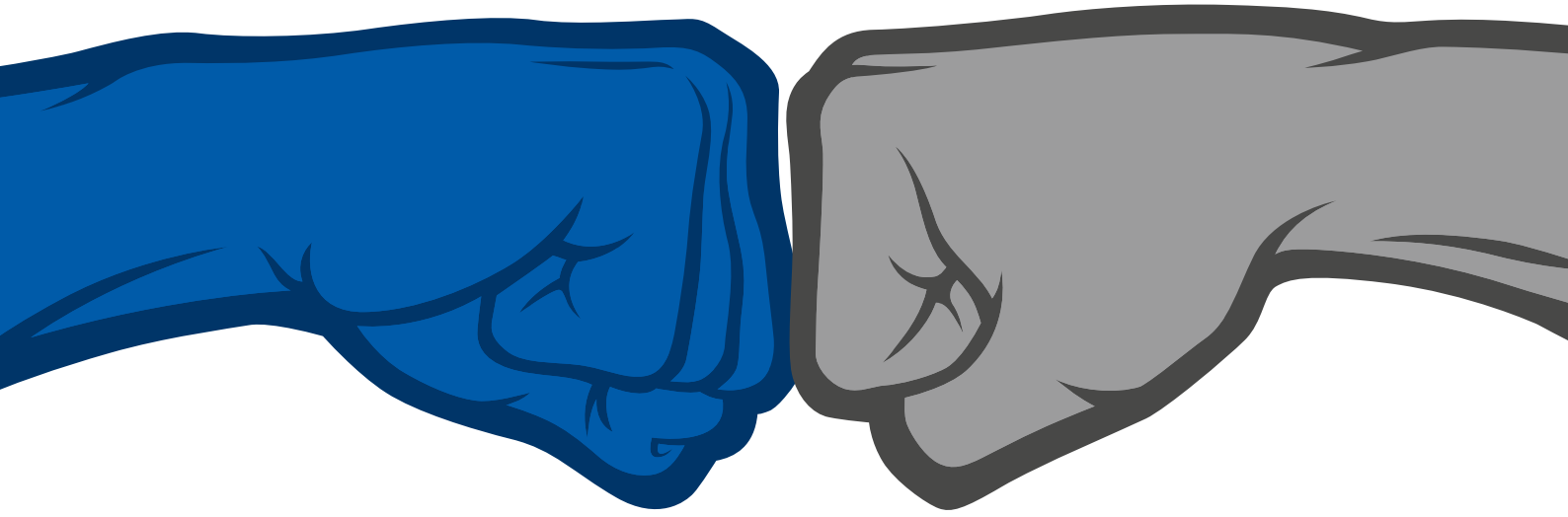
DZ CompliancePartner

Point of Compliance

Das Risikomanagement-Magazin für
unsere Kunden und Geschäftspartner

AUSGABE 3/2020

Partnerschaft bewahren



ab Seite 4

Aktuelle Entwicklungen
in der Geldwäsche-
bekämpfung

ab Seite 12

Sachkunde kompakt:
Wissen wirkt

IMPRESSUM

Point of Compliance
Das Risikomanagement-Magazin für unsere Kunden und Geschäftspartner, Ausgabe 24, 3/2020
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:
Dennis Heinemeyer, Martin Hierlemann, Marc Linnebach, Michael Maier, Jens Saenger, Norbert Schäfer, Lars Schinnerling, Michael Switalla

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: 5. November 2020
Auflage: 2.600 Exemplare
Die aktuellen Mediadaten finden Sie im Internet unter www.dz-cp.de/poc

Vertrauen macht uns stark.

Jens Saenger
Sprecher der Geschäftsführung

Vertrauen hat viel mit einer positiven Grundhaltung zu tun: Alles wird am Ende gut.

Und doch muss Vertrauen auch immer wieder erarbeitet werden. In einer durch Distanz geprägten Pandemie ist das nicht immer leicht. Dem Personen- und auch dem Prozessvertrauen stehen Kontaktbeschränkungen entgegen. Was uns in dieser Zeit tatsächlich hilft, ist das Organisationsvertrauen: Das enge Netz der Genossenschaftlichen FinanzGruppe zahlt sich aus.

Vertrauen zu haben bedeutet, sich Veränderungen stellen zu können, und zwar ohne sich selbst in Frage zu stellen. Wenn wir auf eine gemeinsame Basis vertrauen dürfen, müssen wir diese nicht erst schaffen – und können uns der eigentlichen Aufgabe stellen. Wir bleiben handlungsfähig und nehmen die Herausforderung leichter an.

Nach einem bewegenden Jahr möchte ich mich – im Namen der Gesamtgeschäftsführung und auch im Namen des Aufsichtsrats – für die partnerschaftliche Zusammenarbeit und Ihr Vertrauen bedanken.

Bleiben Sie gesund!

Herzlichst Ihr
Jens Saenger

Geldwäscheprävention

Aktuelle Entwicklungen in Geldwäschebekämpfung

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

Das Geldwäschegesetz (GwG) wurde zuletzt zum 1. Januar 2020 aufgrund der Änderungsrichtlinie zur 4. EU-Geldwäscherichtlinie novelliert. Zwischenzeitlich wurden weitere (Gesetzes-)Initiativen zum verstärkten Kampf gegen Geldwäsche und Terrorfinanzierung auf den Weg gebracht:

Geldwäschegesetzmeldepflichtverordnung-Immobilien – GwGMeldV-Immobilien

Die vom Bundesministerium der Finanzen (BMF) erstellte „Verordnung zu den nach dem Geldwäschegesetz meldepflichtigen Sachverhalten im Immobilienbereich“ vom 20. August 2020 wurde am 31. August 2020 im Bundesgesetzblatt veröffentlicht und trat am 1. Oktober 2020 in Kraft.

Die Verordnung ist durch die zum 1. Januar 2020 in Kraft getretenen Änderungen des GwG bedingt. Diese sehen den Erlass einer Rechtsverordnung vor, mit der Meldepflichten der rechtsberatenden Berufe bei Immobilientransaktionen konkretisiert werden. Die Rechtsverordnung regelt auf dieser Grundlage Sachverhalte bei Immobilientransaktionen, die von diesen Verpflichteten an die Financial Intelligence Unit (FIU / Zentralstelle für Finanztransaktionsuntersuchungen) zu melden sind. Entsprechende Meldepflichten bestehen,

- wenn ein Bezug zu Risikostaaten oder Sanktionslisten besteht,
- bei Auffälligkeiten im Zusammenhang mit den beteiligten Personen oder dem wirtschaftlich Berechtigten sowie im Zusammenhang mit der Stellvertretung,
- bei Auffälligkeiten im Zusammenhang mit dem Preis oder der Kauf- oder Zahlungsmodalität
- und wenn keine Tatsachen vorliegen, die die vorhandenen Anzeichen erklären bzw. entkräften.

Entwurf eines Gesetzes zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche

Der Rat der Europäischen Union hatte bereits am 23. Oktober 2018 die Richtlinie über die strafrechtliche Bekämpfung der Geldwäsche veröffentlicht. Die Richtlinie legt Mindeststandards für die Definition von Vortaten und Sanktionen im Bereich der Geldwäsche fest, mit dem Ziel, die nationalstaatliche Gesetzgebung zu vereinheitlichen. Die Umsetzungsfrist in nationales Recht endet am 3. Dezember 2020. Am 14. Oktober 2020 wurde nun der Gesetzentwurf der Bundesregierung zu § 261 Strafgesetzbuch (StGB) veröffentlicht.

Kernstück des Gesetzentwurfs ist der Verzicht auf einen selektiven Vortatenkatalog. Künftig kann somit jede Straftat Vortat der Geldwäsche sein. Delikte wie Diebstahl, Unterschlagung, Raub, Betrug oder Untreue kamen bisher als Vortaten der Geldwäsche nur dann in Betracht, wenn diese gewerbsmäßig oder von einem Mitglied einer Bande, die sich zur fortgesetzten Begehung solcher Straftaten verbunden hat, begangen wurden. Mit diesem Paradigmenwechsel im deutschen Geldwäschestrafrecht verbindet der Gesetzgeber eine deutlich effektivere Kriminalitätsbekämpfung in diesem Bereich. Dies wird insbesondere für den Bereich der organisierten Kriminalität erhofft, bei der Täter arbeitsteilig vorgehen und daher der Bezug zu bestimmten schweren Vortaten sich nicht immer feststellen lässt.

Zu bedauern ist, dass im Gesetzentwurf der Strafrahmen für leichtfertiges Nichterkennen unverändert geblieben ist. Dieser sieht nach wie vor eine Freiheitsstrafe bis zu zwei Jahren oder eine Geldstrafe für denjenigen vor, der leichtfertig nicht erkennt, dass es sich um einen durch eine Straftat erlangten Vermögensgegenstand handelt. Der Referentenentwurf sah noch den Wegfall der Strafbarkeit des leichtfertigen Nichterkennens einer Geldwäschehandlung vor, die insbesondere für Mitarbeiterinnen

der

AUTOR UND ANSPRECHPARTNER

Norbert Schäfer
Geschäftsführung,
E-Mail: norbert.schaefer@dz-cp.de

und Mitarbeiter von Kreditinstituten bei der Ausübung ihres Berufs durch ihre potenzielle Anwendungsbreite ein unverhältnismäßiges Bedrohungsszenario bei der Abwicklung alltäglicher berufstypischer Tätigkeiten entfaltet. Dies gilt umso mehr auch für die Mitarbeiterinnen und Mitarbeiter, die die Funktion des Geldwäschebeauftragten ausüben.

Hingegen wird erwartet, dass der Verzicht auf einen selektiven Vortatenkatalog sowie auf die Beschränkung auf bestimmte Begehungsweisen eine nochmals gesteigerte Zahl von Verdachtsmeldungen zur Folge haben wird. Dies wird zu einem erheblichen Mehraufwand bei den Verpflichteten des Geldwäschegesetzes, der FIU sowie den Strafverfolgungsbehörden führen.

Aktionsplan der EU-Kommission zur Stärkung der Bekämpfung der Geldwäsche und Terrorismusfinanzierung

Am 7. Mai 2020 hat die EU-Kommission einen Aktionsplan[1] für eine schärfere Politik der Europäischen Union zur Verhinderung von Geldwäsche und Terrorismusfinanzierung (GW/TF) zur Konsultation gestellt. Ziel dieses Aktionsplans ist es, bestehende Divergenzen und Schwächen in der Bekämpfung der GW/TF innerhalb der EU zu beseitigen. Zudem sollen Vorgaben harmonisiert und Regelungen klarer gefasst werden, um unterschiedliche Auslegungen in den jeweiligen Mitgliedstaaten zu vermeiden. Der Aktionsplan beruht auf sechs Säulen:

1. Wirksame Anwendung der EU-Vorschriften
Die Kommission wird weiterhin genau darüber wachen, dass die Mitgliedstaaten die EU-Vorschriften umsetzen, damit die nationalen Vorschriften den höchstmöglichen Standards entsprechen. Parallel dazu wird die Europäische Bankenaufsichtsbehörde (EBA) im Aktionsplan „ermutigt", ihre neuen Befugnisse zur Bekämpfung von GW/TF „voll auszuschöpfen".

Danach wird die EU-Kommission prüfen, wie die Vorschriften zur Bekämpfung von GW/TF in den Mitgliedstaaten in der Praxis angewandt werden, wird daraufhin länderspezifische Empfehlungen formulieren und leistet Mitgliedstaaten bei der Durchführung der notwendigen Reformen technische Hilfe.

2. Ein einheitliches EU-Regelwerk
Die aktuellen EU-Vorschriften sind zwar weitreichend und grundsätzlich wirksam, werden von den Mitgliedstaaten jedoch in unterschiedlicher Weise angewandt. Unterschiedliche Auslegungen der Vorschriften führen zu Schlupflöchern, die von Straftätern ausgenutzt werden können. Um dagegen vorzugehen, wird die Kommission im ersten Quartal 2021 ein stärker harmonisiertes Regelwerk vorschlagen.

Um Unterschiede bei der Auslegung und Anwendung der Vorschriften in Grenzen zu halten, sollen bestimmte Teile der Geldwäscherichtlinie in unmittelbar anwendbare Bestimmungen einer Verordnung umgewandelt werden.

3. Aufsicht auf EU-Ebene
Derzeit ist es Sache der Mitgliedstaaten, über die Anwendung der einschlägigen EU-Vorschriften zu wachen, was Unterschiede bei der Aufsicht zur Folge haben kann. Im ersten Quartal 2021 wird die Kommission die Einrichtung einer auf EU-Ebene angesiedelten Aufsicht vorschlagen.

Des Weiteren ist beabsichtigt, auch für den sogenannten Nichtfinanzsektor (zum Beispiel Notare, Versicherungsvermittler, Dienstleister, nicht verkammerte Rechtsbeistände, Güterhändler) eine EU-Aufsicht zu etablieren. >

[1] https://ec.europa.eu/germany/news/20200507-geldwaesche-und-terrorismusfinanzierung_de

4. Ein Koordinierungs- und Unterstützungsmechanismus für die zentralen Meldestellen der Mitgliedstaaten
Die Adressaten für Geldwäsche-Verdachtsmeldungen in den Mitgliedstaaten spielen eine entscheidende Rolle bei der Ermittlung von Geschäften und Aktivitäten, die mit kriminellen Machenschaften zusammenhängen könnten. Im ersten Quartal 2021 wird die Kommission die Einrichtung eines EU-Mechanismus vorschlagen, der bei der Koordinierung und Unterstützung dieser Meldestellen hilft.

5. Durchsetzung strafrechtlicher Bestimmungen und Informationsaustausch auf EU-Ebene
Die justizielle und polizeiliche Zusammenarbeit auf der Basis von EU-Instrumenten und institutionellen Vereinbarungen ist für einen angemessenen Informationsaustausch von entscheidender Bedeutung. Auch der Privatsektor kann den Kampf gegen GW/TF unterstützen. Die Kommission wird daher Leitlinien zur Rolle öffentlich-privater Partnerschaften herausgeben, um den Datenaustausch zu klären und zu verbessern.

6. Die globale Rolle der EU
Die EU wirkt innerhalb der FATF und weltweit aktiv daran mit, internationale Standards für die Bekämpfung von GW/TF zu prägen. Anpassen muss die EU insbesondere ihren Ansatz für den Umgang mit Drittländern, deren Regelungen zur Bekämpfung von GW/TF strategische Mängel aufweisen und somit eine Bedrohung für den Binnenmarkt darstellen. Die neue Methodik gibt der EU die dafür nötigen Instrumente an die Hand. Bis die überarbeitete Methodik angewandt wird, soll die jeweils aktualisierte EU-Liste für eine bessere Übereinstimmung mit der entsprechenden Liste der FATF sorgen.

Die EU-Kommission plant, spätestens bis Ende März 2021 die geplanten Maßnahmen umzusetzen bzw. zu koordinieren.

Der Bundesrat hat in seiner 993. Sitzung am 18. September 2020 gemäß §§ 3 und 5 EUZBLG (Gesetz über die Zusammenarbeit von Bund und Ländern in Angelegenheiten der Europäischen Union) den Aktionsplan begrüßt und hierzu Stellung genommen (Drucksache 325/20 – Beschluss).

Fokus-Themen der deutschen FATF-Präsidentschaft

Am 1. Juli 2020 hat Deutschland die Präsidentschaft der Financial Action Task Force on Money Laundering (FATF) übernommen und zugleich eine ambitionierte Agenda für diesen Zeitraum vorgelegt:

- So will sich die FATF nicht nur mit den Risiken, sondern auch mit den Chancen der digitalen Transformationen für eine effiziente Geldwäschebekämpfung auseinandersetzen.
- Im Lichte vermehrter Anschläge in verschiedenen Teilen der Welt will Deutschland während der deutschen Präsidentschaft den internationalen Austausch über die Finanzierung von Rechtsterrorismus forcieren.
- Auch das Thema Schleuserkriminalität soll stärker in den Fokus gerückt werden. Es soll eine neue Initiative vorgeschlagen werden, die sich auf die Finanzströme und die Verbindungen der Migrantenschmugglernetzwerke in Bezug auf GW/TF konzentriert.
- Außerdem soll die FATF erstmals umfassend verschiedene Phänomene aus dem Bereich der Umweltkriminalität auf ihre Geldwäscherelevanz hin untersuchen.
- Ferner sollen während der deutschen Präsidentschaft auch ein Dialog zur Rolle des illegalen Waffenhandels bei der Terrorismusfinanzierung angestrebt sowie Handlungsempfehlungen zur Bekämpfung von Geldwäsche im Immobiliensektor erarbeitet werden.

Die DZ CompliancePartner verfolgt die aktuellen Entwicklungen in der Geldwäschebekämpfung und richtet die von ihr angebotenen Dienstleistungen in der Geldwäsche- und Betrugsprävention jeweils an den neuen gesetzlichen Vorschriften aus. ▬

Datenschutz

Datenschutz-Folgenabschätzungen bei der Anonymisierung von Daten

Ist die Anonymisierung personenbezogener Daten rechtfertigungsbedürftig und auf welche Rechtsgrundlage stützt sich eine Anonymisierung? Ein Positionspapier des Bundesbeauftragten für Datenschutz will Orientierung geben.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat am 29. Juni 2020 ein Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche veröffentlicht. Es entstand nach der Durchführung des ersten öffentlichen Konsultationsverfahrens der Behörde.

Hierbei stellte sich der BfDI die Frage, ob die Anonymisierung personenbezogener Daten rechtfertigungsbedürftig ist und auf welche Rechtsgrundlage sich eine Anonymisierung stützen lässt.

Im Positionspapier wurde der aktuelle rechtliche Rahmen für die Anonymisierung aus Sicht des BfDI aufgezeigt. Das Positionspapier soll den Verantwortlichen eine Orientierung bei der datenschutzrechtlichen Bewertung ihrer Anonymisierungspraktiken bieten.

Auch wenn der BfDI nur für öffentliche Stellen des Bundes zuständig ist und seine Ansichten somit keine direkte Wirkung für nicht öffentliche Stellen haben, hat dieses Positionspapier dennoch eine starke Signalwirkung für die für den Finanzsektor zuständigen Landesbehörden.

In der Praxis besteht eine große Spannbreite an möglichen Konstellationen und Anwendungsfällen für Anonymisierungen, und das nicht erst seit Einführung der DSGVO. Rechtliche Fragen rund um eine Anonymisierung im Datenschutzrecht haben eine hohe praktische Bedeutung. Für die Neugestaltung internationaler Datentransfers in unsichere Drittländer – nach der EuGH-Entscheidung Schrems II 2 zum EU-US Privacy Shield – werden auch Anonymisierungsmöglichkeiten als Option für technische Schutzmaßnahmen diskutiert.

Würde ein Verantwortlicher personenbezogene Daten vor einer internationalen Übermittlung anonymisieren, stellten sich datenschutzrechtliche Folgethemen aus Schrems II nicht mehr.

AUTOR UND ANSPRECHPARTNER

Dennis Heinemeyer
Beauftragter Informationssicherheit & Datenschutz,
E-Mail: dennis.heinemeyer@dz-cp.de

Gesetzliche Grundlage

Die DSGVO enthält keine (dem § 3 Abs. 6 BDSG-alt vergleichbare) gesetzliche Regelung zur Anonymisierung. Die DSGVO erwähnt die Anonymisierungsthematik lediglich im Erwägungsgrund Nr. 26 sowie im Erwägungsgrund Nr. 162. Zudem gibt es einen Bezug zu Anonymisierung in Art. 89 Abs. 1 S. 4 DSGVO. Gemäß Erwägungsgrund Nr. 26 S. 5 und S. 6 ist die DSGVO nicht auf Daten anwendbar, die bereits anonym sind. Die DSGVO betreffe somit nicht die (technische) „Verarbeitung" anonymer Daten.

Im deutschen und europäischen Datenschutzrecht gilt das Prinzip des Vorbehaltes des Gesetzes. Danach ist eine Verarbeitung von personenbezogenen Daten im Grundsatz nicht zulässig, wenn diese nicht durch eine Rechtsgrundlage erlaubt ist, z. B. gemäß Art. 6 Abs. 1 S. 1 DSGVO. Wenn ein Verantwortlicher daher personenbezogene Daten verarbeiten möchte, ist eine Rechtsgrundlage erforderlich. Dies gilt nach Ansicht des BfDI aufgrund des weiten Verarbeitungsbegriffes nach Art. 4 Nr. 2 DSGVO auch für Verarbeitungen, um den jeweiligen Personenbezug aufzuheben.

Wann sind Daten anonym

Mit der Breyer-Entscheidung des EuGH ist für den Personenbezug von Daten und damit auch für deren Anonymität davon auszugehen, dass legale Mittel zu berücksichtigen sind, um (Zusatz-)Informationen durch Dritte zu erlangen. >

Anonymisierung ist auch nach Ansicht des BfDI jeder Vorgang, der darauf gerichtet ist, den Personenbezug von Daten aufzuheben. Mit anderen Worten soll mit dem Einsatz von Anonymisierungstechniken erreicht werden, dass die betroffene Person nicht mehr identifiziert werden kann.

Einige Datenschutzgesetze der Länder definieren die Anonymisierung – mit Abweichungen im Detail – als das Verändern personenbezogener Daten wie folgt: Die Einzelangaben über persönliche oder sachliche Verhältnisse können nicht mehr oder nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden.

Eine hinreichende Anonymisierung führt dazu, dass die Grundsätze des Datenschutzrechts – wie z. B. der Grundsatz der Zweckbindung – nicht mehr anwendbar sind.

Anforderungen an die Anonymisierung personenbezogener Daten

Wann eine Anonymisierung als hinreichend angesehen werden kann, darüber gibt die DSGVO, wie auch der BfDI feststellt, keine Auskunft.

Weiter stellt der BfDI fest, dass eine absolute Anonymisierung (Wiederherstellung des Personenbezugs für niemanden möglich) häufig nicht erreichbar sein dürfte und im Regelfall datenschutzrechtlich auch nicht gefordert ist. Ausreichend ist in der Regel, dass der Personenbezug derart aufgehoben wird, dass eine Re-Identifizierung praktisch nicht durchführbar ist, weil der Personenbezug nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft wiederhergestellt werden kann.

Der BfDI hebt hierbei besonders hervor, dass eine valide Anonymisierung – je nach Art der zu anonymisierenden Daten und Kontext der Verarbeitung – eine Herausforderung für den jeweiligen Verantwortlichen bedeuten kann. Er unterstreicht dabei, dass nicht vorschnell von einer hinreichenden Anonymisierung ausgegangen werden darf.

Von anonymisierten Daten abzugrenzen sind insbesondere pseudonymisierte Daten. Darunter versteht die DSGVO gemäß Art. 4 Nr. 5 „die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden".

Während bei den pseudonymisierten Daten der berechtigte Inhaber der zusätzlichen Informationen mittels dieser den Personenbezug wiederherstellen kann, ist die Wiederherstellung des Personenbezugs bei den anonymen Daten für jedermann zumindest praktisch unmöglich. Bei den pseudonymisierten Daten handelt es sich um personenbezogene Daten, auf die das Datenschutzrecht anwendbar ist.

Verpflichtung zur Datenschutz-Folgenabschätzung bei jeder Anonymisierung

Der BfDI stellt insbesondere heraus, dass gemäß Art. 35 Abs. 1 DSGVO eine Datenschutz-Folgenabschätzung durchzuführen ist, wenn die Verarbeitung – insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke – voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Bei einer Anonymisierung müsse demnach der Verantwortliche in der Regel davon ausgehen, dass ein hohes Risiko besteht, weil bei der Anonymisierung eben regelmäßig das Kriterium „Verarbeitung in großem Umfang" und zumindest aktuell immer noch das Kriterium „neue Technologien" zuträfen. Die Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung sei insbesondere deshalb begründet, weil die Generierung eines anonymen Datenbestandes eine komplexe Aufgabe des Verantwortlichen darstellt und viele Fehlerquellen birgt. Dabei hat der Verantwortliche darüber hinaus die Folgen einer möglichen De-Anonymisierung in die Betrachtung einzubeziehen.

Vor einer Anonymisierung ist nach Ansicht des BfDI daher immer eine Datenschutz-Folgenabschätzung durchzuführen.

Unterstützung

Das Thema Datenschutz-Folgenabschätzung ist vielschichtig und komplex. Es erfordert Know-how im rechtlichen und technischen Sektor sowie Kenntnisse des Risikomanagements. Nutzen Sie unsere langjährige Erfahrung und unser breites Fachwissen. Gerne unterstützen wir Sie im Rahmen von Einzelprojekten oder dauerhafter Beratung und entlasten dabei Ihre internen Ressourcen. Selbstverständlich stehen wir auch in allen anderen Fragen zum Datenschutz bis hin zur Auslagerung des Datenschutzbeauftragten zur Verfügung. ▬

WpHG-Compliance

Single Officer – ein Erfahrungsbericht

In einer der letzten Ausgaben haben wir über die mögliche Organisationsstruktur der Funktion des Single Officers berichtet. Inzwischen ist ein halbes Jahr vergangen, und es gibt erste Erkenntnisse über die praktische Umsetzung der Tätigkeit.

Längere Zeit war unklar, an welcher organisatorischen Position der Single Officer im Unternehmen platziert werden sollte. Mit der MaDepot wurde klargestellt, dass der Single Officer ebenfalls eine Funktion der zweiten Verteidigungslinie ist, also eine überwachende, kontrollierende Aufgabe wahrnimmt.

Die Kombination mit dem WpHG-Compliance-Beauftragten wurde „empfohlen", ist aber in keinem Falle zwingend.

Wir haben mittlerweile von der Mehrzahl unserer WpHG-Auslagerungsmandate auch die Funktion des Single Officers übertragen bekommen und betreuen darüber hinaus erste Mandate ausschließlich mit dem Single Officer.

Wie die MaComp vorsieht, wird die Tätigkeit von einer Risikoanalyse bestimmt, die die Überwachungstätigkeit definiert und deren Ergebnisse in einen Jahresbericht (oder Ad-hoc-Bericht) einfließen.

Nähere Ausführungen zu den Inhalten der Risikoanalyse oder des Jahresberichts sind der MaDepot nicht zu entnehmen. Da die Aufgabenstellung derjenigen des WpHG-Beauftragten sehr ähnlich ist, sind wir bei der Konzeption des Compliance-Systems für den Single Officer analog zur MaComp vorgegangen.

Risikoanalyse

In der Risikoanalyse sind Gefährdungen aus Kundenfinanzinstrumenten zu identifizieren, die aus der konkreten Geschäftstätigkeit resultieren. Wie bei der Risikoanalyse des WpHG-Compliance-Beauftragten, bei dem die Analyse Auskunft über „Art, Umfang und Komplexität" des Wertpapiergeschäftes geben soll, besteht auch die Risikoanalyse des Single Officers im ersten Schritt aus einer Bestandaufnahme und Betroffenheitsanalyse.

Unsere Risikoanalysen zeigten, dass in keinem der von uns betreuten Mandate „exotische" Geschäftsmodelle durchgeführt werden, die ein erhöhtes Risiko für die Finanzinstrumente und Kundengelder bedeuten würden.

Dass wir zunächst ein standardisiertes „Grundgerüst" der Volksbanken Raiffeisenbanken beim Umgang mit den Finanzinstrumenten der Kunden vorfinden würden, war für uns allerdings auch aus unserer Tätigkeit als WpHG-Compliance-Beauftragte nicht ganz überraschend.

Sorgfaltspflichten

Eine Vielzahl der Sorgfaltspflichten im Zusammenhang mit dem Depotgeschäft betreffen faktisch nicht die Volksbanken Raiffeisenbanken selbst, sondern werden im Rahmen des Zentralbankmodells von der DZ BANK gewährleistet.

Die Kenntnisnahme und Würdigung der Prüfungsberichte der DZ BANK (über die Deutsche WertpapierService Bank AG) decken damit einen ganz wesentlichen Teil des Aufgabenfeldes des Single Officers ab. Zumindest solange keine erhöhten Verwahrrisiken oder andere Risiken für Finanzinstrumente des Kunden auftreten. >

Kontrollen

Die sich aus der Risikoanalyse ergebende Kontrolltätigkeit erstreckt sich insbesondere auf die Geschäftsfelder, die für Finanz-instrumente von Kunden besondere Risiken bergen. Hierzu gehören die Sicherungsübereignung von Finanzinstrumenten und die Wertpapierleihe. Beide Geschäftsarten werden von Volksbanken Raiffeisenbanken (in aller Regel) nicht angeboten. Zu empfehlen ist, dass der Single Officer darauf hinwirkt, dass das Durchführungsverbot dieser Geschäftsarten nicht nur in der Arbeitsanweisung für das Wertpapiergeschäft verankert ist, sondern auch in den Arbeitsanweisungen für das Kreditgeschäft und ggfs. für das Depot A.

Beratungsaufgabe

Der Single Officer hat auch eine beratende Funktion. Neben den eben beschriebenen, etwas „formalistischen" Tätigkeiten beschäftigten uns in den letzten Monaten deshalb auch konkrete Fragestellungen im operativen Geschäft, wie z. B.

- Lagerstellenumbuchung im Zusammenhang mit Investmentfonds und CSDR-Regelungen oder
- Abgrenzungsfragen zwischen Sicherungsübereignung und Verpfändungen von Wertpapieren.

AUTOR UND ANSPRECHPARTNER

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

Berichtswesen

Über all diese Tätigkeiten hat der Single Officer einmal jährlich zu berichten, und auch wir bereiten derzeit gerade den Jahresbericht vor. Als Mehrmandantendienstleister nutzen wir hier unser IT-System und erstellen einen Musterbericht, der dann aus den individuell im System befüllten Kontrolltätigkeiten für jede Bank befüllt wird.

Diese Vorgehensweise hilft uns, die Aufgaben des Single Officers so effizient wie möglich durchzuführen und den Mehraufwand in Grenzen zu halten. ▬

Informationssicherheit

Notfallmanagement

Die Konsultationen für MaRisk und BAIT sind veröffentlicht. Die Anforderungen an die Durchführung einer Business Impact Analyse wurden konkretisiert.

Die BaFin hat am 26. Oktober 2020 die Konsultationen für die Mindestanforderungen an das Risikomanagement (MaRisk) und die Bankaufsichtlichen Anforderungen an die IT (BAIT) veröffentlicht. Mit Blick auf die EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken (EBA/GL/2019/04) wird insbesondere AT 7.3 als Notfallmanagement neu gefasst und werden dabei die Anforderungen an das Notfallkonzept integriert. Die diesbezüglichen Regelungen stehen in engem Zusammenhang mit der Überarbeitung der BAIT.

So werden in den zu erwartenden MaRisk im AT 7.3 Notfallmanagement die Anforderungen an die Durchführung einer Business Impact Analyse konkretisiert. Dies beinhaltet zum Beispiel die Anforderungen an eine zugrunde liegende Prozesslandkarte sowie die Mindestinhalte der Auswirkungs-(Impact-) Analyse. Dies beinhaltet insbesondere auch die Berücksichtigung der BCM-Szenarien (Ausfall von kritischen Standorten, Personal, IT und Dienstleistern).

AUTOR UND ANSPRECHPARTNER

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

Prozessdifferenzierung zeichnet sich ab

Im Grunde wird die Prozessdifferenzierung deutlicher hervorgehoben: Das Business Continuity Management (BCM) ist ein übergeordneter Prozess und das IT Service Continuity Management (IT SCM) ist ein untergeordneter Prozess. IT SCM ist das Management der optimalen Verfügbarkeit von IT Services mit dem Ziel der Sicherstellung der Verfügbarkeit, unter Berücksichtigung der Wirtschaftlichkeit. Dabei sind nicht die technischen Wünsche und Machbarkeiten, sondern die Geschäftsanforderungen für das IT SCM maßgeblich. Diese ergeben sich eben aus dem BCM. BCM ist ein ganzheitlicher Prozess, der Unternehmen dabei hilft, potenzielle Bedrohungen und deren Einfluss auf ihre Geschäftsprozesse zu identifizieren.

Ferner sind für zeitkritische Aktivitäten und Prozesse Wirksamkeits- und Angemessenheitsprüfungen für alle Szenarien mindestens jährlich und anlassbezogen nachzuweisen. Gerade die konkretisierten und verschärften Anforderungen an die Durchführung von Tests und Übungen erfordern eine gut durchdachte und überwachte Planung. ▬

Schulungen

Sachkunde kompakt: Wissen wirkt

Mitarbeiterschulungen sind ein zentraler Eckpunkt aller Compliance-relevanter Regelungen. Egal ob KWG, GwG, MaRisk, MaComp, DSGVO oder BAIT: Immer werden zur Umsetzung der Verhaltens- und Organisationspflichten von den Instituten Sachkundeschulungen gefordert. Denn diese wirken dreifach.

Sachkundeschulungen dienen
- dem Schutz des Instituts,
- dem Schutz der Kunden und auch
- dem Schutz der Mitarbeiter/-innen selbst.

Um dieser Schutzaufgabe gerecht zu werden, müssen Schulungen mehr leisten, als nur Wissen zu vermitteln: Sie müssen sensibilisieren und die Mitarbeiter handlungsfähig machen. Im Beauftragtenwesen haben Schulungen eine besondere Bedeutung. Sie geht weit über die Erfüllung aufsichtsrechtlicher Anforderungen hinaus. Schulungen müssen relevantes Wissen vermitteln, sie müssen Mitarbeiter für Risiken sensibilisieren und sie müssen Mitarbeiter befähigen, angemessen zu handeln. Angemessen heißt hier: im Sinne des Gesetzgebers, der Aufsicht und auch der eigenen Unternehmens-Compliance.

AUTOR UND ANSPRECHPARTNER

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

Mit Expertenwissen …

Was schätzen Sie, wie viele Unternehmen von Wirtschaftskriminalität betroffen sind?

Tatsächlich liegt der Anteil der Unternehmen über 50 %. Nun ist die Zahl selber gar nicht so wichtig. Entscheidend ist, dass der Bankmitarbeiter einen realistischen Eindruck von der Bedrohungslage hat und vor allem, dass seine Aufmerksamkeit nachhaltig geweckt ist.

Bei der Neukonzeption unserer Schulungsangebote lassen wir uns von dem Gedanken leiten, dass wir zunächst (er)kennen müssen, was uns bedroht. Und dass wir dann im zweiten Schritt wissen sollten, was wir tun können. Faktenwissen allein reicht nicht aus, hinzukommen muss das Handlungswissen. Sachkundeschulung macht erst dann Sinn, wenn sie am Ende des Tages den Bankmitarbeiter befähigt, richtig zu handeln.

Alle Sachkundeschulungen werden inhaltlich von Fachexperten mit hoher praktischer Erfahrung erarbeitet und sind auf die jeweils aufsichtsrechtlich relevanten, aber vor allem auch in der Praxis notwendigen Themen fokussiert.

Ihr Datenschutz-, Geldwäsche-, IT-Sicherheits-, MaRisk-Compliance- oder WpHG-Compliance-Beauftragter tauscht sich jeden Tag aufs Neue mit Ihnen aus. Ihre Erfahrungen poolen wir – auch mit unserer Fachexpertise – und führen sie mit den aufsichtsrechtlichen Anforderungen zusammen. Dieses Wissen spielen wir (u. a.) im Rahmen der Schulungen an Sie zurück. Dann allerdings bedarfsorientiert priorisiert und in didaktischer Form aufbereitet.

… zur aufsichtsrechtlichen Souveränität

Die bedarfsorientierte Aufbereitung folgt Fragestellungen:

- Welche Anforderungen definiert das Aufsichtsrecht bzw. das Gesetz?
- Welche Schulungen brauchen Sie als Unternehmen, um Risiken (besser) abzusichern?
- Und welche Schulungen braucht der Mitarbeiter, um seiner Verantwortung gerecht zu werden?
- Wie kann im Rahmen von Schulungen die First Line of Defense gestärkt werden?

Im Ergebnis werden

- erforderliche Inhalte identifiziert (etwa Grundlagen im Bereich Marktmissbrauch oder auch eine neue Betrugsmasche),
- geeignete Medien ausgewählt (etwa ein WBT oder auch ein Rundschreiben/Warnhinweis) und
- die Teilnehmer bestimmt (etwa alle oder auch nur ausgewählte Mitarbeiter/innen).

Zeit und Aufmerksamkeit sind endlich. Wir müssen sorgsam damit umgehen. Dies gilt einmal mehr im beruflichen Alltag und auch für Schulungen. Schulungen müssen sich einfügen, müssen gut in den Arbeitsalltag integrierbar sein.

Die einzelnen Themen sind deshalb didaktisch von einer renommierten E-Learning-Agentur in Modulen aufbereitet. Sie sind nicht länger als zehn Minuten und über den Browser zeit- und ortsunabhängig abrufbar. Jede Schulung kann jederzeit unterbrochen und auch wiederaufgenommen werden.

Die schwer verdaulichen, teilweise ausufernden (aufsichts) rechtlichen Bestimmungen sind vollständig und fachlich korrekt und trotzdem – oder besser: gerade deshalb – kurz, verständlich und einprägsam dargestellt. Ohne auf die Lernmethodik näher eingehen zu wollen: Wir alle lernen besser, wenn wir die Themen aktiv bearbeiten können. Wir können Informationen besser verarbeiten, speichern und abrufen, wenn wir sie uns „zu eigen" machen. Davon abgesehen macht Lernen dann auch einfach mehr Spaß. Deshalb liegt der Interaktivitätsgrad in den Web-BasedTrainings (WBTs) auch durchgehend zwischen 50 und 70 % der Gesamtinhalte.

Nicht zuletzt: Die Schulungen sind so gestaltet, dass sie einfach aktuell zu halten sind: egal ob nun eine neue Betrugsmasche Erwähnung finden sollte oder ob eine aufsichtsrechtliche Novellierung den Anlass gibt.

Yes, we can do it

Der Mitarbeiter, die Mitarbeiterin wird befähigt, aus der jeweiligen Position heraus richtig zu handeln. Das Unternehmen stärkt seine First Line of Defense und dokumentiert die Durchführung aufsichtskonformer Schulungen.

Aktuell überarbeiten wir alle unsere Schulungen. Derzeit sind bereits folgende WBTs online:

- Grundlagen Geldwäsche- und Betrugsprävention
- Vertiefung Geldwäscheprävention – Privatkundenberater
- Vertiefung Geldwäscheprävention – Geschäftskundenberater
- Grundlagen Datenschutz
- Grundlagen WpHG-Compliance
- Vertiefung WpHG-Compliance – Marktmissbrauch

Weitere werden folgen.

Die Sachkundeschulungen sind Bestandteil der jeweiligen Auslagerungsdienstleistung: Datenschutz, Geldwäsche- und Betrugsprävention, Informationssicherheit und WpHG-Compliance. Aber sie sind auch jeweils außerhalb der Auslagerungsdienstleistung buchbar.

Gerne können Sie die Inhalte selbst und in Ruhe prüfen. Buchen Sie einfach unverbindlich ein vierwöchiges, kostenfreies Schnupper-Abo und machen Sie sich selbst ein Bild, überzeugen Sie sich selbst von den Vorteilen von Sachkunde kompakt:

- Relevantes Expertenwissen
- Praxisnahe Beispiele mit einprägsamen Geschichten-basierten Fällen
- Didaktisch aufbereitete Lerninhalte
- Zeitlich und räumlich unabhängige Lernmöglichkeiten durch Web-Zugang
- Optional
  - Jederzeitige zentrale Kontrolle und Überwachung des Lernfortschritts
  - Revisionssichere Dokumentation der geleisteten Lerneinheiten

Wir freuen uns über Ihr Interesse. ▬

MaRisk-Novelle 2021

Kleines Update oder umfangreiche Umsetzungsanforderungen?

Infolge der COVID-19-Pandemie hat sich die MaRisk-Novelle verzögert und wird nun – aller Voraussicht nach – Ende des ersten Quartals 2021 veröffentlicht. Erwartet werden insbesondere Anpassungen aufgrund der EBA-Leitlinien.

Ursprünglich wurde die Konsultation der novellierten Mindestanforderungen an das Risikomanagement (MaRisk) bereits für das Frühjahr 2020 erwartet. Kurz nach Ausbruch der COVID-19-Pandemie informierte die BaFin jedoch, dass die Arbeiten an der Novellierung der MaRisk mit etwas Verzögerung weitergehen, dass die neuen Vorgaben aber nicht zum Stichtag 31. Dezember 2020 gelten und somit für das Jahr 2020 nicht prüfungsrelevant sein werden.

Anfang August 2020 hat die BaFin dem Fachgremium MaRisk eine inoffizielle Arbeitsfassung zur sechsten MaRisk-Novelle übermittelt. Nach einer öffentlichen Konsultationsphase ist mit einer Veröffentlichung der neuen MaRisk inklusive Umsetzungsfristen für Neuerungen für Ende des ersten Quartals 2021 zu rechnen. Voraussichtlich wird es analog zur fünften MaRisk-Novelle eine Unterscheidung geben:

- Änderungen, die lediglich klarstellender Natur sind, müssen unmittelbar umgesetzt werden,
- neue Anforderungen, die nicht lediglich eine Klarstellung vorhandener Regelungen sind, müssen innerhalb einer Umsetzungsfrist (ein Jahr?) umgesetzt werden.

Wesentliche Änderungen der MaRisk basieren insbesondere auf der Umsetzung der EBA-Leitlinien

- über das Management notleidender und gestundeter Risikopositionen (EBA/GL/2018/06) und
- zu Auslagerungen (EBA/GL/2019/02).

Management notleidender und gestundeter Risikopositionen

Die Leitlinien über das Management notleidender und gestundeter Risikopositionen haben den wirksamen und nachhaltigen Abbau der Bestände sowie den begrenzten Zufluss notleidender Kredite zum Ziel. Zur Umsetzung der Vorgaben ist eine Strategie für notleidende Risikopositionen einzuführen und ein Implementierungsplan zur operativen Umsetzung der Strategie zu erstellen. Darüber hinaus wird die Umsetzung des Implementierungsplans regelmäßig zu überprüfen sein.

Daraus ergeben sich Stand heute aus unserer Sicht nicht unerhebliche Umsetzungsaufwände für die Institute.

Die Aufsicht führte – erschwerend – bereits in der Sitzung des Fachgremiums MaRisk im September 2019 aus, dass es für die Umsetzung der Leitlinien über das Management notleidender und gestundeter Risikopositionen voraussichtlich keine zusätzliche Übergangsfrist geben wird. Es ist jedoch auch davon auszugehen, dass die Vorgaben nur von Instituten mit hohem NPL-Bestand (NPL: Non-Performing Loans) anzuwenden sind.

Auslagerungen

Auch für die Umsetzung der EBA-Leitlinien zu Auslagerungen ist mit zahlreichen Anpassungen zu rechnen. So werden voraussichtlich insbesondere die vertraglich zu fixierenden Anforderungen zur Umsetzung in Auslagerungsverhältnissen steigen. Dazu gehören beispielsweise

- die Vereinbarung des für die Auslagerungsvereinbarung geltenden Rechts,

- eine mögliche Verpflichtung des Auslagerungsunternehmens, eine Versicherung abzuschließen, oder
- Regelungen zur Sicherstellung, dass das Auslagerungsunternehmen im Einklang mit den Werten des auslagernden Instituts handelt.

Weiterhin gehen wir davon aus, dass zukünftig

- ein zentraler Auslagerungsbeauftragter benannt und
- ein Auslagerungsregister mit umfangreichen Informationen zu den Auslagerungsvereinbarungen vorgehalten werden muss.

Mit der ZAM eG hat die Genossenschaftliche FinanzGruppe eine Lösung gefunden, die die aus der MaRisk-Novelle resultierenden Aufwandsaufschwünge bezüglich des Auslagerungsmanagements so geringfügig wie möglich halten soll (siehe S. 16).

Verschärfung bestehender Regelungen

Überdies ist anzunehmen, dass die BaFin im Rahmen der Novellierung auch bereits bestehende Regelungen verschärft – sei es durch die Ausweitung auf einen größeren Anwender- und Produktkreis oder die Verkürzung von Intervallen usw. Zwar werden die EBA-Leitlinien für die Kreditvergabe und Überwachung voraussichtlich erst in der siebten MaRisk-Novelle, und somit nicht in der anstehenden sechsten MaRisk-Novelle, implementiert. Dennoch ist bereits in der anstehenden MaRisk-Novelle mit erhöhten Anforderungen im Kreditgeschäft zu rechnen.

Fazit

Zusammenfassend lässt sich sagen, dass es sich bei der sechsten MaRisk-Novelle wahrscheinlich nicht nur um ein kleines Update handeln wird. Vor dem Hintergrund der Übernahme der EBA-Leitlinien ergibt sich umfassender Umsetzungsbedarf. Für die Institute wird es auch im Jahr 2021 keine Verschnaufpause geben. Neben der MaRisk-Novelle wird die Institute auch beispielsweise das Ende 2019 erschienene BaFin-Merkblatt zum Umgang mit Nachhaltigkeitsrisiken (weiter) beschäftigen, das bedingt durch die COVID-19-Pandemie in den meisten Instituten noch nicht vollständig umgesetzt wurde. Auch die EZB hat in ihrem Leitfaden zu Klima- und Umweltrisiken die Erwartungen der Aufsicht in Bezug auf das Risikomanagement und Offenlegungen zum Ausdruck gebracht. Darüber hinaus ist zu erwarten, dass sich aus dem EBA-Aktionsplan für nachhaltige Finanzierung zusätzliche Vorgaben ergeben werden.

Bei allem, was nun kommt, stehen wir unseren Kunden – im Rahmen unserer Auslagerungsmandate – aktiv zur Seite und bieten darüber hinaus auch anderen Häusern sehr gerne unsere Unterstützung bei der pragmatischen Umsetzung aufsichtsrechtlicher Neuerungen an.

Eines bleibt sicher: Wir werden Sie auch in 2021 tatkräftig unterstützen – und dies auch mit konkreten Produktinnovationen. So dürfen wir Ihnen zeitnah das ersehnte MaRisk-Rechtsmonitoring-Tool „RM kompakt“ vorstellen, das Ihnen mit vielen Funktionen die Arbeit in Bezug auf Abläufe und Dokumentationen weiter erleichtern wird. Mehr dazu in der nächsten Point of Compliance. ▬

AUTOR UND ANSPRECHPARTNER

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

Gastbeitrag

Genossenschaft für zentrales Auslagerungsmanagement – ZAM eG

Die im Juni 2020 gegründete ZAM eG setzt gesetzliche Vorgaben zur Steuerung des Auslagerungsdienstleisters Fiducia & GAD IT AG um. Ihre Aufgabe ist, den Steuerungsaufwand für ihre Mitglieder möglichst gering zu halten.

Ausgehend von der These, dass eine Bank dem Grunde nach durch zwei wesentliche Erfolgstreiber definiert wird, nämlich:

- zum einen durch ihre Mitarbeiterinnen und Mitarbeiter, deren Ideen, Strategien, deren Kundennähe und Fertigkeiten und
- zum anderen durch ihre IT-Systeme,

bedarf die aktive Steuerung und Kontrolle der Informationstechnologie (IT) einer ganz besonderen Aufmerksamkeit. Richtig ist: Nur mithilfe der IT können die Fertigkeiten und Fähigkeiten der Mitarbeiter*innen in Produkte bzw. Dienstleistungen (Daten, Verträge und Urkunden) umgewandelt werden. Damit hat die IT eine hohe strategische Bedeutung für jede Bank.

Das ändert sich auch dann nicht, wenn die Bank ihre IT, wie in der Genossenschaftlichen FinanzGruppe üblich, an einen Spezialanbieter auslagert. IT bleibt, was sie ist: ein wesentlicher Erfolgsfaktor für jedes einzelne Haus.

Ohne IT ist Banking nicht möglich

Die Verlagerung der IT auf einen Spezialisten ist gerade für genossenschaftliche Institute dem Grunde nach positiv.

Warum ist das so? Die für den Bankbetrieb erforderliche IT ist hochkomplex und störanfällig. Das notwendige Know-how, die zwingend erforderlichen Sicherheitsstandards und nicht zuletzt die dauerhafte finanzielle Ausstattung für den IT-Betrieb sind von regional tätigen und damit häufig kleineren Instituten (klein i.S.v. kleiner als nationale und international tätige und relevante Banken) faktisch nicht allein darstellbar. Es macht Sinn, wenn sich diese Institute einen hochspezialisierten Dienstleister suchen und gemeinsam finanzieren.

Insoweit ist auch der Aufsicht zuzustimmen, wenn sie sagt: „Mir ist lieber, Daten liegen in der Cloud eines Dienstleisters, der viel von Sicherheit versteht, als auf einem alten Server im Keller der Bank." (Raimund Röseler, Exekutivdirektor Bankenaufsicht, am 14.08.2020 – https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2020/fa_bj_2008_Cybersecurity-EDBA.html)

Pflichten bei Auslagerung

Die Verlagerung der IT bringt verstärkte Sorgfaltspflichten in der Kontrolle des Dienstleisters mit sich. Wenn eine Bank die IT an einen Dritten ausgelagert hat, ist bereits im Vorfeld auf den Dienstleister zwingend einzuwirken, und zwar in Bezug auf dessen

- Strategie,
- Produktentwicklungspfade,
- Programmierrichtlinien,
- Sicherheitsrichtlinien und vieles mehr.

Denn: Wenn der Auslagerungsdienstleister, im konkreten Fall die Fiducia & GAD, „Fähigkeiten, Ideen, Fertigkeiten und Dienstleistungen der Mitarbeiter*innen der Bank" in IT „übersetzt", dann muss – im Interesse der Bank und aufsichtsrechtlich gefordert – sichergestellt sein, dass das hieraus entstandene IT-Produkt auch dem entspricht, was die Bank gewollt hat. Insoweit muss sich die Bank bereits vor Fertigung der IT-Produkte eng mit dem IT-Dienstleister über Strategien, Produktkataloge, Qualitätssicherungsverfahren etc. abstimmen („Input Management").

Darüber hinaus muss die Bank überprüfen, ob am Ende das daraus entstandene Produkt auch den ursprünglichen Anforderungen des Input Managements entspricht, und wenn nicht, Maßnahmen einfordern, dass diese Deckungsgleichheit zukünftig hergestellt wird („Output Management" oder auch „Auslagerungssteuerung"). Genau diese Kontroll- und Steuerungsaufgaben des Output Managements übernimmt die ZAM eG für ihre Mitglieder. >

3 Fragen an Jens Saenger,

Sprecher der Geschäftsführung DZ CompliancePartner GmbH,
Vorstand der ZAM eG

Ein Mitgliedsbeitrag von 5 T€ plus Jahresentgelt – warum?

Jens Saenger: Lassen Sie mich klar formulieren: Wir sind der Idee eines „Cost plus"-Systems für die ZAM eG verpflichtet.

Zu Beginn des Umsetzungsprojektes haben wir die laufenden Kosten der ZAM eG auf Basis der Aufgabenstellung zusammen mit dem Vorprojekt erhoben. Hieraus haben wir einen „Business Case" für die weitere Projektarbeit abgeleitet. In diesem sind wir von einer Mitglieder- und Kundenanzahl von 300 Banken ausgegangen. Darauf fußt das Vergütungsmodell. Wir wussten, dass bei einer „optimistischen Prognose" die Anzahl der Banken höher und damit die Vergütung niedriger sein wird. Um das Dilemma zwischen einer kaufmännisch vorsichtigen Planung der ZAM eG (Basisannahme) und dem verständlichen Wunsch der Kunden nach niedrigen Kosten (beste Annahme) lösen zu können, haben wir bewusst auf die Genossenschaft zurückgegriffen: Die ZAM eG hat eine betriebswirtschaftlich sichere Grundlage, und den Interessen der Kunden kann durch die Option der genossenschaftlichen Rückvergütung entsprochen werden.

Die Idee der Genossenschaftsgründung hat darüber hinaus den Charme, dass über die Zeichnung von Mitgliederanteilen der Aufbau der Gesellschaft ohne externe Quellen finanziert werden konnte. Dieses Geld ist im Übrigen für die Bank „nicht weg", es wandert in der Bilanz nur vom Kassenbestand in Richtung Beteiligungskonto.

Ist es wahr, das die ZAM eG nur die Fiducia & GAD steuert?

Jens Saenger: Ja, sie wird zunächst „nur" die Fiducia & GAD steuern. Aber mit der formulierten Satzung und dem zentralen Auslagerungsregister ist die Möglichkeit geschaffen, weitere Auslagerungen zentral zu steuern. Ich bin überzeugt, dass die ZAM eG dies in ihren Gremien bereits im nächsten Jahr diskutieren wird.

Eine persönliche Frage: Warum engagieren Sie sich in der ZAM eG?

Jens Saenger: Wir – die DZ CompliancePartner und auch ich ganz persönlich – haben Erfahrungen im Aufbau derartiger Dienstleistungen und auch Unternehmen. Wir wurden gebeten, dies zur Kostenminimierung für den Verbund einzubringen. Das tun wir im Sinne des Verbundgedankens gerne.

Spätestens Ende des erstes Quartals 2021 wird sich die DZ CompliancePartner GmbH wieder aus der ZAM eG zurückziehen. Es gibt heute keine gesellschaftsrechtlichen Verflechtungen und auch die personellen Verbindungen zwischen der ZAM eG und der DZ CompliancePartner GmbH werden zu diesem Zeitpunkt wieder beendet. Für uns als Auslagerungsunternehmen mit der klaren Perspektive, später auch durch die ZAM eG gesteuert zu werden, erscheint mir dies auch angezeigt.

Im Fokus der Aufsicht: Output Management

Weil die IT so wichtig ist, führt kein Weg an einer nachhaltigen Verbesserung des Output Managements vorbei.

Die Aufsicht hatte bereits 2017 klargestellt, dass für sie die IT-Governance und Informationssicherheit den gleichen Stellenwert haben wie die Ausstattung der Institute mit Kapital und Liquidität. Wenn ein Institut wesentliche Tätigkeiten auslagert, dann benötigt es ein zentrales Auslagerungsmanagement.
Nach MaRisk hat das Auslagerungsmanagement

- Kontroll- und Überwachungsprozesse festzulegen und
- zu dokumentieren,
- regelmäßige Risikoanalysen sowie
- angemessene Kontrollen und Überwachungshandlungen im laufenden Betrieb durchzuführen.

Die BAIT ergänzen, dass bei jedem Softwarebezug ein risikosensibles Beurteilungsverfahren anzuwenden ist.

Egal wie groß eine Bank ist, wie ihr Geschäftsmodell aussieht, ob ihre Ambitionen klein oder groß sind: Alle müssen deutlich mehr für das Auslagerungsmanagement aufwenden als bisher.

Es zeichnet sich bereits jetzt ab, dass es für alle Banken ein „level playing field" geben wird, dem sich keiner wird entziehen können. Fakt ist: Auch die gesetzlichen Prüfer sind gehalten, das Auslagerungsmanagement zu prüfen und etwaige Mängel in der Auslagerungssteuerung – Output Management – anzuzeigen.

Leistungen

Die ZAM eG wird zunächst die Auslagerung auf die Fiducia & GAD IT AG steuern und sie unterstützt die interne Revision der Banken bei deren Prüfmaßnahmen durch Berichtsauswertung und Zulieferung geeigneter Dokumentationen.

Darüber hinaus stellt sie ihren Mitgliedern kostenfrei ein „Auslagerungsregister" zur Verfügung. Die EBA Guideline schreibt die Einrichtung eines Auslagerungsregisters pro Bank ab 2021 zwingend vor. Dementsprechend findet sich diese Verpflichtung auch im Konsultationspapier zu den neuen MaRisk. Die ZAM eG wird die Fiducia & GAD über ein solches Register steuern.

Das Register wird mit dem Roll-out ab Januar 2021 zur Verfügung stehen. Es ermöglicht den teilnehmenden Banken, künftig auch ihre anderweitigen Auslagerungen auf dieser Plattform (selber oder über die ZAM eG) zu steuern. Ein gewünschter Nebeneffekt: Durch den verbundweiten Standard wird so auch eine einheitliche Auslagerungssteuerung im Verbund über alle Auslagerungen möglich.

AUTORIN UND ANSPRECHPARTNERIN

Sarah Horn
Vorstand ZAM eG,
E-Mail: info@zam-eg.de

Chancen wahrnehmen

Die relative Homogenität der Gruppenmitglieder des genossenschaftlichen Finanzverbundes ermöglicht es, den unvermeidbaren Aufwandsaufschwung in den einzelnen Banken durch eine zentralisierte Steuerungseinheit über einen gemeinsamen Antritt abzufedern.

Bei allen Unterschieden sind die Geschäftsmodelle der genossenschaftlichen Banken doch so ähnlich, dass eine Vielzahl von Kontrollen und Steuerungsaspekten für alle Banken vergleichbar sind. In ca. 50 % aller Tätigkeiten des Output Managements werden die Aktivitäten der Banken vergleichbar oder sogar identisch sein. Die Bündelung auf einen zentralen Dienstleister vermeidet damit „Doppelarbeiten", genau genommen 850-malige Wiederholung. Ca. 50 % der Aufgaben sind stärker instituts-individuell zu lösen. Allerdings können auch hier Lernkurveneffekte den Aufwandsaufschwung abmildern. Durch die Bündelung der Interessen in einer Genossenschaft, der ZAM eG, können die Steuerungsimpulse des Output Managements deutlich prominenter platziert werden, als das ein einzelnes Institut aus einer Gruppe von 850 Banken könnte.
Kurz: Die Interessen der Banken können gegenüber der Fiducia & GAD besser vertreten werden.

Aber auch die Fiducia & GAD profitiert, denn sie muss nicht 850 Schnittstellen zu den einzelnen Banken bewirtschaften. Sie kann sich vielmehr auf die (wenigen) verbleibenden Schnittstellen konzentrieren und ihre Ressourcen weg von der Schnittstellenbewirtschaftung hin zur Problemlösung ausrichten.

Fazit

Um es auf den Punkt zu bringen: Man muss mehr tun. Kein Institut kann auf Gründe hoffen, nicht in sein Auslagerungsmanagement investieren zu müssen.

Ein zentrales Output Management kann den Kostenaufschwung abmildern und gleichzeitig den Steuerungsimpuls erhöhen. ▬

Interne Revision

Seit der letzten Berichterstattung in der Point of Compliance (2/2020, S. 27) wurden entsprechend der Jahresprüfungsplanung 2020 die Berichte zu den Prüffeldern „Geldwäsche- und Betrugsprävention", „Unternehmenssteuerung – Personalmanagement" und „Unternehmenssteuerung – Rechnungswesen" abgeschlossen und veröffentlicht.

Der Bericht zum Bereich „Geldwäsche- und Betrugsprävention" wurde als dienstleistungsbezogener Bericht an unsere Mandantschaft versandt.

Der Quartalsbericht zum dritten Quartal 2020 wurde turnusgemäß erstellt und ebenfalls unserer Mandantschaft zur Verfügung gestellt.

Darüber hinaus wurde turnusgemäß ein Follow-up-Quartalsbericht für das dritte Quartal 2020 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 – trotz Beeinträchtigungen durch die Corona-Pandemie – weiterhin stabil.

Die Erträge lagen Ende des dritten Quartals 2020 bei +11.962 T€ und damit nur –35 T€ unter Plan. Die Erlösrückgänge der ersten Monate konnten so in den Sommermonaten ausgeglichen werden.

Die Aufwände lagen bei –10.564 T€ und damit +310 T€ unter Plan (3 %). Das Ergebnis lag (unter Einbeziehung des Finanz- und neutralen Ergebnisses) mit +1.392 T€ kumuliert über Plan.

Zum Teil konnten die Corona-bedingten Reisebeschränkungen durch elektronische Medien ausgeglichen werden. Im Übrigen wurden diese Vor-Ort-Präsenztermine in den Sommermonaten nachgeholt oder bereits vorgezogen. Dadurch konnte und kann sichergestellt werden, dass die regulativen Vorgaben an die Beauftragtenfunktionen sicher erfüllt werden konnten und können.

Die DZ CompliancePartner GmbH hat alle Vorkehrungen zur sicheren Aufrechterhaltung ihres Geschäftsbetriebes getroffen. Auch wurde die Leistungsfähigkeit aller wesentlichen Partnerunternehmen regelmäßig überprüft: Alle haben dezidierte Notfallpläne in Kraft gesetzt und halten diese auch konsequent nach. So kann auch die Ausfallwahrscheinlichkeit eines dieser Dienstleister als sehr gering bewertet werden.

Insgesamt sieht sich die DZ CompliancePartner GmbH sicher in der Lage, auf die sich stets ändernden Rahmenbedingungen der Pandemie angemessen reagieren zu können und ihren Geschäftsbetrieb unter besonderer Berücksichtigung der aufsichtsrechtlichen Vorgaben ohne Störung fortführen zu können. ▬

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