DZ CompliancePartner

Point of Compliance

Das Risikomanagement-Magazin für
unsere Kunden und Geschäftspartner

AUSGABE 2/2021

Damit Sie die Fäden in der Hand halten

ab Seite 4

MaRisk und Bait –
was ist neu?

ab Seite 17

Hinweisgebersystem –
was kommt?

Impressum 2

STARTPUNKT 3

SCHWERPUNKT

Zusammenfassung der neuen MaRisk 4

BAIT 2.0 – Umsetzung ohne Übergangfrist 9

MaRisk-Compliance: (Neue) Herausforderungen 11

Geldwäscheprävention: Aktuelle Entwicklungen 14

Neuer Schutz für Hinweisgeber*innen 17

Schrems II, III, IV … 20

Marktmissbrauch – ein Praxisbericht 22

PUNKTUM

Online-Seminar (kostenfrei) 26

Interne Revision 27

Wirtschaftliche Lage 27

Neue Telefonnummern 27

IMPRESSUM

Point of Compliance
Das Risikomanagement-Magazin für unsere Kunden und Geschäftspartner, Ausgabe 26, 2/2021
ISSN: 2194-9514
Herausgeber: DZ CompliancePartner GmbH, Wilhelm-Haas-Platz, 63263 Neu-Isenburg, Telefon 069 6978-3324, Telefax 069 6978-3322, www.dz-cp.de
Handelsregister HRB 11105, Amtsgericht Offenbach, USt.-IdNr.: DE201150917
Geschäftsführung: Jens Saenger (Sprecher), Andreas Marbeiter, Norbert Schäfer

Verantwortlich i. S. d. P.: Jens Saenger
Redaktion: Gabriele Seifert, Leitung (red.),
Redaktionsanschrift: DZ Compliance-Partner GmbH, Redaktion Point of Compliance, Wilhelm-Haas-Platz, 63263 Neu-Isenburg, Telefon 069 6978-3188, Telefax 069 6978-3322, E-Mail: poc@dz-cp.de
Weitere Autoren dieser Ausgabe:
Matthias Hommel, Marc Linnebach, Michael Maier, Andreas Marbeiter, Jens Saenger, Lars Schinnerling, Thomas Schröder, Sarah-Lena Tiburtius, Björn Veit

Bildnachweise: DZ CompliancePartner GmbH, iStockphoto (Titel)
Gestaltung: EGENOLF DESIGN, Wiesbaden, studio@egenolf-design.de
Druck: odd GmbH & Co. KG · Print und Medien, www.odd.de

Redaktionsschluss: 10. September 2021
Auflage: 2.600 Exemplare
Die aktuellen Mediadaten finden Sie im Internet unter www.dz-cp.de/poc

Jens Saenger
Sprecher der Geschäftsführung

Wenn über Regulatorik gesprochen wird, fehlt eines nie: die Klage über unverhältnismäßig steigende Anforderungen im Allgemeinen und damit verbunden die Klage über die – noch den kleinsten Prozess erfassende – Regulationstiefe. Und tatsächlich: Allein im letzten Jahr haben wir gegenüber dem Vorjahr einen Anstieg von über 50 % bei regulatorischen Neuerungen gesehen.

Gerade hat die BaFin die MaRisk, die BAIT und sowie die Auslegungs- und Anwendungshinweise zum GwG novelliert. Daneben trat im Sommer eine Geldwäsche-Novelle in Kraft. Zum Ende des Jahres ist die EU-Hinweisgeberrichtlinie umzusetzen. Weil absehbar ist, dass sich deren Umsetzung in nationales Recht verzögert, stehen die Unternehmen einmal mehr vor juristischen Unsicherheiten.

Das alles ist weder einfach noch bringt es einen Marktvorteil. Aber keiner kann sich dem entziehen, im Gegenteil: Die BaFin unterstreicht die Verantwortung der Institute.

In der genossenschaftlichen Gruppe sind wir, auch aus Sicht der Aufsicht, in gewisser Weise privilegiert. Wir arbeiten vernetzt, um gemeinsam zu schaffen, was einer alleine nicht leisten kann. Als Ihr Compliance-Partner ist es an uns, den qualitätsfördernden Wissensaustausch zu ermöglichen und zertifizierte Sicherheit sowie aufwandsreduzierende Tools bereitzustellen – damit Sie die Fäden in der Hand behalten, wenn die Anforderungen steigen.

In diesem Sinne wünsche ich Ihnen eine spannende Lektüre.

Ihr Jens Saenger

MaRisk-Compliance

Zusammenfassung der neuen MaRisk

Mit Datum vom 16. August 2021 hat die BaFin das Rundschreiben 09/2017 mit dem Rundschreiben 10/2021 Mindestanforderungen an das Risikomanagement – MaRisk aktualisiert.

Damit sind der im Oktober 2020 begonnene Konsultationsprozess und die Diskussionen im Fachgremium MaRisk abgeschlossen. In der Novelle nicht berücksichtigt sind die EBA-Leitlinien für die Kreditvergabe und Überwachung sowie das Thema Nachhaltigkeit. Diese werden, wie bereits von der Aufsicht adressiert, in der nächsten Überarbeitung der MaRisk – der siebten MaRisk-Novelle – Berücksichtigung finden. Mit der Überarbeitung soll zeitnah begonnen werden, sodass im Jahr 2022 mit der offiziellen Konsultation der nächsten Fassung zu rechnen ist.

In der nun veröffentlichten finalen Fassung der MaRisk wird nicht mehr auf „systemrelevante" Institute oder, wie noch in der Konsultationsfassung vorgesehen, auf „große und komplexe Institute" abgestellt. Vielmehr wird auf „bedeutende Institute" im Sinne des Art. 6 der SSM-Verordnung (Verordnung (EU) Nr. 1024/2013) abgestellt. Für bedeutende Institute ergeben sich spezifische Anforderungen hinsichtlich Geschäftsstrategie, Datenmanagement/Datenqualität, Risikocontrolling-Funktion, Compliance-Funktion sowie Risikoberichterstattung.

Doch auch für nicht bedeutende Institute ergeben sich zahlreiche neue Anforderungen sowie Präzisierungen bereits bestehender Anforderungen. Die wesentlichen Überarbeitungen betreffen die folgenden Themenkomplexe:

- Leitlinien der EBA zu notleidenden und gestundeten Risikopositionen (NPE Guidelines),
- Auslagerungen (Outsourcing Guidelines),
- ICT Risk (ICT Guidelines).

Weitere Änderungen gibt es in den Bereichen operationelle Risiken (Definition des Anwendungsbereiches), Handelsgeschäfte (Aufnahme von Kryptowährungen, Bestätigungsverfahren, Kontrolle der Marktgerechtigkeit), Liquidität (Unterscheidung institutionelle und andere professionelle Anleger) und Risikotragfähigkeit (Anpassung an den überarbeiteten Leitfaden zur Risikotragfähigkeit).

Nachfolgend die zentralen Inhalte bei den wesentlichen Überarbeitungen:

NPE Guidelines

Die NPE Guidelines unterscheiden zwischen notleidenden Krediten und notleidenden Risikopositionen. Entscheidend ist dabei, ob das Institut die Quote von 5 % oder mehr notleidender Kredite (brutto) in zwei aufeinanderfolgenden Quartalen überschreitet und damit als Institut mit hohem NPL-Bestand eingestuft wird. Auch wenn nur in einzelnen Portfolios ein wesentlicher Anteil an notleidenden Krediten besteht, kann die Aufsicht die Einhaltung der zusätzlichen Anforderungen von den Instituten verlangen. Zur Berechnung der NPL-Quote ist der Bruttobuchwert der notleidenden Kredite durch den Bruttobuchwert der gesamten Darlehen zu teilen. Zu beachten ist, dass bis zur endgültigen Entscheidung der EBA zu diesem Sachverhalt die Berechnung der NPL-Quote ohne Zentralbankguthaben erfolgt.

Institute mit hohem NPL-Bestand haben eine Strategie für den Abbau von notleidenden Risikopositionen zu erstellen, die regelmäßig zu überprüfen ist. Die Risikocontrolling-Funktion hat den NPL-Bestand sowie die Strategieüberwachung anhand eines Mindestkatalogs von Leistungsindikatoren (KPIs) zu überwachen und die Auswirkungen auf interne sowie regulatorische Eigenmittelanforderungen zu beachten. Die Risikocontrolling-Funktion kann sich zur Erfüllung dieser Vorgaben anderer marktunabhängiger Einheiten und deren Informationen bedienen. Voraussetzung hierfür ist jedoch, dass die Informatio-

AUTOREN UND ANSPRECHPARTNER

Matthias Hommel
Beauftragter MaRisk-Compliance,
E-Mail: matthias.hommel@dz-cp.de

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

nen von der Risikocontrolling-Funktion plausibilisiert werden. Darüber hinaus sind Abwicklungseinheiten für NPEs einzurichten, die organisatorisch außerhalb des Marktbereichs angesiedelt werden müssen. Die Mitarbeiter müssen ausreichend qualifiziert und auf die NPE-Abwicklung spezialisiert sein.

Für alle Institute sind die Anforderungen bei Forbearance-Maßnahmen gestiegen. Dies betrifft sowohl die Prozesse und Richtlinien, die eingerichtet und entwickelt werden müssen, als auch die Anforderungen zur Erfassung notleidender Risikopositionen, die präzisiert und ergänzt werden müssen. Damit verfolgen die Aufsichtsbehörden konsequent ihren Ansatz, den Anteil notleidender Kredite in den Bankbilanzen zu reduzieren.

Outsourcing Guidelines

Die umfassenden Änderungen in AT 9 betreffen den gesamten Auslagerungszyklus. In den Erläuterungen zu AT 9 Tz. 1 MaRisk wurde der Katalog der Leistungen, die einen sonstigen Fremdbezug – und somit keine Auslagerung – darstellen, erweitert. Eine wichtige Voraussetzung für Auslagerungen ist, dass durch die Auslagerungen nicht lediglich eine „leere Hülle“ verbleibt. Aufgrund des Universalbanken-Ansatzes wird dies jedoch in der Genossenschaftlichen FinanzGruppe in der Regel nicht von Relevanz sein.

Ebenso ist vom Institut sicherzustellen, dass das Auslagerungsunternehmen zur Ausübung der auszulagernden Tätigkeiten befugt ist und ggf. über entsprechende Erlaubnisse und Registrierungen verfügt. Bisher sind Zulassungen und Erlaubnisse bereits im Rahmen der Anwendung der Musterklauseln des AK Outsourcing berücksichtigt.

Für die Risikoanalyse zur Auslagerung ist zusätzlich zu berücksichtigen, inwiefern eine auszulagernde Tätigkeit innerhalb der Prozesslandschaft des Instituts von wesentlicher Bedeutung ist. Dabei sind auch Konzentrationsrisiken (z. B. wenn mehrere Auslagerungsverträge mit einem Auslagerungsunternehmen bestehen), politische Risiken, Risiken aus der Weiterverlagerung, Interessenkonflikte sowie Datenschutzaspekte etc. zu berücksichtigen.

Auch an die Auslagerungsverträge werden zusätzliche Anforderungen gestellt. Hierzu gehört u. a., dass auch bei nicht wesentlichen Auslagerungen Informations- und Prüfungsrechte zu vereinbaren sind. Bei wesentlichen Auslagerungen sind beispielsweise die Angabe des Standorts für die Dienstleistungserbringung, eine Verpflichtung zur Reintegrationsunterstützung sowie Angaben zu Beginn und Ende der Auslagerung gefordert. Für bestehende oder in Verhandlung befindliche Auslagerungsverträge besteht eine gesonderte Umsetzungsfrist bis zum 31. Dezember 2022.

Im Ergebnis führen die Änderungen zu höheren Anforderungen an die Steuerung und Überwachung von Auslagerungen, weshalb ein zentraler Auslagerungsbeauftragter verpflichtend einzurichten ist. Die Funktion des zentralen Auslagerungsbeauftragten ist (im Gegensatz zum zentralen Auslagerungsmanagement) nicht auslagerbar.

Insgesamt wurden jedoch die Möglichkeiten der vollständigen Auslagerungen der besonderen Funktionen Risikocontrolling, Compliance und Interne Revision ausgeweitet.

Von den Instituten ist ein aktuelles Auslagerungsregister mit Informationen über alle Auslagerungsvereinbarungen vorzuhalten. Bei Weiterverlagerungen von wesentlichen Auslagerungen ist vom auslagernden Institut festzulegen, ob der weiter zu verlagernde Teil wesentlich ist und folglich im Auslagerungsregister zu erfassen ist. >

Hinsichtlich gruppen- bzw. verbundinterner Auslagerungen können Erleichterungen in Anspruch genommen werden. So darf z. B. das zentrale Auslagerungsmanagement auf Gruppen- bzw. Verbundebene angesiedelt sein, sofern es den Anforderungen des AT 9 entspricht.

Neben den überarbeiteten Anforderungen in AT 9 sind zusätzlich die neuen Vorgaben aus dem Gesetz zur Stärkung der Finanzmarktintegrität (FiSG) zu berücksichtigen: Die Absicht einer wesentlichen Auslagerung, deren Vollzug sowie wesentliche Änderungen und schwerwiegende Vorfälle im Rahmen bestehender wesentlicher Auslagerungen, die einen wesentlichen Einfluss auf das Institut haben können, sind gemäß § 24 Abs. 1 Nr. 19 KWG gegenüber der Aufsichtsbehörde anzuzeigen. Eine Absicht zur Auslagerung ist dann anzunehmen, wenn ein entsprechender Gremienbeschluss gefasst wurde. Diese Regelung gilt ab dem 1. Januar 2022.

ICT Guidelines

Die Anforderungen zum Notfallmanagement werden im neu gefassten Abschnitt AT 7.3 umgesetzt. Die bereits bestehenden Notfallkonzepte sind in einen Notfallmanagementprozess einzubetten. Die Aufsicht erläutert mit den neuen MaRisk, welche Aktivitäten und Prozesse als „zeitkritisch" einzustufen sind. Dies sind Aktivitäten und Prozesse, deren Beeinträchtigung zu einem nicht mehr akzeptablen Schaden für das Institut führen kann. Mittels Auswirkungsanalysen sind diese zu identifizieren. Anschließend erfolgt anhand von Risikoanalysen eine Identifikation und Bewertung potenzieller Gefährdungen, die zu einer Beeinträchtigung der zeitkritischen Geschäftsprozesse führen können.

Das Notfallkonzept ist regelmäßig im Hinblick auf die Wirksamkeit und Angemessenheit zu überprüfen und anlassbezogen anzupassen. Über den Zustand des Notfallmanagements ist dem Vorstand vierteljährlich schriftlich zu berichten.

Regelungen zum Inkrafttreten

Die neue Fassung der MaRisk trat mit Veröffentlichung in Kraft. Soweit Änderungen notwendig sind, gibt es für die Implementierung grundsätzlich eine Übergangsfrist bis zum 31. Dezember 2021.

Insbesondere aus den wesentlichen Themenkomplexen mit Überarbeitungen, also:

- NPE Guidelines,
- Outsourcing Guidelines,
- und ICT Guidelines,

ergibt sich für die Institute unter Umständen ein umfassender Umsetzungsbedarf. ▬

Diese und weitere kostenlose Unterstützungsleistungen finden Sie unter www.dz-cp.de/marisk

MaRisk-Novelle 2021: Anforderungen, die bis zum 1. Januar 2022 umzusetzen sind

Tz.	Anmerkungen	nicht relevant	in Arbeit	umgesetzt
AT 1 Tz. 6	Definition von „bedeutenden" Instituten			
AT 2.1 Tz.1	Anwenderkreis der speziellen Anforderungen für High-NPL-Institute; Berechnung der NPL-Quote; Definition von NPE			
AT 2.3 Tz. 3	Ergänzung von Kryptowerten			
AT 4.2 Tz. 1	Pflicht zur Erstellung einer NPE-Strategie für High-NPL-Institute			
AT 4.2 Tz. 3	Inhalte der NPE-Strategie und des Implementierungsplans; Schritte zur Entwicklung der NPE-Strategie			
AT 4.4.1 Tz. 2	NPE-bezogene Aufgaben der Risikocontrolling-Funktion			
AT 5 Tz. 3f	Regelungen zu Verfahrensweisen bei allen Auslagerungen			
AT 9 Tz. 2	Erweiterte Aufzählung der relevanten Aspekte bei der Risikoanalyse			
AT 9 Tz. 4	Befugnis der Leistungserbringung des Auslagerungsunternehmens			
AT 9 Tz. 5	Erweiterte Möglichkeit der vollständigen Auslagerung der besonderen Funktionen unter bestimmten Bedingungen (Schwesterinstitute)			
AT 9 Tz. 7	Erweiterte Vertragsinhalte; Informations- und Prüfungsrechte bei nicht wesentlichen Auslagerungen; Erläuterungen zu Kündigungsrechten, sonstigen Sicherheitsanforderungen und Ort der Durchführung der Dienstleistung; **gesonderte Umsetzungsfrist bis 31.12.2022 für bestehende oder in Verhandlung befindliche Auslagerungsverträge**			
AT 9 Tz. 9	Leistungsüberwachung bei wesentlichen Auslagerungen z.B. anhand von KPIs und vertraglich vereinbarten Informationen			
AT 9 Tz. 12	Einrichtung eines zentralen Auslagerungsbeauftragten im Institut			
AT 9 Tz. 13	Berichtspflicht auch für kleine Institute ohne zentrales Auslagerungsmanagement			
AT 9 Tz. 14	Einrichtung und Vorhalten eines Auslagerungsregisters			
AT 9 Tz. 15	Erleichterungen für Gruppen und Finanzverbünde mit Ausnahme der folgenden bereits in der alten MaRisk-Fassung enthaltenen Regelungen: ▶ AT 9 Tz. 15 lit. a): war bereits für gruppeninterne Auslagerungen in AT 9 Tz. 2 MaRisk a.F. enthalten ▶ AT 9 Tz. 15 lit. d): war bereits in AT 9 Tz. 6 MaRisk a.F. enthalten			

>

Tz.	Anmerkungen	nicht relevant	in Arbeit	umgesetzt
BTO 1.2 Tz. 3	Anforderungen an die mit der Wertermittlung von Immobiliensicherheiten betrauten sachverständigen Personen (sowohl interne als auch externe Sachverständige); Rotation von Sachverständigen			
BTO 1.2.5 Tz. 1	Berücksichtigung von NPE-Kriterien bei Übergang in Problemkreditbearbeitung; Einrichtung von NPE-Abwicklungseinheiten für High-NPL-Institute			
BTO 1.2.5 Tz. 8	Definition von Rettungserwerben und Entwicklung einer Richtlinie, sobald Rettungserwerbe in Betracht gezogen werden			
BTO 1.2.6 Tz. 3	Durchführen von Rückvergleichen zur Überprüfung der Verfahren und Methoden zur Risikovorsorgebildung			
BTO 1.3.2 Tz. 3	Kriterien zur Einstufung und Umgliederung von Forborne-Risikopositionen als notleidende oder nicht-notleidende Risikopositionen			
BTO 1.3.2 Tz. 4	Beurteilung der finanziellen Lage des Kreditnehmers und Änderungen der Vertragsbedingungen			
BTO 1.3.2 Tz. 5	Bewertung der Tragfähigkeit von Forbearance-Maßnahmen			
BTO 1.3.2 Tz. 6	Überwachung des Prozesses zur Gewährung von Forbearance-Maßnahmen und der Wirksamkeit der Maßnahmen			
BTR 1 Tz. 4	Beschränkung der Nutzung kurzfristiger Emittentenlimite auf im Wesentlichen Handelsbuchgeschäfte			
BTR 1 Tz. 7	Erlösquotensammlung und Rettungserwerbe			
BT 2.1 Tz. 3	Verzicht auf eigene Prüfungshandlungen der Internen Revision unter bestimmten Bedingungen bei allen Auslagerungen; Rückgriff auf Nachweise / Zertifikate auf Basis gängiger Standards			
BT 3.2 Tz. 3	Darstellung von notleidenden und Forborne-Risikopositionen bei Instituten mit hohem NPL-Bestand			
BT 3.2 Tz. 6	Ergänzung Mindestinhalte OpRisk-Berichte			

Diese und weitere kostenlose Unterstützungsleistungen finden Sie unter www.dz-cp.de/marisk

MaRisk-Compliance

BAIT 2.0 – Umsetzung ohne Übergangsfrist

Wie die MaRisk-Novelle ist auch die neue Fassung der BAIT am 16. August 2021 in Kraft getreten. Da aus Sicht der BaFin lediglich bestehende Vorgaben konkretisiert werden, gibt es keine Übergangsfristen.

Die Konkretisierungen in den neuen Bankaufsichtlichen Anforderungen an die IT (BAIT) beziehen sich auf bestehende Vorgaben gemäß § 25a Abs. 1 und § 25b des KWG.

Im November 2017 wurden die BAIT erstmalig veröffentlicht. Die Entwicklung der letzten Jahre begründet jedoch einen erheblichen Bedeutungszuwachs der Informationssicherheit und damit auch der BAIT.

Die Novellierung ist unter anderem auch als Reaktion auf die Anpassung bzw. Digitalisierung von Arbeitsabläufen in der Pandemie zu sehen. Aus der Not heraus geboren, haben sich zwischenzeitlich eine Reihe von digitalisierten Prozessen bewährt. Es ist davon auszugehen, dass sich diese Entwicklung fortsetzen wird. Allerdings wird auch deutlich, dass es im operativen Umgang – sowohl mit der Informationssicherheit als auch mit den technischen Verfahren – einen Anpassungsbedarf gibt: Erklärtes Ziel ist, die Schere zwischen technischem Nutzen und technischen Risiken nicht auseinanderdriften zu lassen.

IT-Sicherheit

In diesem Zusammenhang stellt die BaFin klar, dass die fortlaufende Beachtung der Informationssicherheit und deren Einhaltung auf Basis angemessener und wirksamer Sicherungsmaßnahmen künftig deutlicher von der Aufgabe der Identifikation und Steuerung der mit den digitalen Prozessen einhergehenden Informationssicherheitsrisiken abzugrenzen ist. Dies mündet darin, dass in den BAIT ein völlig neues Kapitel zur operativen IT-Sicherheit aufgenommen wurde. Aus Sicht der Behörde mag dies nur eine Konkretisierung bestehender Vorgaben sein. Operativ bedeutet dies allerdings die Notwendigkeit, sich mit allen Verfahren und Prozessen innerhalb des Hauses auseinanderzusetzen und dabei auch potenzielle Interessenkonflikte im Auge zu behalten.

Die Häuser müssen sich zwangsläufig mit den Fragen beschäftigen, inwieweit Leit- und Richtlinien zum Informationsrisikomanagement und zur Informationssicherheit, aber auch der Umgang mit IT-Projekten und den Anwendungsentwicklungen den überarbeiteten Anforderungen der BAIT gerecht werden. Insbesondere ist zu prüfen, inwieweit die verantwortlichen Mitarbeiter*innen und Strukturen der Häuser hierfür operativ angemessen ausgestattet bzw. ausgelegt sind. Das beginnt bei der Prüfung und Anpassung bestehender Arbeitsanweisungen, setzt sich fort in der Prüfung aktueller Rollen, Verantwortlichkeiten und Dokumentationen und endet in der Aktualisierung des SOIT. Dabei kann der erforderliche Anpassungsbedarf in den Häusern je nach aktueller Organisationslage durchaus unterschiedlich ausfallen.

In der Summe lässt sich aber jetzt schon sagen, dass im Rahmen eines Analyseprozesses der Vorstand, diverse Fachabteilungen, die IT-Organisation, der Notfallbeauftragte und der Informationssicherheitsbeauftragte gefordert sein werden. Diese breite Auffächerung verdeutlicht ein wesentliches operatives Ziel der Novelle:

Die Wahrung der Informationssicherheit ist nicht und kann nie die Aufgabe von einzelnen Mitarbeiter*innen oder Beauftragten sein. Informationssicherheit impliziert vielmehr

- Leitplanken und Vorgaben (Vorstand),
- die Bereitstellung angemessener Mittel und Ressourcen (Vorstand),
- klare Arbeitsanweisungen (Orga),
- eindeutige Verantwortlichkeiten (Vorstand und Orga),
- Umsetzung und Beachtung in den operativen Einheiten sowie
- die fortlaufende Analyse, Steuerung und Beratung der jeweiligen Facheinheiten durch den Informationssicherheitsbeauftragten (ISB).

>

AUTOR UND ANSPRECHPARTNER

Andreas Marbeiter
Geschäftsführung,
E-Mail: andreas.marbeiter@dz-cp.de

Operative Informationssicherheit

Damit unterstreicht die Aufsicht einmal mehr ihr Verständnis der drei Verteidigungslinien. Die operativen Einheiten stehen als „first line of defense" nun mal an vorderster Front und „verantworten" damit die meisten Einfallstore zur Gefährdung der Informationssicherheit.

In diesem Zusammenhang ist auch die Hervorhebung der Bedeutung der Informationseigentümer zu sehen, die sich aus dem neu geschaffenen Kapitel 3 der BAIT – operative Informationssicherheit – ergibt. Die interessenkonfliktfreie Trennung von operativem Handeln einerseits und unterstützender Beratung, Risikoanalyse und -steuerung andererseits verdeutlicht die Erfordernis eines Zusammenwirkens von Fachabteilungen und den dortigen Informationseigentümern mit dem Informationssicherheitsbeauftragten als verantwortlichem Kollegen der „second line of defense". Klare Schnittstellendefinitionen vereinfachen dabei nicht nur die Allokation durchzuführender Tätigkeiten. Sie ermöglichen dem Vorstand darüber hinaus einen transparenten Überblick über erforderliche Ressourcen und Kosten, die den jeweiligen Rollenprofilen innewohnen.

IT-Governance

Ein weiterer wichtiger, operativer Aspekt ist die Rolle der internen Kontrollsysteme (IKS) aus Kapitel 2 der BAIT – IT-Governance. Die Einbindung der ordnungsgemäßen Aufgabenwahrnehmung in das IKS der Bank ist auch hier der wesentliche Faktor.

Wir haben dieser Entwicklung bereits Rechnung getragen und stellen unseren Auslagerungsmandaten seit letztem Jahr zur Bestätigung unserer ordnungsgemäßen Aufgabenwahrnehmung ein Testat nach IDW PS 951 Typ II zur Verfügung. Dieses kann ohne weiteren eigenen Aufwand in die Kontrolldokumentation des eigenen Hauses übernommen und dem Prüfer zur Verfügung gestellt werden.

Schlussendlich thematisieren die neuen BAIT das (IT-)Notfallmanagement. Unserer Einschätzung zufolge gibt es nicht unerhebliche Synergien mit den im Informationssicherheitsprozess definierten Sicherungsmaßnahmen. Insbesondere die Einschätzungen zu Verfügbarkeitsbedarf und Zeitkritikalität können als Basis genutzt werden. Dennoch wird es auch in diesem Segment nicht ohne detaillierte Analyse und ggf. Anpassung bestehender Systeme und Prozesse gehen.

Detaillierte Informationen auf unserer Homepage

Auf unserer Homepage unter www.dz-cp.de/bait können Sie auszugsweise einige wesentliche Änderungen und daraus resultierende Handlungserfordernisse für Ihr Haus in tabellarischer Form herunterladen. Die detaillierten Analysen und Maßnahmenempfehlungen sprechen wir mit unseren Auslagerungsmandaten in den nächsten Wochen systematisch durch.

Auch wenn die BAIT viel enthalten, was in den Häusern bereits heute so durchgeführt wird, haben sich neue Schwerpunkte – insbesondere im Bereich der Einbindung der Informationseigentümer in der Bank, der operativen Informationssicherheit sowie des IT-Notfallmanagements – ergeben. ▬

Einen ersten, tabellarischen Überblick der wesentlichen Änderungen und daraus resultierenden Handlungsempfehlungen finden Sie unter www.dz-cp.de/bait

MaRisk-Compliance

(Neue) Herausforderungen in der Regulatorik meistern

Die immer stärker steigende Anzahl neuer oder aktualisierter regulatorischer Anforderungen bereitet den Instituten Kopfzerbrechen. Diese müssen nicht nur pragmatisch umgesetzt werden. Relevante Änderungen müssen zunächst überhaupt identifiziert, zeitnah gesichtet und analysiert werden.

Dies führt zu steigenden Aufwendungen, die sich jedoch mit dem richtigen Ansatz leicht vermeiden lassen.

Zu den Hauptaufgaben der MaRisk-Compliance-Funktion gehört die Identifizierung der wesentlichen rechtlichen Regelungen und Vorgaben, deren Nichteinhaltung zu einer Gefährdung des Instituts führen kann (AT 4.4.2 Tz. 2 MaRisk). Doch der Aufwand für das Institut und die Compliance-Funktion wird von zahlreichen internen und externen Faktoren beeinflusst.

Der offenkundigste Faktor ist dabei die stetig wachsende Anzahl regulatorischer Anforderungen. Unter anderem bedingt durch die Corona-Pandemie umfasste das von uns angebotene Rechtsmonitoring im Jahr 2020 fast 50 % mehr Einträge als im Jahr 2019. Schnell kommen so mehrere Hundert Seiten Rundschreiben und Umsetzungshilfen im Monat zusammen, die von jedem Compliance-Beauftragten auf Relevanz und Handlungsbedarf untersucht werden müssen.

Hinzu kommt, dass ein immer stärkerer Fokus seitens Aufsicht und Prüfung auch auf die Dokumentation zur Umsetzung von Vorgaben gerichtet wird.

Grundsätze wie „Was nicht dokumentiert ist, wurde nicht gemacht“ oder „Wer schreibt, der bleibt“ bewahrheiten sich zunehmend und werden bei Nichtbeachtung mit zum Teil erheblichen Beanstandungen in Prüfungsberichten quittiert. >

50 %

mehr Compliance-relevante Neuerungen von 2019 auf 2020

ABB. 1 PROZESS ZUM MANAGEMENT DER REGULATORIK

Dadurch wird nicht nur die Compliance-Funktion, sondern das Institut als Ganzes vor die große Herausforderung gestellt, auf eine ausreichende und transparente Dokumentation zu achten.

In den durch uns betreuten Mandaten sehen wir, dass die Institute allein durch Dokumentationen und Ablage stark belastet werden. Darüber hinaus stehen die Institute vor dem Problem, einen Prozess implementieren zu müssen, der eine nachvollziehbare Dokumentation der Umsetzung durch die betroffenen Verantwortlichen ermöglicht.

Diese Aufgabe impliziert einen sehr hohen Abstimmungsbedarf innerhalb des Instituts, der sich zunehmend komplexer gestaltet und ohne begleitende Unterstützungsleistungen kaum mehr zu bewerkstelligen ist. Unsere eigenen Erfahrungen als Beauftragte MaRisk-Compliance zeigen, dass es zwingend notwendig ist, die Steuerung und Abstimmung von Maßnahmen einfacher und transparenter zu gestalten, Verantwortlichkeiten deutlicher zu adressieren, Dokumentationen über Abläufe und terminliche Vorgaben nachzuhalten, um Umsetzungsrisiken für das Institut zu vermeiden. Vieles davon wird aktuell wenig ressourcenschonend durch individuellen und manuellen Aufwand abgebildet.

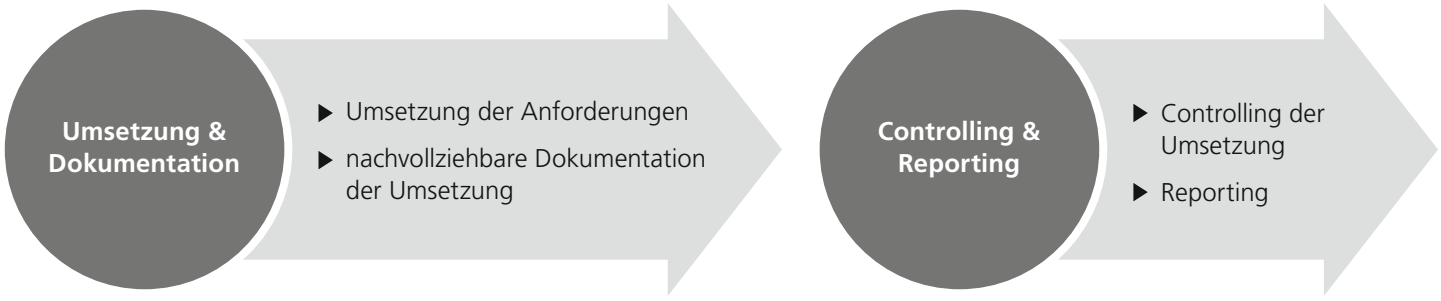
Reduktion von Aufwand und Risiken durch geeignete Unterstützungsleistungen

Uns begegnen viele verschiedene Varianten, wie Banken die Risiken und Aufwände für das Institut und die Compliance-Funktion in den Griff zu bekommen versuchen: Es werden eigene Datenbanken mit Rundschreibendiensten zur Dokumentation und zum Controlling der Umsetzung regulatorischer Anforderungen entwickelt und befüllt. Manche Häuser geben sehr viel Geld für externe Lösungen, z. B. von WP-Gesellschaften, aus und bekommen dabei Informationsinhalte geliefert, die weit über den benötigten Horizont ihrer Geschäftsmodelle hinausgehen. Ergänzend werden bisweilen auch einfache Internetrecherchen in bestimmten zeitlichen Abständen vorgenommen.

Die DZ CompliancePartner ist seit Jahren Anbieter eines Rechtsmonitorings, das monatlich als Word-, Excel- und PDF-Datei an die (Auslagerungs-)Kunden versendet wird. Berücksichtigt werden dabei verschiedene Quellen, insbesondere auch die Rundschreiben des BVR. Die Inhalte werden verständlich

AUTOR UND ANSPRECHPARTNER

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



zusammengefasst und mit pragmatischen Handlungsempfehlungen ergänzt.

Dabei haben wir immer ein offenes Ohr und pflegen eine enge Abstimmung mit zahlreichen Instituten innerhalb und außerhalb der Genossenschaftlichen FinanzGruppe, um den Nutzen und die Erfordernisse unserer Dienstleistung weiter zu optimieren. Mit RM kompakt – der datenbankgestützten Steuerung der Compliance-Prozesse nach MaRisk AT 4.4.2 – haben wir die Rückmeldungen unserer Kunden praxisorientiert umgesetzt.

Aus der Praxis für die Praxis: Das ist zusammengefasst unser auf Basis der BVR-Musterbestandsaufnahme ausgerichtetes Rechtsmonitoring. Das Tool ist webbasiert und ermöglicht eine institutsindividuelle Vorgangsweiterverarbeitung. Dadurch entfallen nahezu alle administrativen Tätigkeiten, die bislang überwiegend manuell und unter Entstehung vielfältiger Medienbrüchen durchgeführt wurden. Die Zuordnung von Zuständigkeiten erfolgt auf Wunsch automatisch, wodurch das Risiko nicht ausreichend geklärter Verantwortlichkeiten minimiert wird.

Ein wesentlicher Nutzen ist, dass die Umsetzung der Inhalte einfach und revisionssicher dokumentiert wird und Umsetzungsfristen einfach und ohne Zusatzaufwand im Blick behalten werden können.

Um den unterschiedlichen Ansprüchen in den Instituten gerecht werden zu können, haben wir großen Wert auf eine hohe Individualisierbarkeit gelegt. So können die Nutzer innerhalb des Instituts oder der Adressatenkreis von Eskalationen frei definiert werden. Darüber hinaus werden die Institute/die Anwender künftig die Möglichkeit haben, bei Bedarf eigene Einträge zu erfassen.

Nach einer umfangreichen Testphase erhalten aktuell unsere MaRisk-Auslagerungskunden ein kostenloses Upgrade auf RM kompakt. Zeitnah werden auch die Kunden unseres aktuellen Rechtsmonitorings kostenfrei upgegradet.

Wir bedanken uns bei den Instituten, die an der Entwicklung mitgewirkt haben. Nur so ist es uns möglich gewesen, den genossenschaftlichen Gedanken pragmatisch weiterzutragen und die Ergebnisse für alle nutzbar zu machen.

Sofern Sie Fragen zur Umstellung oder Interesse an RM kompakt haben, kommen Sie gerne auf uns zu. ▬

Geldwäscheprävention

Aktuelle Entwicklungen auf nationaler und europäischer Ebene

Die Verhinderung von Geldwäsche ist nach wie vor ein wesentlicher Baustein bei der Bekämpfung der organisierten Kriminalität. Die Maßnahmen zur Verhinderung und zum Aufdecken von Geldwäsche, die in immer kürzeren Abständen nachjustiert und ergänzt werden, führen zu stetig steigenden Anforderungen und Aufwänden bei den Kreditinstituten.

Der folgende Beitrag gibt einen Überblick über die aktuellen Entwicklungen in der Geldwäschebekämpfung auf nationaler und europäischer Ebene.

Änderung § 261 (Geldwäsche) Strafgesetzbuch

Durch das am 18. März 2021 in Kraft getretene Gesetz zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche wurde jegliche Straftat als taugliche Geldwäschevortat definiert. In der Kreditwirtschaft führte diese Änderung zu einem nochmaligen Anstieg des Verdachtsmeldeaufkommens.

Novellierung des Glücksspielstaatsvertrages

Zum 1. Juli 2021 wurde der Glücksspielstaatsvertrag (GlüStV) novelliert. Im Hinblick auf die Abwicklung des Zahlungsverkehrs ist insbesondere die Neugestaltung des Mitwirkungsverbotes in § 4 Abs. 1 GlüStV 2021 von Bedeutung. Danach dürfen öffentliche Glücksspiele nur mit Erlaubnis der zuständigen Behörde des jeweiligen Landes veranstaltet oder vermittelt werden. Das Veranstalten und das Vermitteln ohne diese Erlaubnis (unerlaubtes Glücksspiel) sowie die Mitwirkung an Zahlungen im Zusammenhang mit unerlaubtem Glücksspiel sind verboten.

Die Deutsche Kreditwirtschaft hat die Glücksspielaufsicht wiederholt darauf hingewiesen, dass Kreditinstitute grundsätzlich keine Möglichkeit haben, Zahlungen, die im Zusammenhang mit illegalem Glücksspiel stehen, zu identifizieren. Individuelle Erkenntnisse können sich ggf. aus den Maßnahmen zur Geldwäschebekämpfung ergeben. Eine aktuelle Übersicht der in Deutschland zugelassenen (Online-)Glücksspielanbieter – die sogenannte „White List" – finden Sie u. a. auf der Internetseite: https://rp-darmstadt.hessen.de/sicherheit/gl%C3%BCcksspiel/sportwetten

Transparenzregister- und Finanzinformationsgesetz

Im Juni wurde das „Gesetz zur europäischen Vernetzung der Transparenzregister und zur Umsetzung der Richtlinie (EU) 2019/1153 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Nutzung von Finanzinformationen für die Bekämpfung von Geldwäsche, Terrorismusfinanzierung und sonstigen schweren Straftaten" (TraFinG) im Bundesgesetzblatt veröffentlicht.

Zum 1. August 2021 sieht das GwG insbesondere folgende Neuregelungen vor:

- Das Transparenzregister wird auf ein Vollregister umgestellt.
- Alle Rechtseinheiten gemäß § 20 Abs. 1 und § 21 Abs. 1 und 2 GwG sind nun verpflichtet, ihren wirtschaftlich Berechtigten nicht nur zu ermitteln, sondern dem Transparenzregister positiv zur Eintragung mitzuteilen.
- Die sogenannte „Mitteilungsfiktion" entfällt.
- Erleichterung bei der Überprüfung der Angaben zum wirtschaftlich Berechtigten.
- Je nach Rechtsform der Unternehmung bestehen Übergangsfristen:

Frist bis zur verpflichtenden Eintragung / Meldung	Rechtsform
bis spätestens 31.03.2022	AG, SE und KG auf Aktien
bis spätestens 30.06.2022	GmbH, Genossenschaft, europäische Genossenschaft (SCE), Partnerschaft
bis spätestens 31.12.2022	alle anderen Rechtsformen

BaFin veröffentlicht Besonderen Teil ihrer Auslegungs- und Anwendungshinweise

Die BaFin hat am 8. Juni 2021 den bereits seit Längerem avisierten Besonderen Teil ihrer Auslegungs- und Anwendungshinweise für Kreditinstitute (BaFin AuA BT KI) veröffentlicht.

Insbesondere sind die dort unter Ziffer 1 enthaltenen Regelungen zur Herkunftsnachweispflicht bei Bartransaktionen, die spätestens ab dem 8. August 2021 einzuhalten sind, beachtlich:

- Bei Bareinzahlungen innerhalb einer bestehenden Geschäftsbeziehung von mehr als 10.000 € müssen Kunden die Herkunft der Barmittel durch geeignete Dokumente nachweisen.
- Bei Einzahlungen an Geldautomaten von mehr als 10.000 € ist der Kunde im Nachgang zur Transaktion aufzufordern, einen geeigneten Herkunftsnachweis innerhalb einer angemessenen Frist einzureichen.
- Die Vorlage des Herkunftsnachweises durch den Kunden ist in geeigneter Weise zu dokumentieren.
- Bei Kunden, bei denen regelmäßig höhere Bartransaktionen zum Geschäftsmodell gehören, kann von der Vorlage eines Herkunftsnachweises abgesehen werden, sofern die Bartransaktionen risikoorientiert regelmäßig auf Plausibilität überprüft werden.
- Bei Bartransaktionen außerhalb einer bestehenden Geschäftsbeziehung ist die Herkunft der Vermögenswerte bereits bei einem Betrag von mehr als 2.500 € nachzuweisen.

Für die praktische Umsetzung dieser aufsichtsrechtlichen Anforderungen haben wir folgende Unterstützungsleistungen für die von uns betreuten Banken entwickelt bzw. vorgesehen:

- Bereitstellung einer editierbaren Auswertung über Kunden, bei denen auf Basis nachvollziehbarer Kriterien höhere Bartransaktionen zum Geschäftsmodell gehören.
- Regelmäßige Plausibilisierung dieser Liste mittels Geno-SONAR® und Ausweis in der jährlichen Risikoanalyse.
- Überprüfung der bestehenden Indizien und Neuanlage weiterer Indizien in Geno-SONAR®. Damit wird die Erfüllung der neuen aufsichtsrechtlichen Pflichten von uns als prozessimmanente Kontrolle flankierend unterstützt.
- Zudem turnusmäßige Überprüfung der Verpflichtung im Rahmen der Weiterentwicklung unseres Prüfungs- und Kontrollkonzeptes.

Ausblick auf Pläne der EU-Kommission

Die EU-Kommission hat am 20. Juli 2021 ein ehrgeiziges Bündel von Gesetzgebungsvorschlägen vorgelegt, mit denen die Vorschriften der EU zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung weiter gestärkt werden sollen.
Das vorgelegte Paket besteht aus vier Regulierungsvorhaben:

- Verordnung zur Schaffung einer neuen EU-Behörde für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung (AMLA).
  Die AMLA soll ihren operativen Geschäftsbetrieb bis Ende 2024 aufnehmen und insbesondere die Beaufsichtigung für bestimmte Kredit- und Finanzinstitute mit einem hohen inhärenten Risikoprofil übernehmen.
- Verordnung zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung. >

AUTOR UND ANSPRECHPARTNER

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

Das einheitliche EU-Regelwerk für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung soll die einschlägigen Vorschriften EU-weit harmonisieren und beispielsweise detailliertere Bestimmungen zur Kundensorgfaltspflicht, zum wirtschaftlichen Eigentum und zu den Befugnissen und Aufgaben von Aufsichtsbehörden und zentralen Meldestellen enthalten. Hervorzuheben ist in diesem Zusammenhang vor allem die Schaffung einer EU-weiten Bargeldobergrenze von 10.000 € mit einer Ausnahme für Transaktionen zwischen Privatleuten.

- Sechste Richtlinie zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung, die die Richtlinie 2015/849/EU (d. h. die durch die Fünfte Geldwäscherichtlinie geänderte Vierte Geldwäscherichtlinie) ersetzen soll und Bestimmungen enthält, die in nationales Recht umgesetzt werden müssen, wie die Vorschriften zu den nationalen Aufsichtsbehörden und den zentralen Meldestellen in den Mitgliedstaaten.
- Überarbeitete Fassung der Geldtransfer-Verordnung von 2015 (Verordnung 2015/847), die auch die Rückverfolgung von Krypto-Transfers ermöglichen soll.

(Quelle: https://ec.europa.eu/germany/news/20210720-kampf-gegen-geldwaesche_de).

Leitlinienentwurf der Europäischen Bankenaufsichtsbehörde

Auch die Europäische Bankenaufsichtsbehörde (EBA) setzt mit ihren am 2. August 2021 zur Konsultation gestellten Leitlinien einen neuen weiteren Impuls zur Verhinderung von Geldwäsche und Terrorismusfinanzierung. Der Leitlinienentwurf befasst sich dabei erstmals auf EU-Ebene umfassend mit dem gesamten „AML/CFT-Governance-System" (Anti-Money Laundering / Combating the Financing of Terrorism).

Besonders hervorzuheben ist, dass die EBA klare Erwartungen an die Rolle, Aufgaben und Verantwortlichkeiten des Geldwäschebeauftragten (AML/CFT-Compliance-Beauftragten) und des „Leitungsorgans" (Vorstand, Geschäftsführer) formuliert. Danach müssen die AML/CFT-Compliance-Beauftragten u.a.

- über ein ausreichendes „Dienstalter" verfügen und
- die Befugnisse haben, dem „Leitungsorgan" alle notwendigen und geeigneten Maßnahmen vorzuschlagen, die die Einhaltung der Vorschriften zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung gewährleisten.

Die Konsultation endet am 2. November 2021. ▬

Hinweisgebersystem

Neuer Schutz für Hinweisgeber*innen

Whistleblowing, aber auch jedem einzelnen Hinweisgeber kommt immer mehr Bedeutung zu. Die Politik hat erkannt, wie wichtig es für alle Beteiligten sein kann, frühzeitig von möglichen Ungereimtheiten innerhalb von Unternehmen oder Behörden zu erfahren.

Die aktuellen Geschehnisse um aufsehenerregende Betrugsaufdeckungen innerhalb der Finanzbranche passen hier leider nur zu gut ins Bild. Aber sie dokumentieren auch beispielhaft, welche Möglichkeiten zur Verhinderung solcher Vorfälle bestehen könnten. Auch die Politik der Europäischen Union scheint dieses Thema erkannt zu haben.

Am 16. Dezember 2019 ist die Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates zum „Schutz von Personen, die Verstöße gegen das Unionsrecht melden“ (EU-Hinweisgeberrichtlinie) in Kraft getreten. Sie soll den Schutz von Hinweisgebern auf ein EU-weit einheitliches Niveau heben. Die Mitgliedstaaten hatten mit der Veröffentlichung zwei Jahre Zeit, die Vorschriften bis Dezember 2021 in nationales Recht umzusetzen.

Vorgaben der Richtlinie

Die Richtlinie nennt in ihren Regelungen bestimmte Vorschriften des Unionsrechts und ermöglicht es Hinweisgebern, Verstöße hiergegen zu melden. Beispielhaft zu nennen sind hier

- die Vergabe von Aufträgen,
- die Bekämpfung von Terrorismusfinanzierung,
- Vorgaben zu Produktsicherheit,
- Lebensmittel- und Futtermittelsicherheit sowie
- Tierwohl und -gesundheit,
- Verbraucherschutz und viele mehr.

Den nationalen Gesetzgebern ist es im Rahmen der Umsetzung allerdings möglich, den Anwendungsbereich zu erweitern und nationale Regelungen als Meldesachverhalt zu ergänzen. Hierzu finden Sie nähere Informationen weiter unten.

Der Begriff des Hinweisgebers ist in der Richtlinie weit gefasst. Darunter fallen neben Arbeitnehmern und Beamten unter anderem auch Selbstständige, Anteilseigner, Verwaltungs-, Leitungs- und Aufsichtsorgane, Freiwillige und Praktikanten. Hinweisgeber können auch Personen sein, deren Arbeitsverhältnis bereits beendet ist oder noch nicht begonnen hat. Geschützt werden sollen auch Personen, die mit dem Hinweis-geber in Verbindung stehen und an der Meldung beteiligt sind.

Die Richtlinie gibt vor, dass es künftig drei Meldekanäle geben soll:

- intern,
- extern und
- die Offenlegung.

Die Hinweisgeber können wählen, ob sie ihren Hinweis an einen internen oder externen Kanal melden möchten. Intern meint eine Meldestelle innerhalb des Unternehmens oder der Behörde. Externe Meldestellen sind von den Mitgliedstaaten benannte Behörden. Mit Offenlegung ist die Weitergabe der Informationen an die Öffentlichkeit gemeint. Hieran sind jedoch mehr Voraussetzungen geknüpft als an die beiden anderen Meldekanäle. Grundsätzlich ist diese Möglichkeit erst eröffnet, sofern im Rahmen der beiden anderen Meldemöglichkeiten dem Hinweis nicht nachgegangen wurde. Im Ausnahmefall ist auch eine direkte Inanspruchnahme der Offenlegung möglich, dies jedoch nur unter besonderen Voraussetzungen.

Die Hinweisgeber sollen durch die Richtlinie insbesondere vor Repressalien geschützt und somit ermutigt werden, die ihnen bekannt gewordenen Informationen zu melden. Sie sollen insbesondere vor

- Kündigung,
- Suspendierung und
- weiteren nachteiligen Folgen bewahrt werden.

Deutsches Hinweisgeberschutzgesetz

Der deutsche Gesetzgeber ist aufgrund dieser Vorgaben verpflichtet, bis zum 17. Dezember 2021 die in der Richtlinie genannten Erfordernisse in deutsches Recht umzusetzen.

Dies hat er bereits in Form eines Entwurfes zum Hinweisgeberschutzgesetz (HinSchG-E) getan. Aktuell liegt nur ein Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz vor, sodass die Regelungen noch nicht im Bundestag besprochen und diskutiert wurden. Die Diskussionen finden aktuell wohl nur innerhalb der Ministerien statt. Es ist daher davon auszugehen, dass es bis zur Lesung des Entwurfes noch einige Zeit dauern wird.

Der Gesetzesentwurf setzt die Richtlinie in deutsches Recht um. Somit enthält auch die deutsche Regelung die Vorgaben zu den drei Meldekanälen. Eine Verpflichtung zur Einrichtung interner Meldekanäle besteht nach dem Gesetzesentwurf – wie auch aus der Richtlinie – für Unternehmen mit in der Regel mehr als 50 Beschäftigten. Es wurde jedoch für bestimmte Beschäftigungsgeber unabhängig von der Zahl der Beschäftigten eine Pflicht zur Einrichtung interner Meldestellen festgelegt. Hierzu könnten auch alle Kreditinstitute zählen; dies könnte sich aus § 12 Abs. 3 Nr. 4 HinSchG-E ergeben. Für Unternehmen mit bis zu 249 Beschäftigten soll das Gesetz erst zum 17. Dezember 2023 in Kraft treten. Da nicht klar ist, ob diese Abgrenzung auch für Kreditinstitute gilt, ist sicherheitshalber davon auszugehen, dass die Anforderungen mit Inkrafttreten des Gesetzes am 17. Dezember 2021 die Pflicht zur Einrichtung interner Meldestellen umfassen.

Der deutsche Gesetzgeber hat von der Möglichkeit der Richtlinie Gebrauch gemacht und den Anwendungsbereich des Gesetzes ergänzt. Die Gesetze und Vorschriften, gegen die Verstöße gemeldet werden können, wurden erweitert und umfassen nun

- das in der Richtlinie genannte Unionsrecht und
- zusätzlich nationales Recht.

Ergänzung des Anwendungsbereichs

So können die Hinweisgeber auch Sachverhalte melden, die straf- und bußgeldbewährt sind, sodass das gesamte Straf- und Ordnungswidrigkeitenrecht Bestandteil des Gesetzes wird und Hinweise diesbezüglich abgegeben werden können. Das bedeutet, dass auch Vorgänge bzw. Straftaten wie Betrug, Körperverletzung oder Belästigung an eine Meldestelle übermittelt werden können. Dies ist insbesondere in Bezug auf die bereits genannten öffentlichkeitswirksamen Fälle aus den letzten Monaten interessant, denn solche Hinweise sind von der EU-Richtlinie nicht abgedeckt.

Hierin scheint auch der große Streitpunkt innerhalb der Politik zu bestehen.

Die eine Seite hält diese Ergänzung und Erweiterung für erforderlich. Sie möchte den Hinweisgebern den größtmöglichen Nutzen aus der neuen Regelung bieten. Eine vorherige Abwägung, welche Informationen von den Vorgaben abgedeckt sind und welche nicht, würde demnach dem Sinn der Regelungen zuwiderlaufen. Es sei dem Hinweisgeber nicht zuzumuten, erst lange zu recherchieren, welche Verstöße er melden kann und welche nicht.

Die andere Seite vertritt wohl die Meinung, dass eine richtlinienkonforme Umsetzung ausreiche und eine Ergänzung der Meldesachverhalte nicht notwendig sei. Weitere Ausführungen hierzu finden Sie am Ende des Artikels.

Meldestellen

Interne Meldestellen sind innerhalb der Unternehmen zu errichten oder dürfen von Dritten ausgeübt werden. Diese Stellen unterliegen künftig neuen Anforderungen an den Umgang mit eingegangenen Meldungen. So müssen diese z. B.

- dem Meldenden den Eingang des Hinweises bestätigen,
- Kontakt mit ihm halten,
- die Stichhaltigkeit der Meldung prüfen und
- angemessene Folgemaßnahmen ergreifen.

Zudem muss nach dem aktuellen Entwurf dem Hinweisgeber innerhalb von drei Monaten nach Eingang der Meldung eine Rückmeldung gegeben werden.

Die internen Meldekanäle müssen so gestaltet sein, dass sie Meldungen in mündlicher oder in Textform ermöglichen. Zudem ist auf Ersuchen des Hinweisgebers innerhalb einer angemessenen Zeit diesem eine persönliche Zusammenkunft zu ermöglichen.

Externe Meldestelle beim Bund ist grundsätzlich der oder die Bundesbeauftragte für den Datenschutz und die Informations-

freiheit. Diese ist zuständig, soweit nicht eine andere externe Meldestelle zuständig ist. Dies kann sein: eigene Meldestellen der einzelnen
Bundesländer, die Bundesanstalt für Finanzdienstleistungsaufsicht oder eine weitere externe Meldestelle des Bundes (diese aber nur für den Fall, dass sich ein Hinweis gegen die eigentliche externe Meldestelle des Bundes richtet).

Die neuen Regelungen geben einige Anforderungen vor, die die bisherigen Vorgaben übersteigen.

In jedem Fall handelt es sich bei dem Thema Hinweisgeber/Whistleblowing um eine sensible Angelegenheit für alle Seiten, sowohl für die Politik als auch für die potenziellen Hinweisgeber und Unternehmen. Der Nutzen eines funktionierenden Hinweisgebersystems im eigenen Unternehmen liegt auf der Hand und bietet allen Beteiligten Vorteile. Die Verantwortlichen schaffen eine Kultur des offenen Umgangs und zeigen, dass ihnen die Kenntnis von Vorgängen wichtig ist. Die Mitarbeiter haben die Möglichkeit, ihre Informationen an geeigneter Stelle loszuwerden. Ihnen wird gezeigt, dass ihre Meinung und ihr Wissen wichtig sind. Auch die Richtlinie und der Gesetzesentwurf legen dar, dass diese Art der Hinweismeldung die am meisten bevorzugte bzw. gewünschte Variante ist.

Juristische Herausforderung

Die inzwischen sehr wahrscheinliche Verzögerung der Umsetzung der Richtlinie in nationales Recht stellt alle Betroffenen, also sowohl potenzielle Hinweisgeber als auch Unternehmen/Behörden, vor einige Probleme. Es ergeben sich hieraus nämlich juristische Schwierigkeiten. Nach Ablauf der Umsetzungsfrist könnte es dazu kommen, dass einzelne Vorgaben der Richtlinie unmittelbar anwendbar werden. Sie würden also auch ohne nationales Umsetzungsgesetz gelten. Die Regelungen müssten aber u. a.

- klar und präzise sein und
- dürften in ihrer Wirksamkeit nicht von Bedingungen abhängen.

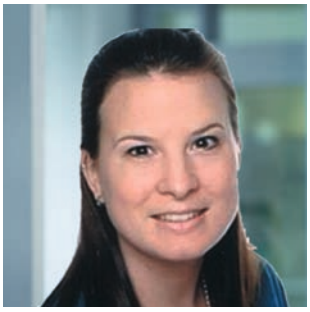
Das trifft jedoch nicht auf alle Normen der Richtlinie zu.

Zudem ist die unmittelbare Wirkung der Richtlinie nur im Verhältnis zwischen Bürger und Staat und somit nicht zwischen Privaten, also z. B. zwischen privaten Arbeitnehmer und privatem Arbeitgeber, möglich. Anders verhält es sich, wenn der Arbeitgeber ein öffentlicher ist.

Es zeichnet sich somit ab, dass eine Nicht-Umsetzung der Richtlinie durch den deutschen Gesetzgeber keine Vorteile mit sich brächte. Es gäbe hingegen einiges an Konsequenzen zu bedenken, sofern das nationale Gesetz tatsächlich weder vom aktuellen noch vom künftigen Bundestag bis zum Ende der Umsetzungsfrist verabschiedet wird. Und dieses Ergebnis wird dem eigentlich gewollten Schutz von Hinweisgebern in keinem Fall förderlich sein.

Die Dienstleistung der DZ CompliancePartner erfüllt für Sie bereits jetzt die Anforderungen des § 25a KWG und übernimmt künftig die Aufgaben der internen Meldestelle zur Entgegennahme von Meldungen der Hinweisgeber. Die Hinweise werden dann der Geschäftsleitung unter Wahrung der Identität des Hinweisgebers weitergeleitet, sodass diese entscheiden kann, wie weiter vorgegangen werden soll. Die Anforderungen der Richtlinie und des deutschen Gesetzesentwurfs lassen sich durch geringfügige Anpassungen in die bereits bestehende Dienstleistung integrieren, sodass Sie mit unserem Produkt die Vorgaben sowohl des KWG als auch des HinSchG erfüllen. ▬

AUTORIN UND ANSPRECHPARTNERIN



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

Datenschutz

Schrems II, III, IV …

Soziale Medien im Spannungsfeld zwischen Datenschutz und Realität

Im Juli vergangenen Jahres erschütterte der Europäische Gerichtshof mit seinem Urteil die Welt des europäischen Datenschutzes. Das Urteil ging als „Schrems II“ in die Rechtsgeschichte ein. Es beschäftigt Praxis, Regulatorik und Literatur bis heute intensiv und geht dabei weit über den Bereich der sozialen Medien hinaus.

Und ein Ende ist vorläufig auch nicht absehbar: Der österreichische Aktivist Max Schrems und seine Organisation noyb bringen die Praktiken von Facebook erneut vor das höchste europäische Gericht.

Das Thema ist hochaktuell. Soziale Medien sind Teil unseres Alltages und weisen hohe Nutzungsraten auf. Grund genug, sich mit den bisherigen Entwicklungen für diesen „Teilbereich“ des Datenschutzes zu beschäftigen.

Eine lange Geschichte: Soziale Medien und Datenschutz

Bereits im Jahr 2015 kippte der EuGH Regelungen zum transatlantischen Datenverkehr („Schrems I“). Das sogenannte „Safe Harbour“-Abkommen als Grundlage der Datenübermittlungen in die USA wurde mit nahezu identischer Begründung wie fünf Jahre später der EU-US Privacy Shield für ungültig und die Praxis für rechtswidrig erklärt.

Ging es damals und 2020 um die Rechtsgrundlage der Übermittlung in die USA, wird es künftig vor allem um die mehr als berechtigte Frage gehen, auf welcher rechtlichen Basis Facebook überhaupt personenbezogene Daten der User verarbeiten darf.

Es bleibt abzuwarten, ob sich Facebook hier ähnlich unbeeindruckt zeigt wie bei vorangegangenen Feststellungen europäischer Institutionen:

- 2018 stellte der EuGH die „gemeinsame Verantwortlichkeit“ (Art. 26 DSGVO) beim Betrieb einer Unternehmensseite fest: Damit ist jedes Unternehmen, das eine Unternehmensseite unterhält, mit Facebook gemeinsam verantwortlich. Facebook veröffentlichte daraufhin das Joint Controller Addendum. Änderungen in der ausgeübten Praxis gab es keine.
- 2019 untersagte das Kartellamt die Weitergabe von Daten zwischen WhatsApp und Facebook wegen marktbeherrschender Stellung. Ungeachtet dessen gibt es kaum Anhaltspunkte dafür, dass nicht – im gesamten Zeitraum von 2015 bis heute – die Weitergabepraxis beibehalten wurde.

Da insgesamt bei Facebook keine Bewegung oder gar substanzielle Besserung erreichbar war, erweiterten die Aufsichtsbehörden die „Frontlinien“ in Richtung der „gemeinsam mit Facebook verantwortlichen Unternehmen“:

- 2020 kritisierte der Landesdatenschutzbeauftragte Baden-Württembergs, Dr. Stefan Brink, die Auftritte öffentlicher Einrichtungen in den sozialen Medien und verlangte Unterlassung.
- 2021 forderte der Bundesdatenschutzbeauftragte Ulrich Kelber die Abschaltung derartiger Auftritte bis zum 31. Dezember 2021.

Ergänzend kündigten die Aufsichtsbehörden der Länder Prüfungen im Rahmen des transatlantischen Datenverkehrs bei den nicht-öffentlichen Verantwortlichen, das heißt den Unternehmen der Privatwirtschaft, an. Diese Prüfungen werden auch und insbesondere Unternehmensseiten auf Facebook oder sonstigen, in gleichem Maß betroffenen Anbietern von sozialen Medien betreffen.

Die Macht der sozialen Medien

Solange es an Lösungen fehlt, bleibt die Marktmacht von Facebook ungebrochen und die Zahlen beeindruckend:

- 86 Mrd. € Jahresumsatz 2020:
  ein Zuwachs von mehr als 12.200 % seit 2009.
- 1,9 Mrd. täglich aktive User:
  ein Zuwachs von mehr als 2.000 % seit 2009.
- 2,9 Mrd. monatlich aktive User:
  ein Zuwachs von mehr als 1.100 % seit 2009.
- Ca. 1 Stunde am Tag verbringt ein User im Durchschnitt auf Facebook.
- Ca. 8 Mal am Tag ruft ein User im Durchschnitt Facebook.
- 63 % der deutschen Internet-User nutzen Facebook, das sind knapp zwei Drittel.
- 68 % der deutschen Internet-User zwischen 20 und 29 Jahren nutzen Facebook.

- 44 % der User geben an, dass Facebook ihr Konsumverhalten beeinflusst.
- 26 % der User, die auf eine Anzeige geklickt haben, geben an, einen Kauf getätigt zu haben. Ein User klickt durchschnittlich elf Anzeigen im Monat an.
- Knapp drei Viertel der deutschen Großunternehmen haben eine Unternehmensseite bei Facebook.
- Knapp zwei Drittel der deutschen kleinen und mittelständischen Unternehmen haben eine Unternehmensseite bei Facebook.

Diese Zahlen sind unbestritten mehr als gute Gründe für ein Unternehmen, eine Unternehmensseite auf Facebook zu betreiben, zumal es keine adäquate europäische und datenschutzgerechte Alternative gibt. Dem gegenüber steht das relativ abstrakte Risiko für die Rechte und Freiheiten betroffener Personen.

Wie die Praxis zeigt, sind datenschutzrechtliche Argumente und die gegebenen Mittel wenig und selten geeignet, um derart effiziente Maßnahmen des Marketings – unabhängig davon, ob öffentlicher oder nicht-öffentlicher Art – faktisch verhindern zu können. Realität ist auch: Die hieraus entstehenden Risiken für die Rechte und Freiheiten betroffener Personen können beim Betrieb einer Unternehmensseite auf Facebook aktuell nicht auf ein rechtlich zulässiges Niveau reduziert werden.

Dies bedeutet jedoch im Umkehrschluss nicht, dass datenschutzrechtliche Aspekte beim Betrieb der Seite außer Acht gelassen werden könnten: Wenn der Betrieb der Seite aus Sicht des Unternehmens unabdingbar ist, sollten – nicht zuletzt auch im Hinblick auf die zu erwartenden Prüfungen – Maßnahmen ergriffen werden, um das Risiko aus datenschutzrechtlicher Sicht so weit wie möglich zu reduzieren.

Risiken reduzieren

Nachfolgend möchten wir Ihnen beispielhaft einige Maßnahmen darstellen, die bei der Nutzung sozialer Medien im Rahmen einer Gesamtkonzeption berücksichtigt werden sollten. Hierzu gehören u. a.

- redaktionelle Festlegungen und Maßnahmen,
- Festlegung von Inhalten,
- Darstellung der Kommunikationswege,
- Definition und Etablierung organisatorischer Maßnahmen,
- Definition und Etablierung entsprechender innerbetrieblicher Prozesse.

Auch wenn diese Maßnahmen das zugrundeliegende Problem nicht vollständig auflösen können: Positiv stimmt das aktuelle Augenmaß in der Prüfungspraxis. Seitens der verantwortlichen Behörden wird die Nutzungsrealität durchaus gesehen. Die Suche nach pragmatischen Lösungen scheint Vorrang vor dem Sanktionieren zu haben.

Allerdings ist die Geduld der Aufsichtsbehörden – zumindest mit den öffentlichen Verantwortlichen – erschöpft: „Ein längeres Abwarten ist mir angesichts der fortdauernden Verletzung des Schutzes personenbezogener Daten nicht möglich. Sofern Sie eine Fanpage betreiben, empfehle ich Ihnen nachdrücklich, diese bis Ende des Jahres abzuschalten. Ab Januar 2022 beabsichtige ich – im Interesse der betroffenen Bürgerinnen und Bürger – schrittweise von den mir … zur Verfügung stehenden Abhilfemaßnahmen Gebrauch zu machen“, so der Bundesbeauftragte in seiner Mitteilung an die Ministerien und Behörden. Es ist anzunehmen, dass diese Deutlichkeit auch den nicht-öffentlichen Verantwortlichen, also privaten Unternehmen, in nicht allzu ferner Zukunft zuteilwerden wird.

Als Datenschutzbeauftragte sehen wir, dass ein Verzicht auf die Nutzung sozialer Medien für die meisten Unternehmen keine Option ist.

Eine 100-prozentige Rechtssicherheit können auch wir als DZ CompliancePartner nicht bieten; de facto gibt es sie auch nicht. Aber die Erfahrung aus über 100 Datenschutzmandaten hat uns gelehrt, dass ein verantwortungsbewusster und dokumentierter Umgang mit Datenschutzrisiken eine wirksame und auch aufsichtskonforme Vorgehensweise ist.

Fazit

Soziale Medien und Datenschutz scheinen aktuell unvereinbar – trennen lassen sich die Themen allerdings auch nicht. Dieses Spannungsfeld lässt sich auf absehbare Zeit nur pragmatisch lösen. Ansatzpunkte sind eine hohe Bewusstheit und eine prüfungsorientierte Dokumentation. ▬

AUTOR UND ANSPRECHPARTNER

Björn Veit
Analyst Informationssicherheit & Datenschutz,
E-Mail: bjoern.veit@dz-cp.de

▶ **WpHG-Compliance**

Marktmissbrauch – ein Praxisbericht

Die Herausforderungen der Marktmissbrauchsüberwachung am Beispiel der CureVac-Aktie

Die Überwachung von Marktmissbrauch erfolgt auf mehreren Ebenen des Wertgeschäftes.

Die BaFin und die Handelsüberwachungsstellen übernehmen aus einer übergeordneten Perspektive die Überwachung sämtlicher Wertpapiertransaktionen. Dort laufen die Daten aller Geschäfte zusammen.

Unterhalb dessen ist darüber hinaus auf der untergeordneten Ebene verpflichtet, , die Wertpapiergeschäfte, die über sie abgewickelt werden, systematisch zu überwachen. Der Blickwinkel auf die Transaktionsdaten ist auf dieser Ebene deutlich eingeschränkt, da die Bank regelmäßig nur die eigene Seite des Geschäfts (Kauf oder Verkauf ihrer Kunden) kennt.

Sofern eine Bank die Wertpapiergeschäfte nicht selbst an einem Handelsplatz ausführt, sondern eine weitere Bank, eine Zentralbank oder einen Wertpapierdienstleister dazwischen einschaltet, werden die gleichen Wertpapieraufträge von diesen ebenfalls systematisch analysiert. Auf dieser mittleren Ebene erfolgt die Überwachung gleichwohl immer mit der Perspektive der zur Verfügung stehenden Daten – aber dort bereits mit einen breiteren „Sichtfeld" aller verarbeiteten Wertpapiergeschäfte gegenüber der unteren Ebene.

Inhaltlich erstreckt sich die Überwachungspflicht auf drei Bereiche:

- Marktmanipulation,
- Insidergeschäfte,
- die unrechtmäßige Offenlegung von Insiderinformationen. (Erwägungsgrund 7 der MAR)

In diesem Artikel soll auf die Überwachung von Insidergeschäften an einem Beispiel der jüngeren Vergangenheit näher eingegangen werden.

Definition und Hintergründe des Insiderhandelsverbotes

Was genau ist ein Insidergeschäft?

„Das wesentliche Merkmal von Insidergeschäften ist ein ungerechtfertigter Vorteil, der mittels Insiderinformationen zum Nachteil Dritter erzielt wird, die diese Informationen nicht kennen, und infolgedessen in der Untergrabung der Integrität der Finanzmärkte und des Vertrauens der Investoren." (Erwägungsgrund 23 der MAR)

Im Wesentlichen ist eine Insiderinformation durch zwei Kriterien definiert:

1. eine (noch) nicht öffentlich bekannte (präzise) Information,
2. die bei Bekanntwerden den Kurs der Aktie beeinflussen wird.

In Art. 7 MAR ist die Insiderinformation genau definiert und weitere ausführliche Informationen sind im Emittentenleitfaden der BaFin im Modul C zu finden. (https://www.bafin.de/DE/Aufsicht/BoersenMaerkte/Emittentenleitfaden/Modul3/Kapitel1/Kapitel1_2/kapitel1_2_node.html)

Die BaFin schreibt hierzu auf ihrer Internetseite: „Insiderinformationen zu nutzen ist verboten und strafbar. Um Insiderhandel auf die Spur zu kommen, wertet die Wertpapieraufsicht Daten über alle Wertpapiergeschäfte aus, die zum Beispiel Banken melden müssen; sie analysiert zudem Ad-hoc-Mitteilungen und geht Hinweisen Dritter nach.

Ein Insider weiß von nicht öffentlich bekannten Umständen rund um börsennotierte Unternehmen, die sich erheblich auf den Preis auswirken können – etwa weil er aufgrund seines Berufs an diese Insiderinformation gelangt ist. So kann eine Insiderinformation das Wissen darum sein, dass bei einem börsennotierten Unternehmen eine Kapitalmaßnahme oder der Erwerb einer wesentlichen Beteiligung bevorstehen.

Doch jeder, der seine Insiderkenntnisse für sich oder andere verwendet und daraufhin Wertpapiere kauft oder verkauft bzw. daraufhin schon aufgegebene Aufträge ändert oder storniert, macht sich strafbar – unabhängig davon, auf welche Weise er

von der Insiderinformation erfahren hat. Verboten ist es auch, einem anderen eine Insiderinformation unbefugt weiterzugeben, ihn auf der Grundlage einer Insiderinformation zum Kauf oder Verkauf eines Wertpapiers zu verleiten oder ihm eine entsprechende Empfehlung zu geben." (https://www.bafin.de/DE/Aufsicht/BoersenMaerkte/Marktmissbrauch/Insiderueberwachung/insiderueberwachung_node.html)

Transparenzpflicht (Ad-hoc-Publizität gemäß Art. 17 MAR)

Um die Fälle zu reduzieren, in denen kursbeeinflussende Informationen nur einem kleinen Kreis bekannt sind, besteht die Verpflichtung, solche Informationen unverzüglich offenzulegen.

„Zweck der Ad-hoc-Publizitätspflicht ist es, einen gleichen Informationsstand der Marktteilnehmer durch eine schnelle und gleichmäßige Unterrichtung des Marktes zu erreichen, damit sich keine unangemessenen Kurse aufgrund fehlerhafter oder unvollständiger Unterrichtung des Marktes bilden. Die Ad-hoc-Publizitätspflicht dient daher dem Interesse des gesamten Anlegerpublikums, sichert die Funktionsfähigkeit des Kapitalmarktes und schafft gleiche Chancen durch Transparenz. Die Pflicht zur Ad-hoc-Publizität ist gleichzeitig eine wichtige Präventivmaßnahme gegen den Missbrauch von Insiderinformationen." (https://www.bafin.de/DE/Aufsicht/BoersenMaerkte/Emittentenleitfaden/Modul3/Kapitel1/Kapitel1_3/Kapitel1_3_1/kapitel1_3_1_node.html)

Beispielfall CureVac Juni 2021

Nun ist eine Ad-hoc-Meldung einer Aktiengesellschaft an sich nichts Besonderes und Kursbewegungen nach einer solchen Meldung sind ebenfalls nichts Ungewöhnliches.

Vor dem Hintergrund der aktuellen SARS-CoV-2-Epidemie erlangte die Ad-hoc-Meldung des Impfstoffentwicklers CureVac AG ein größeres Interesse in der Öffentlichkeit.

Die Ad-hoc-Meldung vom 16. Juni 2021 enthielt eine Information zu einem Studienergebnis, das nicht die erhoffte Wirksamkeit gegen den SARS-CoV-2-Erreger erbrachte. Von den Marktteilnehmern wurde diese Veröffentlichung überwiegend negativ aufgenommen, was zu einem erheblichen Kursverlust der Aktie führte.

In der Presse wurde am 21. und 22. Juni 2021 darüber berichtet, dass die BaFin Untersuchungen zu möglichen Insidervergehen im Zusammenhang damit eingeleitet habe.

Nun ist auch das nichts Ungewöhnliches, denn wie oben schon beschrieben ist es eine der laufenden Aufgaben der BaFin, das Marktgeschehen auf verbotene Geschäfte im Zusammenhang mit Ad-hoc-Mitteilungen zu analysieren. Die BaFin (und die Handelsüberwachungsstellen der Börsen) können hierbei auf sämtliche Geschäfte zugreifen.

Konkrete Überwachungsansätze auf Ebene der Bank

Wie stellt sich nun die Überwachung aus der Perspektive einer depotführenden Bank dar?

Nicht nur auf Ebene der Bank, sondern ganz grundsätzlich besteht die Herausforderung bei der systematischen Marktmissbrauchsüberwachung darin, dass zunächst nur Daten über Wertpapieraufträge vorliegen. Über eine mögliche strafbare Motivation des Auftraggebers gibt es keinerlei Informationen. Um eine sinnvolle Überwachung überhaupt durchführen zu können, müssen daher zunächst aus allen Transaktionen diejenigen herausgefiltert werden, bei denen es möglicherweise „nicht mit rechten Dingen vor sich gegangen ist".

Diese Aufgabe wird wegen der Vielzahl von Transaktionen in der Regel durch ein IT-gestütztes System durchgeführt. Das System benötigt eine Vorgabe – einen Ausgangspunkt –, nach welchen Kriterien es bestimmte Wertpapiergeschäfte anzeigen soll.

Die Insiderüberwachung im Zusammenhang mit einer Ad-hoc-Meldung kann nun aus zwei Richtungen erfolgen.

A. Ausgangspunkt: **Ad-hoc-Meldung** und darauffolgender Untersuchung aller in diesem Wert stattgefundenen Transaktionen auf Kenntnis über mögliche Insidersituation des Auftraggebers für dieses Wertpapier

oder

B. Ausgangspunkt: **Kenntnis über mögliche Insidersituation** eines Auftraggebers für ein bestimmtes Wertpapier (Emittenten) und darauffolgende Untersuchung, ob ein Handel im Zusammenhang mit einer Ad-hoc-Meldung erfolgt ist.

Diese beiden Untersuchungsrichtungen klingen zunächst identisch, unterscheiden sich jedoch erheblich in Untersuchungsaufwand und Trefferwahrscheinlichkeit.

Am Beispiel der oben genannten Ad-hoc-Meldung der CureVac-Aktien stellt sich diese Situation wie folgt dar: >

Variante A

In Variante A werden zunächst alle Käufe, Verkäufe, Auftragserteilungen, Limitänderungen, Stornierungen in der CureVac-Aktie im Überwachungssystem angezeigt, die in einem bestimmten Zeitraum (Stunden, Tage, Wochen) vor der Ad-hoc-Meldung im System vorhanden sind (ab der Veröffentlichung handelt es sich nicht mehr um eine Insidersituation).

Alle diese Geschäfte müssen nun manuell daraufhin untersucht werden, ob es aus Sicht der Bank Hinweise darüber gibt, dass dieses Geschäft unter Ausnutzung einer nicht öffentlichen Information getätigt worden ist.

Im Falle der CureVac-Aktie zeigten sich in den Kursverläufen vor der Ad-hoc-Meldung vom 16. Juni 2021 zwei weitere auffällige Handelstage. Jeweils am 8. und am 11. Juni 2021 zeigten sich an den Börsen bereits erhöhte Verkaufsumsätze. Wir haben daher unser Überwachungssystem sämtliche Transaktionen vom 7. bis zum 16. Juni 2021 auswerten lassen und uns alle Geschäfte mit der CureVac-Aktie anzeigen lassen. Auch in diesen bankindividuellen Überwachungslisten zeigte sich das gleiche Bild der erhöhten Umsätze am 8. und 11. Juni 2021.

Unsere weitergehende Recherche ergab, dass es sich hierbei nicht um „massenhafte" Insidergeschäfte handelte, sondern dass es in der Presse am 8. und am 11. Juni 2021 erste Hinweise gegeben hatte, dass die Erwartungen einer baldigen Zulassung eines Impfstoffes unklar seien.

Aus dem Handelsverhalten ergab sich daher kein Insiderverdacht, da es schon vor der Ad-hoc-Meldung öffentlich verfügbare Informationen gab, die eine Verkaufsentscheidung plausibel machten.

Zusätzlich wurden sämtliche angezeigten Transaktionen daraufhin geprüft, ob aus der Kundenbeziehung eine Verbindung zur Firma CureVac bekannt ist. Dies konnte besonders bei regionalen Banken in der Nähe des Sitzes der Firma relevant sein.

Auffälligkeiten, die den Verdacht eines Insidergeschäfts nahelegten, ergaben sich auch hieraus nicht.

Hierzu muss darauf hingewiesen werden, dass die Bank bei der Analyse der angezeigten Treffer nicht zu einer weitergehenden „detektivischen" Nachforschung verpflichtet ist. Es genügt, wenn die Beurteilung anhand der vorliegenden Tatsachen erfolgt.

Variante B

Bei Variante B setzt die gezielte Überwachung bereits viel früher an und nutzt hierzu Werkzeuge der gezielten Insiderüberwachung.

Gemäß Art. 29 Abs. 1 der delVO 565/2017 muss die Bank im Rahmen der Überwachung der Wertpapiergeschäfte der eigenen Mitarbeiter angemessene Vorkehrungen treffen, um zu verhindern, dass Mitarbeiter Insidergeschäfte tätigen. Zu diesen Vorkehrungen zählt eine Informationspflicht durch jeden Mitarbeiter an die Compliance-Funktion über bekannte potenzielle Insidersachverhalte (siehe auch MaComp BT 2.3 Nr. 2).

Solche Informationen können sich aus der Geschäftsbeziehung zu Einzelpersonen oder zu Firmenkunden ergeben. Beispielsweise aus dem Beratungsgespräch mit einem Vorstand oder sonstigem Entscheider einer Aktiengesellschaft (Insider gemäß Art. 18 MAR) oder der Kreditvergabe für eine börsennotierte Firma und vielen weiteren Szenarien. Üblicherweise führt die Compliance-Funktion regelmäßig konkrete Abfragen bei den Mitarbeitern durch, ob ihnen potenzielle Insidersituationen bekannt sind.

Sofern dies der Fall ist, müssen diese Situationen einer systematischen Überwachung zugeführt werden.

Dies geschieht mithilfe gezielter Überwachungslisten („watchlist").

Durch diese Listen können gezielt alle Transaktionen einer Aktie angezeigt werden, wenn für diese Aktiengesellschaft eine potenzielle Insidersituation bekannt ist. Eine Überwachung ist hier übrigens inklusive Underlying möglich, also inklusive Derivaten, deren Basiswert die Aktie ist.

Sofern sich die bekannt gewordene Insidersituation auf eine konkrete Person bezieht, können alle Geschäfte dieser Person auf einer gesonderten Überwachungsliste angezeigt werden. Diese Überwachungsliste ermöglicht insbesondere die Überwachung der Indizien aus dem Teil B der Anlage zur MAR (informationsgestützte Marktmanipulation), ist aber auch ein wirksames Mittel zur gezielten Überwachung sonstiger personenabhängiger Insidersachverhalte.

Und natürlich können beide Faktoren auch kombiniert werden und gezielt nur die Wertpapiergeschäfte einer Person in einem bestimmten Wert angezeigt werden.

Sofern dann zukünftig auf den erstellten Überwachungslisten Wertpapiergeschäfte angezeigt werden, ist bei der Beurteilung sofort bekannt, aus welchem Grund der Eintrag auf der

AUTOR UND ANSPRECHPARTNER

Marc Linnebach
Leiter WpHG-Compliance,
E-Mail: marc.linnebach@dz-cp.de

Überwachungsliste erfolgt ist, und das Wertpapiergeschäft kann vor diesem Hintergrund bewertet werden.

Für den Beispielfall der CureVac-Aktie wäre daher nur dann ein Treffer auf der Liste, wenn vorab im Hause bekannt wäre, dass ein Kunde bei CureVac (in einer entscheidungsrelevanten Position) arbeitet oder in einer sonstigen Insidersituation zu CureVac steht.

Um den **Unterschied der zwei Varianten A und B** nochmals zu verdeutlichen:

In Variante A erhält man zunächst sämtliche Wertpapiergeschäfte, die in einem zeitlichen Zusammenhang mit einer Adhoc-Meldung auftreten. All diese Geschäfte müssen dann bewertet werden und die Beurteilung muss dokumentiert werden. Die Beurteilung hat danach zu erfolgen, ob Umstände erkennbar sind, dass ein Geschäft auf einer Insidersituation basiert.

In Variante B erhält man lediglich diejenigen Wertpapiergeschäfte, bei denen die Umstände bereits bekannt sind, dass möglicherweise eine Insidersituation bestehen könnte. Nur diese Geschäfte müssen dann entsprechend bewertet werden und die Beurteilung muss dokumentiert werden.

Fazit

In der täglichen Arbeit der Trefferbearbeitung sind die meisten der zur Beurteilung angezeigten Treffer sogenannte „Fehlanzeigen" oder „false positives". Die Beurteilung dieser Treffer ergibt also keinen begründeten Verdacht. Eine Verdachtsmeldung an die BaFin ist daher relativ selten. Dennoch bedeutet jeder angezeigte Treffer viel Aufwand, da er bewertet und dokumentiert werden muss. Umso wichtiger ist eine risikoorientierte Vorgehensweise, die sicherstellt, dass nur diejenigen Wertpapiergeschäfte angezeigt werden, bei denen sich eine weitergehende Beurteilung lohnt.

Wir nutzen dieses Überwachungssystem sowohl für die Mandate, bei denen wir die Aufgabe des Compliance-Beauftragten übernommen haben, als auch für die Mandate, für die wir nur die Trefferbeurteilung (MAR kompakt PLUS) zur Entlastung der Compliance-Funktion durchführen. Aus dieser Erfahrung von Tausenden von Geschäften täglich halten wir den Ansatz der Variante A für wenig zielführend, da sie eine Überwachung nach einem „Gießkannenprinzip" darstellt.

Die Variante B nutzt effizient die sowieso erforderlichen Überwachungswerkzeuge und setzt so das maßgebliche Entscheidungskriterium, ob es eine mögliche Insidersituation gibt, an die erste Stelle. ▬

▶ Online-Seminar (kostenfrei)

„Nachhaltigkeitsrisiken verstehen und managen“

Das Risikomanagement stellt sich neu auf: Das Thema Nachhaltigkeit schlägt mit Macht auf allen Ebenen durch. Und das ist auch richtig so. Wer könnte heute noch guten Gewissens Nachhaltigkeitsrisiken ignorieren. So kann die Veränderung im Risikomanagement als Chance verstanden werden. Immerhin gilt es, Zukunft zu gestalten.

In einem für Sie kostenfreien Online-Seminar werden die regulatorischen Implikationen und Umsetzungserfordernisse vorgestellt und diskutiert. Sie erhalten Einblicke in unsere Umsetzungspraxis, unterlegt mit vielen Fallbeispielen und konkreten Hilfestellungen.

6. Oktober 2021
4. November 2021

Für wen:	Verantwortliche für das Risikomanagement Compliance-Beauftragte Nachhaltigkeits-Beauftragte
Nutzen:	Vorstellung der Implikationen und Umsetzungserfordernisse Einblicke in die Umsetzungspraxis Konkrete Hilfestellungen
Ziel:	**Wir möchten aufzeigen, dass das Management von Nachhaltigkeitsrisiken nicht nur notwendig, sondern auch machbar ist.**
Inhalte:	I. Nachhaltigkeit im Bankensektor II. Sustainable Finance im Fokus der Aufsicht – Risikomanagement ▷ Anforderungen – Risikomanagement ▷ Umsetzung – Risikomanagement ▷ Ausblick III. Unterstützungsangebote
Referent:	Axel Hofmeister, Jörg Scharditzky

Termine:	**6. Oktober 2021, 11:00–12:00 Uhr** alternativ **4. November 2021, 11:00–12:00 Uhr**
Ansprechpartner:	Axel Hofmeister, axel.hofmeister@dz-cp.de Jörg Scharditzky, joerg.scharditzky@dz-cp.de
Anmeldung:	wissen@dz-cp.de Bitte geben Sie Ihren Terminwunsch (6.10.21 bzw. 4.11.21) an. Mit der Bestätigungsmail erhalten Sie die Einwahldaten.
Betreff:	Online-Seminar Nachhaltigkeitsrisiken

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 Internen Revisionen unserer Kunden können auf eigene Prüfungshandlungen verzichten: Die durchgeführte Revisionstätigkeit der DZ CompliancePartner genügt den Anforderungen gemäß MaRisk AT 4.4.3 und BT 2.

Seit der letzten Berichterstattung in der Point of Compliance (1/2021, S. 22) wurden entsprechend der Jahresprüfungsplanung 2021 vier weitere Prüfungen abgeschlossen. Die Berichte zu den Bereichen „MaRisk-Compliance“ und „WpHG-Compliance“ wurden als dienstleistungsbezogene Berichte den Kunden mit der entsprechenden Auslagerung zur Verfügung gestellt.

Des Weiteren wurden Berichte zu den Prüffeldern „Unternehmenssteuerung – Vertragswesen & Interne Compliance“ und „Produktentwicklung und -pflege“ abgeschlossen und, da nicht dienstleistungsbezogen, intern veröffentlicht.

Die Quartalsberichte zum ersten und zweiten Quartal 2021 der Internen Revision wurden fristgerecht erstellt und den Kunden zur Verfügung gestellt.

Darüber hinaus wurden turnusgemäß Follow-up-Quartalsberichte für das erste und zweite Quartal 2021 erstellt und der Geschäftsführung der DZ CompliancePartner vorgelegt. In den Follow-up-Berichten wird die Abarbeitung der von internen und externen Prüfern getroffenen Maßnahmen bzw. Empfehlungen dokumentiert. Offene Punkte werden durch die Interne Revision konsequent nachgehalten.

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

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

Wirtschaftliche Lage

Das Halbjahresergebnis der DZ CompliancePartner GmbH liegt bei +1.422 T€ und damit klar über Plan. Die Erlöse lagen 3 % über Plan, der Aufwand 9 % unter Plan. Es wird erwartet, dass die Erlöse im zweiten Halbjahr auf Plan liegen werden, die Kosten sich hingegen wegen diverser Projektaufwendungen spürbar über Plan entwickeln werden und so die derzeitige Planunterschreitung zumindest zum Teil aufzehren werden. Insgesamt wird mit einem positiven Jahresergebnis leicht über Plan gerechnet. ▬

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

Neue Telefonnummern

Wir wollen für Sie einfacher erreichbar sein. Ein Ansprechpartner – eine Durchwahl: egal welcher Standort, egal ob mobil oder Festnetz. Die Durchwahl Ihrer Ansprechpartnerin bzw. Ihres Ansprechpartners erhalten Sie im Laufe des Oktober.

069 580024-XXX