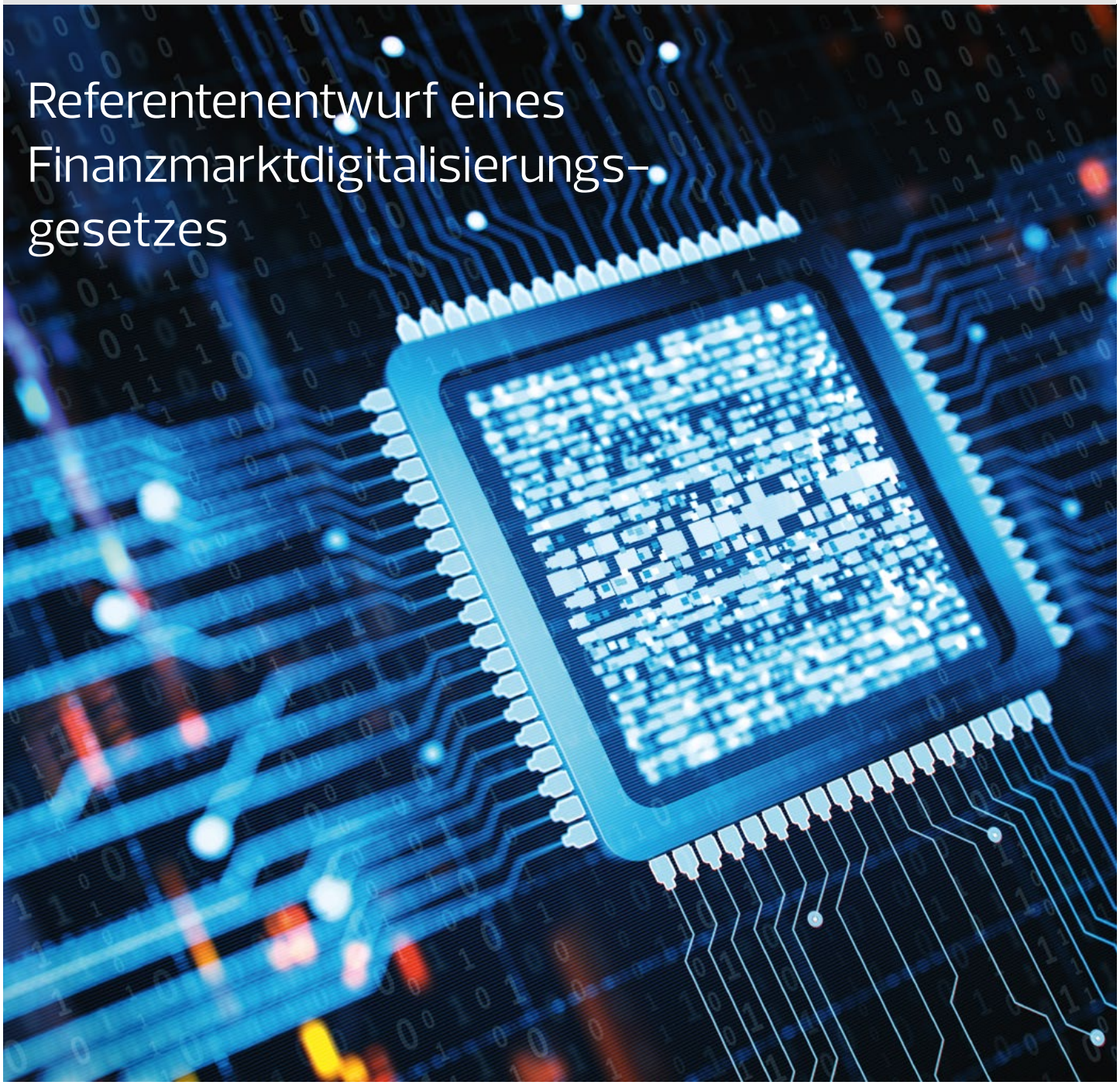
1. AUSGABE 2023

RSM EBNER STOLZ

novus

FINANCIAL SERVICES

Referentenentwurf eines Finanzmarktdigitalisierungs-gesetzes



Vorwort

Sehr geehrte Leserin, sehr geehrter Leser,

die Digitalisierung ist Grundlage einer zukunftsgerichteten und wettbewerbsfähigen Wirtschaft und schreitet auch im Finanzsektor immer weiter voran. Damit wird die IT-Sicherheit sowie der Schutz vor steigenden Cyberrisiken immer bedeutsamer.

Obwohl steigende Risiken in der Informations- und Kommunikationstechnik (IKT) der Unternehmen bereits lange bekannt sind, gab es auf europäischer Ebene für Finanzunternehmen und ihre IKT-Drittdienstleister in der Vergangenheit keine einheitlichen IT-Sicherheitsmindeststandards. Mit dem am 16.01.2023 in Kraft getretenen Digital Operational Resilience Act (kurz: DORA) sollen diese Lücken geschlossen werden. Bei der Umsetzung ist den Finanzunternehmen und IKT-Dienstleistern eine Frist bis Anfang 2025 gewährt. In unserem Leitartikel haben wir Ihnen die betroffenen Arten von Finanzunternehmen und die DORA-Anforderungen im Überblick zusammengefasst. Für kommendes Jahr planen wir zudem eine Informationsveranstaltung zu diesem Thema, hierzu halten wir Sie auf unserer Homepage auf dem Laufenden.

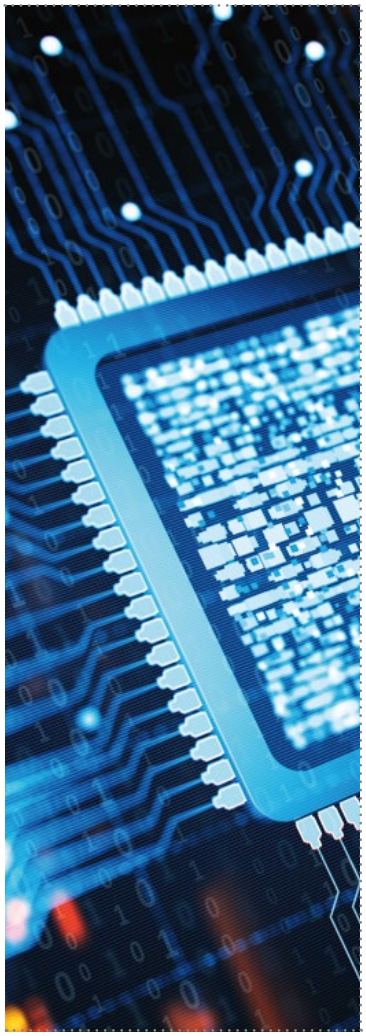
Auch der weiter wachsende Markt von Kryptoassets wird durch zahlreiche Initiativen des Gesetzgebers und der Aufsicht in den Fokus gerückt. So hat das BMF am 23.10.2023 den Referentenentwurf für das Finanzmarktdigitalisierungsgesetz (FinmadiG) veröffentlicht. Der Referentenentwurf des FinmadiG soll die Markets in Crypto Assets Verordnung (kurz: MiCAR), die Neufassung der EU-Geldtransferverordnung sowie das bereits erwähnte DORA-Paket (bestehend aus der DORA-Verordnung (EU) 2022/2554 und Richtlinie (EU) 2022/2556) umsetzen. In einzelnen Beiträgen haben wir Ihnen diese Neuerungen und ausgewählte weitere erwähnenswerte Veröffentlichungen zusammengestellt.

Wir wünschen Ihnen eine anregende Lektüre.

Für eventuelle Fragen stehen wir Ihnen gerne auch persönlich zur Verfügung.

Jens-Uwe Herbst
Wirtschaftsprüfer, Steuerberater und Partner bei RSM Ebner Stolz in Stuttgart

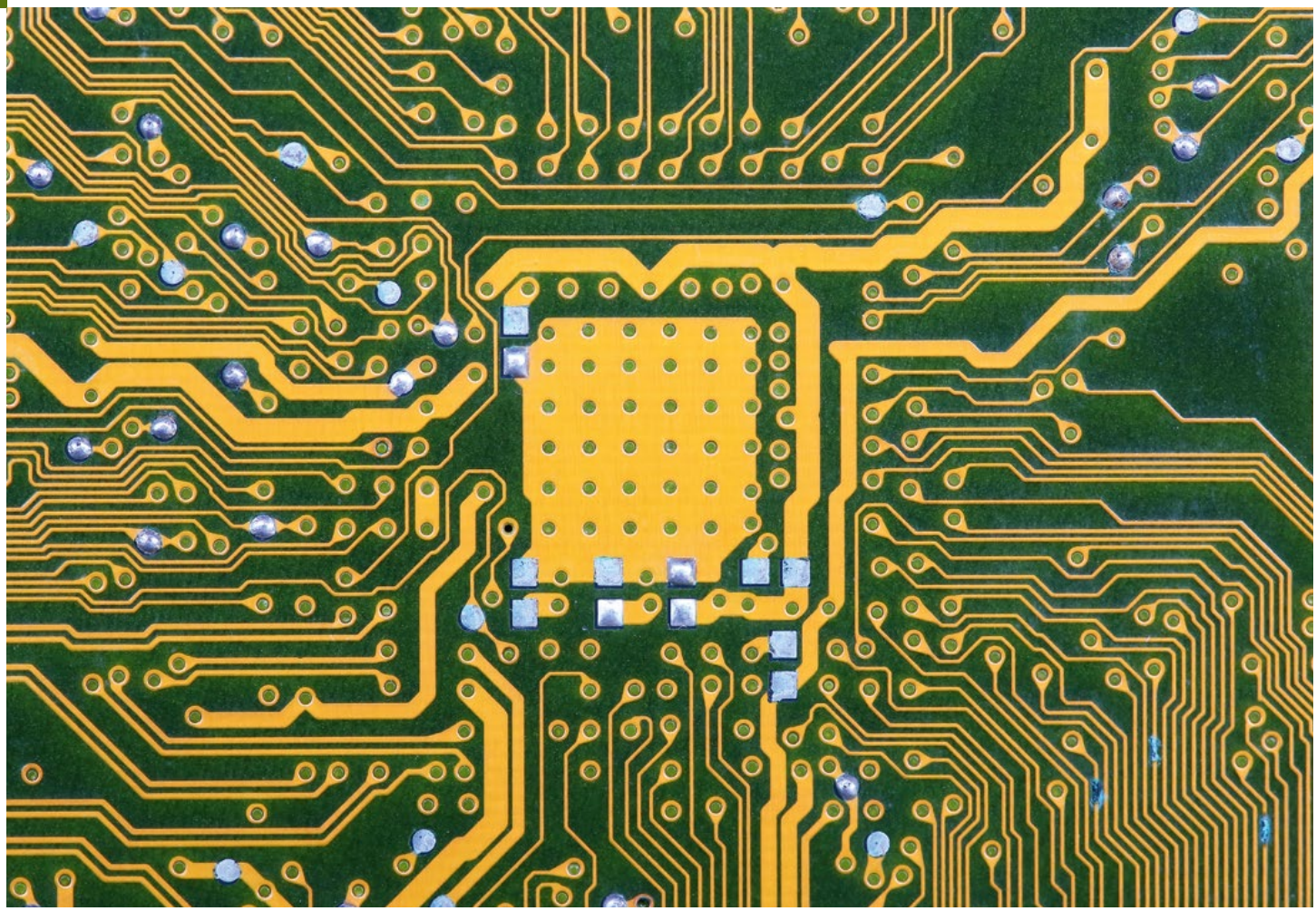
Jutta Kempers
Rechtsanwältin und Senior Managerin bei RSM Ebner Stolz in Köln



AUFSICHTSRECHT

STEUERRECHT

INTERN



Referentenentwurf eines Finanzmarktdigitalisierungsgesetzes

Die kryptospezifische Regulierung auf nationaler Ebene wie auf EU-Ebene schreitet weiter voran. Am 23.10.2023 hat das Bundesfinanzministerium den Referentenentwurf für ein Gesetz über die Digitalisierung des Finanzmarktes (Finanzmarkdigitalisierungsgesetz – kurz: FinmadiG) veröffentlicht.

Ziel des Referentenentwurfs ist die Durchführung jüngster kryptospezifischer EU-Verordnungen sowie die Umsetzung einer kryptospezifischen EU-Richtlinie. Konkret handelt es sich um die MiCAR (Markets in Crypto Assets Regulation (EU) 2023/1114), die durch die Transfer of Funds Regulation (EU) 2023/1113 novellierte Geldtransferverordnung sowie die Verordnung (EU) 2022/2554, die zusammen mit der Richtlinie (EU) 2022/2556) das DORA-Paket (Digital Operational Resilience Act) bildet.

Während die vorgenannten EU-Verordnungen im Inland unmittelbar geltendes Recht sind und durch das FinmadiG lediglich in die vorhandene Gesetzgebung eingepasst werden müssen, um terminologische Einheitlichkeit zu gewährleisten, bedarf die DORA-Richtlinie der vollständigen Umsetzung in das nationale Recht. Inhaltlich handelt es sich beim FinmadiG im Einzelnen um folgende Neuerungen:

DORA-Paket

Durch das sog. DORA-Paket soll die digitale operationale Resilienz bei Finanzunternehmen erhöht werden. Hintergrund ist u. a. die Erkenntnis, dass insbes. Cyberangriffe eine potenziell zu internationalen Finanzkrisen führende Gefahr für den Finanzsektor sind, gegen die es sich daher zu rüsten gilt. Zu diesem Zweck legt das DORA-Paket EU-weit einheitliche Anforderungen an die Sicherheit von Netzwerk- und Informationssystemen fest, die die Geschäftsprozesse von Finanzunternehmen unterstützen sollen. Einen Überblick über die Anforderungen geben wir nachfolgend in einem separaten Beitrag, vgl. „Digital Operational Resilience Act – Neuerungen für Finanzunternehmen und kritische IT-Dienstleister“ auf S. 6 in dieser Ausgabe des novus Financial Services.

Hinweis: Die neuen Regelungen des DORA-Pakets gelten im Fall der Verordnung ab dem 17.01.2025 bzw. sind im Fall der Richtlinie bis zu diesem Zeitpunkt in nationales Recht umzusetzen. Betroffene Unternehmen sind gut beraten, die bis zur Geltung der neuen Vorschriften verbleibende Zeit für die erforderlichen organisatorischen und technischen Anpassungen zu nutzen.

Verordnung Markets in Crypto Assets MICAR

Die MiCAR schafft ein umfassendes Rahmenwerk für Primär- und Sekundärmärkte für Kryptowerte. Kernregelungsinhalte sind:

- Zulassungsvorbehalte für das öffentliche Angebot bestimmter Kryptowerte und Kryptowerte-Dienstleistungen sowie u. a. aufsichtliche Anforderungen an die Organisation und Geschäftsführung,
- Transparenz- und Offenlegungspflichten für das öffentliche Angebot und die Zulassung zum Handel,

- Anforderungen zum Schutz der Inhaber von Kryptowerten und Kunden der Anbieter von Kryptowerte-Dienstleistungen,

- Anforderungen an die Offenlegung von Insiderinformationen, Maßnahmen zur Verhinderung von Insidergeschäften, unrechtmäßiger Offenlegung von Insiderinformationen sowie Marktmanipulation im Zusammenhang mit Kryptowerten.

Neben den vereinzelten Anpassungen des nationalen Rechts an die materiellen Regelungen der MiCAR passt das FinmadiG den derzeit geltenden formalen nationalen Aufsichtsrahmen für das Betreiben bzw. Erbringen von Bank- und Finanzdienstleistungen im Hinblick auf Kryptowerte, einschließlich erteilter Erlaubnisse, in die Vorgaben der MiCAR ein. Dies erfolgt durch ein neues Kryptomärkteaufsichtsgesetz (KMAG), das der neuen Alternativität zwischen Finanzinstrumenten im Sinne der MiFID II und Kryptowerten im Anwendungsbereich der MiCAR Rechnung trägt, Dies erfolgt insbes. dadurch, dass es die bisherigen nationalen auf Kryptowerte bezogenen Regelungen, namentlich des KWG, unter Anpassung an die Besonderheiten der Kryptomärkte in das KMAG überführt und eigenständige Regelungen hinsichtlich der Befugnisse der zuständigen Behörde sowie zur Sanktionierung von Verstößen gegen die MiCAR normiert.

Hinweis: Die MiCAR gilt zum großen Teil erst ab dem 30.12.2024; ihre auf vermögenswertreferenzierte Token (Asset related Token – ART) und E-Geld-Token (E-Money-Token – EMT) bezogenen Vorschriften gelten jedoch bereits ab dem 30.06.2024. Unternehmen, die die Emission von der MiCAR unterfallenden Token planen, sollten sich auf die Geltung der MiCAR zu den vorgenannten Zeitpunkten einrichten. Emittenten von ARTs sollten zudem die seitens der EBA (European Banking Authority) eingeleitete und am 24.01.2024 endende Konsultation zum Entwurf ihrer Guidelines on internal governance arrangements for issuers of ARTs under MiCAR im Blick haben. Institute, die bis zum 30.12.2024 nach nationalem Recht Bankgeschäfte und Finanzdienstleistungen in Bezug auf der MiCAR unterfallende Kryptowerte betreiben bzw. erbringen, profitieren davon, dass die MiCAR für sie eine Übergangsfrist bis zum 01.07.2026 vorsieht, bis zu der sie mit ihrer geltenden Erlaubnis ihr Geschäft fortsetzen können und parallel die Möglichkeit haben, die Zulassung nach den neuen Vorschriften zu beantragen.

Novellierung der Geldtransferverordnung

Das Aufkommen von Kryptowerten hat auch Folgen für die Regulierungen zur Vermeidung von Geldwäsche und Terrorismusfinanzierung. So reagierte die Financial Action Task Force (FATF) hierauf jüngst mit Vorgaben für Anbieter von Dienstleistungen für virtuelle Vermögenswerte, mit denen die Rückverfolgbarkeit von Transfers virtueller Vermögenswerte erleichtert werden soll. Danach müssen Anbieter von Dienstleistungen für virtuelle Vermögenswerte bei Transfers virtueller Vermögenswerte Angaben zu den Auftraggebern und Begünstigten dieser Transfers einholen, aufbewahren, an die Gegenpartei übermitteln und auf Anfrage den zuständigen Behörden zur Verfügung stellen. Diese Vorgaben finden Eingang in die durch die Verordnung (EU) 2023/1113 neugefasste Geldtransferverordnung (EU) 2015/847.

Zur Durchführung der neugefassten Geldtransferverordnung sind Anpassungen im Geldwäschegesetz (GwG) in Bezug auf Kryptowerte-Transfers erforderlich. Dazu gehört insb. die Festlegung der Aufsichtszuständigkeit der BaFin für die Überwachung der Einhaltung der Vorgaben durch die Anbieter von Kryptowerte-Dienstleistungen. Zudem macht die Überführung der bisherigen Regulierung aus dem KWG in das neue KMAG (siehe vorstehend) erforderlich, Anbieter von Kryptowerte-Dienstleistungen im GwG als geldwäscherechtlich Verpflichtete zu definieren. Neu gefasst wird in diesem Zusammenhang die mit dem 5. Geldwäsche-RL-UmsG in das KWG neu aufgenommene Finanzdienstleistung der Kryptoverwahrung. Diese regelt fortan als qualifizierte Kryptoverwahrung die Verwahrung und Sicherung der ebenfalls neu definierten kryptografischen Instrumente, die ihrerseits nach Ausschluss von E-Geld, monetären Werten, Kryptowerten i.S.d. MiCAR, Kryptowertpapieren i.S.d. eWpG und Kryptofondsanteilen i.S.d. KryptoFAV als Restgröße des ursprünglich nationalen Kryptowertebegriffs verbleibt. Als geldwäscherechtlich Verpflichtete neu definiert werden daneben Emittenten vermögenswertereferenzierter Token, soweit die Abwicklung nicht ausschließlich über einen Anbieter von Kryptowerte-Dienstleistungen erfolgt. Ab Geltung der neugefassten Geldtransferverordnung tritt zugleich die bisher geltende Kryptowertetransferverordnung (KryptoWTransferV) außer Kraft.

Hinweis: Die auf der novellierten Geldtransferverordnung beruhenden neuen Vorgaben gelten ab dem 30.12.2024. Die als neue Verpflichtete im GwG definierten Anbieter von Kryptowerte-Dienstleistungen sowie Emittenten vermögenswertereferenzierter Token müssen neben übrigen für sie geltenden neuen aufsichtsrechtlichen Vorgaben zusätzlich die Vorgaben des GwG einhalten und damit ein diesbezügliches Risikomanagementsystem einrichten.

Fazit

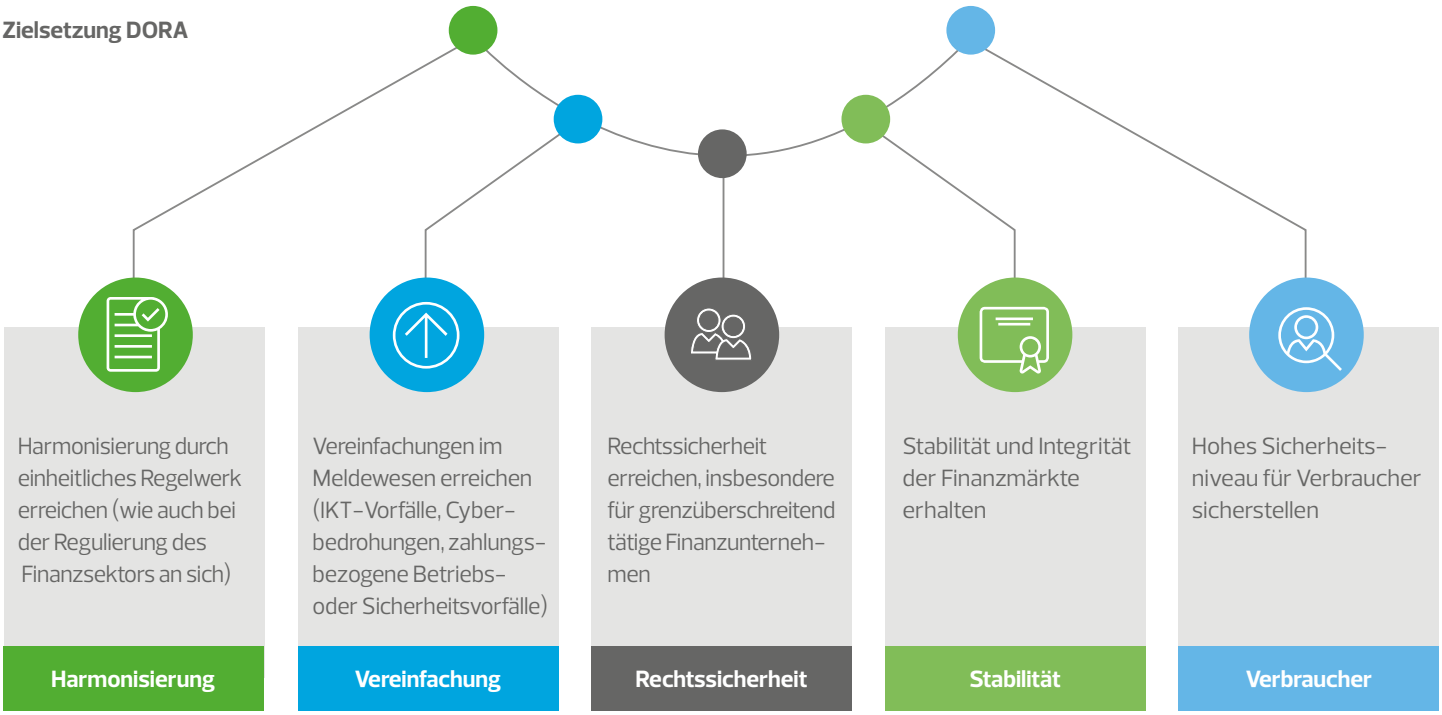
Die Regelungen des FinmadiG, ebenso wie die darin adressierten Regelungen des DORA-Pakets, der MiCAR und der novellierten Geldtransferverordnung, erweitern das in den letzten Jahren schnell gewachsene kryptospezifische Regulierungsregime, zu dem weitere in jüngster Zeit erlassene nationale und EU-Regelungen zählen, so u. a. das DLT Pilot Regime, das Zukunftsfinanzierungsgesetz und das Gesetz zur Einführung elektronischer Wertpapiere (näher dazu siehe hier). Dabei steht bereits fest, dass angesichts der weiterhin vorhandenen nationalen Unterschiede noch weithin eine kryptospezifische Harmonisierungs-Regulierung auf EU-Ebene erforderlich sein wird. Positiv dürfte sich hier auswirken, dass Deutschland mit seinen nationalen kryptospezifischen Regelungen eine Vorreiterrolle einnimmt, die für zukünftige EU-Regulierung als Orientierung dienen kann.

Digital Operational Resilience Act – Neuerungen für Finanzunternehmen und kritische IT-Dienstleister

Die Digitalisierung im Bankgeschäft schreitet immer weiter voran. Hierdurch werden Themen der IT-Sicherheit sowie Cyberrisiken in Finanzunternehmen und bei den dahinterstehenden IT-Dienstleistern immer präsenter. Mangels einheitlicher Regulierung für den Finanzsektor in der EU sind die IT-Sicherheitsmindeststandards, welche Finanzunternehmen umsetzen müssen, in den einzelnen EU-Mitgliedstaaten bislang stark unterschiedlich ausgeprägt.

Mit dem Digital Operational Resilience Act (DORA) hat das europäische Parlament nun ein Regelwerk geschaffen, das der Digitalisierung des Finanzsektors gerecht werden soll und so höhere Rechtssicherheit, zusätzliche Stabilität der Finanzmärkte sowie mehr Verbraucherschutz schaffen soll.

Zielsetzung DORA



Wo kommen wir her und wo geht es hin?

Die Verordnung ist bereits am 16.01.2023 in Kraft getreten und findet in den Mitgliedstaaten ohne weitere Umsetzungsakte direkt Anwendung.

Hinweis: DORA sieht aber für die Finanzunternehmen und deren IT-Dienstleister eine Umsetzungsfrist von 24 Monaten vor, so dass sie erst zum 17.01.2025 unternehmensintern umgesetzt sein muss.

Wer ist von DORA betroffen?

DORA richtet sich primär an Finanzunternehmen. Allerdings ist der Begriff des Finanzunternehmens sehr weit gefasst und erfasst nicht nur klassische Institute (wie Banken oder Zahlungsdienstleister). Der Begriff des „Finanzunternehmens" wird in Art. 2 Abs. 1 a) bis t) DORA legal definiert. Betroffen sind dem Wortlaut nach folgende Unternehmen:

- Kreditinstitute
- Zahlungsinstitute
- Kontoinformationsdienstleister
- E-Geld-Institute
- Wertpapierfirmen
- Anbieter von Krypto-Dienstleistungen
- Zentralverwahrer
- Zentrale Gegenparteien
- Handelsplätze
- Transaktionsregister
- Verwalter alternativer Investmentfonds
- Verwaltungsgesellschaften
- Datenbereitstellungsdienste
- Versicherungs-/Rückversicherungsunternehmen
- Versicherungs-/Rückversicherungsvermittler
- Einrichtungen betrieblicher Altersversorgung
- Ratingagenturen
- Administratoren kritischer Referenzwerte
- Schwarmfinanzierungsdienstleister
- Verbriefungsregister.

Dabei wird zum Teil der Anwendungsbereich durch Verweise auf bestehende Verordnungen bzw. Richtlinien, wie beispielsweise die PSD2 (Richtlinie (EU) 2015/2366), konkretisiert.

In welchem Umfang die jeweiligen Finanzunternehmen von DORA betroffen sind, hängt von deren Größe und Gesamtrisikoprofil sowie der Art, dem Umfang und der Komplexität deren Geschäftstätigkeit ab (vgl. Art. 18 Abs. 4 DORA).

Hinweis: Explizite Erleichterungen sieht DORA für Kleinstunternehmen vor, welche weniger als 10 Mitarbeitende und einen Jahresumsatz bzw. eine Bilanzsumme von unter 10 Mio. Euro ausweisen. Für alle anderen Unternehmen gilt ein abstraktes Proportionalitätsprinzip.

Was sind die Schlüsselthemen?

Das Hauptziel von DORA besteht darin, den Herausforderungen der Digitalisierung in Finanzunternehmen im Wandel der Zeit gerecht zu werden. Hierdurch sollen ein europaweit einheitlich sicherer und stabiler Finanzmarkt gewährleistet und gleiche Wettbewerbsbedingungen für die betroffenen Unternehmen geschaffen werden.

DORA regelt primär drei zentrale Themen:

- **Standards für das IKT-Risikomanagement:** Unternehmen werden verpflichtet, angemessene Strategien zur Identifikation, Bewertung und Bewältigung von IT-Risiken zu entwickeln.

- Anforderungen an **Resilienztests** (z. B. Penetrationstests, siehe Beitrag auf S. 9): Diese sollen sicherzustellen, dass Unternehmen bei Störungen oder Cyberangriffen widerstandsfähig sind und ihre Dienstleistungen kontinuierlich erbringen können.

- Regelungen zur **Auslagerung** von Dienstleistungen an Dritte.

Verpflichtung zur Einführung eines IKT-Risikomanagements

DORA führt die Verpflichtung zur Implementierung eines sog. „IKT-Risikomanagementrahmens" der Unternehmen für ihre Informations- und Kommunikationstechnik (IKT) ein.

Der IKT-Risikomanagementrahmen ist als Werkzeugkasten zu verstehen, der regulierten Unternehmen zur Verfügung steht, um alle Informations- und IKT-Assets angemessen zu schützen. Dies umfasst gemäß Art. 6 Abs. 2 DORA mindestens Strategien, Leit- und Richtlinien, IT- und Risikomanagementprozesse, sowie IKT-Protokolle und Anwendungen. Inhaltlich umfasst der IKT-Risikomanagementrahmen mindestens

- die Strategie für die digitale operationelle Resilienz (Art. 6 DORA),
- die Erhebung des Informationsverbundes (Art. 8 DORA),
- das Informationssicherheitsmanagement (Art. 9 DORA),
- eine Geschäftsfortführungsleitlinie (Art. 11 DORA),
- Datensicherungs- und Wiederherstellungsverfahren (Art. 12 DORA),
- Kommunikationspläne für Incidents (Art. 14 DORA),
- ein umfassendes Testprogramm für die digitale operationelle Resilienz (Art. 24 DORA) und
- das Management des IKT-Drittparteienrisikos (Art. 28 DORA).

Hinweis: Den IKT-Risikomanagementrahmen müssen die Finanzunternehmen zur Sicherstellung eines robusten und belastungsfähigen Sicherheitssystems mindestens einmal im Jahr bzw. anlassbezogen überarbeiten.

Die Implementierung des IKT-Risikomanagementrahmens stellt keine neue Verpflichtung für regulierte Institute dar. Bereits bisher muss das Risikomanagement von regulierten Instituten das IKT-Risiko umfassen und regelmäßig bzw. anlassbezogen überprüft werden. Diese Vorgabe ist in den MaRisk und den aufsichtsrechtlichen Vorgaben an die IT in BAIT, KAIT und ZAIT bereits verankert. Betrachtet man aber die in DORA genannten Anforderungen, wird ersichtlich, dass die Anforderungen an den „IKT-Risikomanagementrahmen" nicht deckungsgleich mit den Anforderungen des IT-Risikomanagements nach MaRisk sein werden. Die neuen DORA-Vorgaben sind an vielen Stellen konkreter. Zudem werden die Anforderungen durch DORA auf Gesetzesebene verankert und stellen nicht mehr nur Verwaltungsvorschriften der BaFin dar.

Einführung von Resilitenztests

Gemäß DORA sind die Unternehmen auch dazu aufgerufen, angesichts der Bedrohungen regelmäßig Resilienztests durchzuführen, um ihre betriebliche Kontinuität zu bewerten. Durch die Ausarbeitung und Durchführung realistischer Stresstestszenarien sollen Schwachstellen und Schwachpunkte aufgedeckt werden.

Änderungen im Rahmen der Anforderungen in Bezug auf Auslagerungen

DORA beinhaltet in Kapital V dezidierte Vorgaben zum Outsourcing von Dienstleistungen. Auch hier sind die Vorgaben für regulierte Institute nicht neu. Die Anforderungen an Auslagerung erinnern in großen Teilen an die

Anforderungen aus z. B. MaRisk oder den EBA-Guidelines zur Auslagerungsvereinbarungen (EBA-Guidelines on outsourcing arrangements). Sofern regulierte Institute derzeit „compliant" sind, werden sie daher in der Regel ihr Auslagerungsmanagement und ihre Auslagerungsverträge nicht gänzlich neu erfinden müssen. Nichtdestotrotz gibt es Unterschiede und Neuerungen, die einen Umsetzungsaufwand begründen können bzw. Potential für wesentlichen Anpassungsbedarf haben.

So unterscheidet der Wortlaut von DORA im Gegensatz zur MaRisk und den BAIT nicht zwischen „Auslagerungen" und „Sonstigem Fremdbezug". DORA unterscheidet lediglich zwischen IKT-Dienstleistungen und solchen Dienstleistungen, die zur Unterstützung kritischer und wichtiger Funktionen erfolgen. Es bleibt daher abzuwarten, ob und wie die BaFin diesbezüglich ihre Verwaltungspraxis anpassen wird.

Zudem konkretisiert DORA den Mindestinhalt der Auslagerungsverträge. Auch diese Vorgaben sind nicht ganz deckungsgleich mit den derzeitigen Vorgaben für regulierte Institute. Daher wird ggf. ein Abgleich und eine Aktualisierung bestehender Auslagerungsverträge notwendig werden.

Überwachung für kritische IKT-Drittdienstleister

Ferner wird mit DORA ein neuer europäischer Überwachungsrahmen für kritische Technologieanbieter, die im Finanzsektor tätig sind, geschaffen. Die Einstufung als kritischer IKT-Drittdienstleister und die damit verbundene Überwachung obliegen den Europäischen Aufsichtsbehörden (EBA, ESMA und EIOPA). Wie diese Einstufung genau ausfallen wird, bleibt noch abzuwarten. Bei der Einstufung orientieren sich die Aufsichtsbehörden gemäß Art. 31 Abs. 2 DORA an folgenden Kriterien:

- Systemische Auswirkungen auf die Finanzdienstleistungen bei Defiziten der Stabilität, Kontinuität und Qualität der IKT-Leistungen
- Abhängigkeit von Finanzunternehmen von den Dienstleistungen des betreffenden IKT-Drittdienstleisters
- Grad der Substituierbarkeit des IKT-Drittanbieters
- Zahl der Mitgliedstaaten, welche die IKT-Leistungen nutzen.

In Deutschland verfügt die BaFin zwar nach § 26 Abs. 3a ZAG und § 25b Abs. 4a KWG bereits über direkte Anordnungsbefugnisse gegenüber IKT-Drittdienstleistern bei wesentlichen Auslagerungen. Allerdings sind diese Befugnisse begrenzt auf Auslagerungsdienstleister, die wesentliche Auslagerungen für KWG- und ZAG-Institute erbringen. Die im Rahmen von DORA übertragenen Befugnisse an die federführende Überwachungsbehörde auf europäischer Ebene sind weitaus umfangreicher als die bisherigen der BaFin (vgl. Art. 39 DORA) und gelten für Auslagerungsdienstleister, die für Finanzunternehmen im Sinne von DORA tätig sind. Diese erweiterten Befugnisse stellen ein Novum dar, ermöglichen sie doch eine umfassende und direkte Aufsicht über kritische IKT-Drittanbieter.

Mögliche Konsequenzen bei Nichteinhaltung der DORA-Vorgaben

Die BaFin verfügt künftig über umfassende Aufsichts-, Untersuchungs- und Sanktionsbefugnisse, um die Erfüllung der Anforderungen der DORA umsetzen zu können. Art. 50 DORA legt hierbei die Mindestanforderungen für Maßnahmen bei einem Verstoß fest. Diese umfassen den Zugriff auf Daten und Dokumente, Vor-Ort-Inspektionen und -Durchsuchungen sowie Korrektur- und Abhilfemaßnahmen.

Gemäß Art. 54 Abs. 1 DORA werden festgesetzte Sanktionen auf der amtlichen Website der Behörde unter namentlicher Nennung der Unternehmen veröffentlicht. Es besteht somit ein nicht zu vernachlässigendes Reputationsrisiko.

Das nationale Recht kann über die DORA-Vorgaben hinausgehen. Ein Absehen von den in der DORA festgelegten Mindestanforderungen für Maßnahmen bei einem Verstoß ist hingegen nur möglich, sofern Verstöße gegen DORA nach nationalem Recht strafrechtlich verfolgt werden (vgl. Art. 52 DORA).

Sanktionen bei Nichteinhaltung der Vorgaben der DORA:

Zugriff auf Daten & Dokumente	Vor-Ort-Inspektionen und Durchsuchungen	Korrektur- & Abhilfemaßnahmen	Veröffentlichung der Sanktionen
▶ die Behörde darf Zugriff auf Daten und Unterlagen jeglicher Form anordnen ▶ nur die für die Untersuchung notwendigen Dokumente ▶ auch Kopien können angefordert werden	▶ Vorladung von Vertretern der Unternehmen zur Erklärung von relevanten Sachverhalten und Unterlagen – Aufzeichnung der Antwort ▶ Befragung von Personen, die der Informationsgewinnung im Zusammenhang einer Untersuchung zustimmen	▶ Forderung nach Korrekturen und Maßnahmen bei Verstößen gegen die DORA	▶ die von der Behörde gewählten Maßnahmen werden auf der amtlichen Website der Behörde veröffentlicht ▶ auch Identität der juristischen oder natürlichen Person werden veröffentlicht

Auswirkungen für mittelständische Finanzunternehmen

Obwohl die DORA-Anforderungen erst ab dem 17.01.2025 umgesetzt sein müssen, ist eine rechtzeitige Bewertung der Betroffenheit bedeutsam. Die Verordnung einschließlich aller noch zu verabschiedender Implementierungsstandards und technischer Regulierungsstandards ist umfangreich und inhaltlich komplex. Während regulierte Institute mit der Analyse, Bewertung und Implementierung von Maßnahmen zur Erfüllung aufsichtlicher Anforderungen grundsätzlich vertraut sind, werden künftig auch ausgewählte IKT-Drittdienstleister in Deutschland erstmals selbst unter die direkte Aufsicht der europäischen Aufsichtsbehörden fallen.

Neben einer Betroffenheitsanalyse sollten die Unternehmen alsbald eine Gap-Analyse zu den DORA-Anforderungen durchführen, um den notwendigen Handlungsbedarf zu evaluieren. Insb. für kleinere Häuser können die durch DORA notwendigen Anpassungen der eigenen IT-Prozesse und des IT-Auslagerungsmanagements Ressourcen belasten und damit eine Herausforderung darstellen.

Penetrationstests: Sinnvolle Erkenntnisse oder nur Spielerei?

Im digitalen Zeitalter ist der Finanzsektor mit einem ständig wachsenden Bedrohungspotenzial konfrontiert. Dabei ist nicht nur die Digitalisierung ein treibender Faktor für die hohe Anzahl an Cyber-Angriffen: Auch die Pandemie, der Ukraine-Krieg oder der jüngst eskalierte Nahost-Konflikt haben Einfluss auf die Cyber-Sicherheitslage in Deutschland. Der Finanzsektor kann in solchen internationalen Konflikten durchaus ein attraktives Ziel sein.

Die Motivation für solche Angriffe kann dabei von Sabotage über Geldwäsche bis hin zu Lösegelderpressung reichen und erhebliche finanzielle Verluste und massive Reputationsschäden mit sich bringen.

Die von der BaFin veröffentlichten bankaufsichtsrechtlichen Anforderungen an die IT (kurz: BAIT) verpflichten Institute in Deutschland dazu, eine Richtlinie über das Testen der Maßnahmen zum Schutz der Informationssicherheit einzuführen (vgl. BAIT II. Nr. 4.8.). Außerdem ist die Sicherheit der IT-Systeme regelmäßig zu überprüfen und sind daraus resultierende Ergebnisse hinsichtlich notwendiger Verbesserungen zu analysieren und Risiken angemessen zu steuern (vgl. BAIT II. Nr. 5.6.).

Die am 16.01.2023 neu in Kraft getretene DORA-Verordnung (vgl. vorstehender Beitrag auf S. 6) erweitert darüber hinaus die Differenzierung der durchzuführenden Tests. Wird in den BAIT lediglich zwischen Gap-Analysen, Schwachstellen-Scans, Penetrationstests und Angriffssimulationen unterschieden, verpflichtet DORA zur „Durchführung angemessener Tests" (z. B. Bewertungen und Überprüfungen von Schwachstellen, Analysen von Open-Source-Software, Bewertungen der Netzwerksicherheit, Lückenanalysen, Analysen der physischen Sicherheit, Fragebögen und Scansoftwarelösungen, Quellcodeprüfungen, szenariobasierte Tests, Kompatibilitätstests, Leistungstests oder End-to-End-Tests).

Darüber hinaus sind erweiterte Tests von IKT-Tools (Komponenten der Informations- und Kommunikationstechnik-Tools), -Systemen und -Prozessen „mindestens alle drei Jahre anhand von TLPT" (Thread-Led-Penetration-Tests) durchzuführen (vgl. Art. 26, Satz 1 DORA).

Die Einhaltung dieser Anforderungen kann durch die Umsetzung verschiedener Maßnahmen erreicht werden, wobei sich die passende Maßnahme immer aus dem Verhältnis zum Risiko ableiten sollte. Die regelmäßige Durchführung von Schwachstellenscans und Penetrationstests sollte hierbei jedoch zum Basis-Werkzeugkasten gehören und als absolut selbstverständlich angesehen werden.

Als Erstbetrachtung oder im Vorfeld einer Neu-Konzeptionierung bietet sich eine **Strukturanalyse** an. Dabei wird eine grundlegende „Table-Top"-Analyse der Infrastruktur durchgeführt und es werden mögliche Angriffswege auf ihre geschäftskritischen Daten und Systeme ausgelotet.

Schwachstellenscans sind eine gute, flächendeckende Lösung, um die relevanten Systeme regelmäßig auf mögliche Angriffsflächen zu überprüfen. Auf diese Weise können anschließend die vorhandenen Hard- und Softwarekomponenten der Institute unter Berücksichtigung einer Vielzahl von Aspekten analysiert werden.

Der der Realität am nächsten kommende und damit effektivste Weg, die jeweilige Infrastruktur gezielt hinsichtlich des vorhandenen Sicherheitsniveaus zu testen und Sicherheitsrisiken aufzudecken, sind sog. **Penetrationstests**. Dabei werden realistische Offensiven eines ambitionierten Angreifers unter verschiedenen Gegebenheiten simuliert. In enger Abstimmung mit den Verantwortlichen wird das charakteristische dreistufige Vorgehen eines Angriffs, bestehend aus

- Reconnaissance (Informationsbeschaffung),
- Enumeration (Angriffsvektoren ausloten) und
- Exploitation (Ausnutzen von Schwachstellen)

nachgebildet.

Penetrationstests können hierbei in verschiedenen Ausprägungen durchgeführt werden:

Bei einem **Black-Box** Penetrationstest wird das übliche Vorgehen eines Hackers von außen ohne Unternehmenskenntnisse simuliert. Hier werden alle notwendigen Informationen selbstständig gesammelt und in Iterationen über das Internet die betreffende Infrastruktur analysiert.

Ein **White-Box** Penetrationstest **von außen** simuliert einen Außenangriff mit erhöhter Kenntnis des Unternehmens (z. B. aufgrund von Informationsweitergabe durch Mitarbeitende).

Die Annahme eines „Innentäters" ist dabei nicht abwegig. Derartige Angriffe lassen sich durch einen **White-Box** Penetrationstest **von innen simulieren**.

Aus den identifizierten Schwachstellen bzw. Sicherheitslücken können Vorschläge zur Beseitigung der Schwachstellen bzw. zur Verbesserung der gesamten Informationssicherheit abgeleitet und in Ergebnisberichten dokumentiert werden.

Nach der **Beseitigung identifizierter Schwachstellen** kann mit einem abschließenden **Retesting** eine angemessene Umsetzung der Maßnahmen nachgewiesen werden.

Hinweis: Sofern ein Institut die Anforderungen der BAIT bereits vollständig erfüllt, hält sich der Handlungsbedarf in Grenzen. Zwingend notwendig sind jedoch ein risikoorientierter mehrjähriger Prüfplan, die Durchführung der Sicherheitsüberprüfungen und die anschließende Bewertung der Ergebnisse sowie eine angemessene Mitigation. Alle Aktivitäten sollten verbindlich in Form geeigneter Richtlinien oder Arbeitsanweisungen vorgegeben und nachvollziehbar dokumentiert werden.

SWIFT Customer Security Programme bietet einheitliches Niveau von Sicherheit und Vertrauen weltweit

Die Society for Worldwide Interbank Financial Telecommunication (kurz: SWIFT) betreibt als in Belgien ansässige Organisation ein globales Netzwerk zur Übermittlung von Finanznachrichten.

SWIFT ermöglicht dem Finanzsektor, sicher und effizient Informationen über grenzüberschreitende Zahlungen, Wertpapiertransaktionen, Handelsfinanzierungen und andere Finanzdienstleistungen auszutauschen und hat sich mittlerweile als de-facto-Standard für den Auslandszahlungsverkehr etabliert. Die Transaktionsvolumen haben mittlerweile eine erhebliche Größe, so dass das Netzwerk nicht nur für Teilnehmende, sondern auch für kriminelle Angreifer durchaus attraktiv ist.

Hinweis: Der spektakulärste Fall bislang war ein Swift-Hack in Bangladesch im Jahr 2016. Hier versuchten Angreifer mithilfe von fingierten SWIFT-Nachrichten ca. 1 Mrd. US-Dollar von der Bangladesch-Bank zu stehlen und waren dabei teilweise auch erfolgreich. Es wurden letztendlich etwa 81 Mio. US-Dollar entwendet.

Um derartigen Vorfällen besser zu begegnen, hat SWIFT in diesem Zusammenhang das sog. Customer Security Program (CSP) initiiert, welches in den bestehenden Kontrollrahmen für Informationssicherheit integriert werden muss. Hierzu verlangt SWIFT seit dem 31.12.2021 eine jährliche Bestätigung über die Einhaltung des SWIFT CSP durch eine unabhängige Instanz. Dieses sieht eine Kombination aus obligatorischen und optionalen Kontrollen für alle Teilnehmenden des Netzwerks vor. Die Maßnahmen von SWIFT zielen in erster Linie darauf ab, die Sicherheit für alle auf das gleiche Mindestmaß anzuheben – unabhängig von der national geltenden Regulatorik. Dadurch soll das Vertrauen in das SWIFT-Netzwerk gestärkt und eine weltweite Interoperabilität gewährleistet werden.

Ziel des CSP ist es, Sicherheitsrisiken bei Finanztransaktionen zu minimieren und die Integrität des gesamten SWIFT-Netzes zu schützen.

Mit der Einführung des CSP hat SWIFT eine angemessene Maßnahme zur Erhöhung der Sicherheit im eigenen Finanztransaktionsnetzwerk getroffen. Mit dem verstärkten Fokus auf Kunden- und Netzwerksicherheit zeigt SWIFT seine Bereitschaft, sich den aktuellen und zukünftigen Herausforderungen in der Finanzwelt zu stellen.

Je nach Architektur der SWIFT-Anbindung gelten unterschiedliche Kontrollanforderungen. Hierbei wird jeweils zwischen obligatorischen und optionalen Kontrollen unterschieden. Dies ermöglicht den Instituten eine gewisse Flexibilität, ohne dabei wesentliche Anforderungen zu umgehen, die im schlimmsten Fall zu einem Ausschluss aus dem SWIFT-Netzwerk führen können.

Sinnvollerweise empfiehlt sich für die Institute die Vornahme eines **Soll-Soll-Vergleichs**.

Hinweis: Der Soll-Soll-Vergleich beinhaltet den Abgleich der SWIFT-Kontrollen mit den schriftlich festgelegten Mindestanforderungen des Auftragsgebers. Der Abgleich ist hierbei in einer von SWIFT vorgegebenen Tabellenstruktur zu dokumentieren. Es empfiehlt sich die Einholung eines externen „Letter of Confirmation". Dieser wird benötigt, um die Übereinstimmung der Maßnahmen mit dem SWIFT-Framework der SWIFT zu bestätigen.

Darauf aufbauend bietet sich die Durchführung eines **Soll-Ist-Vergleichs** an.

Aufbauend auf dem Soll-Soll-Vergleich können aus der schriftlich fixierten Ordnung operative Kontrollen ermittelt werden. Die implementierten Kontrollen sollten plausibilisiert und eine risikoorientierte Bewertung der Kritikalität durchgeführt werden. Zusätzlich sollte in einem Soll-Ist-Vergleich eine materielle Prüfung der implementierten Kontrollen hinsichtlich ihrer jeweiligen Wirksamkeit erfolgen.

Hinweis: Mögliche Optimierungspotenziale bzw. Abweichungen von den Vorgaben können so identifiziert und Maßnahmen zur Beseitigung identifizierter Schwachstellen bzw. zur Verbesserung der IT-Sicherheit im Allgemeinen (weiter-)entwickelt werden.

Neue Datenanforderungen für Meldungen der Wertpapierinstitute

Am 21.09.2022 informierte die Deutsche Bundesbank sämtliche Wertpapierinstitute (WpI) – derzeit rd. 740 in Deutschland – darüber, dass sich ab dem Meldestichtag 31.12.2023 für bestimmte Meldungen das Format der Meldedatei von Excel (XLSX) zu XBRL ändert.

Mit der Richtlinie (EU) 2019/2034 (IFD – Investment Firm Directive) und der Verordnung (EU) 2019/2033 (IFR – Investment Firm Regulation) hatte die EU erstmals einen einheitlichen Berichtsrahmen für WpI hinsichtlich ihrer aufsichtsrechtlichen Meldepflichten vorgegeben. Die Umsetzung der Richtlinie in nationales Recht erfolgte dann durch das Wertpapierinstitutsgesetz (WpIG). Die Regelungen sind seit Juni 2021 in Kraft.

Art. 54 der Verordnung (EU) 2019/2034 umfasst u. a. Meldungen zur/zum

- Höhe und Zusammensetzung der Eigenmittel,
- Berechnung der Eigenmittelanforderungen,
- Berechnung der Anforderungen für fixe Gemeinkosten,
- Konzentrationsrisiko und Liquiditätsanforderungen,

die die WpI der Deutschen Bundesbank übermitteln müssen.

Der Melderhythmus ist für WpI der Klasse 2 (mittlere WpI) vierteljährlich und für WpI der Klasse 3 (kleine WpI) jährlich.

Was ist XBRL?

XBRL steht für „Extensible Business Reporting Language". Diese „Sprache" dient dazu, den Berichtsfluss von Unternehmensinformationen vom Informationsgeber zum Informationsempfänger zu standardisieren und zu rationalisieren. Tatsächlich basiert XBRL auf XML. Reine XML-Meldungen haben einen entscheidenden Nachteil: Das zugrundeliegende XML-Schema definiert lediglich die strukturelle Abbildung der Daten und validiert die korrekten Datentypen auf Vollständigkeit. XBRL hingegen erweitert dies durch eine Semantik, die zudem eine Interpretation der Daten ermöglicht. So kann in XBRL ein komplexes dimensionales Datenmodell abgebildet werden, das beliebig erweiterbar ist.

Hinweis: In einer XML-Meldung können Bilanzdaten abgebildet werden, bspw. Sachanlagen, Finanzanlagen oder andere Aktiva. Die Information und die eigentlich obligatorische Validierung, dass nämlich die Summe aus Sachanlagen und Finanzanlagen das Anlagevermögen abbildet, ist im reinen XML-Format nicht möglich. Daher werden solche Informationen bislang in der Praxis in langen Handbüchern zu XML-Meldungen ergänzt, ohne dass der Ersteller oder Empfänger der Meldungen eine Chance hat, die Regeln automatisch zu verarbeiten. An dieser Stelle kommt dann XBRL zum Einsatz.

RSM Ebner Stolz berät oder unterstützen Sie gerne bei der notwendigen Transformation der Datenformate.

Überwachung und Governance von Bankprodukten im Privatkundengeschäft

Am 30.10.2023 hat die BaFin das Rundschreiben 08/2023 Überwachung und Governance von Bankprodukten im Privatkundengeschäft veröffentlicht. Ein Begleitschreiben mit Erläuterungen zum Rundschreiben ist dabei nicht ergangen.

Mit dem Rundschreiben setzt die BaFin die Leitlinien der EBA für die Überwachung und Governance von Bankprodukten im Privatkundengeschäft (EBA/GL/2015/18) um und orientiert sich eng an diesen.

Hinweis: Da die Rechtsgrundlage für die Guideline angezweifelt wurde, hatte die BaFin die Leitlinien der EBA aus 2015 zunächst lange nicht in ihre Verwaltungspraxis übernommen.

Das Rundschreiben gibt auf der Grundlage von § 25a Abs. 1 KWG und § 27 Abs. 1 ZAG einen Rahmen für die Überwachung und Governance von Bankprodukten, Zahlungsdiensten und E-Geld-Produkten im Privatkundengeschäft von CRR-Kreditinstituten gemäß KWG und Zahlungsinstituten gemäß ZAG vor. Bei den Bankprodukten geht es insb. um (Immobilar-)Verbraucherdarlehensverträge, Einlagenprodukte und Zahlungsdienste.

Das Rundschreiben richtet sich sowohl an Produkthersteller als auch an Produktvertreiber. Die Regelungen beziehen sich auf die internen Prozesse, Funktionen und Strategien für die Konzeption, Markteinführung und Überprüfung dieser Produkte während ihres gesamten Lebenszyklus. Es werden die relevanten Verfahren dargestellt, mit denen sichergestellt werden soll, dass den Interessen, Zielen und Eigenschaften des Zielmarktes entsprochen wird.

Die Anforderungen des Rundschreibens gelten für Produkte, die nach dem Inkrafttreten dieses Rundschreibens in den Markt eingeführt werden, sowie für alle bereits am Markt befindlichen Produkte, die nach dem Inkrafttreten dieses Rundschreibens erheblich verändert werden.

Das Rundschreiben tritt am 01.05.2024 in Kraft.

Konsultation zum Entwurf des Rundschreibens zu den Mindestanforderungen an das Risikomanagement von Zahlungsinstituten

Am 27.09.2023 hat die BaFin eine Konsultation ihres Entwurfs für ein Rundschreibens zu den Mindestanforderungen an das Risikomanagement von ZAG-Instituten (kurz: ZAG-MaRisk) gestartet.

Die erstmals veröffentlichten ZAG-MaRisk orientieren sich an den MaRisk für KWG-Institute und richten sich an alle Zahlungs- und E-Geld-Institute i. S. d. § 1 Abs. 3 bzw. § 42 Abs. 1 Zahlungsdiensteaufsichtsgesetz (ZAG) sowie Zweigniederlassungen deutscher ZAG-Institute im Ausland und sollen künftig einen flexiblen und praxisnahen Rahmen für die Ausgestaltung einer ordnungsgemäßen Geschäftsorganisation der ZAG-Institute vorgeben. Der Regelungsrahmen wird den ZAG-Instituten künftig unter Berücksichtigung des Prinzips der doppelten Proportionalität vorgegeben sein.

Ziel der BaFin ist, über Mindestvorgaben an die Geschäftsorganisation dazu beizutragen, Missständen entgegenzuwirken, die die Sicherheit der den Instituten anvertrauten Vermögenswerte gefährden und die ordnungsgemäße Durchführung der Zahlungsdienste oder E-Geld-Geschäfte beeinträchtigen können.

Eine ordnungsgemäße Geschäftsorganisation umfasst insb. angemessene Maßnahmen der Unternehmenssteuerung sowie Kontrollmechanismen und Verfahren, die gewährleisten, dass das ZAG-Institut seine Verpflichtungen erfüllt. Die internen Kontrollmechanismen bestehen aus dem internen Kontrollsystem und der Internen Revision und umfassen Regelungen zur Aufbau- und Ablauforganisation und Prozesse zur Identifizierung, Beurteilung, Steuerung, Überwachung sowie Kommunikation der Risiken (Risikosteuerungs- und -controllingprozesse). Das interne Kontrollsystem umfasst auch die Einrichtung der sog. Risikocontrolling-Funktion und der sog. Compliance-Funktion.

Hinweis: Soweit ein Aufsichtsorgan z. B. in Form eines Aufsichtsrates besteht, schafft das Risikomanagement auch eine Grundlage für die Wahrnehmung der Überwachungsfunktionen des Aufsichtsorgans und beinhaltet deshalb auch dessen angemessene Einbindung.

Ferner werden im Entwurf des Rundschreibens die Anforderungen der §§ 17 und 18 ZAG (Sicherungsanforderungen) sowie des § 26 ZAG (Auslagerung) präzisiert.

Die Konsultationsfrist der BaFin endet am 06.12.2023, ein konkreter Erstanwendungszeitpunkt für die Zahlungs- und E-Geld-Institute ist derzeit noch nicht terminiert.

Rundschreiben und Formular für die Meldung von Risiken im Zahlungsverkehr nach § 53 Abs. 2 ZAG

Die BaFin hat am 10.10.2023 eine Konsultation 10/2023 für ein Rundschreiben nebst zugehörigem Formular gestartet, das Zahlungsdienstleister und Kreditinstitute, die Zahlungsdienstleister sind, für ihre jährliche Meldung nach § 53 Abs. 2 ZAG künftig verwenden sollen.

Diese Unternehmen müssen der BaFin bereits jetzt jährlich eine aktuelle Bewertung der operationellen und der sicherheitsrelevanten Risiken im Zusammenhang mit den von ihnen erbrachten Zahlungsdiensten und hinsichtlich der Angemessenheit der Risikominderungsmaßnahmen und Kontrollmechanismen, die sie zur Beherrschung dieser Risiken ergriffen haben, übermitteln, wofür sie zukünftig das neue Formular verwenden müssen.

Sicherheitsrelevante Risiken sind eine Teilmenge der operationellen Risiken, so dass diesbezüglich ihrerseits keine Differenzierung erforderlich ist und daher im Meldeformular die Risiken zusammengefasst in einem Feld gemeldet werden sollen.

Die fünf wesentlichsten Risiken im Zusammenhang mit den vom Zahlungsdienstleister erbrachten Zahlungsdiensten sind auf dem Formular anzugeben und zu erläutern.

Risikominderungsmaßnahmen und Kontrollmechanismen werden von der BaFin als Mitigationsmaßnahmen ebenfalls in einer Meldeposition zusammengefasst. Hier ist aus dem Dropdown-Menü im Formularvordruck auszuwählen, ob die angesichts des genannten Risikos aktuell implementierten Mitigationsmaßnahmen angemessen sind („Ja", „Nein", „Teilweise"). Die Einstufung ist zu erläutern.

Die Konsultation endete bereits am 23.11.2023.

Hinweis: Das Formular enthält keine neuen regulatorischen Anforderungen. Vielmehr soll es Zahlungsdienstleistern helfen, eine mit der Erwartungshaltung der BaFin korrespondierende Meldung abzugeben. Dazu soll es von den Zahlungsdienstleistern erstmalig bis zum 31.08.2024 und anschließend jährlich für die Übermittlung der Angaben verwendet werden.

Referentenentwurf eines Gesetzes zur Verbesserung der Bekämpfung von Finanzkriminalität

Am 13.09.2023 wurde der Referentenentwurf eines Gesetzes zur Verbesserung der Bekämpfung von Finanzkriminalität (Finanzkriminalitätsbekämpfungsgesetz, kurz: FKBG) durch das BMF veröffentlicht. Der Entwurf enthält Regelungen zur Errichtung des neuen Bundesamtes zur Bekämpfung von Finanzkriminalität (BBF), seiner Aufgaben und Befugnisse sowie die notwendigen fachgesetzlichen Anpassungen u. a. im Bereich der Geldwäscheaufsicht und Sanktionen. Darüber hinaus sollen mit Umsetzung des FKBG Regelungen für die Einrichtung eines Immobilientransaktionsregisters geschaffen werden.

Das FKBG soll die Geldwäschebekämpfung in Deutschland nachhaltig verbessern und hierzu eine Bundesoberbehörde zur Bekämpfung von Finanzkriminalität errichten, welche in einem ganzheitlichen Ansatz Analyse, straf- und verwaltungsrechtliche Ermittlungen und Aufsicht unter einem Dach zusammenführt. Damit unternimmt der Gesetzgeber einen neuen Versuch, Strukturen und Kompetenzen zu schaffen, die eine Priorisierung der Geldwäschebekämpfung, internationaler und bedeutsamer Fälle mit Bezug auf Deutschland, sicherstellen.

Ein wesentlicher Teil des Konzepts zur Verbesserung der Bekämpfung der Geldwäsche soll durch die Errichtung des Ermittlungszentrums Geldwäsche (EZG) innerhalb der Bundesoberbehörde zur Bekämpfung von Finanzkriminalität umgesetzt werden, das künftig Strafermittlungen durchführen wird. Das EZG soll eine originäre Zuständigkeit für die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung von bedeutsamen Fällen der internationalen Geldwäsche mit Deutschlandbezug erhalten. Darüber hinaus sollen die zuständigen Strafverfolgungsbehörden des Bundes und der Länder das EZG um die Ermittlung von weiteren bedeutsamen Fällen der Geldwäsche in Deutschland ersuchen können.

Das Konzept sieht zudem vor, dass die Zuständigkeiten des BKA als polizeiliche Zentralstelle im nationalen und internationalen Verbund sowie die Zuständigkeit für Ermittlungen von Geldwäsche und die Ermittlung der Vortaten, im Bereich der Organisierten Kriminalität sowie die Zuständigkeit für Ermittlungen im Bereich der Abwehr von Gefahren des internationalen Terrorismus unberührt bleiben. Um der Forderung der FATF zur quantitativen Stärkung der Ressourcen in diesem Bereich gerecht zu werden, soll parallel ein nachhaltiger Ressourcenaufbau beim BKA erfolgen und mit den bereits vorhandenen Ressourcen in einer neuen Organisationsstruktur „Geldwäsche, Wirtschafts- und Finanzkriminalität", gebündelt werden. Die Geldwäscheermittlungen beim BKA sollen dabei künftig in konkreter Abgrenzung zur Aufgabenwahrnehmung des BBF mit Fokus auf den Bereich der deliktsspezifischen Geldwäsche geführt werden.

ESMA-Leitlinien für Meldungen gemäß EMIR

Am 23.10.2023 hat die ESMA Leitlinien für Meldungen gemäß European Market Infrastructure Regulation (EMIR) veröffentlicht. Diese Leitlinien gelten bezüglich der Meldepflicht für Derivate gemäß Art. 9 EMIR und Pflichten von Transaktionsregistern gemäß Art. 78 und 81 EMIR.

Die Leitlinien basieren auf Art. 16 Abs. 1 Verordnung (EU) Nr. 1095/2010 des EU-Parlaments und des EU-Rates (ESMA-VO) und dienen der Harmonisierung und Standardisierung der Meldungen gemäß EMIR. Gegenstand der Leitlinien sind daher insb. die Meldelogik sowie Hinweise zum Ausfüllen der Felder im Meldebogen, aber auch Befreiungsregelungen z. B. für gruppeninterne Derivate.

Die ESMA-Leitlinien gelten für finanzielle und nichtfinanzielle Gegenparteien von Derivaten gemäß Art. 2 Abs. 8 und 9 EMIR, für Transaktionsregister gemäß Art. 2 Abs. 2 EMIR und für zuständige Behörden.

Die ESMA-Leitlinien sind ab dem 29.04.2024 anzuwenden.

EBA-Bericht über die Rolle ökologischer und sozialer Risiken im Aufsichtsrecht für Kreditinstitute und Wertpapierfirmen

Die EBA hat am 12.10.2023 einen Bericht über die Rolle ökologischer und sozialer Risiken im Aufsichtsrecht für Kreditinstitute und Wertpapierfirmen veröffentlicht, dem noch weitere Berichte folgen sollen. Der Bericht richtet sich an die Institute und nationalen Aufsichtsbehörden sowie die europäischen Gesetzgeber, beschreibt aber auch das geplante zukünftige Vorgehen der EBA.

Umwelt- und Sozialrisiken verändern das Risikoprofil des Bankensektors und werden voraussichtlich im Laufe der Zeit an Bedeutung gewinnen. Sie wirken sich auf traditionelle Kategorien finanzieller Risiken wie Kredit-, Markt- und operationelle Risiken aus. Daher können sich ökologische und soziale Faktoren sowohl auf die Risiken einzelner Institute als auch auf die finanzielle Stabilität des gesamten Finanzsystems auswirken.

Der Bericht bewertet, wie das derzeitige europäische aufsichtsrechtliche Rahmenwerk ökologische und soziale Risiken erfasst. Er empfiehlt gezielte Verbesserungen, um die Integration von Umwelt- und Sozialrisiken in die Säule 1 zu beschleunigen sowie insb. risikobasierte Erweiterungen der Risikokategorien der Säule 1. Er enthält auch Überlegungen zum möglichen Einsatz makroprudenzieller Instrumente. Der Bericht erläutert auch, warum die EBA die Einführung eines grünen Stützungsfaktors oder eines braunen Sanktionsfaktors zum jetzigen Zeitpunkt nicht unterstützt. Die Verwendung solcher Anpassungsfaktoren ist mit Herausforderungen in Bezug auf die Gestaltung, die Kalibrierung und die komplexe Interaktion mit dem bestehenden Rahmen der Säule 1 verbunden.

Die EBA schlägt aufgrund der Ergebnisse des Berichts sowohl kurzfristige und als auch mittel- bis längerfristige Maßnahmen vor, um den Übergang zu einer nachhaltigeren Wirtschaft zu unterstützen und gleichzeitig sicherzustellen, dass der Bankensektor widerstandsfähig bleibt. Diese sollen in den nächsten drei Jahren im Rahmen der Umsetzung der überarbeiteten Eigenkapitalverordnung und Eigenkapitalrichtlinie (CRR3/CRD6) ergriffen werden.

Als **kurzfristige Maßnahmen** schlägt die EBA insb. Folgendes vor:

- Einbeziehung von Umweltrisiken in Stresstests sowohl im Rahmen des auf internen Ratings basierenden Ansatzes (IRB) als auch im Rahmen des auf internen Modellen basierenden Ansatzes (IMA) bei der grundlegenden Überprüfung des Handelsbuchs (FRTB).
- Förderung der Einbeziehung ökologischer und sozialer Faktoren als Teil der externen Bonitätsbeurteilungen durch Ratingagenturen.
- Förderung der Einbeziehung ökologischer und sozialer Faktoren als Teil der Due Diligence Anforderungen und der Bewertung von Immobiliensicherheiten.
- Verankerung einer Pflicht für Institute zur Ermittlung, ob ökologische und soziale Faktoren Auslöser für Verluste bei operationellen Risiken sind.
- schrittweise Entwicklung von umweltbezogenen Konzentrationsrisikokennzahlen als Teil der aufsichtlichen Berichterstattung.

Aus einer **mittel- bis längerfristigen Perspektive** werden in dem Bericht auch mögliche Überarbeitungen des Rahmens der Säule 1 vorgestellt, die die wachsende Bedeutung von Umwelt- und Sozialrisiken widerspiegeln. Dazu gehören u. a.:

- der mögliche Einsatz von Szenarioanalysen zur Verbesserung der zukunftsorientierten Elemente des aufsichtsrechtlichen Rahmenwerks,
- die Rolle, die Übergangspläne in der Zukunft als Teil der Entwicklung weiterer risikobasierter Verbesserungen der Säule-1-Regelung spielen könnten,
- die Überprüfung der Angemessenheit einer Überarbeitung der IRB-Aufsichtsformel und des entsprechenden Standardansatzes (SA) für das Kreditrisiko zur besseren Berücksichtigung von Umweltrisikoelementen und
- die Einführung umweltbezogener Konzentrationsrisikokennzahlen im Rahmen der Säule 1.

Hinweis: Die vorgeschlagenen Maßnahmen sollen nach den Ausführungen der EBA in den nächsten drei Jahren im Rahmen der Umsetzung der überarbeiteten Eigenkapitalverordnung und Eigenkapitalrichtlinie (CRR3/CRD6) ergriffen werden.

Verordnung (EU) über Green Bonds im EU-Amtsblatt veröffentlicht

Die EU hat sich ehrgeizige Klimaziele gesetzt und möchte bis 2050 klimaneutral sein. Um diese Ziele zu erreichen, wird auch die Finanzierung von umweltfreundlichen Projekten und Technologien immer wichtiger. Im Rahmen des European Green Deal hat der Rat der Europäischen Union am 23.10.2023 die Verordnung (EU) über europäische grüne Anleihen und freiwillige Offenlegungen für als umweltfreundlich vermarktete Anleihen und nachhaltigkeitsbezogene Anleihen angenommen.

Die VO (EU) 2023/2631 über europäische grüne Anleihen sowie fakultative Offenlegungen zu als ökologisch nachhaltig vermarkteten Anleihen und zu an Nachhaltigkeitsziele geknüpften Anleihen (Green Bond Standard) wurde am 30.11.2023 im EU-Amtsblatt veröffentlicht (vgl. hier). Die Verordnung wird zwanzig Tage nach ihrer Veröffentlichung im EU-Amtsblatt in Kraft treten und im Wesentlichen 12 Monate nach dem Inkrafttreten Anwendung finden. Die Verordnung enthält diverse Grandfathering-Regelungen von 5, 7 und 10 Jahren für bereits emittierte grüne Anleihen.

Inhalt der Verordnung, insb. des European Green Bond Standards

Mit der Verordnung wird ein Standard etabliert, der sicherstellen soll, dass die Mittel aus Anleihen, die die Bezeichnung „Europäische Grüne Anleihe" bzw. „European Green Bond" oder „EuGB" tragen sollen, tatsächlich zur Finanzierung von umweltfreundlichen Projekten verwendet werden. Basierend auf der EU-Taxonomie definiert der Standard, welche Projekte als „grün" gelten und legt Kriterien für die Transparenz, die Berichterstattung und die Verwendung der Mittel fest.

Hervorzuheben sind insb. die folgenden Regelungen:

1. **Einklang mit den Taxonomieanforderungen**
   Mindestens 85 % der Verwendung der Emissionserlöse muss mit der EU-Taxonomie-Verordnung übereinstimmen. Die verbleibenden 15 % dürfen zwar nicht zweckfrei sein, aber dennoch flexibel in Sektoren, die derzeit nicht von der EU-Taxonomie erfasst werden und bestimmte Aktivitäten ver-wendet werden (sog. Flexibilitätsquote). Sie müssen aber einen wesentlichen Beitrag zu mindestens einem der sechs Umweltziele der Taxonomie leisten.

2. **Transparenz**
   Über die Gesamtlaufzeit der Anleihe muss der Emittent des EuGB umfassende Transparenzpflichten erfüllen, um so die Transparenz hinsichtlich des Gebots der zweckgebundenen Mittelverwendung zu gewährleisten. Hierzu zählt die Erstellung eines Informationsblattes (European Green Bond Factsheet), ein jährlicher Allokationsbericht sowie ein einmaliger Wirkungsbericht zu den Umweltauswirkungen der Anleihe. Der Emittent unterliegt hinsichtlich dieser Pflichten der Aufsicht der zuständigen Behörde, in Deutschland mithin der BaFin.

3. **Externe Prüfung**
   Die Qualität der Berichterstattung, einschließlich das European Green Bond Fact Sheet, muss von einem externen Prüfer überwacht werden.

4. **Registrierung und Überwachung**
   Zur Gewährleistung einer qualitativ hochwertigen Prüfung müssen sich die externen Prüfer bei der Europäischen Wertpapier- und Marktaufsichtsbehörde (ESMA) registrieren, bestimmte Anforderungen u. a. hinsichtlich ihrer Qualifikationen, Erfahrungen und Organisation erfüllen, und sie unterliegen der Überwachung durch die ESMA.

5. **Optionale Offenlegungsprinzipien für Nicht-EuGB**
   Optionale Offenlegungsprinzipien (Vor- und Nach-Emission-Veröffentlichungen) für als umweltfreundlich vermarktete Anleihen und nachhaltigkeitsbezogene Anleihen, die jedoch nicht als EuGB vermarktet werden, müssen eingehalten werden. Die Regelung nimmt Rücksicht auf die bereits nach internationalen Standards (u. a. Green Bond Principles der ICMA und Climate Bond Standards der CBI) emissionsfähigen Bonds. Ziel ist, für den Anleger eine Vergleichbarkeit hinsichtlich der offengelegten Informationen zwischen diesen und den EuGB zu erreichen.

Der European Green Bond Standard stellt ein freiwilliges Qualitätssiegel dar, dessen Bezeichnung „europäische grüne Anleihe" allen Emittenten – sowohl innerhalb als auch außerhalb der EU – zur Verfügung stehen soll, vorausgesetzt die Anforderungen der Verordnung werden erfüllt. Die Entscheidung über die Nutzung des EuGB-Labels bleibt daher den Anleiheemittenten überlassen. Möglich ist somit auch eine Nutzung anderer Standards wie z. B. der Green Bond Principles der International Capital Market Association (ICMA). Dem Wettbewerb zwischen der Nutzung solcher anderer Standards und dem European Green Bond Standard stellt sich die EU bewusst, indem sie die Einhaltung der vorgenannten optionalen Offenlegungsprinzipen anregt. Insofern bleibt abzuwarten, ob und wie sich der European Green Bond Standard gegenüber den bereits etablierten anderen Standards durchsetzt.

Hinweis: Das IDW hat noch für das 4. Quartal 2023 eine Arbeitshilfe für die „Prüfung von Green Bonds" im IDWLife angekündigt.

Fazit

Der neue European Green Bond Standard dient Investoren wie Emittenten. Investoren erhalten die Möglichkeit, verlässlicher in grüne Projekte zu investieren bzw. ihr Risiko, in Produkte zu investieren, die „Greenwashing" betreiben, zu reduzieren. Emittenten können nachweisen, dass sie grüne Projekte finanzieren, die mit der EU-Taxonomie im Einklang stehen und sich über EU Green Bonds neue Investorenschichten erschließen. Grüne Anleihen nach dem neuen European Green Bond Standard sollen damit künftig insb. auch für den Mittelstand eine attraktive Finanzierungsmöglichkeit darstellen.

Entwurf einer EU-Richtlinie für eine einfachere Quellenbesteuerung von Kapitaleinkünften

Am 19.06.2023 hat die EU-Kommission den Entwurf für eine Richtlinie über schnellere und sicherere Verfahren für die Entlastung von Quellensteuern (Directive on Faster and Safer Relief of Excess Withholding Taxes, „FASTER"-Richtlinie) veröffentlicht.

Dieser Entwurf sieht insb. die Einführung einer gemeinsamen digitalen EU-Ansässigkeitsbescheinigung, eines nationalen Registers und standardisierter Meldepflichten sowie sog. Schnellverfahren vor, um eine EU-weite Harmonisierung und Beschleunigung der Erstattungsverfahren zu fördern. Laut dem Entwurf sind die Mitgliedstaaten zur nationalen Umsetzung der Richtlinie bis zum 31.12.2026 verpflichtet. Die Regelungen sollen ab dem 01.01.2027 anwendbar sein.

Der Regelungsbedarf besteht ausweislich der Begründung des Richtlinien-Entwurfs der EU-Kommission darin, dass den bestehenden Quellensteuerverfahren in grenzüberschreitenden Sachverhalten ein Doppelbesteuerungsrisiko innewohnt, da Einkünfte aus dem Halten von Wertpapieren zunächst im Land des Emittenten der Wertpapiere (Quellenstaat) sowie im Land der Ansässigkeit des Anlegers (Wohnsitzstaat) einer Besteuerung unterliegen. Die Erstattungsverfahren für gebietsfremde Anleger, sei es auf Grund von Doppelbesteuerungsabkommen (DBA) oder inländischen Vorschriften, sind jedoch häufig aufwendig, kostspielig und langwierig, da sie – sowohl hinsichtlich der benötigten Unterlagen als auch des Digitalisierungsgrades – von Mitgliedstaat zu Mitgliedstaat sehr unterschiedlich ausgeprägt sind. Die Inanspruchnahme von Vorteilen nach DBA hängt regelmäßig davon ab, dass die Steuerpflichtigen in einem Vertragsstaat ansässig sind. Für den Nachweis schreiben die DBA zwar grundsätzlich keine bestimmte Form vor, gleichwohl haben sich in der Praxis Ansässigkeitsbescheinigungen etabliert. Das deutsche Steuerrecht sieht in § 50c Abs. 5 S. 2

EStG sogar vor, dass der Antragsteller seinem in digitaler Form zu stellenden Freistellungs- bzw. Erstattungsantrag eine solche Bescheinigung beifügen muss. Anstelle von Ansässigkeitsbescheinigungen in Papierform soll durch die FASTER-Richtlinie eine gemeinsame digitale EU-Ansässigkeitsbescheinigung (electronic tax residency certificate, eTRC) eingeführt werden, die innerhalb eines Werktages nach Antragstellung ausgestellt werden soll. Damit soll EU-weit die Umstellung auf ein elektronisches Verfahren erfolgen. Die eTRC soll von allen Mitgliedstaaten eingeführt werden und ein schnelles, einfaches und sicheres Verwaltungsverfahren zur Bestätigung der steuerlichen Ansässigkeit der Steuerpflichtigen in der EU ermöglichen.

Zertifizierte Finanzintermediäre sollen der zuständigen Steuerverwaltung melden, von wem und an wen quellensteuerpflichtige Zahlungen erfolgen, damit diese die Transaktion nachvollziehen kann. Insb. große Finanzintermediäre (z. B. Banken) in der EU müssen sich laut Entwurf in ein nationales Register zertifizierter Finanzintermediäre eintragen, welches in jedem Mitgliedstaat eingerichtet und von einer neu benannten jeweiligen Behörde verwaltet werden soll. Der Finanzintermediär als Teil der Wertpapierzahlungskette zwischen dem Emittenten von Wertpapieren und dem registrierten Eigentümer führt das Anlagekonto seiner Investoren und beantragt, sofern gewünscht, zulässige Steuererleichterungen. Demnach verpflichtet sich der Finanzintermediär, sich in die jeweiligen Register der unterschiedlichen Mitgliedstaaten einzutragen, in denen seine Kunden investiert sind. Darauf folgt eine Meldepflicht gegenüber den zuständigen Behörden, um die notwendigen Informationen zu melden, um die Wertpapierzahlungskette bei Dividendenzahlungen und Zinszahlungen für Quellenländer und andere Mitgliedstaaten zu rekonstruieren. Dadurch wird die Identifizierung des endgültigen Investors erleichtert, was zur Reduzierung des Missbrauchs mehrfacher Erstattungen der Quellensteuer von mehreren Investoren desselben Wertpapiers führt. Finanzintermediäre müssen außerdem ihre eigenen Investoren regelmäßig im Hinblick auf Betrugs- und Kreditrisiken überprüfen.

Die EU-weite Harmonisierung und Beschleunigung der Erstattungsverfahren soll durch zwei sog. Schnellverfahren erreicht werden, welche die bestehenden Regelungen ergänzen. Ausweislich des Richtlinienentwurfs sollen sich die Mitgliedstaaten für eines der beiden Verfahren oder eine Kombination aus beiden entscheiden können. Einerseits besteht die Möglichkeit der sofortigen Entlastung („Relief at source"), so dass bereits zum Zeitpunkt der Zahlung von Zinsen oder Dividenden der nach den geltenden Bestimmungen des DBA zutreffende Quellensteuersatz angewandt wird. Andererseits wird ein Schnell-Erstattungsverfahren („Quick refund") eingeführt, durch das eine Erstattung von Quellensteuern binnen 50 Tagen nach Zahlung sichergestellt werden soll.

Die digitale und nicht auf einzelne Einkunftsquellen beschränkte Ansässigkeitsbescheinigung verspricht erhebliche Erleichterungen für Steuerpflichtige und Finanzbehörden. Die derzeit langen Erstattungsverfahren stellen eine Beeinträchtigung der Kapitalverkehrsfreiheit dar. Die beiden von der EU-Kommission vorgeschlagenen Instrumente sowie die Einführung eines nationalen Registers für zertifizierte Finanzintermediäre in Verbindung mit einer Meldepflicht dürften grundsätzlich geeignete Instrumente sein, um die Umsetzung der Ziele der Richtlinie zu fördern.

Der Richtlinien-Entwurf erfasst börsennotierte Wertpapiere. Der Anwendungsbereich besteht daher im Wesentlichen aus Anlegern, die grenzüberschreitend Aktien oder Anleihen von börsennotierten Aktiengesellschaften halten und hieraus laufende Zinsen oder Dividenden beziehen, die einer Quellenbesteuerung unterliegen. Daneben werden Kreditinstitute von der Richtlinie erfasst, denen durch die Einführung des nationalen Registers im Bereich der Kapitalertragsteuer weitere umfassende Compliance-Pflichten (und mögliche Haftungsrisiken) auferlegt werden.

Keine Besteuerung von Sachzuwendungen eines Kreditinstituts an seine Privatkunden im Rahmen der allgemeinen Kundenpflege

Mit Urteil vom 09.08.2023 (Az. VI R 10/21) hat der Bundesfinanzhof entschieden, dass Sachzuwendungen eines Kreditinstituts an seine Privatkunden nicht pauschalversteuert werden müssen. Damit bestätigt der BFH die Auffassung der Vorinstanz (Urteil des Finanzgerichts Baden-Württemberg vom 19.04.2021, Az.10 K 577/21).

Im Streitfall lud ein Kreditinstitut vermögende Privatkunden zu zwei Veranstaltungen, eine Schifffahrt mit Weinprobe und ein Golfturnier, ein. Bei diesen Veranstaltungen wurde neben der Kontaktpflege die Marke eines Produktanbieters imagewirksam präsentiert. Es wurde jedoch davon abgesehen, konkrete eigene oder fremde Finanzprodukte zu bewerben. Auch die Einladungen enthielten keinen Hinweis auf eine bestimmte Geldanlage oder mögliche Beratungsgespräche. Das Kreditinstitut betrieb für die eingeladenen Kunden die Vermögensverwaltung u. a. in der Form des Einlagegeschäfts (Sparkonten und Festgelder) und des Depotgeschäfts sowie für einen kleinen Teil der Kunden das Kreditgeschäft. Das Kreditinstitut unterwarf die Sachzuwendungen der Pauschalbesteuerung gemäß § 37b EStG, meldete die Pauschalsteuern an und führte diese an das Finanzamt ab. In der Folge wandte sich das Kreditinstitut gegen die Pauschalbesteuerung.

Zu Recht, wie der BFH in seinem Urteil entschied. Gemäß § 37b Abs. 1 Satz 1 Nr. 1 EStG können Steuerpflichtige die Einkommensteuer einheitlich für alle innerhalb eines Wirtschaftsjahres gewährten betrieblich veranlassten Zuwendungen, die zusätzlich zur ohnehin vereinbarten Leistung oder Gegenleistung erbracht werden, und die nicht in Geld bestehen, mit einem Pauschsteuersatz von 30 % erheben. Entsprechendes gilt nach § 37b Abs. 1 Satz 1 Nr. 2 EStG für alle innerhalb eines Wirtschaftsjahres gewährten Geschenke im Sinne des § 4 Abs. 5 Satz 1 Nr. 1 EStG.

Bei Sachzuwendungen an Arbeitnehmer, Geschäftspartner und deren Arbeitnehmer handelt es sich oft um einen steuerpflichtigen geldwerten Vorteil, dessen Bewertung für den Begünstigten nicht selten schwierig ist. Daher soll die Pauschalversteuerung dieser Zuwendungen wie im Falle des § 37a EStG der Vereinfachung dienen.

Die Pauschalierung der Einkommensteuer nach § 37b EStG erfasst allerdings nur solche betrieblich veranlassten Zuwendungen, die bei den Zuwendungsempfängern dem Grunde nach zu einkommensteuerpflichtigen Einkünften führen. Denn § 37b EStG begründet keine weitere eigenständige Einkunftsart und keinen sonstigen originären (Einkommen-)Steuertatbestand, sondern stellt lediglich eine besondere pauschalierende Erhebungsform der Einkommensteuer dar. Nach diesen Maßstäben kommt eine Pauschalierung der Einkommensteuer für die streitigen Zuwendungen nach § 37b Abs. 1 Satz 1 Nr. 1 EStG nach Auffassung des BFH nicht in Betracht.

Zwar waren die Zuwendungen als Marketingmaßnahmen betrieblich veranlasst. Gleichwohl schuldete die Klägerin hierfür keine Pauschalsteuer gemäß § 37b Abs. 1 Satz 1 Nr. 1 EStG, da die von ihr gewährten, betrieblich veranlassten Zuwendungen bei den Zuwendungsempfängern – als einzige in Betracht kommende Einkunftsart – nicht zu einkommensteuerbaren Einkünften aus Kapitalvermögen im Sinne des § 20 EStG führten. Im Urteilsfall haben die Kunden zwar im Rahmen von Spar-, Girokonto- und Festgeldverträgen sowie durch den Erwerb von Aktien, Investmentanteilen oder Schuldverschreibungen Kapital an die Klägerin bzw. an Dritte überlassen und aus diesen Kapitalanlagen Einkünfte aus Kapitalvermögen erzielen können. Die streitigen Sachzuwendungen des Kreditinstituts waren aber weder ein durch diese Kapitalanlagen veranlasstes zusätzliches Entgelt noch ein ggf. vorgezogenes Entgelt für eine geplante künftige Kapitalüberlassung. Vielmehr handelte es sich bei den Veranstaltungen um (Werbe-)Maßnahmen der Kundenpflege und -bindung, welche den Kundenberatern Chancen auf künftige Geschäftsabschlüsse, insb. die Vermittlung weiterer Kapitalanlagen erhöhen sollten. Die Zuwendungen wurden unabhängig von einem Leistungsaustausch erbracht und fallen damit laut BFH nicht in den Anwendungsbereich des § 37b Abs. 1 Satz 1 Nr. 1 EStG.

Auch § 37b Abs. 1 Satz 1 Nr. 2 EStG scheidet nach Auffassung des BFH aus, da diese Vorschrift nur die Einkommensteuer erfasst, die durch Geschenke (im Sinne des § 4 Abs. 5 Satz 1 Nr. 1 EStG) entsteht, wenn und soweit der Empfänger dieser Geschenke dadurch Einkünfte erzielt. Vorliegend wurden durch die Kunden jedoch keine Einkünfte aus Kapitalvermögen erzielt.

ANSPRECHPARTNER

FRANKFURT

Nasim Jenkouk
Rechtsanwältin
Tel.: +49 69 450907-110
E-Mail: nasim.jenkouk@ebnerstolz.de

Marco Brinkmann
Steuerberater
Tel. +49 69 450907-165
E-Mail: marco.brinkmann@ebnerstolz.de

HAMBURG

Dr. Ludger C. Verfürth LL.M.
Rechtsanwalt
Tel. +49 40 37097-129
E-Mail: ludger.verfuerth@ebnerstolz.de

KÖLN

Marc Lilienthal
Wirtschaftsprüfer, Steuerberater
Tel. +49 211 20643-115
E-Mail: marc.lilienthal@ebnerstolz.de

Ingo van Dyck
CISA, CDPSE
Tel. +49 221 20643-707
E-Mail: ingo.vandyck@ebnerstolz.de

Matthias Schütte
Tel. +49 211 20643-708
E-Mail: matthias.schuette@ebnerstolz.de

STUTTGART

Matthias Kopka
Wirtschaftsprüfer, Steuerberater
Tel. +49 711 2049-1202
E-Mail: matthias.kopka@ebnerstolz.de

Lorenz Muschal
Wirtschaftsprüfer, Steuerberater
Tel. +49 711 2049-1263
E-Mail: lorenz.muschal@ebnerstolz.de

Jens-Uwe Herbst
Wirtschaftsprüfer, Steuerberater
Tel. +49 711 2049-1306
E-Mail: jens-uwe.herbst@ebnerstolz.de

REDAKTION:

Jutta Kempers
Rechtsanwältin
Tel. +49 711 2049-1163
E-Mail: jutta.kempers@ebnerstolz.de

RSM EBNER STOLZ

IMPRESSUM

Herausgeber:
Ebner Stolz Mönning Bachem
Wirtschaftsprüfer Steuerberater Rechtsanwälte
Partnerschaft mbB
www.ebnerstolz.de

Ludwig-Erhard-Straße 1, 20459 Hamburg
Tel. +49 40 37097-0

Holzmarkt 1, 50676 Köln
Tel. +49 221 20643-0

Kronenstraße 30, 70174 Stuttgart
Tel. +49 711 2049-0

Redaktion:
Jens-Uwe Herbst, Tel. +49 711 2049-1306
Jutta Kempers, Tel. +49 711 2049 1163
Dr. Ulrike Höreth, Tel. +49 711 2049-1371
novusfs@ebnerstolz.de

Wir legen großen Wert auf Gleichbehandlung. Aus Gründen der besseren Lesbarkeit verzichten wir jedoch auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers. Im Sinne der Gleichbehandlung gelten entsprechende Begriffe grundsätzlich für alle Geschlechter. Die verkürzte Sprachform beinhaltet also keine Wertung, sondern hat lediglich redaktionelle Gründe.

Fotonachweis:
Alle Bilder: © www.gettyimages.com