsätzliche Einigung durch eine Verfügung des US-Präsidenten („Executive Order on Enhancing Safeguards for United States Signal Intelligence Activities“) in US-Recht umgesetzt. Sie richtet sich an die Intelligence Community, also an alle 18 US-Geheimdienste, und sieht u. a. die Einführung eines Verhältnismäßigkeitsgrundsatzes sowie weiterer Rechtsbehelfsmechanismen vor (so z. B. die Möglichkeit, Entscheidungen des Civil Liberties Protection Officer vor dem Data Protection Review Court anzufechten).

Der Europäische Datenschutzausschuss (EDSA) begrüßt die Verbesserungen, äußert in seiner Stellungnahme vom 28. Februar 2023 jedoch auch einige Bedenken.

Der neue Angemessenheitsbeschluss, auch als Privacy Framework bezeichnet, dürfte den aktuellen Prognosen zufolge dennoch etwa Mitte des Jahres 2023 wirksam werden. Allerdings erscheint der künftige Gang zum Europäischen Gerichtshof (EuGH) als vorhersehbarer Verlauf.

Für den Fall, dass kein Angemessenheitsbeschluss zustande kommen sollte oder dieser vor dem EuGH erneut für ungültig erklärt wird, will Microsoft mit der sogenannten EU Data Boundary aber bereits Vorsorge treffen. Danach soll bis 2024 sichergestellt werden, dass grundsätzlich alle personenbezogenen Daten in europäischen Rechenzentren verarbeitet werden. Bei der Bewertung der Wirksamkeit dieser Strategie sind jedoch etwaige extraterritorial wirkende Rechtsvorschriften (wie der US-CLOUD-Act) zu berücksichtigen.

Risikobeurteilung und -behandlung

Die Diskussionen rund um den DSK-Beschluss und die Befugnisse US-amerikanischer Geheimdienste sollten jedoch zu keiner Schieflage gegenüber der Einhaltung elementarer datenschutzrechtlicher Anforderungen führen.

So stellt sich beispielsweise schon zu Beginn eines Projekts die Frage nach der Notwendigkeit zur Durchführung einer Datenschutz-Folgenabschätzung (DSFA). Der Blick ins Gesetz und auf die Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, liefert hierzu jedoch keine eindeutige Antwort. Verantwortliche müssen daher im Vorfeld unternehmensindividuell evaluieren, ob durch die Nutzung von Microsoft 365 die Schwelle eines voraussichtlich hohen Risikos für die Betroffenen überschritten wird. Hierzu ist eine ganzheitliche Bewertung vorzunehmen, bei der verschiedene Aspekte des jeweiligen Einzelfalls berücksichtigt werden müssen, insbesondere die Art, der Umfang, die Umstände und die Zwecke der geplanten Datenverarbeitung. Denkbar ist dabei auch, dass zwar nicht für das Gesamtprodukt, wohl aber für einzelne, besonders problematische Dienste eine Datenschutz-Folgenabschätzung durchgeführt wird.

Die Nutzung vorkonfektionierter Datenschutz-Folgenabschätzungen ist häufig nicht zielführend und in Unternehmen mit erprobtem Prozess zur Erstellung einer DSFA auch nicht erforderlich. Eine DSFA für Microsoft 365 (oder Teile davon) sollte dem Standard-Unternehmensmuster folgen und in die eigene DSFA-Landschaft passen.

Technische und organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen, die gemäß DSGVO erforderlich sind, um die Datensicherheit bei der Verarbeitung personenbezogener Daten in Microsoft 365 sicherzustellen, können je nach Größe, Art und Umfang des Unternehmens variieren. Deren Festlegung und Dokumentation ist auch dann erforderlich, wenn keine DSFA durchgeführt wird. Microsoft bietet hierzu zahl-

reiche Optionen, deren Verfügbarkeit jedoch von der gewählten Lizenz abhängt. Exemplarisch kann Folgendes genannt werden:

- Datenverschlüsselung (Microsoft Managed Key, Customer Key, DKE)
- E-Mail-Verschlüsselung (OME, IRM, S/MIME)
- Nutzung der „Customer Lockbox“
- Nutzung von Bordmitteln zur Steuerung und Visualisierung der Sicherheit des Tenants
- Conditional Access und Multi-factor Authentication (MFA)

Das bestehende Löschkonzept muss überarbeitet und im Übrigen auf Microsoft 365 angewendet werden. Dies kann unter Verwendung von Datenklassifizierungswerkzeugen erfolgen.

Überdies bedarf es Festlegungen organisatorischer Art, etwa zum Umgang mit Funktionen, die im Rahmen des operativen Datenschutzes zum Einsatz kommen können, über grundlegende Entscheidungen zur Aktivierung/Deaktivierung kritischer Dienste bzw. Komponenten und zu einem fortlaufenden Monitoring von Updates, Erweiterungen und sonstigen Änderungen.

Weitere Vorgaben für Sicherheitsmaßnahmen werden für gewöhnlich nach einer bekannten Methodik aus dem Informationssicherheitsmanagement abgeleitet und in den entsprechenden Standards und Richtlinien detailliert beschrieben.

Die Prognose: Wechselhafte Wetterlage mit sonnigen Aussichten

Das Datenschutzgewitter scheint abzuflauen und stattdessen heitere Schönwetterwolken am Microsoft-365-Horizont aufzuziehen. In allen relevanten Bereichen sind – wie oben dargelegt – deutliche Fortschritte erkennbar. Die Restrisiken, die im Wesentlichen mit Anhörungen bzw. Maßnahmen seitens der zuständigen Datenschutz-Aufsichtsbehörde verbunden sind, müssen akzeptiert werden.

Eine erfolgreiche Einführung von Microsoft 365 erfordert jedoch eine sorgfältige Planung und Umsetzung. Da Datenschutz- und Compliance-Anforderungen in jeder Umsetzungsphase zu berücksichtigen sind, gilt dies auch für die Einbindung der entsprechenden Fachexperten.

Gerade in kleinen und mittleren Unternehmen wird hierzu in Ermangelung entsprechender Funktionsträger mit Verantwortung für Datenschutz und Informationssicherheit häufig auf die jeweiligen Beauftragten zurückgegriffen. Mit diesen sollte daher vor Beginn des Projekts eine klare Absprache bezüglich der Ressourcenplanung und -verwaltung getroffen werden. Bei Bedarf sollten die Kontingente angepasst werden.

Die datenschutzrechtlichen Fragen bleiben trotz des neuen Angemessenheitsbeschlusses und der EU Data Boundary zahlreich und die Aufgaben zur Einhaltung und Aufrechterhaltung der formalen Rechtmäßigkeit vielfältig. Neben einer gewissenhaften Dokumentation von DSFA und TOM sowie der Prüfung der vertraglichen Rahmenbedingungen (und deren regelmäßiger Aktualisierung) muss schließlich auch eine laufende Überprüfung und Bewertung der technischen Änderungen sichergestellt sein.

Nicht zuletzt müssen auch die Beschäftigten von den neuen Lösungen überzeugt werden und muss die Datenverarbeitung ihnen gegenüber transparent dargestellt werden. Der Betriebsrat ist aufgrund seines Mitbestimmungsrechts einzubinden, wobei etwaige datenschutzrechtliche Bedenken ausgeräumt und entsprechende Festlegungen und Absprachen Eingang in eine Betriebsvereinbarung finden sollten.

Die Einführung und Nutzung von Microsoft 365 kann nur als Gemeinschaftsleistung gelingen, bei der jeder einzelne Beitrag zum Schutz der Daten von Beschäftigten und Kunden sowie zur effizienten Nutzung der Plattform unverzichtbar ist. ▬

Maximilian Schmidt
Beauftragter Informationssicherheit und Datenschutz,
E-Mail: maximilian.schmidt@dz-cp.de

Digitale operationale Resilienz

Die neue EU-Verordnung zur digitalen operationalen Resilienz im Finanzsektor (DORA) legt ihren Fokus auf eine angemessene Cybersicherheit.

Im Dezember des vergangenen Jahres wurde eine neue, für Finanzunternehmen compliancerelevante Verordnung durch die europäische Legislative verabschiedet. Die Verordnung zur digitalen operationalen Resilienz im Finanzsektor – **D**igital **O**perational **R**esilience **A**ct, kurz DORA – trägt der zunehmenden Digitalisierung und Vernetzung dieses Sektors Rechnung. Sie normiert Standards, für einen EU-weit harmonisierten Umgang mit Risiken aus der Nutzung von Informations- und Kommunikationstechnologien (IKT).

Als „digitale operationale Resilienz" im Sinne der DORA-Verordnung wird die Fähigkeit verstanden, operative Integrität und Betriebszuverlässigkeit aufzubauen, fortwährend zu gewährleisten und zu überprüfen. Dazu gehören alle Maßnahmen des Instituts, die notwendig sind, um die Sicherheit der Informationssysteme und Netzwerke zur kontinuierlichen Erbringung von Finanzdienstleistungen und deren Qualität zu gewährleisten.

Mit der DORA werden damit erstmals konkrete und konsolidierte Anforderungen an die Finanzunternehmen gerichtet, die nicht durch finanzielle Resilienz zur Finanzstabilität und Marktintegrität beitragen, sondern diese auch durch angemessene Cybersicherheit stärken.

Im Fokus steht nunmehr konkret das operationelle Risiko aus dem Bezug von Informations- und Kommunikationstechnologie und somit die Kategorie der nicht-finanziellen Risiken.

DORA-Check-up

Wie bereits bei der Veröffentlichung der bankaufsichtlichen Anforderungen an die IT (BAIT) unterstützt die DZ CompliancePartner Sie gerne bei der Umsetzung der DORA. So führen wir gemeinsam mit Ihnen eine Reifegradanalyse Ihres Unternehmens bzgl. der DORA durch und ermitteln so relevante Gaps. Basierend auf den Ergebnissen können anschließend angemessene Handlungsbedarfe ermittelt und eine Priorisierung der nachfolgenden Schritte vorgenommen werden. So kann der Aufwand für die Umsetzung der komplexen Anforderungen bestmöglich eingeschätzt werden. Mit Veröffentlichung der Rechtsakte im kommenden Jahr erhalten Sie eine konkrete Maßnahmenliste von uns, anhand derer Sie sämtliche Anforderungen anhand der Zuständigkeiten festhalten und terminieren können.

Umsetzungsfristen und -anforderungen

Analog der Datenschutz-Grundverordnung (DSGVO), existiert eine Implementierungsfrist von 24 Monaten, womit die DORA verbindlich ab dem 17. Januar 2025 in den Mitgliedstaaten anzuwenden ist.

Inhaltlich soll das hohe Niveau an digitaler operationaler Resilienz durch folgende Anforderungen erreicht werden:

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

Michael Switalla
Abteilungsleiter
Informationssicherheit & Datenschutz,
E-Mail: michael.switalla@dz-cp.de

- Risikomanagement im Bereich der Informations- und Kommunikationstechnologie (IKT)
- Meldung schwerwiegender IKT-bezogener Vorfälle und – auf freiwilliger Basis – erheblicher Cyber-Bedrohungen an die zuständigen Behörden
- Meldung schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfälle durch bestimmte Finanzunternehmen an die zuständigen Behörden
- Tests der digitalen operationalen Resilienz
- Austausch von Informationen und Erkenntnissen in Bezug auf Cyber-Bedrohungen und Schwachstellen
- Maßnahmen für das solide Management des IKT-Drittparteienrisikos

Anders als bei früheren Rechtsakten der Union rückt der traditionelle quantitative Risikomanagement-Ansatz hier in den Hintergrund und weicht einem gezielt qualitativen Ansatz, welcher einen eindeutigen Bezug zu den IKT-Risiken herstellt.

Im Ergebnis sollen Finanzunternehmen europaweit dazu befähigt werden, die IKT-Risiken nach denselben Grundregeln zu bewältigen. Proportional werden hier Faktoren wie das jeweilige Gesamtrisikoprofil oder die Größe des Unternehmens berücksichtigt.

Wie der BVR in seinem Rundschreiben vom 10. Januar 2023 informierte, ist der konkrete Handlungsbedarf für die Genossenschaftsbanken erst nach Vorliegen der technischen Regulierungsstandards vollständig ermittelbar. Diese werden über delegierte Rechtsakte planungsgemäß zu Beginn des Jahres 2024 bis hin zur zweiten Jahreshälfte 2024 erstellt. Innerhalb der Genossenschaftlichen FinanzGruppe werden geeignete Aktivitäten aufgesetzt und sukzessive ein Umsetzungsfahrplan für DORA im Zusammenspiel mit den technischen Regulierungsstandards erarbeitet. ▬

Anzeigenverordnung und Auslagerungsmanagement

Änderung der Anzeigenverordnung führt zur Anzeigepflicht wesentlicher Auslagerungen

Mit Inkrafttreten der 4. Änderung der Anzeigenverordnung (AnzV) am 29. November 2022 sind die Anzeigepflichten bei Auslagerungen konkretisiert worden. Inhaltlich geht es dabei um

- die Anzeige der Absicht,
- des Vollzugs,
- wesentlicher Änderungen sowie
- schwerwiegender Vorfälle

im Rahmen von bestehenden oder beabsichtigten (wesentlichen) Auslagerungen.

Damit einhergehend steht nun auch das neue Fachverfahren zur Anzeige von Auslagerungen im BaFin-Portal zur Melde- und Veröffentlichungsplattform (MVP-Portal) zur Verfügung.

In Gesprächen mit unseren Kunden haben wir diesbezüglich Klärungsbedarf festgestellt. Im folgenden Artikel wollen wir daher einen Überblick zum praktischen Umgang mit der Pflicht zur Anzeige von Auslagerungen und der Arbeit im MVP-Portal geben.

Hintergrund

Mit den Anzeigepflichten verbindet die Aufsicht das Ziel, potenziellen Konzentrationsrisiken aus der zunehmenden Anzahl von Auslagerungen im Finanzsektor entgegenzuwirken und eine entsprechende Überwachung sicherzustellen. Aus diesem Grunde wurden mit dem Finanzmarktintegritätsstärkungsgesetz und dem Wertpapierinstitutsgesetz neue, umfangreiche Anzeigepflichten für Auslagerungen beschlossen. Diese Pflichten sollten eigentlich ab dem 1. Januar 2022 gelten.

Im Januar 2022 hat die BaFin dann mitgeteilt, dass die Änderungen der KWG- (und KAGB-)AnzV nicht bereits am 1. Januar 2022 in Kraft treten, sondern bis zum Inkrafttreten der Änderung der AnzV keine Auslagerungsanzeigen einzureichen sind.

Anzeigepflichten

Mit Inkrafttreten der 4. Änderung der AnzV Ende November 2022 sind nun vielfältige Pflichten der Institute eingetreten:

1. Anzeige der Absicht und des Vollzugs von wesentlichen Auslagerungen

Steht eine neue wesentliche Auslagerung an, so sind die Meldungen mehrstufig abzugeben: Zunächst ist die Absicht und dann der Vollzug der Auslagerung der BaFin zu melden. Unter Absicht einer Auslagerung kann man den finalen Willen oder die getroffene Entscheidung zur Auslagerung verstehen, z. B. wenn die Bank sich für einen konkreten Dienstleister entschieden hat. Zu diesem Zeitpunkt sind die Daten des Dienstleisters auch bekannt und können in der Absichtsanzeige mitgeteilt werden.

Unter Vollzug der Auslagerung wird der Abschluss des entsprechenden Auslagerungsvertrages verstanden. Auch ist der Zeitpunkt des Vertragsbeginns anzugeben, also wann die ausgelagerte Tätigkeit vom Auslagerungsdienstleister aufgenommen wird. Das ist nach den Vorgaben der AT 9 MaRisk zwingend zu vereinbaren.

Absicht und Vollzug sind auch dann zu melden, wenn die interne Entscheidung zur Auslagerung (Absicht) und die Unterzeichnung des Auslagerungsvertrages (Vollzug) sehr eng beieinander liegen, z. B. ein bis zwei Wochen. Eine zusammengefasste Meldung oder ein Verzicht auf die Abgabe der Absichtsmeldung ist nicht zulässig.

2. Anzeige von wesentlichen Änderungen von wesentlichen Auslagerungen

Bei diesem Themenkomplex wird es spannend, da vielfältige Möglichkeiten denkbar sind. So kann es inzident zu einer Nachmeldung einer wesentlichen Auslagerung kommen, selbst wenn diese vor dem 1. Januar 2022 bestand. Eine wesentliche Änderung einer wesentlichen Auslagerung ist u. a. in folgenden Fällen gegeben:

- Vertragsänderungen von wesentlicher Bedeutung,
- Vereinbarungen zusätzlicher vertraglicher Regelungen, insbesondere der Vereinbarung zusätzlicher Leistungen,
- Änderung der Bewertung, ob eine Auslagerung als wesentlich oder unwesentlich einzustufen ist,
- wesentlichen Abweichungen, die sich aufgrund einer neuen oder geänderten Risikoanalyse bezüglich der Auslagerung ergeben,
- Abschluss neuer Subauslagerungen wesentlicher Teile einer wesentlichen Aktivität oder eines wesentlichen Prozesses,
- Änderung der Einschätzung zur Ersetzbarkeit des Auslagerungsunternehmens,
- nachträglicher Verlagerung der Erbringung von Dienstleistungen in Drittstaaten durch das Auslagerungsunternehmen oder seine beauftragten Subunternehmen,
- Kündigung oder sonstiger Beendigung des Auslagerungsvertrags,
- Kenntnis des Instituts von der Übernahme der Kontrolle über das Auslagerungsunternehmen durch ein anderes Unternehmen.

Liegt einer der zuvor genannten Fälle vor, so hat zwingend eine Meldung über das MVP-Portal an die Bafin zu erfolgen, wenn die wesentliche Änderung ab dem 1. Januar 2022 eingetreten ist.

Die Besonderheit besteht nun darin, dass nicht isoliert eine bloße Änderungsmitteilung (u. a. braucht es eine Referenznummer) über das MVP-Portal abgegeben werden kann, sondern zuvor

- die Absicht der wesentlichen Auslagerung anzuzeigen ist (nachträglich),
- der Vollzug der wesentlichen Auslagerung anzuzeigen ist (nachträglich) und
- die wesentliche Änderung der wesentlichen Auslagerung anzuzeigen ist.

Hierdurch kommt es rein praktisch zu einer Nachmeldung einer wesentlichen Auslagerung, auch wenn bloß eine Änderungstatsache eingetreten ist.

Damit ist faktisch eine Nachmeldepflicht von Auslagerungen, die vor dem 1. Januar 2022 bestanden – sozusagen durch die Hintertür – eingeführt worden: nämlich für den Fall, dass eine wesentliche Änderung der wesentlichen Auslagerung im Jahr 2022 stattgefunden hat.

Viele der Auslagerungsunternehmen haben im Jahr 2022 ihre Auslagerungsverträge an die zwingenden Anforderungen des AT 9 Tz. 7 MaRisk bei wesentlichen Auslagerungen angepasst. Diese Anpassungen dürften nicht nur redaktionelle Änderungen, sondern Vertragsänderungen von wesentlicher Bedeutung im Sinne der AnzV sein. Das bedeutet, dass die zugrundeliegenden wesentlichen Auslagerungen nachzumelden sind.

Es besteht jedoch auch die Möglichkeit, dass für einen Auslagerungstatbestand gleich mehrere Meldungen abzugeben sind. Bestand die Auslagerung vor dem 1. Januar 2022 und es erfolgt ein Dienstleisterwechsel, so sind grundsätzlich folgende Meldungen notwendig:

(1) Vollzug über den Auslagerungsvertrag mit Dienstleister A
(2) Änderungsanzeige für die Beendigung des Vertrages mit Dienstleister A
(3) Absichtsanzeige für Dienstleister B

Fallen die Anzeigen (1) und (2) zeitlich zusammen, z. B. aufgrund mangelnder Pflicht zur Anzeige von Auslagerungen von vor dem 1. Januar 2022 oder aufgrund der Frist zur Nachmeldung der Anzeigen ab dem 1. Januar 2022, so kann ausnahmsweise auf die Anzeigen (1) und (2) verzichtet werden. Durch den engen zeitlichen Zusammenhang besteht in diesen Fällen für die Aufsicht kein Handlungsbedarf mehr. In einem solchen Fall ist dann nur die Anzeige (3) vorzunehmen.

Beruht eine wesentliche Änderung auf mehreren Sachverhalten, so sollen alle bekannten Änderungsgründe in einer Anzeige gemeldet werden. Abmeldungen von Subauslagerungen können über eine Änderungsmeldung erfolgen.

Bei Fusionen muss das übernommene Institut die Beendigung der Auslagerung mit einer Änderungsanzeige anzeigen (§ 3 Abs. 2 Nr. 8 AnzV) und das übernehmende Institut die übernommenen Auslagerungen anzeigen. Details sollten mit dem Fachaufseher abgestimmt werden. Im Falle der Kündigung eines Auslagerungsvertrages sind sowohl der Zeitpunkt der Kündigung als auch der letzte Tag des Auslagerungsverhältnisses anzugeben.

3. Anzeige schwerwiegender Vorfälle im Rahmen von wesentlichen Auslagerungen

Schwerwiegende Vorfälle im Rahmen einer bestehenden wesentlichen Auslagerung sind ebenfalls der BaFin zu melden. Entsprechende schwerwiegende Vorfälle sind bspw.

- nicht nur kurzfristige Unterbrechung oder Unmöglichkeit der Erbringung der ausgelagerten wesentlichen Aktivität oder des wesentlichen Prozesses,
- erhebliche Vertragsverletzungen durch das Auslagerungsunternehmen,
- erhebliche Rechtsverstöße, insbesondere durch den Wegfall der aufsichtsrechtlichen Voraussetzungen der Auslagerung, durch umfassende Einschränkungen von Informations- und Prüfrechten des Instituts oder der Aufsichtsbehörde oder durch Verstöße des Auslagerungsunternehmens gegen datenschutzrechtliche Bestimmungen,
- fehlende oder unzureichende Bereitschaft des Auslagerungsunternehmens, aufsichtliche Anordnungen umzusetzen oder an deren Umsetzung mitzuwirken, insbesondere im Rahmen der Missstandsbeseitigung und -vermeidung,
- erhebliche Sicherheitsvorfälle im Zusammenhang mit den ausgelagerten Aktivitäten und Prozessen beim Institut oder beim Auslagerungsunternehmen,
- unzureichendes Risiko- und Notfallmanagement des Auslagerungsunternehmens,
- unzureichende Ressourcen des Auslagerungsunternehmens für die ordnungsgemäße Ausführung der ausgelagerten Aktivitäten oder Prozesse,
- Kenntnis des Instituts von Umständen, nach denen eine leitende Person des Auslagerungsunternehmens nicht als zuverlässig betrachtet werden kann,
- fehlende oder unzureichende Unterstützung durch das Auslagerungsunternehmen bei Beendigung der Auslagerung,
- drohende Zahlungsunfähigkeit des Auslagerungsunternehmens,
- Kenntnis des Instituts von schwerwiegenden Reputationsschäden beim Auslagerungsunternehmen,
- Konflikte am Sitz des Auslagerungsunternehmens in einem Drittstaat, die zu einer wesentlichen Gefährdung der ausgelagerten Aktivitäten und Prozesse führen oder dazu führen könnten.

Dies alles sind Sachverhalte, die einen wesentlichen Einfluss auf die Tätigkeit und somit mittelbar auf die Zuverlässigkeit des Auslagerungsunternehmens haben können und dementsprechend an die Aufsicht zu melden sind.

Fristen

Mit Inkrafttreten der 4. Verordnung zur Änderung der AnzV besteht seit dem 29. November 2022 eine umfassende Anzeigepflicht von Vorfällen bei wesentlichen Auslagerungen.

Mit Inkrafttreten der Anzeigenverordnung waren darüber hinaus die ab dem 1. Januar 2022 bis zum 28. November 2022 erfolgten Auslagerungen entsprechend den Vorgaben der genannten Verordnung bis zum 1. März 2023 über das MVP-Portal nachzumelden.

Eine Nachmeldepflicht für vor dem 1. Januar 2022 bestehende wesentliche Auslagerungen ist in der 4. Verordnung zur Änderung der AnzV nicht mehr vorgesehen. Für diese Vorgänge bedarf es daher keiner Nachmeldung – es sei denn, eine wesentliche Änderung ist eingetreten (siehe oben bei „Anzeige von wesentlichen Änderungen"). Die Aufnahme ins Auslagerungsregister der Bank ist gleichwohl vorzunehmen.

Seit dem 1. Januar 2022 eingetretene Vorgänge zu wesentlichen Auslagerungen lassen sich wie folgt zusammenfassen:

- Anzuzeigen ist die Absicht einer wesentlichen Auslagerung.
- Anzuzeigen ist der Vollzug einer wesentlichen Auslagerung.
- Anzuzeigen ist ebenfalls die wesentliche Änderung einer wesentlichen Auslagerung.
- Anzuzeigen ist ein schwerwiegender Vorfall bei einer wesentlichen Auslagerung.
- Sofort anzuzeigen sind Vorgänge, die ab dem 29. November 2022 eingetreten sind.
- Vorgänge, die zwischen dem 1. Januar 2022 und dem 28. November 2022 eingetreten waren, mussten bis zum 1. März 2023 nachgemeldet werden.

MVP-Portal

Anzeigen betreffend Absicht, Vollzug oder wesentliche Änderungen von wesentlichen Auslagerungen sind über das MVP-Portal der BaFin auf elektronischem Weg durchzuführen.

1. Technische Besonderheiten des MVP-Portals
Beim MVP-Portal gibt es einige technische Besonderheiten zu beachten: Das MVP hat keinen Zugriff auf alte Meldungen und kann somit Felder nicht automatisch befüllen. Auch sind abgegebene Meldungen nicht mehr nachträglich einsehbar, sondern müssen zum Zeitpunkt der Erstellung von der Bank selbst abgespeichert werden. Darüber hinaus besteht keine Möglichkeit, die im MVP hinterlegten Daten insgesamt oder pro Auslagerung einzusehen. Ein Zwischenspeichern von Daten ist nicht vorgesehen, auch erfolgt nach 60 Minuten eine automatische Abmeldung und nicht versendete Daten sind nicht mehr vorhanden.

2. Inhaltliche Besonderheiten des MVP-Portals
Neben den technischen Besonderheiten weist das MVP-Portal auch inhaltliche Besonderheiten auf, dies betrifft u. a. die Fragen nach dem Grund der Auslagerung (als Pflichtfeld gekennzeichnet), nach den Interessenkonflikten sowie nach dem Namen der Kontaktperson beim Auslagerungsunternehmen, die allesamt keine Pflichtfelder für Kreditinstitute im MVP-Portal sind.

Bei Cloud-Auslagerungen wird nur auf den ersten Grad der Auslagerung abgestellt, handelt es sich hingegen erst bei der Weiterverlagerung um eine Cloud-Auslagerung, so ist dies kein Fall einer Auslagerungsanzeige nach § 3 Absatz 1 Nr. 9 AnzV.

Erfolgt eine gruppen- oder verbundinterne Auslagerung, so findet hinsichtlich des Begriffs „verbundintern" das bestehende MaRisk-Verständnis von „verbundintern" Anwendung: Es greift die Erleichterung nach AT 9 Tz. 15 lit. d MaRisk, wonach bei gruppen- und verbundinternen Auslagerungen auf die Erstellung von Ausstiegsprozessen und Handlungsoptionen verzichtet werden kann. In diesen Fällen müssen keine Ausstiegs- und Handlungs-

optionen beschrieben werden, sondern es muss lediglich eine Risikoeinschätzung vorgenommen werden.

Auch ist in der AnzV eine Änderung dahingehend geplant, dass der Einreichungsweg für verbundangehörige Institute über den Prüfungsverband lediglich optional und nicht verpflichtend ist. Bei dem anderslautenden Wortlaut in § 1 Absatz 2 AnzV handelt es sich um ein redaktionelles Versehen und die Empfehlung lautet, die Anzeigen nach § 24 Absatz 1 Nr. 19 KWG direkt an die Aufsicht zu richten.

Excel-Template bei Anzeige schwerwiegender Vorfälle

Schwerwiegende Sicherheitsvorfälle sind per Excel-Template an die BaFin und die Bundesbank zu melden. Für das Excel-Template gibt es keine Ausfüllhilfe, eine solche ist nach bisherigem Wissen auch nicht geplant. Auch ist es nicht geplant, die Anzeige der schwerwiegenden Vorfälle in das MVP-Portal zu integrieren. Sofern ein PSD2-Zahlungssicherheitsvorfall vorliegt, ist keine Doppelmeldung erforderlich. Meldungen über schwerwiegende Betriebs- und Sicherheitsvorfälle bei Zahlungsdienstleistungen (PSD2-Meldungen) sind auch weiterhin ausschließlich über das MVP-Portal der BaFin zu versenden, da das Verfahren zur Abgabe von PSD2-Meldungen spezieller als die allgemeine Anzeige schwerwiegender Vorfälle ist.

Fazit

Mit der Umsetzung der Anzeigenverordnung und dem damit einhergehenden Fokus der Aufsicht auf die Auslagerungen wird die Auswahl verlässlicher Dienstleister noch wichtiger. ▬

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

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

Sind Beauftragtentätigkeiten in Eigenregie noch leist- und bezahlbar?

Ist es vorteilhafter, die Beauftragtentätigkeiten mit bankeigenen Ressourcen selbst auszuführen oder sich diese von einem spezialisierten Dienstleister einzukaufen? Vor über zehn Jahren wurde die klassische „Make or Buy"- Entscheidung (MoB) in dieser Zeitschrift diskutiert. Zur Untersuchung dienten dabei vier strategische Leitfragen:

1. Ist die Beauftragtentätigkeit für die Bank strategisch relevant?
2. Gibt es aufsichtsrechtliche Restriktionen, die eine MoB-Entscheidung beeinflussen oder gar determinieren?
3. Wie hoch sind die Produktionskosten bzw. Kaufpreise der beiden Varianten Make or Buy?
4. Welche Transaktionskosten sind neben den reinen Produktionskosten zu berücksichtigen (vor allem beim Einkauf der Leistungen)?

Mit Beauftragtentätigkeiten kann sich eine Bank kein strategisches Alleinstellungs- oder Differenzierungsmerkmal erarbeiten. Für sogenannte (nationale) Less-significant Institutions (LSIs) oder nach den MaRisk unbedeutende Institute (im Umkehrschluss zu AT 1 TZ 6) existieren bis heute keine oder wenige Auslagerungshürden.

Die Aufwände der Eigenfertigung der Beauftragtentätigkeiten hängen also stark von den damit verbundenen Kosten ab.

Doch was hat sich in den vergangenen zehn Jahren getan? Die Aufwände sind gestiegen. Dieses allgemeine Urteil wird so weit allgemein akzeptiert. Es lohnt sich, genauer hinzuschauen und einzelne Bereiche zu betrachten, damit plausible Einschätzungen qualifiziert und quantifiziert werden können (siehe Übersicht der wesentlichen Änderungen auf der Folgeseite).

Mehr Komplexität, mehr Anspruch, mehr Verantwortung

Die starke Entwicklung der Anforderungen an die einzelnen Beauftragtenfelder wirkt sich direkt auf die Aufgabenstellungen der Beauftragtenfunktionen aus. Durch die massive Ausweitung führt das zu steigenden qualitativen und quantitativen Anforderungen an die Ressourcen in der Bank und damit zu Aufwandserhöhungen und damit zu einem quantitativen Aufwandsaufwuchs.

Darüber hinaus leidet auch unsere Branche unter einem erheblichen Fachkräftemangel. Beauftragtenfunktionen sind Spezialistenfunktionen, das bedeutet, dass entsprechende Qualifikationen nicht so ohne Weiteres zu finden sind. Und selbst wenn sie gefunden werden, wie lange können sie gehalten werden? Gerade Spezialisten sind umworben auf dem Arbeitsmarkt.

Es ist heute noch anspruchsvoller als vor zehn Jahren, die Beauftragtenfunktionen mit eigenen verfügbaren Mitteln der Bank darzustellen. Das gilt bezüglich des Zuwachses und der allgemeinen Menge der zu bewältigenden Aufgaben und der erforderlichen Qualifikationen des Personals in Zeiten von Personalmangel. Zudem ist eine große Herausforderung die Pflicht zur laufenden Fort- und Weiterbildung, die gewährleistet sein muss, damit das aufsichtsrechtliche Wissen immer auf dem aktuellen Stand ist.

Fazit

Eine Standortbestimmung zum Thema Beauftragtenfunktionen ist für jede Bank wichtig, damit zukünftige Planungen hierzu klar und tragfähig werden. ▬

Wesentliche Entwicklungen und Änderungen in den Beauftragtentätigkeiten der letzten zehn Jahre

Eckpunkte in der WpHG-Compliance

1. Die MAR (Market Abuse Regulation) ist eine EU-Verordnung, die im Juli 2016 in Kraft getreten ist und darauf abzielt, den Marktmissbrauch im europäischen Finanzmarkt zu bekämpfen. Die wichtigsten Regelungen der MAR sind:
   – Insiderhandel
   – Marktmanipulation
   – Meldepflichten
   – Verbot von Marktmanipulation, Insidergeschäften und unrechtmäßiger Offenlegung von Insiderinformationen
   – Sanktionen

2. Die Wertpapierdienstleistungs-Verhaltens-und Organisationsverordnung (WpDVerOV) von Oktober 2017 legt weitere Anforderungen an die Organisation von Wertpapierdienstleistungsunternehmen fest, einschließlich der qualitätsverbessernden Verwendung von Zuwendungen. Abgerundet wird dies durch Bestimmungen zur Dokumentation von Geschäftsprozessen, zur Durchführung von Kundenaufträgen und zu Anforderungen an das Produktfreigabeverfahren.

3. Die MiFID II (Markets in Financial Instruments Directive II) ist eine EU-Richtlinie, die im Januar 2018 in Kraft getreten ist. Die Richtlinie enthält umfassende Bestimmungen zum Anlegerschutz. Weiterhin legt die Richtlinie die Pflichten von Banken und Wertpapierdienstleistungsunternehmen fest. Die MiFID II enthält Bestimmungen zur „bestmöglichen Ausführung" (Best execution) von Aufträgen, um sicherzustellen, dass Banken und Wertpapierdienstleistungsunternehmen die bestmöglichen Ergebnisse für ihre Kunden erzielen. Die Richtlinie verlangt von Banken und Wertpapierdienstleistungsunternehmen die Aufzeichnung und Meldung von Transaktionen, um die Marktintegrität und Überwachung von Marktmissbrauch zu stärken.

4. Die Mindestanforderungen an die Compliance-Funktion und die weiteren Verhaltens-, Organisations- und Transparenzpflichten (MaComp) sind eine Sammlung von Standards für die WpHG-Compliance-Organisation und konkretisieren die Anforderungen des WpHG. Die MaComp wurden mehrfach aktualisiert, zuletzt im März 2021.

Eckpunkte in der Geldwäsche- und Betrugsprävention

Nachdem das **Geldwäschegesetz** (GwG) in 2008 vollständig überarbeitet wurde (u. a. Einführung von „PEP" und des risikobasierten Ansatzes), erfolgten auch in den Folgejahren regelmäßige Anpassungen. So führte z. B. in **2017** die Umsetzung der Vierten EU-Geldwäscherichtlinie zu erheblichen Erweiterungen der Kundensorgfaltspflichten. Die Umsetzung der Fünften EU-Geldwäscherichtlinie in **2020** hatte weitere Erweiterungen und Verschärfungen des GwG zur Folge (u. a. Erweiterung der Anwendungsfälle verstärkter Sorgfaltspflichten bei Hochrisikoländern, Einrichtung eines Transparenzregisters). Darüber hinaus sah das „Transparenzregister- und Finanzinformationsgesetz" (TraFinG) in **2021** weitere Änderungen im GwG vor.

Als Kernelemente des **risikobasierten Ansatzes** führten die „Erste Nationale Risikoanalyse" aus **2019**, die von der BaFin in 2020 veröffentlichte „**Subnationale Risikoanalyse**" sowie die erstmals ab 2018 anzuwendenden „Leitlinien der EBA zu Risikofaktoren", die **2020** novelliert wurden, zu stetig steigenden Anforderungen.

Neben der Veröffentlichung der „**Allgemeinen Auslegungs- und Anwendungshinweise**" in **2018** (Aktualisierung in 2021) hat die BaFin in **2021** „**Besondere Auslegungs- und Anwendungshinweise für Kreditinstitute**" erlassen, die insbesondere detaillierte Leitlinien für den institutsindividuellen Einsatz von Monitoring-Systemen („Geno-SONAR") sowie die Beibringung von Herkunftsnachweisen bei Bartransaktionen vorsehen.

Mit dem **Gesetz zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche** wurde in **2021** durch den Wegfall des selektiven Vortatenkatalogs jede Straftat Vortat zur Geldwäsche.

Nicht zuletzt sind die steigenden Anforderungen aus den **Embargo- und Sanktionsvorschriften** zu nennen.

Ausblick: Aufbauend auf ihrem Aktionsplan von 2020 hat die **Europäische Kommission** in **2021** ein Legislativpaket vorgelegt, mit dem die Vorschriften der EU zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung gestärkt werden sollen. Das vorgelegte Paket besteht aus vier Gesetzgebungsvorschlägen:

– Verordnung zur Schaffung einer neuen EU-Behörde
– Verordnung mit unmittelbar geltenden Vorschriften in allen Mitgliedsländern
– Sechste EU-Geldwäscherichtlinie
– Überarbeitete Fassung der Geldtransfer-Verordnung

Eckpunkte im Datenschutz

2014: Die Europäische Union verabschiedet mit der Datenschutz-Grundverordnung (DSGVO), die 2018 in Kraft tritt, eine tiefgehende Reform des Datenschutzrechtes. Die DSGVO gilt auch für Banken und stärkt die Rechte von Kunden im Hinblick auf ihre personenbezogenen Daten. Neben Datenschutzverstößen werden auch Verstöße gegen datenschutzrechtliche Vorgaben an unternehmerische Prozesse bußgeldbewehrt und die Strafvorschriften massiv verschärft. Unter anderem müssen Banken für jede personenbezogene Verarbeitungstätigkeit eine Rechtsgrundlage (z. B. Einholung einer Einwilligungslösung, vertragliche oder vorvertragliche Verpflichtung) nachweisen können, bevor sie personenbezogene Daten von Kunden verarbeiten.

2018: Änderung des BDSG, um es an die DSGVO anzupassen. Die Änderungen enthalten u. a. spezifische Regelungen für die Verarbeitung von Kundendaten durch Banken. Der Datenschutz bleibt Ländersache, wodurch die Auslegung der Regelungen des BDSG und der DSGVO regionale Spezialitäten ausbildet.

2019: Das Bundesministerium der Finanzen veröffentlicht einen Entwurf für ein „Gesetz zur Stärkung des Datenschutzes im Finanzsektor" (FinDSG), das spezielle Datenschutzregeln für Banken und Versicherungen vorsieht. Das Gesetz wurde jedoch noch nicht verabschiedet.

2020: Der Europäische Gerichtshof (EuGH) entscheidet in einem Urteil, dass die deutsche Praxis der Speicherung von IP-Adressen durch Banken möglicherweise gegen die DSGVO verstößt.

Eckpunkte in der Informationssicherheit

2015: Die BaFin gibt eine Neufassung des „Rundschreibens 11/2011 (BA) - Mindestanforderungen an die Geschäftsorganisation von Banken" heraus. Es werden zusätzliche Anforderungen an die Informationssicherheit eingeführt, wie z. B. die Notwendigkeit eines IT-Sicherheitskonzepts.

2017: Das IT-Sicherheitsgesetz tritt in Kraft. Es verpflichtet Betreiber kritischer Infrastrukturen, einschließlich Banken, bestimmte Mindeststandards für die IT-Sicherheit einzuhalten und sicherheitsrelevante Vorfälle zu melden.

2017: Die BaFin veröffentlicht die BAIT (Bankausichtliche Anforderungen an die IT). Diese bündeln erstmalig die rechtlichen Anforderungen an die technisch-organisatorische Ausstattung der IT-Systeme, unter besonderer Berücksichtigung der Anforderungen an die Informationssicherheit sowie eines angemessenen Notfallkonzepts. Sie novelliert diese Regelungen bereits 2018 erstmalig, um sie dann 2021 ein weiteres Mal zu erneuern und zu ergänzen

2018: Die BaFin veröffentlicht eine neue Fassung des „Rundschreibens 10/2017 (BA) - Mindestanforderungen an das Risikomanagement (MaRisk)" mit spezifischen Anforderungen an das IT-Risikomanagement und die Informationssicherheit von Banken.

2019: Der Bundesverband deutscher Banken veröffentlicht ein neues „IT-Sicherheitsprofil für Kreditinstitute", das einen branchenspezifischen Ansatz zur Verbesserung der Informationssicherheit von Banken enthält.

2021: Am 12. August 2021 veröffentlicht die BaFin die BAIT-Novelle, die u.a. Schwerpunkte im Bereich „IT-Notfallmanagement" und „Operative Informationssicherheit" weiter konkretisiert.

2023: Der EU Digital Operational Resilience Act (DORA) wird verabschiedet und wird den Rahmen des ehedem schon komplexen Informationssicherheitsrechts in Deutschland bis 2025 nochmals spürbar neu ausrichten.

Eckpunkte in der MaRisk-Compliance

Die MaRisk-Compliance-Funktion wurde mit der 4. Novellierung der MaRisk 2012 als Bestandteil der Besonderen Funktionen nach AT 4.4. MaRisk verbindlich eingeführt und war mit Frist zum 1. Januar 2014 in den Instituten zu implementieren. Zwei weitere Novellen folgten, die 7. Novellierung steht bereits unmittelbar bevor.

1. **Erweiterung der Aufgabenbereiche:**
   War zu Beginn der MaRisk-Compliance-Funktion die Notwendigkeit von eigenen Kontrollhandlungen zumindest umstritten, hat sich in dem Verlauf der Jahre eine deutliche Erwartungshaltung zu eigenen Kontrollhandlungen der MaRisk-Commpliance-Funktion manifestiert.

2. **Steigerung regulatorischer Anforderungen:**
   Aufgabe der Compliance-Funktion ist es, den Risiken, die sich aus der Nichteinhaltung rechtlicher Regelungen und Vorgaben ergeben können, entgegenzuwirken. Nach einer Antwort der Bundesregierung (Druckssache 20/721) gab es im Jahr 2022 1.773 Gesetze (Anstieg 9 % ggü. 2012) mit rd. 50.700 Einzelnormen (Anstieg 17 %) und 2.795 Rechtsverordnungen (Anstieg 6 %) mit rd. 42.600 Einzelnormen (Anstieg 15 %).

3. **Umfassendes Berichtswesen:**
   Auch das zu sichtende Berichtswesen hat sich über die Jahre gewandelt. Neben immer umfangreicheren Berichten kommen auch weitere Berichte hinzu, zu nennen sind hier beispielsweise die Berichte des Single-Officers oder des Auslagerungsbeauftragten.

Martin Hierlemann
Bereichsleiter Vertrieb,
E-Mail: martin.hierlemann@dz-cp.de

Änderung in der Geschäftsführung

Dirk Pagel ist zum 1. Januar 2023 in die Geschäftsführung der DZ CompliancePartner GmbH berufen worden. Er wird die Nachfolge von Norbert Schäfer antreten und hat zunächst das Ressort Compliance (Wertpapier- und MaRisk-Compliance) übernommen.

Dirk Pagel war zunächst 16 Jahre in der WGZ BANK als Gruppen- und Abteilungsleiter tätig, ehe er seit 2016 in der DZ BANK unterschiedliche leitende Funktionen übernahm. Zuletzt hat er die Digitalisierung des End-to-End-Kreditprozesses verantwortet. Dirk Pagel ist ausgewiesener Experte im Bankgeschäft und zeichnet sich durch eine tiefe Kenntnis der Geschäftsmodelle der Volksbanken Raiffeisenbanken aus.

Norbert Schäfer wird – wie bei seinem Eintritt in die Gesellschaft im Frühjahr 2019 vorgesehen und seinem Wunsch entsprechend – am 1. Juli 2023 nach 42 Berufsjahren in den Vorruhestand treten. Die Ressorts Geldwäsche- und Betrugsprävention sowie Compliance-Spezialisten wird er bis zu seinem Ausscheiden fortführen und dann an Dirk Pagel übergeben. (red.) ▬

DZ CompliancePartner: Unternehmerischen Spielraum verschaffen – Regelkonformität gemeinsam sicherstellen.

Als Vollsortimenter im Beauftragtenwesen, tief verwurzelt im genossenschaftlichen Finanzverbund, stellen wir Ihnen eine Bandbreite an unterschiedlichen Lösungen von der Auslagerungsoption bis hin zu gezielten Beratungs- und Unterstützungsleistungen im sich stetig verändernden regulatorischen Umfeld zur Verfügung. Unser Ziel ist es dabei, Ihnen die größtmögliche unternehmerische Entlastung und gleichzeitig regulatorische Sicherheit zu verschaffen.

Ein partnerschaftlicher Dialog in der Zusammenarbeit, standardisierte, IT-unterstützte und effizient strukturierte Prozesse – vom Kunden her gedacht – sind für uns nicht nur eine Selbstverständlichkeit, sondern Teil unserer Unternehmens-DNA.

Eine stetige Weiterentwicklung dieses vorhandenen Fundaments zum Nutzen unserer Mandanten in einem auch zukünftig sich ändernden regulatorischen Umfeld ist mir persönlich wichtig.

Seit Januar 2023 in der Geschäftsführung der DZ-CompliancePartner: Dirk Pagel

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 gemäß MaRisk AT 4.4.3 und BT 2.

Seit der letzten Berichterstattung in der Point of Compliance (3/2022, S. 27) wurde aus der Jahresprüfungsplanung 2022 die Prüfung des Bereichs „Unternehmenssteuerung – Rechnungswesen & Controlling" abgeschlossen und, da nicht dienstleistungsbezogen, intern veröffentlicht. Darüber hinaus wurde turnusgemäß ein Bericht zum Prüffeld des Geschäftsbereichs „Geldwäsche- und Betrugsprävention" abgeschlossen und dieser dienstleistungsbezogene Bericht der Mandantschaft mit der entsprechenden Auslagerung zur Verfügung gestellt. Mit Abschluss dieser Prüfung wurde gleichzeitig der Prüfungsplan 2022 vollumfänglich erfüllt.

Der Jahresprüfungsplan der Internen Revision für 2023 wurde von der Geschäftsführung genehmigt. Aus dem Prüfungsplan wurde das Prüffeld „Vertriebsmanagement" bereits abgeschlossen und, da nicht dienstleistungsbezogen, intern veröffentlicht. Darüber hinaus wurde die Prüfung des Bereichs „Hinweisgebersystem" abgeschlossen. Dieser Bericht wird nach der Unterschriftsleistung durch die Geschäftsführung an die Mandantschaft versandt werden.

Der Quartalsbericht zum vierten Quartal 2022 der Internen Revision wurde fristgerecht erstellt und unserer Mandantschaft zur Verfügung gestellt. Ebenso wurde der Jahresbericht 2022 der Internen Revision fristgerecht an die Mandantschaft, die 2022 zu unserem Kundenstamm zählte, versandt.

Darüber hinaus wurde turnusgemäß ein Follow-up-Quartalsbericht für das vierte Quartal 2022 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 der DZ CompliancePartner GmbH und der Internen Revision regelmäßige Jours fixes statt.

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

Die externe Prüfung der Funktion Hinweisgebersystem nach IDW PS 331 erfolgte ebenfalls durch die Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft. Zum Zeitpunkt des Redaktionsschlusses war diese Prüfung noch nicht abgeschlossen und über das Ergebnis wird in der nächsten PoC berichtet werden. ▬

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