DZ CompliancePartner

Point of Compliance

Das Risikomanagement-Magazin für
unsere Kunden und Geschäftspartner

AUSGABE 3/2021

Bündelung der Kräfte

ab Seite 4

Wozu Spezialisten gut sind

ab Seite 8

Anforderungen an Monitoring-Systeme in der Geldwäscheprävention

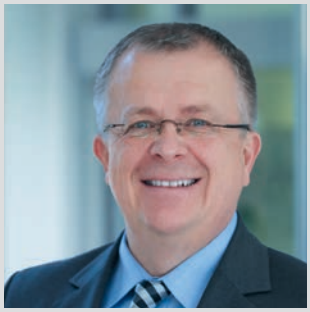
IMPRESSUM

Point of Compliance
Das Risikomanagement-Magazin für unsere Kunden und Geschäftspartner, Ausgabe 27, 3/2021
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), 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 580024-0, Telefax 069 580024-900, E-Mail: poc@dz-cp.de
Weitere Autoren dieser Ausgabe: Martin Hierlemann, Kevin Lohmann, Christian Nahmmacher, Jens Saenger, Lars Schinnerling, Michael Switalla, Sarah-Lena Tiburtius, Thomas Wagener

Bildnachweise: DZ CompliancePartner GmbH, iStockphoto (Titel)
Gestaltung: Ralf Egenolf
Druck: odd GmbH & Co. KG · Print und Medien, www.odd.de

Redaktionsschluss: 15. November 2021
Auflage: 2.600 Exemplare
Die aktuellen Mediadaten finden Sie im Internet unter www.dz-cp.de/poc



Jens Saenger
Sprecher der Geschäftsführung

Es ist gut zu sehen, wie sich Menschen beistehen. Das gilt im Großen – etwa wenn, wie im Ahrtal, von überall her Hilfswillige kommen und anpacken. Aber auch im Kleinen, wie wir es im Verlauf der Pandemie in der Zusammenarbeit mit Ihnen, unseren Kunden, durchweg erlebt haben.

Ob nun in Form der Nachbarschaftshilfe oder – wie in unserem genossenschaftlichen Kosmos – der Bündelung der Kräfte: Die Gemeinschaft macht stark.

Ich glaube fest daran, dass wir – als Dienstleister in der Genossenschaftlichen FinanzGruppe – nur dann unsere Möglichkeiten voll ausschöpfen, wenn wir uns nicht im Gegeneinander verlieren, sondern uns immer wieder gemeinsam fragen: Was hilft Ihnen, der Bank vor Ort?

In diesem Sinne wünsche ich Ihnen eine anregende Lektüre und ruhige Festtage im Kreise Ihrer Lieben,

Ihr Jens Saenger

Bündelung der Kräfte

Wozu Spezial

Die „Bündelung der Kräfte“ ist mehr als eine Worthülse. Sie ist beispielsweise Ausdruck einer vertrauensvollen Zusammenarbeit, um am Ende die Position der Banken vor Ort zu stärken. Die AWADO GmbH WPG StBG (AWADO) übernimmt die Sparte „IT-Revision“ von der DZ CompliancePartner GmbH.

Unter der Überschrift „Bündelung der Kräfte im Verbund“ hat der BVR im Auftrag der gesamten Genossenschaftlichen FinanzGruppe eine Überprüfung etwaiger Doppelarbeiten im Verbund angestoßen. Ziel dieser Initiative ist, die Anzahl der Überschneidungen im Leistungsangebot zum Vorteil der Volksbanken Raiffeisenbanken, der PSD Banken, Sparda Banken sowie der Spezialbanken zurückzufahren und die Qualität der Dienstleistungserbringung zu befördern.

Die Position der Bank vor Ort stärken

Letztlich steht die Bündelung der Kräfte für die Bereitschaft, sich in einer Kooperation gemeinsam zum Nutzen der Mitglieder zu engagieren.

Jeder Dienstleister in der Gruppe hat zunächst nur eine Aufgabe: die Position der Bank vor Ort zu stärken. Das bedarf selbstverständlich der unternehmerischen Stabilität. Aber im Vordergrund steht, dass die Bank das Angebot erhält, das ihr wirklich hilft. Nicht mehr, nicht weniger.

Das gilt einmal mehr für das regulatorische Beauftragtenwesen und auch für prüfungsnahe Dienstleistungen wie die IT-Revision, die als kundenferne Aufgabenstel-

isten gut sind

lungen kein Differenzierungskriterium gegenüber ihren Kunden darstellen.

Tatsächlich erleben wir, dass Beauftragtenthemen wie Geldwäscheprävention, Informationssicherheit, Datenschutz, MaRisk- und WpHG-Compliance auch für Endkunden immer präsenter werden. Datenschutz beispielsweise wird in manchen FinTechs nach wie vor anders ausgelegt, als der deutsche bzw. der europäische Standard das vorsehen. Kunden nehmen das wahr und reagieren kritisch. Fakt ist jedoch: Jede Bank muss hier gut aufgestellt sein. Das ist ein Hygienefaktor und kein Motivator im engeren Sinn. Gute Compliance ist zwingende Voraussetzung einer jeden Bank, aber kein Alleinstellungsmerkmal.

Abgrenzung regulatorisches Beauftragtenwesen und IT-Revision

Das Beauftragtenwesen mit seinem präventiven Ansatz ist in der First und vor allem Second Line of Defense angesiedelt: Risiken werden auf der operativen Ebene – durch jeden einzelnen Mitarbeiter – identifiziert, bewertet und bearbeitet. Diese Ebene kontrolliert nicht nur, sondern unterstützt die Bank, insbesondere macht sie Lösungsvorschläge zur Einrichtung, Anwendung und Verbesserung der Compliance-Risiken.

Dagegen ist die IT-Revision als Teil der Internen Revision der Third Line of Defense zuzuordnen. Sie ist eine unabhängige Instanz, die das Risikomanagement – also auch die Beauftragten – kontrolliert.

Wir haben es hier mit einer anderen Perspektive zu tun: Im Namen – IT-Revision – klingt es an: Es ist eine rückschauende Überprüfung, während das Beauftragtenwesen einem präventiven Blickwinkel folgt.

Eine Gemeinsamkeit ist, dass sowohl die Bedeutung des Beauftragtenwesens als auch die der IT-Revision steigt. >

AUTOR UND
ANSPRECHPARTNER

Jens Saenger
Geschäftsführer
DZ CompliancePartner GmbH,
E-Mail: jens.saenger@dz-cp.de

Die IT-Revision wird immer wichtiger, weil das Prüffeld „IT“ immer wichtiger wird. Die Anforderungen an die Prüfungen werden weiter steigen, sowohl was den Umfang als auch was die Qualifizierung und die systemische Unterstützung betrifft. Fakt ist: Wenn die IT-Revision auch künftig effektiv und effizient dargestellt werden soll, dann bedarf es eines nicht unerheblichen Aufwands – egal, wer sich dessen annimmt. Es liegt im Interesse aller, Doppelarbeiten zu vermeiden.

Doppelarbeiten vermeiden

Genau so stellt sich die Situation im Beauftragtenwesen dar. Wir haben allein von 2019 auf 2020 einen Zuwachs von 50 % bei Compliance-relevanten Neuerungen verzeichnet. Und das ist nur die halbe Wahrheit: Auch die Sanktionen – für die Bank und für den Beauftragten – sind bei Fehlverhalten deutlich gestiegen. Erst im vergangenen Monat hat die BaFin angekündigt, eine „Aufsicht mit Biss“ werden zu wollen. Das mag man werten, wie man möchte. Unterm Strich besteht auch für das regulatorische Beauftragtenwesen eine alternativlose Notwendigkeit zur Spezialisierung.

Um all den Anforderungen gerecht zu werden, um auch die eigenen Sicherheitsinteressen zu erfüllen, müssen wir alle – als Dienstleister in der Genossenschaftlichen FinanzGruppe – uns fokussieren auf unser Spezialgebiet. Es ist unsere Aufgabe, hochkomplexe Sachverhalte kompakt darzustellen.

Dazu gehören auch IDW PS-testierte und im Verbund abgestimmte Aufsichtskonformität oder die Angemessenheit der Dienstleistungen. Wir stecken viel Know-how und Ressourcen in die Entwicklung transparenter und nachvollziehbarer Prozesse, die auch immer mehr IT-getrieben sind bzw. sein müssen. Die DZ CompliancePartner GmbH beispielsweise baut auf den Erfahrungen von über 130 Mitarbeiter*innen in über 700 Mandaten auf. Und eben dort liegt auch der Mehrwert für unsere Kunden: Je mehr Mandate wir betreuen, umso höher die Qualität und umso effizienter der Prozess.

Zusammengefasst eint die IT-Revision und das Beauftragtenwesen die Risikoorientierung und die vergleichsweise hohe Komplexität. Es trennt sie die Perspektive: einerseits die Retrospektive, andererseits der präventive Ansatz.

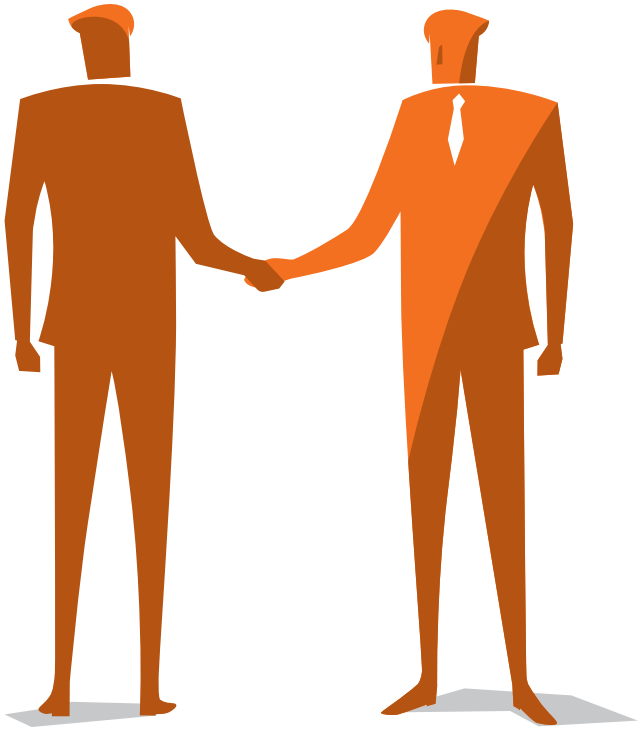
Arrondieren der Geschäftsfelder

Sowohl die AWADO als auch die DZ CompliancePartner GmbH haben bislang in ihrem Produkt-Portfolio IT-Revision angeboten.

Wir haben nunmehr der AWADO angeboten, dass die DZ CompliancePartner GmbH ihr Geschäftsfeld IT-Revision an die AWADO überträgt. Hintergrund ist, dass die IT-Revision nicht dem regulativen Beauftragtenwesen zuzurechnen ist. Und wir sind überzeugt, dass – mit Blick auf die steigenden Anforderungen – es im Interesse der Kunden liegt, die weitere Entwicklung des Geschäftsfeldes auf die AWADO zu fokussieren.

Dabei haben wir uns gemeinsam mit der AWADO auf die Fahnen geschrieben, dass der Betriebsübergang für die Kunden nahezu geräuschlos verläuft. Die übernommenen Mandate werden im gleichen Umfang und zu den gleichen Konditionen weitergeführt.

Die Bündelung der Kräfte ist keine Einbahnstraße. Wir sind bereit, selber Mandate zu übernehmen und sind im engen Austausch mit weiteren Netzwerkpartner im Verbund. Sicher können wir bereits in den nächsten Tagen hierüber berichten. Angesichts der enormen strategischen Herausforderungen, vor denen die Banken heute stehen, ist es unsere Aufgabe, die Banken bestmöglich zu entlasten. Es gilt, die jeweiligen Stärken im Verbund zu erkennen und auszubauen und unseren Teil dazu beizutragen, den Verbund als Ganzes fit für die Zukunft zu machen – im Sinne der Banken vor Ort. ▬



▶ **Geldwäscheprävention**

Aktuelle Anforderungen an Monitoring-Systeme

Die institutsspezifische Kalibrierung und auch die regelmäßige Überprüfung sowie Anpassung von Geno-SONAR© ist eine herausfordernde Aufgabenstellung. Nachfolgend werden die Anforderungen und auch Unterstützungsleistungen an das „Backtesting" von Geno-SONAR© vorgestellt.

Kreditinstitute sind verpflichtet, die mit der Ausübung ihrer Geschäftstätigkeit verbundenen Risiken in Bezug auf Geldwäsche, Terrorismusfinanzierung und strafbare Handlungen zu kennen, zu erkennen und Maßnahmen zur Prävention zu ergreifen. Die Kundenbeziehung steht hierbei im Mittelpunkt.

Die Herausforderung

Das GwG verpflichtet Institute, die Geschäftsbeziehungen kontinuierlich zu überwachen (§ 10 Abs.1 Nr. 5 GwG). Sie sind nach dem KWG verpflichtet, Datenverarbeitungssysteme zu betreiben und zu aktualisieren. Mithilfe der Datenverarbeitungssysteme sollen Geschäftsbeziehungen und einzelne Transaktionen im Zahlungsverkehr erkannt bzw. identifiziert werden, die – aufgrund des öffentlich und im Kreditinstitut verfügbaren Erfahrungswissens über die Methoden der Geldwäsche, der Terrorismusfinanzierung und über strafbare Handlungen – im Verhältnis zu vergleichbaren Fällen

- besonders komplex oder groß sind,
- ungewöhnlich ablaufen oder
- ohne offensichtlichen wirtschaftlichen oder rechtmäßigen Zweck erfolgen (§ 25h Abs. 2 KWG).

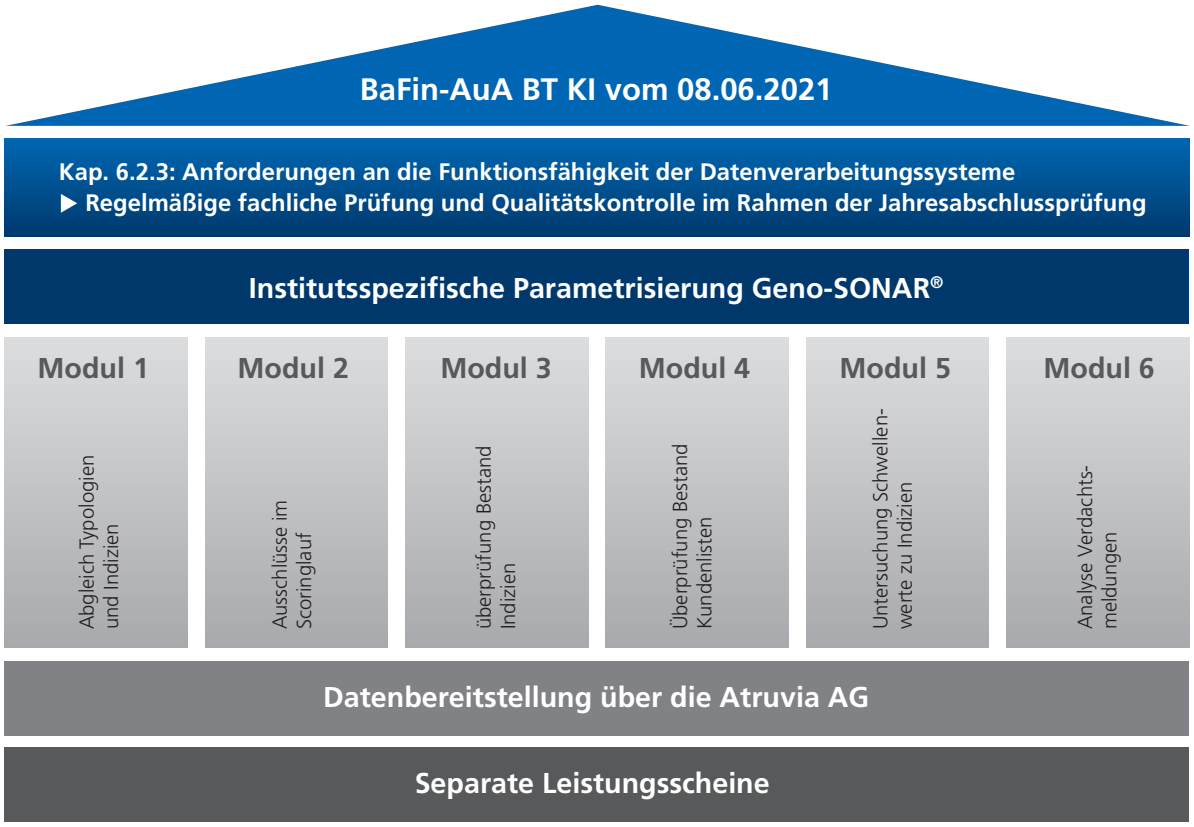
Hierfür setzt die Genossenschaftliche FinanzGruppe Volksbanken Raiffeisenbanken die von der Atruvia AG entwickelte Anwendung Geno-SONAR© ein.

Mit Veröffentlichung der BaFin-Auslegungs- und Anwendungshinweise – Besonderer Teil für Kreditinstitute (BaFin-AuA BT KI) im Juni 2021 hat die Aufsicht ihre Anforderungen an die Ausgestaltung und den Umgang mit den Monitoring-Systemen ausführlich dargelegt. Die Ausgestaltung und Steuerung der Systeme müssen danach den individuellen Gegebenheiten des Instituts Rechnung tragen. Auch die Erkenntnisse aus der institutsspezifischen Risikoanalyse müssen in das System einfließen. Die fachliche Prüfung des Monitoring-Systems ist dabei regelmäßig und anlassbezogen vorzunehmen und zu dokumentieren.

In die Monitoring-Systeme fließen automatisiert eine Vielzahl von Kunden-, Konto- und Transaktionsdaten ein, die in einem buchungstäglichen Scoring-Lauf verarbeitet werden. Grundlage dieser Verarbeitung bildet das in Geno-SONAR© integrierte Indizienmodell, das bereits im Auslieferungszustand aus mehr als 130 Indizien besteht. Mit den Indizien werden unterschiedlichste Sachverhalte berücksichtigt – von der Überprüfung des Kundenbestandes über die Betrachtung der einzelnen Umsätze bis hin zur Untersuchung des Umsatzverhaltens über vordefinierte Zeiträume oder einen Peergroup-Vergleich.

Geno-SONAR© wird seit mittlerweile 16 Jahren eingesetzt und stetig weiterentwickelt, um den gestiegenen Anforderungen an die Prävention von Geldwäsche, Terrorismusfinanzierung sowie strafbaren Handlungen Rechnung zu tragen. Mit der Weiterentwicklung von Geno-SONAR© ist aber auch die Komplexität stark gestiegen. Das korrekte Zusammenspiel zwischen Indizien, Kundensegmenten und Listen ist dabei von entscheidender Bedeutung, um eine gute Trefferqualität zu erzielen.

Daher ist sowohl die institutsspezifische Kalibrierung von Geno-SONAR© als auch die regelmäßige Überprüfung und Anpassung eine herausfordernde Aufgabenstellung. Vorrangiges Ziel sollte dabei sein, ein ausgewogenes Treffervolumen zu erreichen: Zu wenige Treffer könnten



bedeuten, dass z. B. Schwellenwerte zu hoch sind. Zu viele Treffer können darauf hindeuten, dass ein oder auch mehrere Schwellenwerte möglicherweise zu niedrig angesetzt sind – insbesondere dann, wenn die Überprüfung der Treffer keine Verdachtsmomente ergeben hat.

Backtesting Geno-SONAR©

Um Sie hierbei zu unterstützen, bieten wir Ihnen mehrere Module an, die individuell beauftragt werden können.

Zu jedem beauftragten Modul stellen wir Ihnen einen schriftlichen Bericht mit Handlungsempfehlungen zur Verfügung.

Modul 1: Abgleich des Typologienpapiers mit den vorhandenen Indizien

Ziel dieses Moduls ist es, einen Überblick zu gewinnen, inwieweit das Indizienmodell das Typologienpapier der FIU berücksichtigt. Hierzu werden jeder Typologie so weit wie möglich Indizien zugeordnet, die zu einer frühzeitigen Erkennung potenziell verdächtiger Sachverhalte geeignet sind. In Abhängigkeit vom jeweiligen Indiz können eine oder auch mehrere Typologien abgedeckt werden.

Bei der Typologienzuordnung unterscheiden wir zwischen sogenannten „harten“ und „weichen“ Typologien. Die „harten“ Typologien bieten durchaus Ansatzpunkte zur Abbildung eines verdächtigen Sachverhaltes über ein Indiz. Dagegen treten die „weichen“ Typologien vorwiegend im Kontakt zwischen Berater und Kunde auf und können somit nicht von einem Monitoring-System erkannt werden.

Beispiele:

- Ein Kunde legt auch nach wiederholter Aufforderung nur Kopien von Ausweisdokumenten vor.
- Eine Identifizierung wird verzögert bzw. der Kunde bricht das Vorhaben ab, sobald eine Identifizierung verlangt oder erweitert wird.

>

AUTOREN

Thomas Wagener
Compliance-Spezialist,
E-Mail: thomas.wagener@dz-cp.de

Christian Nahmmacher
Geldwäsche- und Betrugsprävention,
E-Mail: christian.nahmmacher@dz-cp.de

- Die Identität des wirtschaftlich Berechtigten ist nicht bzw. nur mit erheblichem Aufwand zu ermitteln.
- Ein Kunde vermeidet konkrete Angaben zu seiner Adresse oder seinen Erreichbarkeiten (z. B. lediglich Angabe von Postfächern, vage Angaben verschiedener ähnlicher Adressen).
- Ein Kunde drängt auf ungewöhnliche Weise auf die sofortige Durchführung einer (für ihn unüblichen) Transaktion.

Der Anteil der „weichen" Typologien liegt bei ca. 50 %. Daher ist neben der Parametrisierung von Geno-SONAR© auch die Sensibilisierung der Mitarbeiter von großer Bedeutung.

Modul 2: Ausschlüsse im Scoring-Lauf
Über Geno-SONAR© lassen sich zahlreiche Ausschlüsse definieren. Von entscheidender Bedeutung sind dabei Ausschlüsse, die sich nicht nur auf einzelne Kunden, sondern auf die Verarbeitung des gesamten Kundenbestandes auswirken.
Beispiele:

- Genereller Kundenausschluss (ein oder mehrere Kundensegmente und/oder Kundenlisten)
- Bankverbindungen, zu denen Umsätze generell aus dem Scoring-Lauf herausgehalten werden
- Verwendungszwecke
- Bankindividuelle Textschlüssel (vollständiger Ausschluss von Buchungen mit bestimmten Textschlüsseln)
- Bankindividuelle Primanoten (vollständiger Ausschluss einzelner Primanoten)

Da diese Parameter Veränderungen unterliegen, ist eine regelmäßige Überprüfung besonders wichtig.

Modul 3: Überprüfung des Indizienbestandes
Die Überprüfung des Indizienbestandes umfasst nicht nur eine Überprüfung der einzelnen Indizien, sondern auch der für die Trefferbearbeitung festgelegten organisatorischen Regelungen. Diese Überprüfung ist von grundlegender Bedeutung. Auch dann, wenn ein angemessenes Indizienmodell vorhanden ist, können unzureichende organisatorische Regelungen bzw. falsch vorgenommene Einstellungen dazu führen, dass Treffer zu geldwäscherelevanten Sachverhalten nicht in die tägliche Bearbeitung einbezogen werden.

Weiterhin überprüfen wir auch die Definition bankeigener Indizien. In der Vergangenheit hat sich immer wieder herausgestellt, dass fehlerhaft programmierte Indizien entweder zu keinen oder auch zu einer Vielzahl von von Treffern führen können, die keine verwertbaren Ergebnisse liefern und einen hohen Zeitaufwand bei der täglichen Bearbeitung verursachen. Indizien, die keine Treffer liefern, können dennoch korrekt programmiert sein. Auch dies sollte überprüft werden.

Über die Trefferstatistik untersuchen wir dabei auch das Treffervolumen.

Modul 4: Überprüfung des Kundenlistenbestandes
Good-Guy-Kundenlisten sind ein wichtiges Instrument, um positiv beurteilte Trefferkunden zumindest für einen befristeten Zeitraum von der Verarbeitung ein oder mehrerer Indizien auszuschließen. In diesem Zusammenhang untersuchen wir die Nutzungsintensität sowie die Steuerung der Befristungen zu den Kundenlisteneinträgen.

Eine weitere wichtige Funktion von Kundenlisten ist die Steuerung der Risikoklassifizierung. Die Zuordnung in eine Risikoklasse kann sowohl durch eine automatische

ANSPRECHPARTNER

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

Listenbefüllung mit einem entsprechend definierten Regelwerk als auch durch eine einzelfallbezogene Zuordnung erfolgen.

Falsch oder unzureichend definierte Befüllungsregeln können gravierende Folgen für die Risikoklassifizierung des Kundenbestandes haben. Daher ist eine regelmäßige Überprüfung von wesentlicher Bedeutung.

Zu berücksichtigen ist dabei auch, dass die Kriterien zur Risikoklassifizierung aus externen Quellen (z. B. EBA-Guidelines, Nationale Risikoanalyse) Veränderungen unterliegen und bereits aus diesem Grund eine regelmäßige Überprüfung erfordern.

Modul 5: Untersuchung der Schwellenwerte zu ausgewählten Indizien
Dieses Modul dient der Überprüfung, ob die innerhalb eines Indizes verwendeten, ggf. auch kundensegmentabhängigen Schwellenwerte für den unbaren In- und Auslandszahlungsverkehr sowie für den Barverkehr sachgerecht sind. Hierzu werden zu den vorliegenden Trefferumsätzen statistische Werte ermittelt und mit den im einzelnen Indiz definierten Schwellenwerten verglichen.

Modul 6: Analyse der Verdachtsmeldungen
Dieses Modul dient der Überprüfung, ob Sachverhalte aus Verdachtsmeldungen auch über ein oder mehrere Indizien erkannt wurden bzw. erkennbar gewesen wären. Hierzu ist es erforderlich, die Sachverhalte zu ausgewählten Verdachtsmeldungen zu überprüfen und Möglichkeiten zur Erstellung neuer bzw. zur Anpassung bestehender Indizien zu bewerten.

Bei der Bewertung ist zu beachten, dass z. B. eine Reduzierung des Schwellenwertes zwar zu einer früheren Erkennung eines potenziell verdächtigen Sachverhaltes führen kann, dass sich aber im Gegenzug der Anteil der falsch-positiven Treffer überproportional erhöhen kann.

Fazit

Das Monitorings-System ist ein wesentlicher Faktor bei der Bekämpfung von Geldwäsche, Terrorismusfinanzierung und strafbaren Handlungen. Eine regelmäßige fachliche Überprüfung wird in den BaFin-AuA BT KI gefordert.

Gerne unterstützen wir Sie ab Ende des ersten Quartals 2022 mit unserem Angebot bei dem durchzuführenden „Backtesting". ▬

Informationssicherheit

Lagebild 2021 der IT-Sicherheit

Mit der Bedeutung der IT steigt deren Komplexität und damit verändert sich auch die Gefährdungslage. Das BSI bezeichnet die Sicherheitslage in Deutschland als angespannt bis kritisch und empfiehlt entsprechende Gegenmaßnahmen.

Die Digitalisierung prägt uns Tag für Tag. Immer mehr Prozesse in der Bank werden automatisiert und mit anderen Prozessen vernetzt. Zahlreiche Innovationen eröffnen Potenziale für neue IT-Projekte wie z. B. die Themen künstliche Intelligenz und Blockchain. Daneben verändert sich die Arbeitswelt durch äußere Einflüsse, aktuell sehr geprägt durch die Corona-Pandemie. Entsprechend steigt die Komplexität und verändert sich die Gefährdungslage. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) berichtet deshalb u. a. jährlich über die Lage der IT-Sicherheit in Deutschland. Vor kurzem wurde der Bericht für das Jahr 2021 veröffentlicht.

Die IT-Sicherheitslage in Deutschland wird demnach als angespannt bis kritisch bezeichnet.

Anstieg bei Schadsoftware und Cyber-Erpressungen

Maßgeblichen Anteil an der Einschätzung trägt die immer schneller werdende Produktion von Schadsoftware. Im Berichtszeitraum betrug alleine der durchschnittliche tägliche Zuwachs an neuen Schadprogramm-Varianten etwa 394.000. Im Vorjahreszeitraum lag die Anzahl bei 250.000.

Aber auch die Ausweitung der Lösegelderpressung auf Basis von Cyber-Angriffen – in der Regel mit Verschlüsselungstrojanern – ist atemberaubend. Inzwischen nehmen auch Schweigegelderpressung unter Androhung der Enthüllung kompromittierender Informationen und Schutzgelderpressung unter Androhung eines DDoS-Angriffs zu (Distributed Denial of Service, bewirkt z. B. eine Überlastung bzw. Nichterreichbarkeit des Netzwerks oder der Internetseite).

Identitätsdatendiebstahl und Missbrauch bleiben insgesamt konstant, jedoch werden diese – meist über sogenannte Phishing-Mails ausgeführten – Angriffe zum Teil besser auf aktuelle Themen angepasst, um den Nutzer zur Preisgabe seiner Daten zu überreden. So nehmen die Mails häufig auf aktuelle Themen Bezug, z. B. Corona-Hilfen, Änderung der Gesetzgebung und insbesondere bei Bankkunden konkrete regionale Themen wie Fusionen und Filialschließungen.

Corona als zusätzlicher Stressfaktor in der IT-Sicherheit

Die Corona-Pandemie war überhaupt ein wichtiger Treiber, denn die Situation bot zahlreiche neue Angriffsmöglichkeiten. Allen voran konnten Angriffe via Social Engineering (Beeinflussung eines Menschen, um sein Handeln zu manipulieren) erfolgreich abgesetzt werden. Die neue Arbeitssituation im Homeoffice verunsicherte Mitarbeiter und manchmal fehlte dann auch der Kollege „gegenüber“, um die „komisch wirkende Mail“ zu besprechen. Hinzu kam der Druck, den Digitalisierungsprozess schnell zu beschleunigen, um die Handlungsfähigkeit während der Pandemie zu erhalten. So mussten mit den Kontakteinschrän-

144 MIO.
neue Schadprogramm-Varianten

+22%
gegenüber 2020:
117,4 MIO.

DURCHSCHNITTLICH
394.000
neue Schadprogramm-Varianten pro Tag
2020: 322.000

IM HÖCHSTWERT
553.000
2020: 470.000

Quelle: Die Lage der IT-Sicherheit in Deutschland 2021 (bund.de)

kungen zahlreiche Remote-Arbeitsplätze eingerichtet und neue Kommunikationssysteme genutzt werden. Entsprechend stiegen auch die Angriffe auf Videokonferenzsysteme.

Zur Erhöhung der IT-Sicherheit im Homeoffice empfiehlt das BSI folgende Maßnahmen:

- Nutzung von VPN-Verbindungen (Virtual Private Network)
- Absicherung der Zugänge durch Mehr-Faktor-Authentifizierung
- Verwaltung mobiler Endgeräte über ein MDM (Mobile Device Management)
- Awareness-Maßnahmen für Mitarbeiter
- Regelmäßige Übung von Cyber- und IT-Notfällen

Insbesondere dem letzten Punkt wurde im Bankenbereich mit der Veröffentlichung der BAIT und des dort enthaltenen neuen Kapitels 10 IT-Notfallmanagement Rechnung getragen.

IT-Sicherheit als Wettbewerbsvorteil

Das Fazit überschreibt das BSI mit „Digitalisierung braucht Sicherheit". Entwicklungen und Veränderungen in Gesellschaft und Wirtschaft müssen mit entsprechenden Sicherheitsmaßnahmen einhergehen. Die größte Bedrohung stellt derzeit die Cyber-Erpressung dar. Als größte Herausforderung wird der Umgang mit Schwachstellen in IT-Systemen genannt.

Dabei sollte Cyber- bzw. IT-Sicherheit als Wettbewerbsvorteil in den Fokus rücken. Denn: „Informationssicherheit schafft Vertrauen, und sie schafft Akzeptanz bei Verbraucherinnen und Verbrauchern." ▬

AUTOR UND ANSPRECHPARTNER

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

Hinweisgebersystem

Hinweisgeberschutzgesetz

Das Hinweisgeberschutzgesetz könnte am 17. Dezember 2021 in Kraft treten. Institute mit mehr als 249 Mitarbeiter*innen müssen danach ab 17. Dezember 2021 eine interne Meldestelle eingerichtet haben. Wichtig ist eine Umsetzung mit Augenmaß.

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.

Aktuell liegt allerdings nur ein Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz vor. Die Regelungen wurden bis zum Redaktionsschluss noch nicht in den Bundestag eingebracht, das Hinweisgeberschutzgesetz wurde daher noch nicht verabschiedet.

Dennoch macht es Sinn, sich damit auseinanderzusetzen – zumal die Umsetzung „machbar" erscheint.

Anforderungen

Der aktuelle Entwurf zum Hinweisgeberschutzgesetz (HinSchG-E) setzt die Richtlinie in deutsches Recht um. Auch die deutsche Regelung setzt – aller Voraussicht nach – die Vorgaben zu den drei Meldekanälen (intern, extern, Offenlegung) um. 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 (§ 12 Abs. 3 Nr. 4 HinSchG-E).

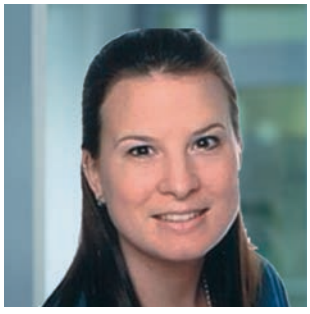
Für Unternehmen mit bis zu 249 Beschäftigten soll das Gesetz erst zum 17. Dezember 2023 in Kraft treten. Da nicht klar ist, ob diese Abgrenzung auch für Kreditinstitute gilt, ist sicherheitshalber davon auszugehen, dass die Anforderungen mit dem möglichen Inkrafttreten des Gesetzes am 17. Dezember 2021 die Pflicht zur Einrichtung interner Meldestellen umfassen.

Der Entwurf sieht weiter vor, den Anwendungsbereich zu ergänzen. 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. So können die Hinweisgeber auch Sachverhalte melden, die straf- und bußgeldbewehrt sind. Das bedeutet, dass auch Vorgänge bzw. Straftaten wie Betrug, Körperverletzung oder Belästigung an eine Meldestelle übermittelt werden können.

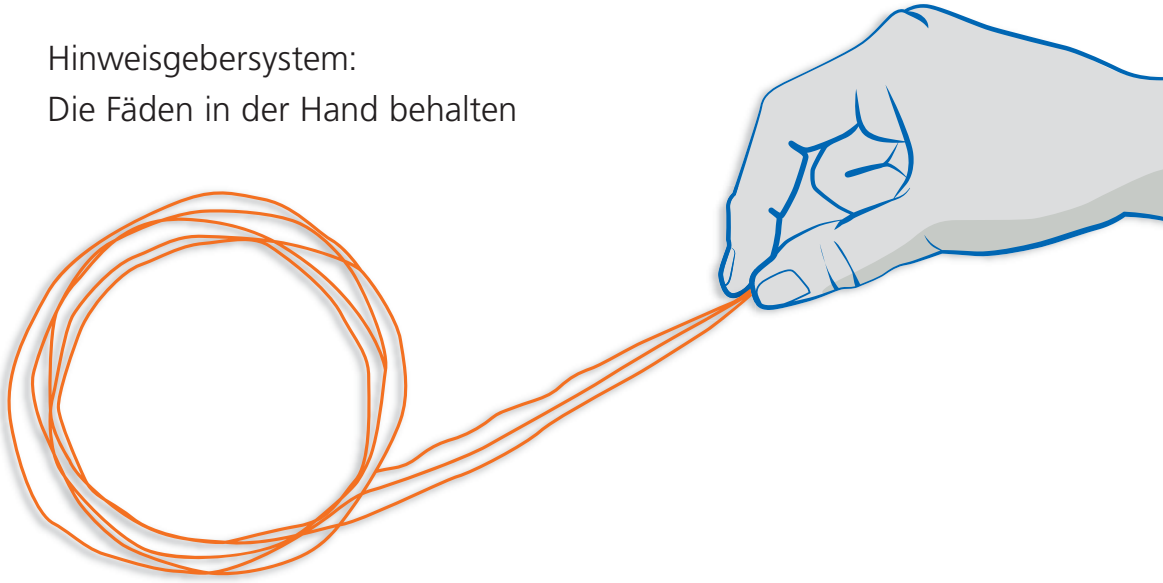
Die internen Meldestellen unterliegen dem Entwurf zufolge künftig neuen Anforderungen: So müssen diese z. B. dem Meldenden den Eingang des Hinweises bestätigen, Kontakt mit ihm halten, die Stichhaltigkeit der Meldung prüfen und angemessene Folgemaßnahmen ergreifen.

Die neuen Regelungen geben einige Anforderungen vor, die die bisherigen Vorgaben übersteigen dürften. Sollte das Hinweisgeberschutzgesetz nicht bis zum 17. Dezember verabschiedet sein, wäre das nach unserer Einschätzung kein Vorteil für die Banken. Einzelne Vorgaben der EU-Richtlinie könnten trotzdem als unmittelbar anwendbar erklärt werden.

AUTORIN UND ANSPRECHPARTNERIN



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



Umsetzung „machbar“

Wie dem auch sei: Nach unseren Erfahrungen mit Hinweisgebersystemen – im Rahmen der Auslagerung Geldwäscheprävention oder als Stand-alone-Dienstleistung – sind die zentralen Anforderungen der EU-Richtlinie vergleichsweise „einfach“ und ohne viel Aufwand umsetzbar.

Im Kern geht es heute wie künftig um die frühzeitige, transparente Aufdeckung bzw. Prävention von Missständen – bei höchster Anonymitätswahrung und arbeits- und strafrechtlichem Schutz des Hinweisgebers.

Die neuen Anforderungen der Richtlinie bzw. des deutschen Gesetzesentwurfs – u. a. zwei gleichwertig nebeneinanderstehende Meldewege (interner/externer Meldekanal), Ausweitung des sachlichen Anwendungsbereichs (straf- und bußgeldbewehrte Vorschriften) – sollten sich durch geringfügige Anpassungen in bereits bestehende Umsetzungen (bzw. Dienstleistungen von Dritten) integrieren lassen.

Fakt ist: Auch in der Genossenschaftlichen FinanzGruppe gab und gibt es meldepflichtige Vorfälle, die nicht durch den genossenschaftlichen Wertekanon verhindert wurden bzw. werden können. Ein Hinweisgebersystem erscheint deshalb nicht nur hilfreich, sondern auch notwendig.

Aber wir wissen auch, dass „meldepflichtige Vorfälle“ nicht das vornehmliche Problem der Volksbanken Raiffeisenbanken darstellen.

Fazit: Jetzt handeln – aber angemessen

Wichtig ist aus unserer Sicht deshalb:

- Das Hinweisgebersystem und die vorgesehenen Kommunikationskanäle dürfen keine Hürden darstellen, sie müssen sowohl für die Banken als auch für die Hinweisgeber einfach zu erreichen und zu bedienen sein.
- Das Hinweisgebersystem muss sicherstellen, dass sowohl die Banken als auch der Hinweisgeber jederzeit „die Fäden in der Hand“ behalten.
- Das Hinweisgebersystem muss zwingend den gesetzlichen Vorgaben entsprechen, im besten Fall nach IDW PS 331 testiert sein und vor allem die Vorgaben mit Augenmaß umsetzen. ▬

Auslagerungsmanagement

Augen auf bei der Wahl des Auslagerungsdienstleisters

Banken und Finanzdienstleistungsinstitute sind schon immer verpflichtet, bei der Wahl ihres Auslagerungspartners wählerisch und umsichtig zu sein. Die aktuellen Novellen der MaRisk und der BAIT verschärfen diese Ansprüche jedoch erheblich. Neu hinzugekommen sind jene Regularien, die im Finanzmarktintegritäts- und Stabilitätsgesetz formuliert werden.

Das Finanzmarktintegritäts- und Stabilitätsgesetz (FISG) ist die Reaktion des Gesetzgebers auf den Wirecard-Skandal. Im Fall Wirecard wurde als Defizit gesehen, dass die Befugnisse der Aufsicht vor den Toren der Auslagerungsdienstleister endeten. Das hat sich nun geändert. Dieser Artikel soll die Konsequenzen des FISG für die Banken und Finanzdienstleister sowie „Ihre" Auslagerungspartner beleuchten.

Die Novellierungen der MaRisk und der BAIT einerseits und die Verabschiedung des neuen FISG andererseits stellen das Verhältnis zwischen Banken bzw. Finanzdienstleistern und ihren (potenziellen) Auslagerungspartner auf ein neues Fundament. Beide Parteien müssen nun diese Regelungen umsetzen bzw. gegen sich gelten lassen, was die Geschäftsanbahnung und den damit verbundenen Auswahlprozess auf ein neues Niveau hebt.

Wie sehen nun die neuen Anforderungen aus? Zunächst sollen die Neuerungen der MaRisk und der BAIT auf das Auslagerungsmanagement skizziert werden. Anschließend wird der Fokus auf das FISG gerichtet.

Neuerungen aus den MaRisk und den BAIT

Die Regelungen zwischen Banken bzw. Finanzdienstleistern und Auslagerungsunternehmen umfassen drei Anforderungsgruppen:

1. Vertragliche Anforderungen
2. Prozessuale Anforderungen
3. Reporting- und Kontrollanforderungen

Zu den eher statischen **vertraglichen Anforderungen,** die bisher in den MaRisk dokumentiert waren, gesellen sich nun eher dynamische Anforderungen hinzu. Die Standorte der Leistungserbringung, der Versicherungsschutz und -umfang und schließlich die Dienstleistungsgüte mit genauen qualitativen und quantitativen Leistungszielen sind in den Vertragswerken zu regeln.

Bei den **prozessualen Anforderungen** sind für alle vom Auslagerungsunternehmen übernommenen Aufgaben vollständige Schnittstellenbeschreibungen anzufertigen. Das beinhaltet klare und eindeutige Beschreibungen der – pro Prozess – auszuübenden Tätigkeiten. Damit soll gewährleistet werden, dass Zuständigkeiten zwischen den Vertragspartnern klar geregelt sind und jeder weiß, wofür wer verantwortlich ist.

Auch Weiterverlagerungen an Subunternehmer des Auslagerungsunternehmens stehen ab sofort unter verstärkter Beobachtung. Handelt es sich dabei um „institutsrelevante" Prozesse, sind an diese die gleichen Qualitätsanforderungen zu stellen wie an die Prozesse des Auslagerungsunternehmens selber. Einem Verwässern der Qualität durch Weitergabe an Subunternehmer ist damit ein Riegel vorgeschoben.

Ausgelagerte Prozesse können zeitkritische Leistungsbezüge enthalten. In diesen Fällen müssen das auslagernde Institut und das Auslagerungsunternehmen über aufeinander abgestimmte Notfallkonzepte verfügen. Die Wirksamkeit und Angemessenheit des generellen Notfallkonzepts und besonders der aufeinander abgestimmten Notfallkonzepte bei zeitkritischen Prozessen ist während der Vertragslaufzeit regelmäßig zu überprüfen.

Banken bzw. Finanzdienstleister sind verpflichtet, ein angemessenes und wirksames Risikomanagementsystem zu installieren. Ein essenzieller Baustein dafür ist das interne Kontrollsystem (IKS). Werden Prozesse und Aktivitäten ausgelagert, die sonst vom Institut selbst erbracht würden, ist für diese ebenfalls ein IKS einzurichten. Deshalb ist es eine regelmäßige Anforderung an Auslagerungsunternehmen, ein sogenanntes dienstleistungsbezogenes Internes Kontrollsystem (dIKS) zu implementieren. Die Angemessenheit und Funktionsfähigkeit des dIKS sollte regelmäßig/jährlich von einem unabhängigen Dritten überprüft werden (Prüfung nach IDW PS 951).

Neben dieser externen Prüfung sind die dienstleistungbezogenen Prozesse und Aktivitäten einer fortlaufenden internen Revision zu unterziehen. Sollte das Auslagerungsunternehmen dies nicht umsetzen, ist das auslagernde Unternehmen selbst verpflichtet, die interne Revision nach den Vorgaben der MaRisk vorzunehmen. Das wäre mit erheblichen finanziellen, personellen und zeitlichen Ressourcen verbunden.

Dienstleistungsbezogenes Kontrollsystem, interne Revision und Notfallmanagement erfordern vom Auslagerungspartner ein professionelles und standardisiertes Berichts- und Reporting-System, damit zeitnah und wirksam auf mögliche Risiken reagiert werden kann. Und zwar sowohl vom Auslagerungspartner selbst als auch vom auslagernden Unternehmen.

Die vertraglichen, prozessualen und **Berichts- und Reporting-Anforderungen** erfordern vom Auslagerungsunternehmen eine kulturelle Bereitschaft oder Reife. Wer sich erst in diese Materie einarbeiten oder aufrüsten muss, wird es schwer haben, sich als Partner für beaufsichtigte Unternehmen zu halten bzw. zu etablieren.

Oder anders formuliert: Die Kulturen zwischen beaufsichtigten Unternehmen und ihren Auslagerungspartnern müssen sich annähern, da die Grenzen zwischen ihnen immer mehr verschwimmen.

Finanzmarktintegritäts- und Stabilitätsgesetz

Kommen wir nun zu den Befugnissen, die das FISG der Aufsicht gegenüber den Auslagerungsunternehmen einräumt. Diese lassen sich in vier Themenbereiche aufgliedern:

1. Legaldefinition von Auslagerungen
2. Anzeige von Auslagerungen
3. Anordnungs- und Eingriffsbefugnisse
4. Auslagerung in Drittstaaten

Die bisherige **Legaldefinition** von Auslagerungsunternehmen fristet eher auf den hinteren Rängen der Paragraphen des KWG ihr Dasein. Sie wird nun prominent in den §1 des KWG vorgezogen und inhaltlich erweitert.

Die Eingrenzung auf wesentliche Auslagerungen entfällt, und es werden auch alle Subunternehmen bei Weiterverlagerungen von Aktivitäten und Prozessen vom Begriff des Auslagerungsunternehmens erfasst. Zumindest erfolgt bei den Subunternehmen die Eingrenzung auf wesentliche oder institutsrelevante Prozesse. >

Damit erstrecken sich künftig die Aufsichtsbefugnisse
- auf alle Auslagerungsunternehmen unabhängig davon, ob sie wesentliche oder andere Prozesse von beaufsichtigten Unternehmen übernehmen, sowie
- auf alle Subunternehmen die für Auslagerungsunternehmen institutsrelevante Prozesse übernehmen.

Die Grenzen zwischen beaufsichtigten und nicht beaufsichtigten Unternehmen lösen sich auf.

Anzeige von Auslagerungen: Auslagerungen sind künftig der Aufsicht anzuzeigen. Institute müssen vier Tatbestände im Zusammenhang mit Auslagerungen melden:
- die Absicht einer wesentlichen Auslagerung,
- den Vollzug einer wesentlichen und nicht wesentlichen Auslagerung,
- jede Änderung der Beurteilung der Wesentlichkeit einer Auslagerung,
- wesentliche Änderungen und schwerwiegende Vorfälle im Rahmen von bestehenden Auslagerungsvereinbarungen, die einen wesentlichen Einfluss auf die Geschäftstätigkeit des Instituts haben können.

Davon verspricht sich die Aufsicht eine höhere Transparenz über das gesamte Auslagerungsgeschehen. Auf der Ebene der Institute kann sie nachvollziehen, welche Tätigkeiten in welchem Umfang ausgelagert werden. Und bei den Auslagerungsunternehmen kann sie erkennen, welche Konzentrationstendenzen und -risiken sich dort auftun.

Die **Anordnungs- und Eingriffsbefugnisse** sind nun im KWG § 44 (Auskünfte und Prüfungen), § 45b (Maßnahmen bei organisatorischen Mängeln) und § 56 (Bußgeldvorschriften und Eingriffe) dokumentiert. Damit wird ein Großteil der Aufsichtsbefugnisse, die bisher für beaufsichtigte Unternehmen reserviert waren, auch auf Auslagerungsunternehmen ausgeweitet.

Das reicht von Auskunftsverpflichtungen zu allen Geschäftsangelegenheiten über die direkte Anordnung von Prüfungen und Maßnahmen bei Verstößen gegen Pflichten aus dem Auslagerungsvertrag bis zur Forderung zum Aufbau von Sachkompetenz in der Geschäftsleitung und geht weiter bis hin zu Berichtspflichten sowie Bußgeldverfahren bei Nichtbeachtung.

Die Begründung für diese weitreichenden Eingriffskompetenzen formuliert der Gesetzgeber folgendermaßen: Die Aufsicht muss in der Lage sein, nicht nur auf das beaufsichtigte Unternehmen zuzugreifen, sondern im Fall aufgespaltener Wertschöpfungsketten auch auf externe Dienstleister, auf die Aktivitäten und Prozesse ausgelagert werden.

Auslagerung in Drittstaaten: Damit diese Regelungen nicht durch Auslagerungen ins Ausland umgangen werden, fordert das FISG, einen inländischen Zustellungsbevollmächtigten zu benennen, an den Bekanntgaben und Zustellungen durch die Bundesanstalt bewirkt werden können. Diese Funktion muss vertraglich vereinbart werden. Inwiefern solche Bekanntgaben und Zustellungen dann in einem Drittland Wirkung zeigen, wird sich erweisen. Im Zweifelsfall wird sich die Aufsicht voraussichtlich wieder an das auslagernde Institut im Inland wenden.

AUTOR UND ANSPRECHPARTNER

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

Erste Hilfe zur Einwertung nach den neuen Vorgaben

Was bedeuten nun diese Neuerungen und Verschärfungen durch MaRisk, BAIT und FISG? Die Geschäftspartner, auslagerndes Unternehmen und Auslagerungsunternehmen, müssen sich selbst und ihren Partner neu einwerten:

- Komme ich selbst mit diesen Anforderungen klar und kann ich sie umsetzen?
- Ist auch mein Geschäftspartner, das Auslagerungsunternehmen, in der Lage, diese Regeln zu realisieren und zu installieren, damit ich als auslagerndes Unternehmen weiterhin die Vorteile der Arbeitsteilung nutzen und genießen kann?

Folgende Checkliste mit Fragen an mein Auslagerungsunternehmen kann dabei helfen:

1. Sind alle vertraglichen Pflichten der MaRisk und BAIT vollumfänglich umgesetzt?
2. Hat mein Auslagerungspartner alle ausgelagerten Prozesse in Schnittstellenbeschreibungen nachvollziehbar und transparent dokumentiert?
3. Sind Weiterverlagerungen von institutsrelevanten Prozessen an Dritte den gleichen Regeln unterworfen wie für das Auslagerungsunternehmen selber?
4. Hat der Dienstleister ein IKS installiert, das von einem externen WP-Unternehmen nach dem IDW PS 951 Typ 2 jährlich zertifiziert und geprüft wird? Wenn ja, seit wie vielen Jahren?
5. Verfügt mein Auslagerungsunternehmen über eine eigene Innenrevision?
6. Hat mein Auslagerungspartner ein professionelles und standardisiertes Reporting-System installiert, bei dem ich unaufgefordert und regelmäßig die Berichte zum IKS, zur internen Revision und zum Risiko- und Notfallmanagement erhalte?
7. Habe ich ein Meldesystem installiert, um die Absicht, den Vollzug und Änderungen (Wesentlichkeit/Vorfälle) der Aufsicht anzuzeigen?
8. Kann mein Auslagerungspartner den Anordnungs- und Eingriffsbefugnissen der Aufsicht personell, inhaltlich und finanziell standhalten?
9. Verfügt mein Auslagerungspartner über einen inländischen Zustellungsbevollmächtigten, wenn er im Ausland sitzt bzw. Weiterverlagerungen von institutsrelevanten Prozessen ins Ausland vornimmt?

Nur wenn diese Fragen positiv beantwortet werden können, ist das bestehende oder künftige Auslagerungsunternehmen auch der Partner für die Zukunft. ▬

Rechnungswesen

Umstellung des Rechnungswesens

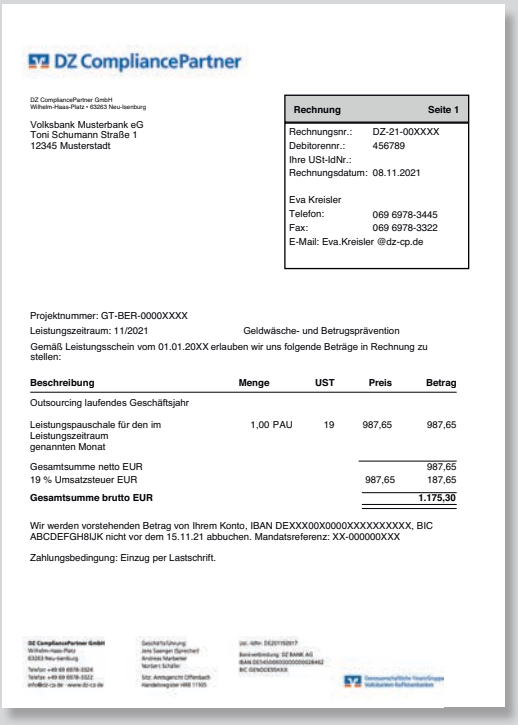
Ab dem 1. Januar 2022 nutzt die DZ CompliancePartner im Rechnungswesen SAP. Im Wesentlichen wird sich für Sie nichts ändern:

- Sie haben nach wie vor die Wahl zwischen Papier- oder elektronischer Rechnung. Standardmäßig übernehmen wir die bisherige Einstellung, würden uns aber freuen, wenn Sie auf die elektronische Rechnungsstellung wechseln würden.
- Die Rechnungsinhalte und das Rechnungslayout bleiben ebenfalls größtenteils unverändert. Alle bisherigen Informationen finden Sie selbstverständlich auch auf der neuen Rechnung.

Nachdem wir in 2021 die Migration von Microsoft Navision auf SAP gründlich vorbereitet haben, ist der Kern der Umstellung ein besser auf unser Geschäftsmodell ausgerichtetes ERP-System.

Sie profitieren, da wir so

- die Aufwände in unserem Rechnungswesen niedrig halten,
- die Prozesse in der Projekterfassung und Abrechnung aller Mitarbeiter*innen straffen und Aufwände reduzieren können.



DZ CompliancePartner

DZ CompliancePartner GmbH
Wilhelm-Haas-Platz · 63263 Neu-Isenburg

Volksbank Musterbank eG
Toni Schumann Straße 1
12345 Musterstadt

Rechnung	Seite 1
Rechnungsnr.:	DZ-21-00XXXX
Debitorennr.:	456789
Ihre USt-IdNr.:	
Rechnungsdatum:	08.11.2021

Eva Kreisler
Telefon: 069 6978-3445
Fax: 069 6978-3322
E-Mail: Eva.Kreisler @dz-cp.de

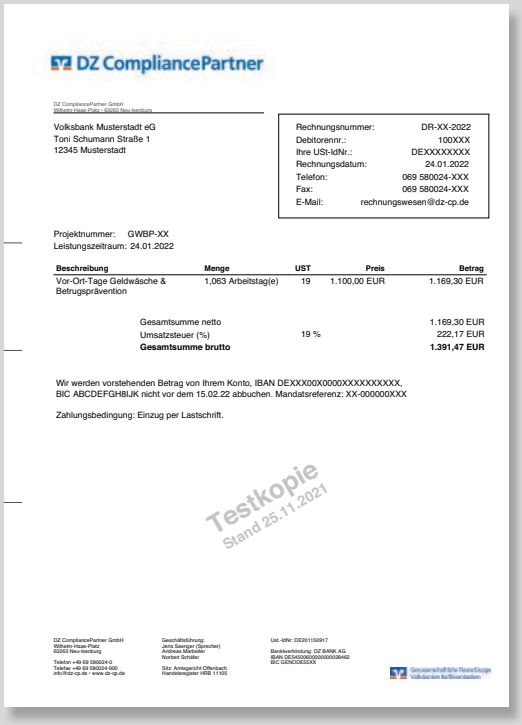
Projektnummer: GT-BER-0000XXXX
Leistungszeitraum: 11/2021 Geldwäsche- und Betrugsprävention
Gemäß Leistungsschein vom 01.01.20XX erlauben wir uns folgende Beträge in Rechnung zu stellen:

Beschreibung	Menge	UST	Preis	Betrag
Outsourcing laufendes Geschäftsjahr				
Leistungspauschale für den im Leistungszeitraum genannten Monat	1,00 PAU	19	987,65	987,65
Gesamtsumme netto EUR				987,65
19 % Umsatzsteuer EUR			987,65	187,65
Gesamtsumme brutto EUR				**1.175,30**

Wir werden vorstehenden Betrag von Ihrem Konto, IBAN DEXXX00X0000XXXXXXXXX, BIC ABCDEFGH8IJK nicht vor dem 15.11.21 abbuchen. Mandatsreferenz: XX-000000XXX

Zahlungsbedingung: Einzug per Lastschrift.

NEU in 2022



DZ CompliancePartner

DZ CompliancePartner GmbH
Wilhelm-Haas-Platz · 63263 Neu-Isenburg

Volksbank Musterstadt eG
Toni Schumann Straße 1
12345 Musterstadt

Rechnungsnummer:	DR-XX-2022
Debitorennr.:	100XXX
Ihre USt-IdNr.:	DEXXXXXXXX
Rechnungsdatum:	24.01.2022
Telefon:	069 580024-XXX
Fax:	069 580024-XXX
E-Mail:	rechnungswesen@dz-cp.de

Projektnummer: GWBP-XX
Leistungszeitraum: 24.01.2022

Beschreibung	Menge	UST	Preis	Betrag
Vor-Ort-Tage Geldwäsche & Betrugsprävention	1,063 Arbeitstag(e)	19	1.100,00 EUR	1.169,30 EUR
Gesamtsumme netto				1.169,30 EUR
Umsatzsteuer (%)		19 %		222,17 EUR
Gesamtsumme brutto				**1.391,47 EUR**

Wir werden vorstehenden Betrag von Ihrem Konto, IBAN DEXXX00X0000XXXXXXXXX, BIC ABCDEFGH8IJK nicht vor dem 15.02.22 abbuchen. Mandatsreferenz: XX-000000XXX

Zahlungsbedingung: Einzug per Lastschrift.

Testkopie
Stand 25.11.2021

ANSPRECHPARTNER

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

Trotz aller Anstrengungen kann es (und wird es voraussichtlich auch) während der Umstellung vereinzelt zu Fehlern oder Verzögerungen kommen. Dies bitten wir bereits hier und heute zu entschuldigen. Wir haben aber alle Vorkehrungen getroffen, um diese Störungen so gering wie möglich zu halten und im Fall der Fälle schnelle Lösungen sicherzustellen. Dazu gehört auch, dass wir direkt die verantwortliche Person in Ihrem Haus kontaktieren und informieren werden.

Schlussendlich und zusammenfassend überführen wir das Rechnungswesen in ein modernes System, um auch künftig den Anforderungen einer digitalisierten Geschäftstätigkeit gerecht zu werden und Ihnen ein ebenso sicherer wie transparenter Partner – auch und insbesondere – im Rechnungswesen sein zu können. ▬

Telefonie

Neue Durchwahlen ab 1. Januar 2022

Wir wollen für Sie einfacher erreichbar sein.
Ein Ansprechpartner – eine Durchwahl: egal welcher Standort, egal ob mobil oder Festnetz.

Unsere Zentrale erreichen Sie unter
Telefon 069 580024-0
Telefax 069 580024-900

Nachfolgend die wichtigsten Durchwahlen der DZ CompliancePartner GmbH:

	Bereich	Telefon	Telefax
Jens Saenger	Sprecher der Geschäftsführung	069 580024-100	069 580024-900
Andreas Marbeiter	Geschäftsführung	069 580024-101	069 580024-900
Norbert Schäfer	Geschäftsführung	069 580024-102	069 580024-901
Marco Becker	Geldwäsche- und Betrugsprävention	069 580024-130	069 580024-901
Thomas Grebe	IT-Audit	069 580024-159	069 580024-900
Esra Güner	Bewerbermanagement	069 580024-161	069 580024-900
Iris Hauptführer	Produktentwicklung & Qualitätssicherung	069 580024-166	069 580024-900
Martin Hierlemann	Vertrieb	069 580024-172	069 580024-900
Marc Linnebach	WpHG-Compliance	069 580024-189	069 580024-902
Michael Maier	MaRisk-Compliance	069 580024-194	069 580024-900
Andreas Marbeiter	Informationssicherheit & Datenschutz (komm.)	069 580024-101	069 580024-900
Lars Schinnerling	Interne Revision	069 580024-219	069 580024-900
Thorsten Schmeil	Geldwäsche- und Betrugsprävention	069 580024-220	069 580024-901
Gabriele Seifert	Kommunikation & Bildung	069 580024-228	069 580024-900
Sandra Sitter	Projekte & IT	069 580024-230	069 580024-900
Dominik Tiburtius	Geldwäsche- und Betrugsprävention	069 580024-235	069 580024-901
Thomas Wagener	Compliance-Spezialist	069 580024-241	069 580024-901

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 genügt den Anforderungen gemäß MaRisk AT 4.4.3 und BT 2.

Seit der letzten Berichterstattung in der Point of Compliance (2/2021, S. 27) wurden entsprechend der Jahresprüfungsplanung 2021 vier weitere Prüfungen abgeschlossen. Die Berichte zu den Bereichen „Geldwäsche- und Betrugsprävention / Compliance-Spezialisten", „Datenschutz", „IT-Audit" und „Informationssicherheit" wurden als dienstleistungsbezogene Berichte der Mandantschaft mit der entsprechenden Auslagerung zur Verfügung gestellt.

Die Quartalsberichte zum dritten Quartal 2021 der Internen Revision wurden fristgerecht erstellt und unserer Mandantschaft zur Verfügung gestellt.

Darüber hinaus wurde turnusgemäß ein Follow-up-Quartalsbericht für das dritte Quartal 2021 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. ▬

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

Wirtschaftliche Lage

Die Ertragslage ist weiterhin stabil. Die DZ CompliancePartner GmbH rechnet mit einer leichten Planüberschreitung zum Jahresende von ca. 350 T€. Die Umsatzrendite von ca. 10 % als Zielmarke wird auch in 2021 erreicht. Die wirtschaftliche Lage ist damit als stabil zu bezeichnen.

Die Änderungen der MaRisk und BAIT wurden in die Dienstleistungen ebenso übernommen, wie auch die sich abzeichnenden Änderungen im Dienstleistungsangebot des Hinweisgebersystems. Die Vertragsanpassungen aus den Änderungen der MaRisk AT 9 wurden bereits in den AK Vertragsprüfung beim DGRV eingebracht, so dass die Änderungen sicher in der Übergangsphase bis Ende 2022 umgesetzt werden können. Das Unternehmen wird in der Zwischenzeit die notwendigen Vertragsanpassungen als Ergänzung zu den bestehenden Vereinbarungen an alle Kunden übersenden und gegen sich gelten lassen.

Die DZ CompliancePartner GmbH hat weiterhin alle Vorkehrungen zur sicheren Aufrechterhaltung ihres Geschäftsbetriebes im Rahmen der Corona-Pandemie getroffen. Auch wurde die Leistungsfähigkeit aller wesentlichen Partnerunternehmen regelmäßig überprüft. Die DZ CompliancePartner GmbH ist auch weiterhin sicher in der Lage, auf die sich stets ändernden Rahmenbedingungen der Pandemie angemessen reagieren zu können. Im übrigen verweisen wir auf die vierteljährlichen Risikoberichte der Gesellschaft. ▬

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