Point of Compliance
Das Risikomanagement-Magazin

AUSGABE 2 / 2024

PoC

Resilienz

DZ CompliancePartner

Folgen Sie der DZ CompliancePartner GmbH auf Social Media.

IMPRESSUM

PoC – Point of Compliance
Das Risikomanagement-Magazin,
Ausgabe 33, 2/2024
ISSN: 2194-9514
Herausgeber: DZ CompliancePartner GmbH, Wilhelm-Haas-Platz, 63263 Neu-Isenburg, Telefon 069 580024-0,
Telefax 069 580024-900, www.dz-cp.de
Handelsregister HRB 11105, Amtsgericht Offenbach, USt.-IdNr.: DE201150917
Geschäftsführung: Jens Saenger (Sprecher), Dirk Pagel

Verantwortlich i. S. d. P.: Jens Saenger
Redaktion: Gabriele Seifert, Leitung (red.)
Redaktionsanschrift: DZ Compliance-Partner GmbH, Redaktion Point of Compliance, Wilhelm-Haas-Platz, 63263 Neu-Isenburg, Telefon 069 580024-0, Telefax 069 580024-900, E-Mail: poc@dz-cp.de
Weitere Autoren dieser Ausgabe: Fabian Baaß, Axel Hofmeister, Najat Lissner, Jens Saenger, Jörg Scharditzky, Lars Schinnerling, Katja Schlüter, Thomas Schröder, Sandra Sitter, Benjamin Wellnitz

Bildnachweise: DZ CompliancePartner GmbH, iStock.com/Ivan Bajic
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 Online-zugänglichmachung 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: 30. April 2024
Auflage: 2.400 Exemplare

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

DORA ist in aller Munde. Bei aller Aufregung sind aber vor allem zwei Punkte wichtig:

1. Der Digital Operational Resilience Act (DORA) folgt dem richtigen Ansatz im Kampf gegen eine länder- und branchenübergreifende Cyberkriminalität. Einem organisierten und hochprofessionalisierten „Cybercrime as a service" ist in der Tat wirksam allein durch ein entschiedenes und koordiniertes Handeln auf EU-Ebene zu begegnen.

2. DORA ist machbar. Richtig ist, dass die Umsetzungsfrist bis zum 17. Januar 2025 denkbar knapp ist, zumal die Anforderungen hoch sind und einige technische Regulierungs- und Implementierungsstandards noch nicht vorliegen. Mit den BAIT ist jedoch die Finanzbranche vergleichsweise gut aufgestellt, so dass die DORA-Umsetzung mit der nötigen Konsequenz, aber auch mit Ruhe angegangen werden kann.

In der vorliegenden Ausgabe der Point of Compliance setzen wir den Schwerpunkt auf die Widerstandsfähigkeit gegenüber IT-Risiken (S. 4 und S. 8), fragen, wie Produktinnovationen aus Sicht der Geldwäscheprävention zu bewerten sind (S. 11), was gegen Marktmissbrauch zu tun ist (S. 14), wo wir in Sachen Nachhaltigkeit stehen (S. 17) und schließlich, ob der Schufa-Score noch ein Entscheidungskriterium für Kredite ist (S. 23).

Ich wünsche Ihnen eine anregende Lektüre.

Herzlichst
Ihr Jens Saenger

Jens Saenger
Sprecher der Geschäftsführung

Umsetzung in der Bank DORA

Der **D**igital **O**perational **R**esilience **A**ct **(DORA)** ist ab dem 17. Januar 2025 verbindlich anzuwenden. Allerdings sind noch viele Fragen offen: Für wen gilt DORA? Wie sind die BAIT hinsichtlich DORA zu berücksichtigen? Und vor allem: Wie sieht die praktische Umsetzung aus? Mit welchem Aufwand ist zu rechnen und welche Sanktionen drohen bei Nicht-Einhaltung?

Die Verordnung über die digitale operationale Resilienz im Finanzsektor (DORA) ist als Antwort auf den digitalen Wandel und die zunehmende Gefahr von Cyberbedrohungen im Finanzsektor zu verstehen. Sie setzt ihren Fokus auf einen angemessenen Umgang mit der zunehmenden Abhängigkeit des Finanzsektors von Drittanbietern. Die Finanzsysteme der Europäischen Union sollen in die Lage versetzt sein, die Betriebsstabilität im Falle einer schwerwiegenden Störung aufrechtzuerhalten.

Entsprechend ist der Geltungsbereich von DORA geregelt. Es fallen nicht nur die typischen Finanzunternehmen unter die EU-Verordnung, sondern auch Dienstleister, die Informations- und Kommunikationstechnologie-Dienstleistungen (IKT) Unternehmen im Finanzsektor anbieten und durchführen (Art. 2 Abs. 1 lit. u DORA).

DORA stellt eine EU-Verordnung dar und ist gemäß der anzuwendenden Normenhierarchie höherrangig als Gesetzgebungen und Verordnungen auf nationaler Ebene. Insofern sind beispielsweise die nationalen Gesetze wie das KWG, ZAG, KAGB und VAG sowie diverse Verwaltungsanweisungen, wie z. B. MaRisk, BAIT, VAIT, KAIT und ZAIT, der DORA untergeordnet.

Im Folgenden setzen wir den Schwerpunkt auf die bankspezifische Sichtweise.

Mit der Einführung einer EU-Verordnung müssen die nationalen Gesetze mit dem höherrangigen internationalen Recht harmonisiert werden. Nationale Regelungen können über die Öffnungsklauseln das internationale Recht nur ergänzen oder erweitern – nicht aber einschränken. So werden beispielsweise die BAIT in Teilen angepasst werden müssen. So sehen die BAIT noch eine Beschränkung der Auslagerungsfähigkeit des Informationssicherheitsbeauftragten vor (BAIT Tz. 4.6). Diese Beschränkung ist mit Anwendung von DORA (Art. 6 Abs. 10 DORA) in der bisherigen Form jedoch nicht mehr anwendbar. Insofern ist eine allgemeine Überprüfung bzw. Überarbeitung der BAIT vorgesehen.[1]

Dessen ungeachtet stellen jedoch die BAIT in der Fassung vom 16. August 2021 ein gutes Fundament zur Umsetzung von DORA dar.

In der Praxis ergeben sich folgende Umsetzungsschritte:

- Durchführung als Projekt und Aufwandsschätzung
- Durchführung einer Gap Analyse
- Beseitigung der Gaps gemäß der Gap-Analyse
- Beendigung des Projektes und Überführung in den Regelkreislauf

Durchführung als Projekt und Aufwandsschätzung

Die Umsetzung von DORA sollte als Projekt in der Bank erfolgen. Wir empfehlen, folgende Punkte zu klären:

- Aufwandsabschätzung (eigener Personalaufwand, Schulungs- und Fortbildungskosten für die Mitarbeiterinnen und Mitarbeiter, ggf. Beratungsunterstützung weiterer Dienstleister)
- Festlegung des Projektziels
- Festlegung des Projektanfangs und -endes sowie der Meilensteine, der Projektleitung und der einzelnen Verantwortlichkeiten
- Ermittlung des möglichen Mehraufwands zur nachhaltigen Anwendung von DORA im Regelkreislauf

Der Aufwand zur Umsetzung der vier unten genannten Handlungsfelder kann bankindividuell ausfallen. Hierbei spielt u. a. auch die Heterogenität der IT-Landschaft, der Umfang selbst betriebener und ausgelagerter IT-Systeme eine Rolle.

Durchführung einer Gap-Analyse

Die Gap-Analyse bzw. Analyse der strategischen Lücke ist ein wichtiger Schritt, um den Ist-Zustand Ihrer Bank zu ermitteln. Die konkreten Handlungsempfehlungen zeigen Ihnen, welche operativen Maßnahmen Sie ergreifen müssen, um diese Lücken zu schließen. Hierzu empfehlen wir u. a. die Hilfstabelle des BVR zu nutzen.[2]

Die Gap-Analyse erstreckt sich auf vier Handlungsfelder:

1. IKT-Risikomanagement
2. Management IKT-bezogene Vorfälle
3. Testen der digitalen operationalen Resilienz
4. IKT-Drittparteien-Risikomanagement

Beseitigung der Gaps gemäß der Gap-Analyse

Nach der Durchführung der Gap-Analyse ergeben sich konkrete Handlungsbedarfe, die in der Bank umgesetzt werden müssen.

1. Monitoring: IKT-Risikomanagement (Kapitel 2, Art. 5–16 DORA)

Um IKT-Risiken schnell, effizient und umfassend zu erkennen und ein hohes Maß an digitaler Widerstandsfähigkeit zu gewährleisten, fordert DORA nach Kapitel 2, Art. 6 einen soliden, umfassenden und gut dokumentierten Rahmen für das IKT-Risikomanagement.

Dieser Rahmen umfasst u. a. folgende Punkte:

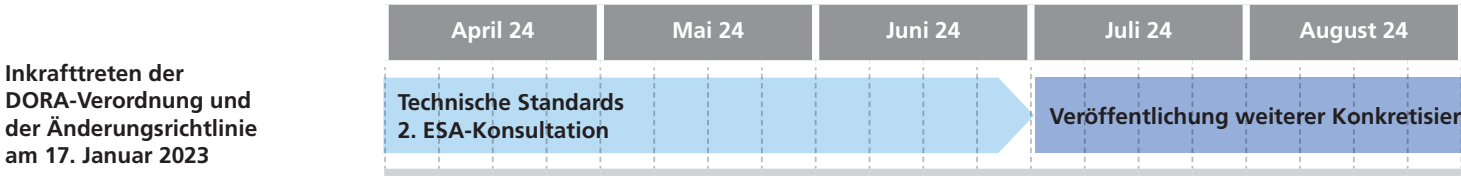
- Ergänzung der IT-Strategie durch eine DORA-Strategie
- Überprüfung und Anpassung des Governance- und Kontrollrahmens (Einrichtung einer IKT-Risikokontrollfunktion) inkl. des Berichtswesens
- Durchführung der erforderlichen Anpassungen im Informationsverbund
- Identifizierung und Klassifizierung der IKT-Systeme und IKT-Dienstleister nach dem neuen Begriff „kritische oder wichtige Funktion“ sowie nach den Abhängigkeiten und Risiken
- Anpassung der Sicherheitsmaßnahmen (z. B. System-, Netzwerk- und Datensicherheit, Schwachstellen- und Patchmanagement, IKT-Änderungsmanagement)
- Überarbeitung des bisherigen Notfallmanagements
- Überprüfung und Anpassung der schriftlich fixierten Ordnung (interne Arbeitsanweisungen)
- Einführung von nachhaltigen Schulungsprogrammen (z. B. Awareness-Maßnahmen)

2. Management IKT-bezogener Vorfälle (Kapitel 3, Art. 17–23 DORA)

Das Management von IKT-bezogenen Vorfällen bezieht sich auf die proaktive Planung, Organisation und Koordination von Maßnahmen zur Reaktion auf und Bewältigung von Vorfällen. Dies umfasst die Erkennung, Bewertung, Eindämmung und Wiederherstellung nach Vorfällen wie Cyberangriffen, Datenlecks, Systemausfällen oder anderen Sicherheitsverletzungen. Das Ziel ist es, die Auswirkungen zu minimieren, die Geschäftskontinuität aufrechtzuerhalten und die Sicherheit der digitalen Infrastruktur zu gewährleisten. Dies beinhaltet auch die Dokumentation von Vorfällen, um aus ihnen zu lernen und zukünftige Sicherheitsmaßnahmen zu verbessern.

Dieser Rahmen umfasst u. a. folgende Punkte:

- Klassifizierung aller IKT-bezogenen Vorfälle und Anpassung des damit verbundenen Meldewesens/ der Meldeverpflichtungen



- Anwendung von Lernprozessen aus IKT-bezogenen Vorfällen und Kommunikationspläne
- Freiwilliger Informationsaustausch zwischen Finanzunternehmen für bessere Sicherheits- und Abwehrmaßnahmen

3. Testen der digitalen operationalen Resilienz (Kapitel 4, Art. 24–27 DORA)

Das Testen der digitalen operationalen Resilienz bezieht sich darauf, wie gut die Bank auf digitale Bedrohungen und Herausforderungen vorbereitet ist und wie effektiv hier reagiert werden kann. Dabei werden verschiedene Aspekte der digitalen Infrastruktur und Sicherheitsmaßnahmen überprüft, um die Widerstandskraft gegen Cyberangriffe, Datenverlust und weitere digitale Risiken zu bewerten. Das Testen der digitalen operationalen Resilienz hilft dabei, Schwachstellen zu identifizieren und Maßnahmen zur Stärkung der Sicherheit und des Schutzes digitaler Ressourcen zu entwickeln.

Dabei können auch Lösungen Dritter in die Tests einbezogen werden.

DORA – Position und Unterstützungsangebot der DZ CompliancePartner GmbH

1. Wir werden die IKT-Risikokontrollfunktion (Art. 6 Abs. 4 DORA) als Auslagerungsdienstleistung anbieten (Art. 6 Abs. 10 DORA):
   – präferiert in Form der Weiterentwicklung der heutigen Funktion des/r Informationssicherheitsbeauftragten (ISB)
   – oder alternativ als ergänzende Funktion.
2. Wir setzen uns in den Gremien der Genossenschaftlichen FinanzGruppe für die Weiterentwicklungslösung des/r ISB ein.
3. Wir unterstützen unsere Kunden in der Implementierung von DORA durch Umsetzungsprojekte mit Augenmaß. Dabei werden wir die Auslagerungskunden in der Informationssicherheit priorisieren.

4. IKT-Drittparteien-Risikomanagement (Kapitel 5, Abschnitt 1, Art. 28–30 DORA)

Das IKT-Drittparteienrisiko bezieht sich auf die Gefahr, die von externen Parteien ausgeht. Dazu gehören Risiken wie Datenlecks, Cyberangriffe oder Sicherheitslücken, die durch Drittanbieter von Software, Dienstleistungen oder Infrastruktur verursacht werden.

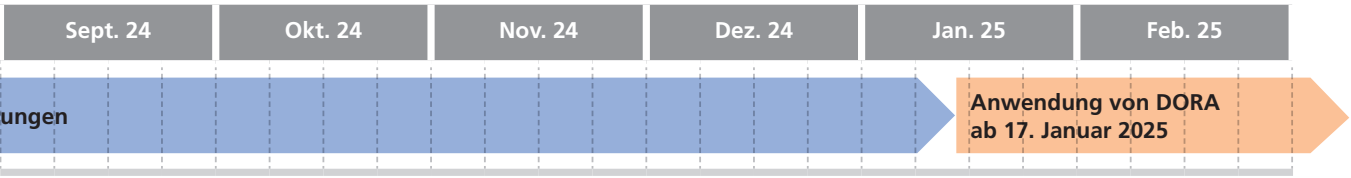
Das Ziel ist die Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit von Informationen und Systemen. Durch angemessene Risikominderung und -kontrolle kann sichergestellt werden, dass externe Anbieter keine unangemessenen Risiken für Ihre IKT-Infrastruktur darstellen und die Kontinuität Ihrer Geschäftsprozesse gewährleistet bleibt.

Unter anderem werden folgende Punkte vorgesehen:

- Implementierung eines Prozesses für den Einsatz von IKT-Dienstleistern
- Implementierung eines Prozesses zur Ermittlung und Überprüfung der entsprechenden Risiken
- Anpassung der Verträge mit IKT-Drittparteien auf DORA-Konformität inkl. Aufnahme einer Exit-Strategie
- Sicherstellung der DORA-Anforderungen durch das Auslagerungsmanagement
- Identifikation und Dokumentation des IKT-Drittparteienrisikos durch Ausübung der Zugangs-, Inspektions- und Auditrechte
- Erstellung eines Informationsregisters, welches die vollständige Übersicht aller in der Bank enthaltenen IKT-Dienstleistungen beinhaltet etc.

Beendigung des Projektes und Überführung in den Regelkreislauf

Nach erfolgter DORA-Umsetzung empfehlen wir, den Projektabschluss zu dokumentieren und in den Regelkreislauf überzugehen. Hierbei ist z. B. die Planung von IKS-Aufgaben vorzunehmen, damit die Aktualität der Governance und des Kontrollrahmens, der Durchführung der erforderlichen IKT-Notfallübungen etc. nachhaltig sichergestellt ist.



Sanktionen

Können Sanktionen bei Nicht-Einhaltung von DORA drohen? Die Umsetzung und Anwendung von DORA kann gem. Art. 50 DORA durch die zuständige Aufsicht kontrolliert werden. Auch Sanktionen können gem. Art. 50 Abs. 1 DORA verhängt werden. Dabei werden Kriterien zum Sanktionsumfang gem. Art. 51 Abs. 2 DORA entsprechend berücksichtigt (z. B. Wesentlichkeit, Schwere und Dauer des Verstoßes, Finanzkraft der verantwortlichen natürlichen oder juristischen Person).

Hinsichtlich der Umsetzungsphase werden weitere technische Regulierungs- und Implementierungsstandards (Regulatory Technical Standards – RTS und Implementing Technical Standards – ITS) im Laufe des Jahres 2024 veröffentlicht.[3]

Einige Entwürfe zu den technischen Regulierungs- und Implementierungsstandards liegen bereits vor. Einige weitere werden noch veröffentlicht.

Dennoch ist es ratsam, die Veröffentlichung nicht abzuwarten, sondern zeitnah mit der Umsetzung zu beginnen, da Umfang und Komplexität nicht unterschätzt werden sollten. ▬

Weiterführende Infos zu DORA und unserem Leitfaden für Banken: https://www.dz-cp.de/informationssicherheit/dora

Katja Schlüter
Beauftragte Informationssicherheit & Datenschutz,
E-Mail: katja.schlueter@dz-cp.de

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

[1] https://www.bundesbank.de/de/aufgaben/bankenaufsicht/einzelaspekte/risikomanagement/bait-dora-598580 (abgerufen am 09.04.2024)

[2] BVR-Rundschreiben „Umsetzung der EU-Verordnung ‚Digitale operationale Resilienz im Finanzsektor (DORA)': Handlungsempfehlungen und Unterstützungsleistungen für 2024" vom 08.01.2024

[3] https://www.bafin.de/DE/Aufsicht/DORA/DORA_node.html (abgerufen am 09.04.2024)

Gemeinsam gegen Cyber-Risiken

Die aktuelle Bedrohungslage durch Cyberangriffe steigt unaufhaltsam. Fast schon täglich ist der Presse zu entnehmen, dass wieder ein Unternehmen gehackt wurde und dadurch über Wochen handlungsunfähig ist. Dabei ist die Finanzbranche ein attraktives Ziel.

In 2023 wurden pro Tag 250.000 neue Schadprogamm-Varianten identifiziert. Allein diese Zahl macht deutlich, dass es extrem aufwendig ist, einen Angriff zu identifizieren, geschweige denn, ihn abzuwehren. Es liegt auf der Hand, dass wir in der Genossenschaftlichen FinanzGruppe hier einen Vorteil haben: Das gemeinsame Vorgehen macht den Unterschied und sichert am Ende den Betrieb – trotz Notfall. Wie das in der DZ CompliancePartner GmbH aussieht, soll im Folgenden skizziert werden.

Was tun, wenn der Notfall eintritt

Spielen wir das doch mal durch: Was passiert, wenn der Notfall eintritt?

Der erste Impuls ist, sich zu fragen, welche Daten konkret betroffen sind und wo sie genau liegen. Welche Systeme und Prozesse hat es erwischt? Wird es Folgeschäden geben und welches Ausmaß wird am Ende der Datenschutzvorfall haben? Als betroffenes Unternehmen versucht man sich zunächst einen Überblick zu verschaffen, um den Schaden und die davon ausgehenden Risiken einschätzen zu können – um dann in einem zweiten Schritt entsprechende Gegenmaßnahmen zu starten.

Aber: Ist das dann überhaupt noch möglich? Was kann das Unternehmen leisten, wenn es nicht mehr auf seine IT zugreifen kann? Die Feststellung des Schadens erscheint fast als das geringste Problem. Die Frage ist dann schlicht: Wie können die vertraglichen, aber auch regulatorischen Pflichten in einer solchen Situation noch erfüllt werden? Glücklich ist, wer rechtzeitig Sicherheitsvorkehrungen getroffen hat.

Aus IT-Sicht steht der Ausfall einzelner Anwendungen oder des Rechenzentrums im Zentrum der Überlegungen. In der Regel greifen die Sicherheitsregelungen und Fall-Back-Lösungen des Business Continuity Management (BCM) – bei uns in der DZ CompliancePartner GmbH sind das u. a. Redundanzen im IT-Betrieb, vertragliche Vereinbarungen zu Wiederherstellzeiten, Notfallnummern, Notstrom und vieles mehr.

Und wenn es noch schlimmer kommt?

Was ist, wenn alle Verbindungen zu den IT-Systemen getrennt, alle Server, alle Leitungen, alle Rechner abgeschaltet werden müssen? Was ist dann zu tun?

Diese Fragen haben wir in der DZ CompliancePartner GmbHuns nicht nur gestellt, weil es in den MaRisk, den BAIT und auch in DORA gefordert ist. Wir haben sie uns gestellt, weil das die Realität bei angegriffenen Unternehmen wurde und wir dazu eine Antwort haben wollen und müssen: Wie können wir unsere Dienstleistung erfüllen, sollten wir einen „Black Screen Day“ haben.

Ein Blick ins Notfallhandbuch auf die zeitkritischen Prozesse ist dabei nur eingeschränkt hilfreich. Es geht darum, den Mitarbeiterinnen und Mitarbeitern der DZ CompliancePartner GmbH möglichst schnell wieder ihre Aufgabenerfüllung zu ermöglichen, damit wir letztlich unseren Verpflichtungen gegenüber unseren Kunden nachkommen können. Und das im schlimmsten Fall parallel und unabhängig von der ggf. notwendigen Neu-Inbetriebnahme der IT, die – und auch damit muss man rechnen – unter Umständen mehrere Wochen andauern kann.

In der DZ CompliancePartner GmbH setzen wir – zusätzlich zum BCM – auf eine dreifache Absicherung:

1. Alle Notfallnummern sind analog und zudem lokal auf Firmenhandys verfügbar, der Austausch untereinander ist möglich.
2. Die Zusammenarbeit mit der Atruvia ermöglicht, zeitkritische Prozesse in der Dienstleistungserbringung über den Bankenarbeitsplatz durchzuführen.
3. Ein Pool von Ersatz-Hardware ermöglicht den schnellen Austausch infizierter Geräte und damit eine zügige Weiterarbeit.

1. Verfügbarkeit von Notfallnummern

Die DZ CompliancePartner arbeitet nahezu papierlos und über ganz Deutschland verteilt. Aber an den Standorten steht selbstverständlich der papierhafte Notfallordner. Zugriff darauf haben in erster Linie die Mitarbeiterinnen und Mitarbeiter, die an den Standorten bzw. in deren Nähe arbeiten.

Für alle anderen Mitarbeiter haben wir eine Lösung geschaffen, die einen gesicherten Zugriff auf die wichtigsten Kontaktdaten und Informationen auf Firmengeräten – z. B. Handys – ermöglicht. Die Daten werden dabei lokal auf den Geräten zur Verfügung gestellt. Ein Prozess sichert die Aktualität der Daten und eine entsprechende firmeninterne Kommunikation samt Arbeitsanweisung

klärt die Mitwirkungspflichten der Mitarbeitenden – beginnend mit der aktiven Nutzung des Firmenhandys bis hin zu regelmäßigen Updates.

2. Verfügbarkeit eines dezentralen Zugriffs über Atruvia-Anwendungen

In der Zusammenarbeitsbeziehung zu unseren Kunden nutzen wir – wo immer es machbar ist – die Möglichkeiten, die Atruvia zur Verfügung stellt. Dadurch, dass sie ihre Anwendungen zum großen Teil Agentur-fähig bereitstellt, sind unsere Beauftragten immer auch als Mitarbeiter des jeweiligen Kunden eingerichtet: Das heißt, sie haben eine User-ID der jeweils betreuten Bank. Zudem können wir bereits seit längerem bei einigen Banken über den Bank-managed-Client einer Bank direkt auf die Anwendungen der Bank zugreifen.

Mit Blick auf das Notfallszenario sind diese modernen Technologien eine große Hilfe. Über den Weg der Atruvia-Anwendungen ist der Zugriff auf die benötigten Mandantendaten auch im Notfall gewährleistet. Damit sind wir in der Lage, den rechtlichen Verpflichtungen nachzukommen und insbesondere (zeit)kritische Prozesse zu bearbeiten.

Für die internen Prozesse im Rechnungswesen und in der Personalabteilung haben wir ebenfalls ein entsprechendes Notfallkonzept hinterlegt. So sind wir auch hier schnell in der Lage, den Mitarbeitenden Zugriffe auf die Buchhaltungsdaten, jenseits der „normalen" Infrastruktur, zur Verfügung zu stellen.

3. Verfügbarkeit von Ersatz-Hardware

Zu guter Letzt halten wir (Ersatz-)Hardware vor, die im „worst case" schnell ausgerollt werden kann. Das sind Notebooks, die schnell mit einem Image bespielt und an die Mitarbeiter ausgegeben werden können. Für diese „Grundbetankung" halten wir z. B. auch extra entsprechende USB-Sticks vor, um unabhängig vom Netzwerk zu sein.

Zusammengefasst haben wir Respekt vor dem Risiko eines Cyberangriffs. Selbst mit dem beschriebenen Plan in der Hinterhand werden die anfallenden Nacharbeiten und Umsetzungsschritte in den „Normalbetrieb" anspruchsvoll sein. Aber: Wir sehen uns gut aufgestellt mit unserem Notfallkonzept einerseits und der Zusammenarbeit mit Atruvia andererseits, über deren risikoorientierte und intelligente IT-Struktur der Betrieb auch im Notfall möglich ist.

Wenn Sie Fragen zu unserem Sicherheitskonzept haben, kommen Sie gerne jederzeit auf uns zu. ▬

Sandra Sitter
Bereichsleiterin IT & Projekte,
E-Mail: sandra.sitter@dz-cp.de

Produktinnovationen in der Finanzwirtschaft

Im Spannungsfeld zwischen betriebswirtschaftlichen Interessen und regulatorischen Vorgaben gehören in der Finanzwirtschaft auch Produktinnovationen, Digitalisierung und zunehmende Technisierung zum Alltag. Die zu beachtenden regulatorischen Anforderungen sind vielfältig und bleiben anspruchsvoll.

Der nachfolgende Artikel beleuchtet wichtige geldwäscherechtliche Vorgaben bezüglich der Einführung von neuen Produkten und Technologien. Unabhängig hiervon sind die Vorgaben der MaRisk AT 8.1 zum Neu-Produkt-Prozess als Rahmensetzung zu beachten.

Von Robo-Advisors in der Vermögensverwaltung über Kryptoanlagen bis hin zu vollständig digitalisierten Vertriebswegen durch Banking-Apps: Benutzerfreundliche Anwendungssoftware, innovative Anlagesegmente und mobile Vertriebskanäle prägen den Alltag in der Finanzbranche. Die moderne Bank ist mittlerweile ein Multikanal-Unternehmen. Sowohl Produktneuheiten als auch innovative Vertriebs- und Kommunikationswege sollen beim Kunden – oder besser: Nutzer – keine Wünsche offenlassen.

Dabei müssen Finanzinstitute sicherstellen, dass neue Produkte, Vertriebswege oder Technologien nicht die Anonymität von Geschäftsbeziehungen und Zahlungsströmen begünstigen und für Geldwäsche oder Terrorismusfinanzierung missbraucht werden können. Sie müssen sicherstellen, dass die internen Sicherungsmaßnahmen Schritt halten mit den neuen Entwicklungen und Technologien.

Dies gilt umso mehr, wenn Teile der Wertschöpfungskette auf externe Kooperationspartner übertragen oder interne Sicherungsmaßnahmen ausgelagert werden. Die BaFin hat bei ihrer jüngsten Fachtagung zur Geldwäscheverhinderung im Spätherbst 2023 genau hier Defizite aufgezeigt.

Verhinderung von Missbrauch

Der Gesetzgeber hat den GwG-Verpflichteten einen klaren rechtlichen Rahmen für den Umgang mit neuen Produkten und Technologien gegeben.

Gemäß § 6 Abs. 2 Nr. 4 GwG gehört zu den internen Sicherungsmaßnahmen *„[…] die Schaffung und Fortentwicklung geeigneter Maßnahmen zur Verhinderung des Missbrauchs von neuen Produkten und Technologien zur Begehung von Geldwäsche und von Terrorismusfinanzierung oder für Zwecke der Begünstigung der Anonymität von Geschäftsbeziehungen oder von Transaktionen“.*

Die BaFin hat diese gesetzliche Anforderung in Abschnitt 3.4 ihrer allgemeinen Auslegungs- und Anwendungshinweise (Stand 10/2021) um folgenden Satz ausgeweitet: *„Geeignet ist die Maßnahme, wenn mit ihr in Bezug auf die jeweilige Risikosituation der verfolgte Zweck erreicht werden kann.“*

Ungeachtet dieser gesetzlichen und regulatorischen Vorgaben zeigt die BaFin regelmäßig auch im Rahmen ihrer Öffentlichkeitsarbeit, welche Bedeutung sie der genauen risikoanalytischen Kenntnis neuer Produkte und/oder Geschäftsmodelle beimisst. So hat die Exekutivdirektorin der BaFin für den Bereich „Abwicklung und Geldwäscheprävention“, Birgit Rodolphe, auf der bereits erwähnten Fachtagung mehrfach und ausdrücklich betont, dass Verpflichtete neue Produkte und Geschäftsmodelle

kennen, verstehen und auch hinterfragen müssen, um die sich daraus ergebenden Geldwäscherisiken richtig einschätzen zu können.

In diesem Kontext stellen die nachfolgenden Überlegungen und Ausführungen einen Best-Practice-Ansatz dar. Sie sind nicht als abschließend zu verstehen.

Eingehende Überprüfung

Um eine angemessene Analyse neuer Produkte und Technologien vornehmen zu können, benötigt der Beauftragte Geldwäsche- und Betrugsprävention konkrete Informationen zum beabsichtigten Vorhaben. Art und Umfang dieser Informationen sind dabei vom geplanten Vorhaben abhängig.

Zu Beginn der Analyse sollten zumindest

- das Konzept mit einer entsprechenden Produktbeschreibung zum Projektvorhaben,
- der Vorstandsbeschluss zur Planung bzw. geplanten Umsetzung dieses Vorhabens sowie
- bereits durchgeführte Risikoeinschätzungen anderer Geschäftsbereiche des Instituts (z. B. der Internen Revision oder des Compliance-Beauftragten)

vorliegen.

In Abhängigkeit von Verlauf und eventuellen Zwischen-ergebnissen der weiteren Analyse sind unter Umständen noch weitere Informationen oder Unterlagen hinzuzuziehen.

Analysephase

Die Analyse des neuen Produktes bzw. der neuen Technologie sollte in Anlehnung an die jährliche Risikoanalyse i.S.d. § 4 GwG in Risikofelder aufgegliedert werden. Dabei kann es je nach Vorhaben durchaus vorkommen, dass einige dieser Risikofelder kaum oder gar nicht tangiert werden. Dennoch sollte auch dies entsprechend dokumentiert werden.

Als Orientierung kann die Aufteilung in nachfolgende Risikofelder genutzt werden:

- Produkte
- Transaktionen
- Länder
- Kunden
- Vertriebswege
- Organisatorische Veränderungen

Dabei sollte zu Beginn der Analysephase ein Mindestmaß an sog. Leitfragen abgearbeitet werden, aus denen sich dann, sofern einschlägig, Folgefragen und/oder der weitere Handlungsbedarf ergeben.

Auf Basis der nachstehenden Übersicht sollte das Projektvorhaben analysiert und bewertet werden.

Produkte

- Werden bestehende Produkte beeinflusst?
- Ermöglicht das neue Produkt die Anonymität der Kunden/Transaktionen?
- Decken die bestehenden Typologien alle Einfallstore des neuen Produktes ab?
- Sind weitere Sicherungsmaßnahmen erforderlich?
- Wird das Produkt in der Risikoanalyse ausreichend analysiert?
- Handelt es sich um ein klassisches Bankprodukt?
- Handelt es sich um ein standardisiertes Produkt der Bank oder der Bankengruppe?
- Ist ein ggfs. nicht reguliertes Fintech-Unternehmen eingebunden?

Transaktionen

- Wird die bestehende Transaktionsabwicklung beeinflusst?
- Können die Transaktionen über ein Monitoring-System überwacht werden? Sind ggf. spezielle Indizien hierfür notwendig?
- Erfolgt die Verbuchung als Sammeltransaktion?
- Sind die echten Auftraggeber der Zahlungen erkennbar?
- Sind Transaktionen nur für bereits identifizierte Kunden möglich?

Länder

- Sind Geschäftsbeziehungen/Transaktionen mit Bezug zu FATF-Risikoländern möglich?
- Sind Geschäftsbeziehungen/Transaktionen mit Bezug zu Drittstaaten mit hohem Risiko gemäß EU-Kommission möglich?
- Sind Geschäftsbeziehungen/Transaktionen mit Bezug zu sanktionierten Ländern möglich?
- Sind andere Länder verstärkt an dem Vorgang beteiligt?

Kunden

- Wird der bestehende Kundenannahmeprozess eingehalten?
- Ist die PEP-Prüfung sichergestellt?
- Ist die Embargo-Prüfung sichergestellt? (Hinweis: Diese Prüfung liegt in der Zuständigkeit der Verpflichteten.)
- Ist die Erfassung der Kundendaten im EDV-System der Bank sichergestellt?
- Ist die Erfüllung sämtlicher geldwäscherechtlicher Vorschriften sichergestellt?
  – Identifizierung
  – Feststellung wirtschaftlich Berechtigter
  – Überwachung
  – Aktualisierung der Kundendaten
- Spricht das Produkt bestimme Risikokundengruppen an (bspw. bargeldintensive Unternehmen)?
- Findet ein persönlicher Kundenkontakt statt?

Vertriebswege

- Werden bestehende Vertriebswege beeinflusst?
- Unterstützt der neue Vertriebsweg die Anonymität?

Organisatorische Veränderungen

- Findet die gesamte Wertschöpfungskette ausschließlich in der Bank statt?
- Gibt es Veränderungen von Zuständigkeiten?
- Sind Veränderungen des IKS notwendig?
- Sind zusätzliche Kontrollen des Geldwäschebeauftragten notwendig?

Bewertung und Maßnahmenplanung

Die im Rahmen der Analyse gewonnenen institutsspezifischen Erkenntnisse sind im Hinblick auf mögliche Maßnahmen zu bewerten. Das Ergebnis ist zu dokumentieren. Ergibt sich Handlungsbedarf im Hinblick auf die Ausgestaltung der institutsspezifischen Vorkehrungen zur Prävention von Geldwäsche, Terrorismusfinanzierung und strafbaren Handlungen, ist auch für die eingeleiteten und durchgeführten Maßnahmen eine entsprechende Dokumentation vorzunehmen.

Abhängig von dem Ergebnis der Gesamtbewertung sowie der Anpassung von bestehenden Sicherungsmaßnahmen, Kontrollmaßnahmen und der Ergänzung zusätzlicher Sicherungsmaßnahmen hat u.U. eine unterjährige Anpassung der Risikoanalyse zu erfolgen.

Fazit

Produktinnovationen und neue Technologien gehören für Finanzinstitute mittlerweile zum Alltagsgeschäft. Um ihren Missbrauch zur Begehung von Geldwäsche und Terrorismusfinanzierung und die Begünstigung der Anonymität von Geschäftsbeziehungen oder Transaktionen zu verhindern, müssen Finanzinstitute geeignete Maßnahmen schaffen und auch weiterentwickeln.

Die Analyse des neuen Produktes bzw. der neuen Technologie sollte analog der jährlichen Risikoanalyse in Risikofelder aufgegliedert werden. Die angemessene Dokumentation von Analyse, Bewertung und Maßnahmenplanung sollte dabei ebenso selbstverständlich sein wie die frühzeitige Einbindung des Geldwäschebeauftragten in den Gesamtprozess. ▬

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

Umsetzung der Marktmissbrauchsverordnung

Marktmissbrauch, Marktmanipulation, Insiderüberwachung, Insiderinformationen – viel Fachliches, doch was steckt dahinter? Im Folgenden werden der rechtliche Hintergrund der Marktmissbrauchsverordnung, die sich daraus ergebenden Aufgaben und Umsetzungsoptionen besprochen.

Die Marktmissbrauchsverordnung (MAR, Kapitel 2) regelt in den Artikeln 7, 12 und Artikel 15 die entscheidenden Kriterien und Definitionen rund um das Thema Marktmissbrauch.

Der Begriff **Marktmanipulation** (Art. 12) beinhaltet den Abschluss von Geschäften und die Erteilung von Aufträgen, die

- ein irreführendes Signal hinsichtlich des Angebots, der Nachfrage oder des Preises eines Finanzinstruments senden,
- mit dem Ziel, ein anormales Kursniveau zu erzeugen, Kurse zu manipulieren oder das Handelssystem selbst zu stören oder zu verzögern.

Als **Insiderinformationen** (Art. 7) werden dabei Informationen definiert, die

- nicht öffentlich bekannt sind,
- präzise sind und
- direkt oder indirekt einen oder mehrere Emittenten oder ein oder mehrere Finanzinstrumente betreffen.
- Weiterhin sind sie bei einer öffentlichen Bekanntmachung geeignet, den Kurs dieser Finanzinstrumente oder den Kurs damit verbundener derivativer Finanzinstrumente erheblich zu beeinflussen.

In Art. 15 MAR wird schließlich klargestellt: Marktmanipulation und der Versuch hierzu sind verboten. Es gilt also, diese zu verhindern.

Das Börsenjahr 2023 war aus Sicht der Anleger ein gutes Jahr: Der Weltaktienmarkt konnte einen Zuwachs von knapp 20 % verbuchen. Deutschland befindet sich dabei mit 19,77 % Renditeplus im Durchschnitt der weltweiten Industrieländer. Allein an den Handelsplätzen Börse Frankfurt und Xetra wurde im vergangenen Jahr ein Orderbuchumsatz von 1,2 Bio. Euro erzielt – ein Handelsvolumen, das es zu überwachen gilt.

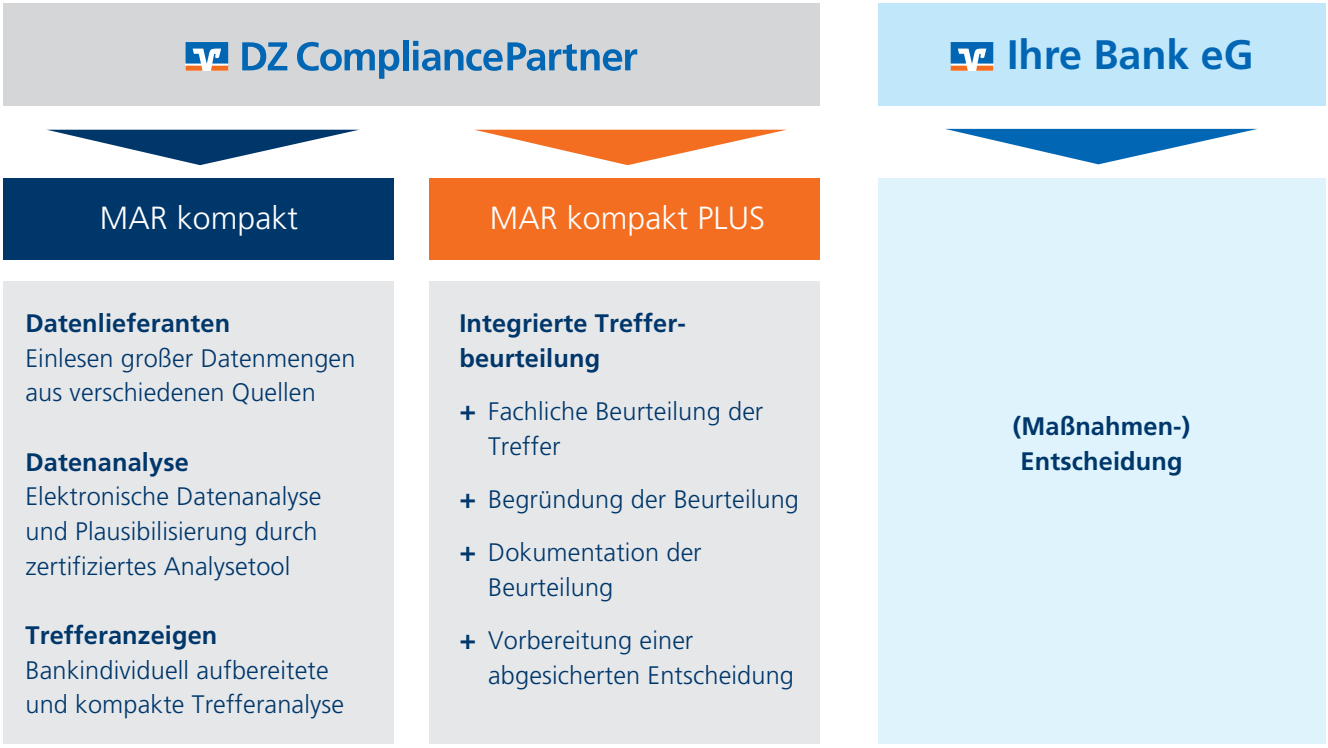
Doch was bedeutet dies nun für Wertpapierinstitute? Was ist zu tun, sollten tatsächlich Indizien für Marktmissbrauch vorliegen?

Die BaFin formuliert hierzu eine klare Vorgabe, ebenfalls basierend auf der MAR: „Betreiber von Märkten, Wertpapierfirmen, die einen Handelsplatz betreiben, und Personen, die gewerbsmäßig Geschäfte vermitteln oder ausführen, sind ab dem 2. Juli 2016 gem. Art. 16 Abs. 1 und 2 der MAR verpflichtet, Aufträge und Geschäfte, die Insidergeschäfte, Marktmanipulationen oder der Versuch hierzu sein könnten, unverzüglich der BaFin zu melden." (https://www.bafin.de/DE/DieBaFin/Service/MVPportal/Verdacht_MAR/verdacht_mar_node.html)

Trefferlisten – der erste Schritt zur Übersichtlichkeit

Eine Überwachung gemäß den Anforderungen der MAR ist anspruchsvoll und kann zumeist nur mit hohem Zeit- und Personaleinsatz bewältigt werden. Treffer-Tools können helfen, den Aufwand gering zu halten. Doch auch diese Tools müssen mit den richtigen Parametern konfigu-

ABB. 1 MIT MAR KOMPAKT PLUS LAGERN SIE DIE TREFFERBEURTEILUNG AUS



riert werden, damit sie ihre Wirkung entfalten können. Und das ist wiederum mit erheblichem Aufwand verbunden ist.

Bewährt hat sich dagegen der Bezug täglich generierter Trefferlisten wie MAR kompakt (siehe Abbildung): Sie dokumentieren auffällige bzw. potenziell verdächtige Geschäfte und dienen der systematischen Überwachung der Kunden-, Mitarbeiter- und eigenen Bankgeschäfte in Finanzinstrumenten und damit der Erkennung potenziell marktmanipulativer Handlungen.

Eine komfortable Ergänzung ist die Trefferbearbeitung und -beurteilung durch einen Dienstleister, wie beispielsweise mit MAR kompakt PLUS (siehe Abbildung). Dabei wird sowohl die Bearbeitung verdächtiger Geschäfte als auch deren Bewertung ausgelagert.
Im Folgenden beschreiben wir, wie wir die Marktmissbrauchsverordnung für Sie als Kunde umsetzen. Dabei greifen wir auf die Expertise von aktuell 25 Beauftragten und Analysten in 89 Wertpapier-Compliance-Mandaten zurück. Unsere Lösung ist überdies (in der Teilauslagerung) nach IDW-Standard PS 951 Typ 11 zertifiziert, so dass sie als Best Practice bzw. Orientierungsrahmen dienen kann.

Um eine gezielte Insiderüberwachung zu ermöglichen, greifen bei unserer Lösung verschiedene Instrumente ineinander. Zunächst werden die Ergebnisse aus Befragungen der Mitarbeiter zu möglichen Insidersituationen genutzt, um eine Watchlist zu erstellen und gezielt besondere Marktteilnehmer überwachen zu können. Zusätzlich besteht die Möglichkeit, diese Listen in Bezug auf Underlyings zu überwachen und diese an dynamische Großorderberechnungen, abhängig vom Handelsvolumen, zu

knüpfen. Dies ist die Basis für eine qualifizierte Trefferanzeige. Weiterführend werden die notwendigen Parameter, wie z. B. Zeitintervalle bei getätigten Orders, Schwellenwerte und Anzahl von getätigten bzw. in Auftrag gegebenen Geschäften, in die Überwachung integriert.

Das Ergebnis für Sie ist eine tägliche Zusammenfassung aller, möglicherweise kritischen, Geschäfte in den relevanten Bereichen: Marktmissbrauch, Großordergeschäfte, Überwachungslisten und Überwachung besonderer Marktteilnehmer sowie eine Übersicht der Mitarbeitergeschäfte und Transaktionen im Bereich Depot A Ihrer Bank durch unser Produkt MAR kompakt. Anhand dieser Listen können Sie Ihre Überwachungshandlungen umfangreich und ausreichend gemäß der MAR dokumentieren, da Sie durch uns alle für die Bearbeitung wichtigen Information kompakt zur Verfügung gestellt bekommen.

Trefferbearbeitung – Einordnung und Entscheidungsvorbereitung

Die Trefferbearbeitung sollte immer taggleich erfolgen, um die Vorgaben der MAR ordnungsgemäß umzusetzen. Die Treffer sind fachlich einzuordnen, wobei die Einordnung zu begründen und auch zu dokumentieren ist. Letztlich gilt es, eine Entscheidungsvorlage zur Maßnahmenergreifung zu erarbeiten und die Maßnahmen dann durchzuführen. Dieser Prozess der Prüfung, Einordnung und Dokumentation ist die nächste Möglichkeit zur Unterstützung seitens der DZ CompliancePartner GmbH, aufbauend auf dem Produkt MAR kompakt mit folgender Überleitung in unser weiterführendes Tool MAR kompakt PLUS. Wie auch im vorherigen Tool erfolgt eine gezielte Auswertung sämtlicher für die Marktmissbrauchsüberwachung notwendigen Daten, Pflege von Insiderlisten, Parametrisierung und Anpassung gemäß Ihren Vorgaben bis hin zur Auswertung und Einordnung der erstellten täglichen Treffer.

Sollte es in dieser täglichen Kontrolle zu einem begründeten Verdacht auf Marktmissbrauch bzw. zu einem Handlungsbedarf für Ihr Haus kommen, ist dem unmittelbar nachzugehen. Für uns heißt das, umgehend den Kontakt mit der vorher festgelegten Kontaktperson in der Bank aufzunehmen. Ergibt sich die Notwendigkeit einer Anzeige gegenüber der BaFin, so wird diese mittels Meldeformular bereits für den Upload im MVP-Portal für Sie vorbereitet. Darüber hinaus stehen wir beratend zur Seite.

Die Bewertung ist revisionssicher zu dokumentieren. Sie als Bank erhalten quartalsweise eine Zusammenfassung der geprüften Geschäfte, einschließlich der durchgeführten Verdachtsmeldungen und Verstöße gegen die Mitarbeiterleitsätze. Alle Systematiken und Kriterien zur Bewertung der Geschäfte müssen transparent und nachvollziehbar sein – das gilt für die hausinterne Umsetzung und selbstverständlich auch in der Teilauslagerung.

Fazit

Das Börsenjahr 2023 hat gezeigt, dass das Interesse und die Bereitschaft zum Handel an den Börsen auch in Zukunft stetig wachsen wird. Zu erwarten ist, dass damit auch weitere Ressourcen zur Verhinderung von Marktmissbrauch in den Instituten gebunden sein werden.

Damit ist auch klar, dass es sich frühzeitig mit der weiteren Entwicklung zu befassen gilt, um auf ausreichend Personalressourcen oder aber alternativ einen Umsetzungspartner für die Bewältigung der anstehenden Aufgaben zurückgreifen zu können. ▬

Fabian Baaß
Produktverantwortlicher MAR kompakt,
Beauftragter WpHG-Compliance,
E-Mail: fabian.baass@dz-cp.de

Nachhaltigkeit: Wo kommen wir her?

Mit der Veröffentlichung der 7. MaRisk-Novelle im Jahr 2023 formuliert die BaFin erstmals prüfungspflichtige Anforderungen an eine nachvollziehbare, konkrete und dokumentierte Auseinandersetzung mit Risiken im Zusammenhang mit **E**nvironmental (Umwelt), **S**ocial (Soziales) und **G**overnance (Aufsichtsstrukturen).

Es lohnt sich ein Blick zurück: Wo kommen wir eigentlich her? Die Europäische Union hat sich mit der Unterzeichnung des Pariser Klimaschutzabkommens im Jahr 2015 zur Verfolgung der darin vereinbarten Klimaziele verpflichtet. Zur Umsetzung der Klima- und Energiepolitik der EU sind laut Europäischer Investitionsbank weiterhin zusätzliche jährliche Investitionen von rund 180 Mrd. Euro bis 2030 notwendig.

Da die erforderlichen Mittel nicht ausschließlich von staatlichen Institutionen aufgebracht werden können, hat die EU-Kommission im März 2018 mit dem sog. Aktionsplan zur Finanzierung eines nachhaltigen Wachstums erste Maßnahmen initiiert, um zusätzlich private Investitionen über den Kapitalmarkt zu mobilisieren. Der Aktionsplan beinhaltete in seiner ursprünglichen Form folgende zehn Kernaspekte:

1. Einführung eines EU-Klassifikationssystems für nachhaltige Wirtschaftsaktivitäten (sog. EU-Taxonomie)
2. Entwicklung von Standards und Labels für „grüne" Finanzprodukte
3. Förderung von Investitionen in nachhaltige Projekte
4. Berücksichtigung von Nachhaltigkeit in der Finanzberatung
5. Entwicklung von Nachhaltigkeits-Benchmarks
6. Bessere Einbeziehung von Nachhaltigkeit in Ratings und Marktanalysen
7. Klarstellung der Pflichten von institutionellen Anlegern und Vermögensverwaltern (Offenlegungsverordnung)
8. Integration von Nachhaltigkeit in aufsichtsrechtliche Anforderungen
9. Stärkung der Vorschriften zur Offenlegung von Nachhaltigkeitsinformationen und zur Rechnungslegung
10. Förderung nachhaltiger Unternehmens-Governance und Bekämpfung des kurzfristigen Denkens an den Finanzmärkten

Im Dezember 2019 verabschiedete die EU mit ihrem sog. Green Deal einen Maßnahmenkatalog, wie die EU bis 2050 klimaneutral und ein von der Ressourcennutzung unabhängiges Wirtschaftswachstum erreicht werden soll.

Im selben Monat veröffentlichte die BaFin ihr Merkblatt zum Umgang mit Nachhaltigkeitsrisiken. Das Merkblatt sollte den Instituten als Orientierungshilfe dienen und enthält insbesondere unverbindliche Verfahrensweisen bzw. Good-Practice-Ansätze. Vor diesem Hintergrund erwartete die BaFin eine ganzheitliche Betrachtung der Nachhaltigkeitsrisiken von der Überprüfung und ggf. Anpassung der Geschäfts- und Risikostrategie über die Eingliederung in die Geschäftsorganisation bis hin zum eigentlichen Risikomanagement.

Mit Veröffentlichung der Neufassung der MaRisk (7. Novelle) am 29. Juni 2023 erstrecken sich insgesamt 47 Nennungen der ESG-Risiken vom Allgemeinen Teil

(AT) über den Besonderen Teil (BT) inkl. Orga (BTO) bis zum Risikomanagement (BTR) und stellen somit erstmalig prüfungspflichtige Anforderungen dar.

Aus den bereits dargestellten Kernaspekten des Aktionsplans der Europäischen Union zur Finanzierung eines nachhaltigen Wachstums möchten wir uns folgende Aspekte einmal näher ansehen:

1. EU-Taxonomie
2. Offenlegungsvorschriften
3. Berücksichtigung von Nachhaltigkeit in der Finanzberatung
4. Offenlegung von Nachhaltigkeitsinformationen (CSRD – Corporate Sustainability Reporting Directive)
5. ESG-Ratings und ESG-Labels für nachhaltige Finanzinstrumente

EU-Taxonomie

Die sog. Taxonomie stellt ein EU-weites Klassifikationssystem für ökologisch nachhaltige Wirtschaftsaktivitäten dar.

Durch die EU-Taxonomie werden für den Begriff der ökologischen Nachhaltigkeit klare Rahmenbedingungen geschaffen, da Wirtschaftsaktivitäten nun nach konkreten Regeln und Maßstäben (sog. Technische Bewertungskriterien (TSC)) bewertet werden. So wird objektiver erkennbar, ob diese Wirtschaftsaktivitäten gemäß EU-Taxonomie als ökologisch nachhaltig angesehen werden. Ziel ist es, den Markt für ein breiteres Spektrum potenzieller Teilnehmer zu öffnen, indem Unternehmen und Finanzinstrumente mit leicht vergleichbaren Nachhaltigkeitsnachweisen ausgestattet werden.

Am 18. Juni 2020 wurde die sog. Taxonomie-Verordnung (Verordnung (EU) 2020/852) vom EU-Parlament verabschiedet.

Zusammen mit dem sog. EU Green Bond Standard soll die EU-Taxonomie helfen, die von – von der EU-Kommission beauftragten – Technical Expert Group (kurz: TEG) identifizierten Hindernisse für die Entwicklung eines europäischen Markts für grüne Finanzprodukte zu überwinden und die für die Bekämpfung des Klimawandels und die Anpassung an dessen Folgen erforderlichen finanziellen Mittel zu generieren. Durch die bis dato fehlende einheitliche Definition von „grünen“ Projekten bestand ein Interpretationsspielraum, wie nachhaltig „grüne“ Projekte sein müssen. Die Taxonomie soll dieses Risiko wie auch die Gefahr des Greenwashings (Unternehmen geben vor, nachhaltiger zu sein, als sie in Wirklichkeit sind) verringern.

Grundlegend dafür ist der Aufbau der EU-Taxonomie. So stehen an vorderster Stelle sechs Umweltziele, nach der sich die Klassifizierung von nachhaltigen Wirtschaftsaktivitäten richtet:

1. Klimaschutz
2. Anpassung an den Klimawandel
3. Nachhaltiger Einsatz und Gebrauch von Wasser oder Meeresressourcen
4. Übergang zu einer Kreislaufwirtschaft
5. Vorbeugung oder Kontrolle von Umweltverschmutzung
6. Schutz und Wiederherstellung von Biodiversität und Ökosystemen

Die sechs EU-Umweltziele sind abstrakt formuliert und werden erst durch die jeweiligen Kriterien für jedes dieser Umweltziele in separaten Verordnungen konkretisiert.

EU-Offenlegungsverordnung

Die EU-Offenlegungsverordnung (Sustainable Finance Disclosure Regulations, SFDR) schreibt vor, dass Finanzunternehmen ihren Kunden offenlegen müssen, inwieweit Nachhaltigkeitsfaktoren in den Entscheidungsprozess für ihre Finanzprodukte einbezogen worden sind und welche wesentlichen negativen Nachhaltigkeitsauswirkungen ihre Finanzprodukte haben.

Die SFDR wurde bereits im Jahr 2019 verabschiedet und ihre Veröffentlichungspflichten wurden schrittweise in den Jahren 2021 bis 2023 eingeführt. Die meisten gemäß SFDR offenzulegenden Informationen müssen bereits ab dem 30. März 2021 veröffentlicht werden. Dies betrifft vor allem die Pflichtangaben auf der Website oder auch Angaben in den sog. vorvertraglichen Informationen zu Finanzprodukten.

Ziel der Verordnung ist die Harmonisierung der Transparenzanforderungen in Bezug auf Nachhaltigkeitsaspekte im Anlageentscheidungs-, Anlageberatungs- und Versicherungsberatungsprozess von Finanzmarktteilnehmern und Finanzberatern.

Die SFDR richtet sich an Finanzunternehmen in der EU, die ESG-Portfolios managen und nachhaltige Finanzprodukte anbieten. Sie betrifft insbesondere Entwickler und Anbieter von Finanzprodukten sowie Finanzberater wie Banken, Vermögensverwalter, institutionelle Anleger oder Versicherungen. Zu den Finanzprodukten im Anwendungsbereich gehören u. a. Investment- und Anlagefonds, private und betriebliche Altersvorsorge, Versicherungsanlageprodukte sowie Versicherungs- und Anlageberatung.

Die SFDR schreibt vor, dass Finanzunternehmen ihren Kunden offenlegen müssen, inwieweit sie Nachhaltigkeitsfaktoren in den Entscheidungsprozess für ihre Finanzprodukte einbeziehen und welche wesentlichen negativen Nachhaltigkeitsauswirkungen ihre Finanzprodukte haben. Dies gilt insbesondere für ESG-Finanzprodukte, die entweder mit ESG-Eigenschaften werben (sog. Artikel-8-Produkte) oder sich selbst als „nachhaltige Geldanlage" bezeichnen (Artikel-9-Produkte).

Die SFDR-Vorschriften gelten für Finanzmarktteilnehmer und Finanzberater in Mitgliedsstaaten der Europäischen Union und für jedes Finanzprodukt, das unter die EU-Offenlegungsverordnung (SFDR-Vorschriften) fällt. Dabei gibt es drei verschiedene Kategorien, die nach dem jeweils anwendbaren Teil der SFDR-Verordnung benannt sind:

- Artikel 6: Produkte nach Artikel 6 sind solche, die nur Nachhaltigkeitsrisiken bewerten und berücksichtigen.
- Artikel 8: Produkte nach Artikel 8 sind solche, die ökologische und soziale Merkmale fördern und ESG-Kriterien als Teil des Investmentprozesses berücksichtigen.
- Artikel 9: Produkte im Sinne von Artikel 9 verfolgen ein Nachhaltigkeitsziel und streben daher neben finanziellen Renditezielen auch spezifische Nachhaltigkeitsergebnisse an. Sie zielen darauf ab, negative Auswirkungen auf die Umwelt, die Gesellschaft und die Arbeitnehmer so gering wie möglich zu halten.

Zusätzlich zu den bisherigen Pflichten von Finanzmarktteilnehmern und Beratern müssen diese neben allen relevanten finanziellen Risiken auch alle relevanten Nachhaltigkeitsrisiken, die den Ertrag einer Investition oder Beratung erheblich negativ beeinflussen können, in ihren Prozessen berücksichtigen, fortlaufend bewerten und in den vorvertraglichen Informationen erläutern.

Berücksichtigung von Nachhaltigkeit in der Finanzberatung

Der im April 2021 veröffentlichte Entwurf der Delegierten Verordnung (EU) 2021/1253 zur Änderung der Delegierten Richtlinie (EU) 2017/565 legt fest, ob Wertpapierfirmen eine verpflichtende Bewertung der Nachhaltigkeitspräferenzen ihrer Kunden und potenziellen Kunden durchführen müssen. Die Bewertung soll Aufschluss darüber geben, ob und welche ökologisch, sozial und in Hinblick auf die Unternehmensführung nachhaltigen Anlagemöglichkeiten für die Kunden in Frage kommen. Ab dem 2. August 2022 müssen Unternehmen, die in den Anwendungsbereich der EU-MiFID II fallen, die Nachhaltigkeitspräferenzen ihrer Kunden im Rahmen von Eignungsprüfungen ermitteln.

Die Änderungsrichtlinie zur Delegierten Verordnung (EU) 2017/565 sieht vor, dass im Rahmen einer Investitionsberatung oder Portfoliomanagemententscheidung bei der Durchführung der Geeignetheitsprüfung auch Nachhaltigkeitspräferenzen abzufragen bzw. zu berücksichtigen sind.

Offenlegung von Nachhaltigkeitsinformationen (CSRD – Corporate Sustainability Reporting Directive)

Die Corporate Sustainability Reporting Directive ist die jüngste Gesetzgebung zur Berichterstattung nichtfinanzieller Informationen.

Die CSRD-Richtlinie trat am 1. Januar 2023 in Kraft und löst die bisherige Non Financial Reporting Directive (NFRD) ab. Die CSRD-Richtlinie beinhaltet einen jährlichen Bericht zu Nachhaltigkeitsthemen, d.h. zu Umwelt-, Sozial- und Menschenrechtsfragen sowie zu Governance-Faktoren.

Die neue CSRD-Pflicht betrifft deutlich mehr Unternehmen als die NFRD-Pflicht. Zunächst sind nur Großunternehmen und große Unternehmen von öffentlichem Interesse (Banken, Versicherungen, börsennotierte Unternehmen) berichtspflichtig, in den nächsten Jahren werden jedoch weitere Unternehmen betroffen sein. So müssen ab 2026 auch börsennotierte KMU oder Kleinstunternehmen sowie Tochtergesellschaften und Zweigniederlassungen (Umsatz > 40 Mio. Euro) von Nicht-EU-Unternehmen mit signifikanter Präsenz in der EU (Umsatz > 150 Mio. Euro in der EU) berichten. Ab 2027 generell alle Unternehmen, die zwei der drei folgenden Merkmale erfüllen:

- Bilanzsumme > 20 Mio. Euro
- Umsatz > 40 Mio. Euro
- Anzahl der Mitarbeiter > 250

Eine grundlegende Neuerung der CSRD ist die Einführung der sog. doppelten Wesentlichkeit (Double Materiality). Im Rahmen von ESG bedeutet die doppelte Wesentlichkeit, dass nicht nur der Einfluss von Umweltfaktoren auf das Unternehmen betrachtet wird, sondern auch die Auswirkungen des Unternehmens auf die Umwelt. Infolge dieses Ansatzes soll das Bewusstsein gestärkt werden, dass jeder Akteur Einfluss auf den Klimawandel hat und somit sein Handeln und seine Geschäftsbeziehungen entsprechend bewerten muss.

Zukünftig sollen Nachhaltigkeitsinformationen im Lagebericht anhand einheitlicher EU-Berichtsstandards offengelegt werden. Hierzu hat die European Financial Reporting Advisory Group (EFRAG) im Auftrag der EU-Kommission einen finalen Entwurf für sektorübergreifende Standards veröffentlicht.

Überblick über die anstehenden Verpflichtungen der nächsten Jahre:

- **30. Juni 2024** – Zweite FMP-PAI (Principal Adverse Impact)-Erklärung gemäß der delegierten SFDR-Verordnung.
- **1. Januar 2025** – CSRD gilt für alle großen Unternehmen, die nicht unter die NFRD fallen (Bericht 2026 für GJ 2025).
- **1. Januar 2026** – Die CSRD gilt für kapitalmarktorientierte KMU und kleine und nicht komplexe Kreditinstitute im Sinne von Art. 4 Abs. 1 Nr. 145 CRR Finanzinstitute auf fakultativer Basis. (Bericht 2027 für GJ 2026)
  Hinweis: Um als ein kleines und nicht komplexes Institut (Small Non-Complex Institute – SNCI) eingestuft zu werden, müssen die Kriterien des Art. 4 Abs. 1 Nr. 145 CRR kumulativ erfüllt sein. U.a. darf die Bilanzsumme im Durchschnitt der letzten vier Jahre nicht über 5 Mrd. Euro liegen, das Institut darf keinen oder nur vereinfachten Anforderungen in Bezug auf die Sanierungs- und Abwicklungsplanung unterliegen und es dürfen andere aufsichtsrechtliche Schwellenwerte für die Geschäftstätigkeit nicht überschritten werden (z. B. Derivategeschäfte).
- **1. Januar 2028** – CSRD gilt für Drittlandunternehmen und börsennotierte KMU sowie kleine Finanzinstitute.

ESG-Ratings und -Labels für nachhaltige Finanzinstrumente

Aufgrund der Bedeutung des Themas Nachhaltigkeit sowie der Regulatorik beziehen professionelle Anleger Nachhaltigkeitskriterien in ihre Entscheidungen ein. Dazu benötigen sie Informationen. Diese Informationen finden sich in ESG-Ratings oder ESG-Labels.

ESG-Ratings

ESG-Ratings sind Produkte, die bei der ESG-Bewertung eingesetzt werden, sie sollen Investoren Transparenz darüber geben, wie verantwortungsvoll Unternehmen in ESG-Fragen handeln. ESG-Ratings liefern einen aggregierten Überblick über Nachhaltigkeitsfaktoren.

ESG-Ratinganbieter nutzen auch nicht finanzielle Daten. Zu den Kunden von ESG-Ratings gehören häufig institutionelle Investoren, Banken und Unternehmen. Anbieter von ESG-Ratings sind u. a.:

- ISS ESG
- MSCI
- Morningstar

Zur Bewertung werden Ratingskalen genutzt. Diese gehen von „AAA“ zu „CCC“ (MSCI) oder von „A+“ zu „D-“ (ISS ESG). Der Ratingprozess kann ganz unterschiedlich ausgestaltet sein. Von der Outside-in- zur Inside-out-Methode, über flexible oder fixe Kriterien bis hin zu einer sektorbezogenen Bewertung, die auch das Geschäftsmodell des jeweiligen Unternehmens berücksichtigt.

Nutzer von ESG-Ratings sollten sich darüber bewusst sein, dass es unterschiedliche Ratingmethoden gibt, und wissen, welche Ratingagentur welchen Ratingansatz verwendet. Je nach gewählter Methode oder Ansatz können unterschiedliche ESG-Rating-Ergebnisse entstehen.

ESG-Labels

Wir alle kennen bei Lebensmitteln ganz unterschiedliche Bio-Siegel, sei es das EU-Bio-Logo, Bioland, Demeter oder MSC, um nur einige zu nennen. Genauso vielfältig ist die Label-Landschaft bei nachhaltigen Finanzprodukten, wobei unter einem Label ein „Gütesiegel“ verstanden wird. Ohne Anspruch auf Vollständigkeit seien nur folgende Labels für Finanzprodukte genannt:

- FNG-Siegel
- Ecoreporter-Siegel
- Österreichisches Umweltzeichen
- Nordic Swan Ecolabel für nachhaltige Investmentfonds

Ziel der ESG-Labels ist es, vorwiegend nicht professionellen Anlegern zu helfen, Finanzprodukte zu finden, die Nachhaltigkeitskriterien erfüllen.

Was man bei den unterschiedlichen ESG-Labels wissen muss: Sie werden von unterschiedlichen Akteuren vergeben und haben unterschiedliche Schwerpunkte. Staaten, Verbände oder Firmen vergeben Nachhaltigkeitssiegel. Jeder Akteur legt dabei eigene Kriterien fest, nach denen er die Siegel vergibt.

In der Regel sind es Ausschlusskriterien, z.B. keine Investitionen in Atomkraft, Kohle oder Waffen bzw. Tabak, in Kombination mit Positivkriterien, z.B. Investitionen in Umwelttechniken, erneuerbare Energien oder nachhaltige Produkte.

Trotz der unterschiedlichen Konzepte von Labels und Ratings macht es vor dem Hintergrund der ESG-Risiken und insbesondere der Klimarisiken gleichwohl Sinn, nachhaltige Finanzprodukte zu konzipieren bzw. zu erwerben. ESG-Ratings und/oder -Labels sind ein guter Ansatz, um sich diesbezüglich zu informieren und nachhaltige Finanzprodukte zu finden.

Integration von Klimarisiken am Beispiel der 7. MaRisk-Novelle

Mit der 7. MaRisk-Novelle vom Juni 2023 hat die BaFin die – ehemals freiwilligen – Good-Practice-Ansätze aus dem Merkblatt zum Umgang mit Nachhaltigkeitsrisiken aus dem Jahr 2019 sowie ESG-Faktoren aus den Leitlinien für die Kreditvergabe und Überwachung nun in formales Aufsichtsrecht überführt. Damit werden die ESG-Risiken, insbesondere Umweltrisiken, prominent fokussiert und stellen prüfungsrelevante Anforderungen auf. Die ESG-Risiken betreffen alle Bereiche einer Bank, insbesondere aber das Risikomanagement, AT 2.2 und AT 4.1 MaRisk.

Die Aufsicht bringt in den MaRisk und dem Begleitschreiben unmissverständlich zum Ausdruck, dass sie Nachhaltigkeitsrisiken als strategische Befassung sieht und die Risiken insbesondere verortet in

- dem Geschäftsmodell und
- dem Risikoprofil (Mess-, Steuerungs- und Risikominderungsinstrumente)

der Institute, wobei diese Risiken sich als physische Risiken und Transitionsrisiken kurz-, mittel- und langfristig realisieren können.

Vielfach wurde übersehen, dass die Aufsicht der Finanzindustrie auch Hilfsmittel zum Management der Klimarisiken an die Hand gegeben hat, insbesondere was die Verwendung von Szenarien betrifft. Explizit werden beispielsweise die physischen und transitorischen Szenarien

- des Networks of Central Banks and Supervisors for Greening the Financial System (NGFS),
- der EBA,
- der Internationalen Energieagentur,
- des Potsdam-Instituts für Klimafolgenforschung oder des
- Helmholtz-Zentrums

einschließlich der Quellen genannt. Das Merkblatt zum Umgang mit Nachhaltigkeitsrisiken ist durch die Integration von ESG-Risiken in die MaRisk nicht obsolet geworden, es kann weiterhin als Auslegungshilfe verwendet werden. Dementsprechend kann auch der von uns konzipierte Quick-Check Nachhaltigkeitsrisiken weiterverwendet werden.

Zusammenfassung/Ausblick

Die Rahmenbedingungen bzw. regulatorischen Vorgaben zur Erreichung der Nachhaltigkeitsziele bedeuten zunächst einmal – zusätzliche – Arbeit für die Banken. Diese Arbeit ist allerdings notwendig und sinnvoll, um insbesondere den weltweiten klimatischen Veränderungen zu begegnen. Gleichzeitig geben die Rahmenbedingungen den Banken auch Hilfsmittel zur Hand, wie die Vorgaben umzusetzen sind. Das Thema Nachhaltigkeit wird die Industrie einschließlich der Finanzindustrie zukünftig auf Dauer beschäftigen. ▬

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

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

Schufa-Score – kein Entscheidungskriterium für Kredite?

Der Schufa-Score wurde vom EuGH als eine automatisierte Entscheidung im Sinne des Art. 22 Abs. 1 DSGVO definiert. Kreditinstitute dürfen grundsätzlich das Schufa-Scoring nicht verwenden, sofern der Score eine „maßgebliche“ Rolle zur Entscheidungsfindung beiträgt.

Gem. Art. 15 Abs. 1 lit. h DSGVO haben Betroffene ein Auskunftsrecht gegenüber dem Verantwortlichen im Sinne der DSGVO über eine „aussagekräftige Information über die involvierte Logik sowie die Tragweite und Auswirkungen einer derartigen Verarbeitung für den Betroffenen“.

Es war einmal

Täglich bewertet sie die Kreditwürdigkeit von Betroffenen. Je höher der sog. Schufa-Score ist, desto bessere Kreditkonditionen können sich die Betroffenen erhoffen und umso höher stehen die Chancen auf eine Kreditzusage. Umgekehrt kann ein schlechter Score maßgeblich für eine Kreditabsage sein. Die Betroffene forderte bei der Schufa, fehlerhafte Eintragungen zu löschen und die Berechnungsdaten offenzulegen. Aufgrund des Geschäftsgeheimnisses der Schufa konnten der Betroffenen nur eingeschränkte Informationen mitgeteilt werden, weshalb sie sich – jedoch erfolglos – an den Hessischen Datenschutzbeauftragten wendete.[1] Daraufhin klagte sie vor dem Verwaltungsgericht Wiesbaden.

Das Verwaltungsgericht Wiesbaden setzte das Verfahren aus und legte zwei Fragen zu den Vorabentscheidungen dem EuGH vor, die vielleicht schon überfällig waren. Die erste, und im vorliegenden Fall entscheidende, Frage lautete, ob es sich beim Schufa-Score um eine automatisierte Entscheidung im Sinne des Art. 22 Abs. 1 DSGVO handelt. Das Verwaltungsgericht Wiesbaden äußerte mit dieser Frage somit seine Bedenken zur Europarechtskonformität. Das EuGH bejahte die Frage am 7. Dezember 2023 (Rechtssache C-634/21).

Das Verbot der automatisierten Entscheidung gem. Art. 22 Abs. 1 DSGVO

Grundsätzlich bietet die Datenschutz-Grundverordnung dem Verantwortlichen die Möglichkeit, personenbezogene Daten zu verarbeiten. Im Falle des Schufa-Scores greift dieser Ansatz nur bedingt. Danach dürfe der Verantwortliche gem. Art. 22 Abs. 1 DSGVO den Betroffenen nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterwerfen, die ihm gegenüber eine rechtliche Wirkung entfaltet oder ihn in ähnlicher Weise erheblich beeinträchtigt. Die Schufa als Wirtschaftsauskunftei übermittelt Informationen zur Kreditwürdigkeit an ihre Vertragspartner. Dabei handelt es sich u.a. um relevante Merkmale, auf deren Grundlage ein mathematisch-statistisches Verfahren verwendet wird, um den sog. Score-Wert zu ermitteln. Dieser bewertet die zukünftige Wahrscheinlichkeit eines möglichen Zahlungsausfalles des Betroffenen.[2]

Diese Merkmale umfassen Informationen zu vertragsgemäßem Verhalten z. B. bei Girokonten, Kreditkarten, Leasingverträgen, aber auch nicht vertragsgemäßem Verhalten wie bei Zahlungsrückständen und -ausfällen.[3]

Nach dem Urteil des obersten Gerichts der EU verstößt der Schufa-Score nicht gegen die Datenschutz-Grundverordnung, wenn der Vertragspartner der Schufa dem Score keine „maßgebliche" Rolle bei der Entscheidung über eine Zusage gegenüber dem Betroffenen gebe. Eine Verarbeitung nach Art. 22 DSGVO liegt somit unter drei Voraussetzungen vor:

1. wenn eine Entscheidung auf einer automatisierten Verarbeitung beruht
2. und gegenüber der betroffenen Person rechtliche Wirkung entfaltet
3. oder sie in ähnlicher Weise erheblich beeinträchtigt.[4]

Die Schufa entscheidet auf Grundlage des berechneten Wertes zwar nicht über die Zu- oder Absage eines Kredits. Dies ist aber nicht entscheidend für den Anwendungsbereich des Art. 22 DSGVO. Die Entscheidung kann auch im Zusammenwirken mehrerer Stellen erfolgen und wäre somit nicht nur dem Kreditinstitut zuzurechnen.[5] Andernfalls wäre dieser Tatbestand leicht zu umgehen. Somit kann die auf dem Score-Wert beruhende Entscheidung durch mehrere Handlungen von Akteuren ausgeführt werden. Die Entscheidung muss lediglich „maßgeblich" sein. Wirft man einen Blick in die DSGVO, findet man keine Legaldefinition zur Maßgeblichkeit. Fragt man den Juristen, erhält man eine „Es kommt darauf an"-Antwort. Zwischenfazit hier: Wir haben etwas Argumentationsspielraum, in welchen Fällen eine Maßgeblichkeit in Betracht käme. Das Gute an dem EuGH-Urteil ist: Es lässt uns nicht im Dschungel der Argumentationskünste stehen, sondern verweist auf die Gerichte (Verwaltungsgericht Wiesbaden), welche den Begriff der „Maßgeblichkeit" konkretisieren sollen.

Die Ausnahme von der Regel

Nun gibt es in der Juristerei von der Regel auch immer eine Ausnahme. Im vorliegenden Fall sogar mehrere. Der EuGH, aber auch der Gesetzeswortlaut des Art. 22 DSGVO sagen, dass der Score dennoch genutzt werden kann, wenn dies „maßgeblich" zur Entscheidung beitrage, falls eine der folgenden Ausnahmen vorliege:

1. wenn es für den Abschluss oder die Erfüllung eines Vertrags zwischen dem Vertragspartner, der Schufa und dem Betroffenen erforderlich sei;
2. wenn der nationale Gesetzgeber, in unserem Fall der deutsche Gesetzgeber, eine Rechtsvorschrift geschaffen habe, die zulässig ist und angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen des Betroffenen enthält.
3. wenn der Betroffene ausdrücklich eingewilligt habe.

Die in Nr. 1 genannte Ausnahme wird bei der Nutzung des Scores bei Kreditanfragen nicht möglich sein, da es „mildere" Mittel gibt, um die Zahlungsliquidität eines Betroffenen bewerten zu können. Eine ausdrückliche Einwilligung nach Nr. 3 wird auch scheitern, da nicht gewährleistet werden kann, dass diese Einwilligung gegenüber dem Kreditgeber freiwillig erteilt wurde. Somit bleibt für den Kreditgeber in Deutschland nur der Rückgriff auf das Bundesdatenschutzgesetz (BDSG).

Derzeit ist im § 31 BDSG definiert, dass die Verwendung eines Wahrscheinlichkeitswerts über ein bestimmtes zukünftiges Verhalten einer natürlichen Person zum Zweck der Entscheidung, d.h. des Score-Werts, zulässig sein kann, falls die Voraussetzungen gemäß der Norm vorliegen. Nun verwendet nicht die Schufa den erstellten Wert, sondern der Kreditgeber. Diese Rechtslücke möchte der deutsche Gesetzgeber füllen und hat einen Gesetzesentwurf vorgelegt.

In dem geplanten § 37a BDSG (Entwurf von Februar 2024) soll das Verbot, einer automatisierten Entscheidung gem. Art. 22 DSGVO unterworfen zu werden, nicht eintreten, wenn Wahrscheinlichkeitswerte einer natürlichen

Person erstellt oder verwendet werden. Diese Ausnahme tritt ein, wenn der erstellte oder verwendete Wert über

1. ein bestimmtes zukünftiges Verhalten der Person zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dieser Person oder
2. ihre Zahlungsfähig- und willigkeit durch Auskunfteien und unter Einbeziehung von Informationen über Forderungen bewertet.[6]

Sollte der geplante § 37a BDSG n.F. in Kraft treten, würde die Problematik der Nutzung des Schufa-Scores gelöst werden. Weiterhin ist auf eine Entscheidung des Verwaltungsgerichts Wiesbaden zu warten, wie dieses den Begriff der „Maßgeblichkeit“ im Rahmen des Art. 22 Abs. 1 DSGVO definiert, damit nicht nur Kreditinstitute, sondern auch weitere Vertragspartner der Schufa und Betroffene eine Orientierungshilfe haben, ihre Rechte und Pflichten umzusetzen.

Najat Lissner
Beauftragte Informationssicherheit und Datenschutz,
E-Mail: najat.lissner@dz-cp.de

To-dos für Sie als Kreditgeber

Unabhängig vom Inkrafttreten des § 37a BDSG sollten Sie zusätzliche Maßnahmen ergreifen, um Risiken von Datenschutzverstößen durch die Verwendung des Schufa-Scores zu vermeiden.

- Prüfen Sie, ob die von Ihnen getroffenen Entscheidungen, gestützt durch den Schufa-Score, „maßgeblich“ für die Kreditvergabe sind bzw. waren. Konsultieren Sie hierfür Ihren Datenschutzbeauftragten, um eine Risikobewertung durchzuführen.
- Ergreifen Sie zusätzliche Maßnahmen zur Wahrung von Betroffenenrechten.
- Sie sollten auf das Bestehen einer automatisierten Entscheidung sowie auf die Auswirkungen hinweisen, um den Transparenzpflichten gegenüber den Betroffenen nachzukommen, Art. 13 Abs. 2 lit. f; Art. 14 Abs. 2 lit. g; Art. 15 Abs. 1 lit. h DSGVO.
- Überprüfen Sie Ihre Prozesse zur Kreditvergabe und beziehen Sie dabei Ihren Datenschutzbeauftragten ein.

Bis zum Inkrafttreten des § 37a BDSG wird eine Rechtsgrundlage benötigt. Dies kann nach einer Interessensabwägung auf Art. 6 Abs. 1 lit. f DSGVO erfolgen. Beziehen Sie hierbei auch Ihren Datenschutzbeauftragten rechtzeitig ein. Ggf. werden sich weitere Anforderungen und zusätzliche Maßnahmen zur Umsetzung aus § 37a BDSG ergeben.

Ein vorbereitendes „Profiling“ kann ebenfalls eine Entscheidung im Sinne des Art. 22 Abs. 1 DSGVO bedeuten, sofern diese Verarbeitung „maßgebliche“ Entscheidungswirkung besitzt.[7] ▬

[1+2] EuGH, NZA 2024, 45.

[3] https://www.schufa.de/scoring-daten/scoring.schufa/index.jsp (abgerufen am 27.03.2024)

[4] https://curia.europa.eu/juris/document/document.jsf?text=&docid=280426&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=3551922 (abgerufen am 27.03.2024)

[5] Taeger, BKR 2024, 41, 46.

[6] https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/VII4/aendg-bdsg.pdf?__blob=publicationFile&v=3, (abgerufen am 27.03.2024)

[7] https://curia.europa.eu/juris/document/document.jsf?text=&docid=280426&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=3551922, (abgerufen am 27.03.2024)

Zukunftsfähigkeit bescheinigt: Unser Compliance Management System „CompAkt“ und „CMP“

IT-Unterstützung ist heute die Grundlage einer effizienten Dienstleistungskompetenz. Dies gilt auch für die DZ CompliancePartner GmbH. Da es am Markt keine geeignete Software für Compliance-Dienstleistungen eines Mehrmandantendienstleisters gab und gibt, hat die DZ CompliancePartner GmbH eine eigene Compliance Management-Anwendung entwickelt. Im Zentrum der Entwicklung standen Sicherheit, Performance, Kosten und größtmögliche Prozessunterstützung. Wissensmanagement war für uns dabei besonders wichtig: Kopfwissen wird in Systemwissen überführt. So können wir Lernkurveneffekte aus dem Wissens- und Erfahrungsschatz unserer Mitarbeiterinnen und Mitarbeiter erzielen und Fluktuationsrisiken weitestgehend ausschließen.

Die Veränderungsprozesse in der IT-Landschaft der Gruppe (z. B. MS 365, Mendix) haben wir zum Anlass genommen, die Zukunftsfähigkeit unserer Systeme erneut dezidiert analysieren und bewerten zu lassen. Zur Sicherstellung eines „unverbauten“ Blicks haben wir ein namhaftes Beratungsunternehmen mit dieser Analyse und Beurteilung beauftragt. Nach einem Review der Systeme hat das Beratungsunternehmen in einem mehrwöchigen Projekt die vorhandenen IT-Systeme und -Anwendungen nach zuvor definierten Kriterien (z. B. Betriebssicherheit, Personal, Kosten, Innovation, Weiterentwicklung) bewertet. In diesem Review werden unsere Geschäfts- und IT-Strategie und die sich in Ableitung daraus ergebenden Anforderungen an die IT-Infrastruktur berücksichtigt.

Das Ergebnis ist klar und ohne Einschränkungen ausgefallen:

- Die Zukunftsfähigkeit der Anwendung ist unter Berücksichtigung der vom Softwarelieferanten veröffentlichten Roadmap für die nächsten ca. 5–10 Jahre gegeben.
- Eine Untersuchung der Qualitätsmerkmale wie z. B. Wartung, Sicherheit, Verlässlichkeit hat keine gravierenden Mängel erkennen lassen.
- Die Nutzung der Plattform bringt auch in Zukunft in der Anwendungsentwicklung Vorteile, da viele, teilweise kritische Funktionalitäten (z. B. Security, Replikation) inkludiert sind und einen hohen Reifegrad aufweisen.
- Die Software unterstützt alle bisher umgesetzten und die für die Zukunft prognostizierten Anwendungsfälle der DZ CompliancePartner.
- Eine Betrachtung der Roadmap des Softwarelieferanten legt den Schluss nahe, dass es möglich sein wird, die neuen Anforderungen und Möglichkeiten der digitalen Evolution mit den Mitteln der Plattform zu realisieren, da diese aktuellen Entwicklungen und Trends folgt.
- Eine Anbindung externer Systeme kann über REST-APIs erfolgen.
- Die Lizenzkosten sind bei dem gegebenen Funktionsumfang niedrig und die Anforderungen an die Ressourcen moderat. Im Marktvergleich ergibt sich ein niedriger „Total Cost of Ownership“ (TCO).

Besonders wichtig war uns die Betrachtung der Sicherheitsmerkmale unserer Software. Denn in unserem Tätigkeitsbereich ist die Sicherheit der genutzten und übertragenen Daten von wesentlicher Bedeutung. Gerade im Hinblick auf die Sicherheitsstandards unserer Software wurde laut Analyse ein sehr hoher Reifegrad attestiert (s.o.).

Schlussendlich ergab die an ISO 25010 angelehnte Untersuchung des Beratungsunternehmens ein sehr hohes Qualitätsniveau (94 von 100 Punkten). Einige wenige verbesserungsfähige Bereiche wurden identifiziert und mit Empfehlungen versehen, die wir systematisch und zeitnah bearbeiten werden.

Damit können sich unsere Kunden weiterhin auf eine sichere, zukunftsfähige und kostengünstige IT-Systemlandschaft verlassen, die über alle notwendigen Schnittstellen zu anderen Systemen der Gruppe verfügt. ▬

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

Interne Revision

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

Seit der letzten Berichterstattung in der Point of Compliance (1/2024, S. 23) wurden aus der von der Geschäftsführung genehmigten Jahresprüfungsplanung 2024 die Prüfungen der Bereiche „IT & Projekte, hier: Projektorganisation & -abwicklung“ und „Hinweisgebersystem“ abgeschlossen und letzterer an die Mandanten der jeweiligen Auslagerungen versandt. Der erstgenannte Prüfungsbericht ist nicht dienstleistungsbezogen und wurde daher intern veröffentlicht.

Die externe Prüfung der Geschäftsbereiche Datenschutz, Geldwäsche- und Betrugsprävention, Informationssicherheit, MaRisk-Compliance und WpHG-Compliance nach IDW PS 951 (Typ 2) wurde wiederum 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. Es wurde die Ordnungsmäßigkeit testiert und der Prüfungsbericht an die Mandantschaft versandt.

Der Quartalsbericht Q1 2024 der Internen Revision wurde fristgerecht erstellt und den Mandanten, die im Zeitraum zu unseren Kunden gehörten, zur Verfügung gestellt.

Weiterhin wurde turnusgemäß ein Follow-up-Quartalsbericht für das erste Quartal 2024 erstellt und der Geschäftsführung der DZ CompliancePartner GmbH vorgelegt. In den Follow-up-Berichten wird die Abarbeitung der von internen und externen Prüfern getroffenen Maßnahmen / Empfehlungen dokumentiert. Offene Punkte werden durch die Interne Revision konsequent nachgehalten.

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

Wie bereits seit 2008 wurde uns erneut eine TÜV-Zertifizierung zum Notfall-Management vom TÜV Saarland erteilt, der damit die Konformität des Notfallkonzepts nach MaRisk AT 7.3 testiert. ▬

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