Point of Compliance
Das Risikomanagement-Magazin

AUSGABE 3/2022

PoC

DZ CompliancePartner

IMPRESSUM

PoC – Point of Compliance
Das Risikomanagement-Magazin,
Ausgabe 29, 3/2022
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),
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:
Christina Fiedler, Martin Hierlemann, Derya Isikli, Martin Reglinski, Jens Saenger, Jörg Scharditzky, Lars Schinnerling, Katja Schlüter, Maximilian Schmidt, Thomas Schröder, Thomas Wagener, Benjamin Wellnitz

Bildnachweise: DZ CompliancePartner GmbH, iStockphoto
Gestaltung: Ralf Egenolf
Druck: Thomadruck, Dreieich

Redaktionsschluss: 17. November 2022
Auflage: 2.600 Exemplare

UNSER ANSPRUCH IST ES, Sie im Beauftragtenwesen zu entlasten und Ihnen nachhaltig den Rücken zu stärken. Dazu gehört auch, die komplexen und komplizierten regulativen Vorgaben handhabbar, praktisch und im Sinne des Verbundes umzusetzen und zu erläutern.

Das beginnt im Formalen – beispielsweise in unserer neugestalteten PoC, die nun klimaneutral auf FSC®-zertifiziertem Papier gedruckt ist – und zieht sich durch unser gesamtes Handeln: Wir übernehmen mit Ihnen Verantwortung.

Das Geldwäschegesetz wurde in den letzten 15 Jahren mehrfach geändert. Das Datenschutzrecht ist grundsätzlich neu geregelt. Auch die bankaufsichtlichen Anforderungen an die IT gewinnen immer mehr an Bedeutung angesichts der zwingend erforderlichen Sicherung der Banksysteme. In der MaRisk-Compliance ist eine deutlich höhere Taktung zu beobachten: Nachdem die letzte Novelle gerade mal ein Jahr alt ist, wird aktuell schon wieder eine Novelle konsultiert. Ein weiteres Beispiel ist die Nachhaltigkeitspräferenzabfrage in der WpHG-Compliance, deren Umsetzung zu einem erheblichen Mehraufwand führt. Schlussendlich steht eine Novelle des Hinweisgeberrechts in den nächsten Monaten an.

Im vorliegenden Heft berichten wir hierüber – wie immer nicht ganz „leichte Kost“, aber praxisorientiert und hoffentlich hilfreich. In diesem Sinn wünsche ich Ihnen eine anregende Lektüre.

Herzlichst

Ihr Jens Saenger

Jens Saenger
Sprecher der Geschäftsführung

Drittlandsübertragung von personenbezogenen Daten

Die neuen Standardvertragsklauseln (SCC) sollen mehr Sicherheit beim Datentransfer in ein Drittland ohne Angemessenheitsbeschluss schaffen. Jedoch herrscht Unsicherheit, wie dies in der Praxis datenschutzkonform umzusetzen ist und wie die damit einhergehenden datenschutzrechtlichen Herausforderungen gemeistert werden sollen.

Historie oder was bisher geschah

Bereits mit der Datenschutzrichtlinie 95/46/EG war es verboten, personenbezogene Daten (pbD) aus EU-Staaten in einen Drittstaat, also einen Staat außerhalb der EU, zu übertragen, wenn das Schutzniveau des Drittstaates nicht mit dem der EU vergleichbar war.

Daher galt bis 2015 das Safe-Harbour-Abkommen zwischen der EU und den USA. Es regelte die Einhaltung der Datenschutzgrundsätze durch US-Unternehmen. Dies geschah durch einen Eintrag auf die entsprechende Liste des US- Handelsministeriums (http://safeharbor.export.gov/list.aspx). Dadurch sollte eine Äquivalenz des Datenschutzniveaus in dem jeweiligen US-Unternehmen zum europäischen Datenschutz hergestellt werden und den Unternehmen die Übermittlung von personenbezogenen Daten aus der Europäischen Union in die USA ermöglicht werden.

Durch das Schrems-I-Urteil vom 6. Oktober 2015 wurde das Abkommen jedoch für nicht bindend und ungültig erklärt. In der Folge waren die US-Unternehmen, auch wenn sie sich der Einhaltung unterworfen hatten, verpflichtet, personenbezogene Daten jederzeit an die Sicherheitsbehörden herauszugeben. Daraufhin wurde das Privacy-Shield-Abkommen als Angemessenheitsbeschluss zwischen der EU und den USA eingeführt, das jedoch wiederum durch das Schrems-II-Urteil am 20. Juli 2020 für ungültig erklärt wurde.

Schlussendlich wurden die Anforderungen aus Art. 44 ff. DSGVO hinsichtlich der Datenübermittlung in Drittländer konkretisiert und in neue EU-Standardvertragsklauseln – Standard Contractual Clauses (SCC) – gefasst. Sie wurden zum 27. September 2021 in Kraft gesetzt. Sämtliche Verträge, die noch alte Standardvertragsklauseln enthalten, sind danach bis zum 27. Dezember 2022 durch neue zu ersetzen.

Die neuen EU-Standardvertragsklauseln

Am 4. Juni 2021 verabschiedete die EU-Kommission die neuen SCC, die als geeignete Garantien gemäß Art. 46 abs. 2 lit. c DSGVO gelten (Beschluss 2021/914/EU der Europäischen Kommission). Die neuen Standardvertragsklauseln legen die Rechtsgrundlage für den Daten-

transfer in Staaten fest, deren Datenschutzniveau nicht dem der EU gleichgestellt ist, und zu denen es auch keinen Angemessenheitsbeschluss der Europäischen Kommission gibt.

Bereits vor dem Schrems-II-Urteil des EuGH gab es Standardvertragsklauseln. Im Vergleich zu den alten Standardvertragsklauseln, die aus mehreren Sets bestanden und insgesamt zwölf Klauseln aufwiesen, gibt es nun ein Regelwerk aus insgesamt 18 Klauseln.Es ist modular aufgebaut und richtet sich an der jeweiligen Konstellation der Vertragsbeziehung und den entsprechenden Rollen der Vertragspartner aus.

Beispielsweise ist in Klausel 14 nun schriftlich geregelt, dass „bevor" Daten in ein Drittland transferiert werden, der jeweilige Stand und die Qualität des Datenschutzes im Verhältnis zum Europäischen Datenschutzniveau zu bewerten sind. Dies erfolgt unter dem Prüfungspunkt Transfer Impact Assessment (TIA).

Ferner ist in Klausel 15 neu reguliert, dass dem Datenimporteur eine Informationspflicht gegenüber dem Datenexporteur auferlegt ist. Dem Exporteur wird hierdurch die Möglichkeit der Überprüfung der Rechtmäßigkeit eines Auskunftsersuchens einer nationalen Behörde geschaffen.

Eine weitere Neuregulierung ist die in Klausel 7 eröffnete Möglichkeit, weitere Parteien zu den Standardvertragsklauseln beitreten zu lassen, die sogenannten „Kopplungsmöglichkeit".

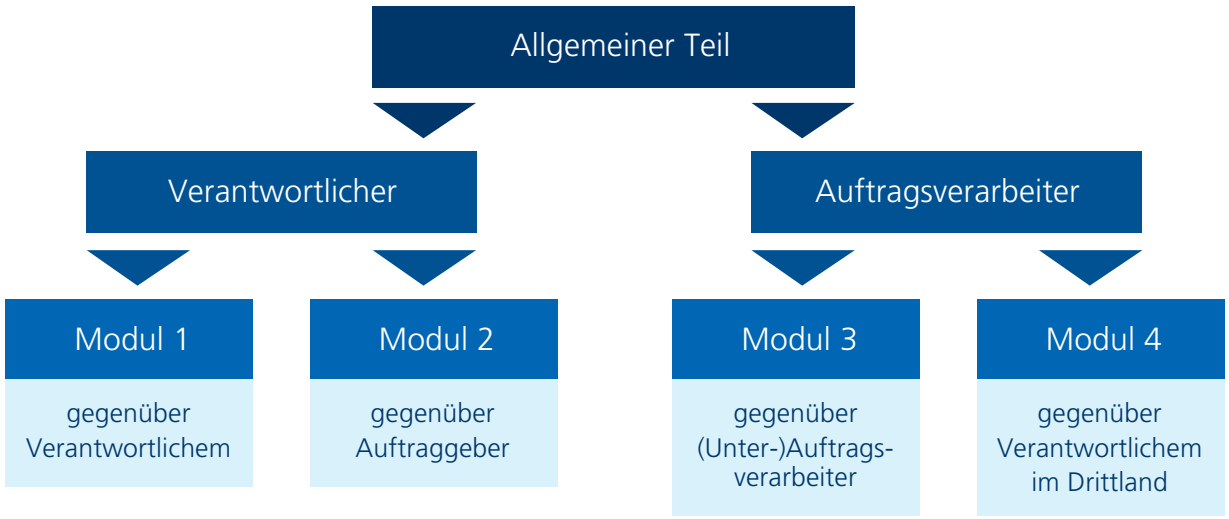
Zudem besteht nun in Klausel 12 lit. b eine Haftungsregelung bei Verletzung von Betroffenenrechten.

Durch den modularen Aufbau, unter strenger Einhaltung des allgemeinen Teils, werden nun verschiedene Situationen von Vertragspartnern abgebildet und wird daher eine flexible Gestaltung des Vertrages erwirkt.

Dieser Beitrag (Teil II) beschreibt die Standardvertragsklauseln (Methodik)
Teil I: Regulatorische Vorgaben aus Heft 2/2022 finden Sie hier:

SCAN ME

Abb. 1. **Aufbau Standardvertragsklauseln**



Vorgehensweise

Ob Daten in Staaten außerhalb der EU rechtmäßig übermittelt werden können, ist in einem mehrstufigen Prüfungsverfahren festzustellen.

1. Taugliche Rechtsgrundlage

Zunächst ist festzuhalten, dass es auch für die Übermittlung, die eine Verarbeitung von personenbezogenen Daten im Sinne des Art. 4 Nr. 2 DSGVO darstellt, einer Rechtsgrundlage bedarf. Dies ergibt sich ebenso aus den Vorschriften des Art. 6 Abs. 1 lit. a bis f DSGVO zur Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten, da die Regeln des Art. 44 ff. DSGVO lediglich die Übermittlung von personenbezogenen Daten in ein Drittland regeln und legitimieren.[1] Die Verarbeitung ist daher weiterhin an die Voraussetzungen der DSGVO geknüpft, Art. 44 HS. 4 DSGVO.

Ebenso gilt dies für die Einhaltung der rechtlichen Vorgaben hinsichtlich der Informationspflicht gemäß Art. 12 ff. DSGVO sowie der technisch-organisatorischen Maßnahmen gemäß Art. 32 DSGVO.

2. Angemessenes Schutzniveau

Nachdem die Rechtsgrundlage der Verarbeitung und die weiteren Voraussetzungen der DSGVO eingehalten sind, bedarf es der Prüfung, ob ein Angemessenheitsbeschluss für das konkrete Drittland vorliegt und hierdurch die Einstufung als sicheres Drittland bereits besteht.[2]

Sollte dies gegeben sein, dann bedarf es keiner weiteren Prüfung.

Besteht jedoch kein Angemessenheitsbeschluss, kommen die neuen Standardvertragsklauseln in Betracht, sofern keine anderen geeigneten Garantien gemäß Art. 46 ff. DSGVO vorliegen sollten.

3. Standardvertragsklauseln

Wichtig ist, dass das richtige Modul der Standardvertragsklauseln genutzt wird. Je nach Vertragsbeziehung der Parteien ist das entsprechende Modul auszuwählen und ist unveränderbar. Daher besteht bei Standardvertragsklauseln keinerlei Vertragsgestaltungsspielraum zwischen den Parteien.

4. Transfer Impact Assessment (TIA)

Durch das Transfer Impact Assessment soll eine risikobasierte individuelle Betrachtung des Drittlandtransfers erfolgen.

Gemäß der Klausel 14 der neuen Standardvertragsklauseln ist die Bewertung und Prüfung des Datenschutzniveaus im Zielland nun verpflichtend. Insbesondere die Zugriffsbefugnisse seitens staatlicher Behörden sind hierbei von Bedeutung.

Bei einer solchen Prüfung ist daher die Zugriffsmöglichkeit der staatlichen Behörde auf die personenbezogenen Daten sowie die Prüfung, wie der Datenimporteur im Drittland diese abwendet und vermeidet, miteinzubeziehen.

Bei der Bewertung hinsichtlich des Datenschutzniveaus bedarf es daher der Unterstützung des Datenimporteurs, denn nur dieser kann beurteilen, ob und wie Zugriffe staatlichen Behörden möglich sind und durchsetzbar sind. Diese Mitwirkung ist in Klausel 14 c auch schriftlich reguliert.

Auch ist der Datenimporteur verpflichtet, notwendige Informationen für die Prüfung bereitzustellen sowie der gemeinsamen Dokumentationspflicht nach Klausel 14 e nachzukommen.

Daher müssen beide Parteien das Transfer Impact Assessment gemeinsam durchführen.

Es ist darüber hinaus sinnvoll, eine Datenschutz-Folgenabschätzung (DSFA) gemeinsam mit dem jeweiligen Vertragspartner durchzuführen. Dadurch können alle wichtigen Punkte entsprechend gewürdigt und in die Bewertung einbezogen werden.

Weitere mögliche Maßnahmen zu den Standardvertragsklauseln

Aufgrund der kritischen Stimmen der deutschen Aufsichtsbehörden vor allem hinsichtlich des Drittlandtransfers in die USA sollten insbesondere die technisch-organisatorischen Maßnahmen eine hohe Beachtung bei der Prüfung finden.[3] Eine Vorlage des Datenschutz- und Sicherheitskonzepts des Vertragspartners im Drittland ist daher von Vorteil.

Derya Isikli
Beauftragte Informationssicherheit & Datenschutz,
E-Mail: derya.isikli@dz-cp.de

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

Weitere Maßnahmen sind die Speicherung und der Support in der EU. Von Bedeutung sind auch eine spezielle Risikoanalyse und eine Datenschutz-Folgenabschätzung für den Transfer in ein Drittland.

Zudem könnte eine geeignete Maßnahme darin bestehen, die Daten nach der Einstufung des jeweiligen Risikos bei der Verarbeitung aufzuteilen.

Im Rahmen von Dienstleisterketten sollte der Verantwortliche das Transfer Impact Assessment zwischen den Dienstleistern im Rahmen des Auftragsverarbeitungsvertrages gemäß Art. 28 DSGVO überprüfen.

Besonderheit bei Drittlandtransfer von personenbezogenen Daten in die USA

Am 7. Oktober 2022 hat der derzeitige Präsident Joe Biden den „Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities" unterzeichnet. Hierdurch soll eine Grundlage geschaffen werden, dass der Datentransfer zwischen europäischen und US-Unternehmen wieder DSGVO-konform, ohne rechtlichen und umständlichen Mehraufwand, erfolgen kann.[4]

Zwar können sich danach EU-Bürger beim „Civil Liberties Protection Officer" der US-Geheimdienste über möglichen Datenmissbrauch beschweren und auf der zweiten Ebene dann die jeweilige Entscheidung beim „Data Protection Review Court" anfechten. Jedoch besteht das eigentliche Problem weiterhin: Die US-Sicherheitsgesetze, wie der Foreign Intelligence Surveillance Act (FISA) oder Cloud Act, ermöglichen die Überwachung von EU-Bürgern, sofern die Daten im Zugriff eines US-Konzerns liegen.

Wie sich die EU-Kommission hierzu letztlich äußern wird, bleibt offen.

Resümee

Hinsichtlich der personenbezogenen Datenverarbeitung sowie des Datentransfers in ein Drittland gelten besondere Anforderungen gemäß der DSGVO. Es ist ratsam, regelmäßig den Datenschutzbeauftragten einzubinden und Verarbeitungen, die im Verzeichnis für Verarbeitungstätigkeiten gemäß Art. 30 DSGVO dokumentiert sein sollten, auf Drittlandsübertragungen zu überprüfen. Im Anschluss sollten die Verträge hierzu geprüft werden, inwiefern diese die aktuellen Standardvertragsklauseln verwenden. Sofern alte Standardvertragsklauseln verwendet werden, sollten diese zeitnah durch die aktuellen Standardvertragsklauseln ersetzt werden.

Eine gesonderte stichprobenartige Überprüfung durch die Landesdatenschutzbehörden kann in diesem Zusammenhang nicht ausgeschlossen werden.[5] ▬

[1] Übertragung personenbezogener Daten in ein Drittland | DSGVO (keyed.de), abgerufen am 14.11.2022

[2] Beispiele für Drittländer mit bestehendem Angemessenheitsbeschluss: Andorra, Argentinien, Färöer, Guernsey, Isle of Man, Israel, Japan, Jersey, Neuseeland, Schweiz, Uruguay

[3] https://www.it-daily.net/it-sicherheit/datenschutz-grc/was-beim-tia-transfer-impact-assessment-beachtet-werden-muss, abgerufen am 14.11.2022

[4] Neues EU-US-Datentransfer-Abkommen nimmt erste Hürde | heise online, abgerufen am 14.11.2022

[5] https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/neue-standardvertragsklauseln-frist-fur-die-umstellung-von-altvertragen-endet-demnachst-216765.html, abgerufen am 14.11.2022

Der Datenschutzbeauftragte als Tausendsassa?

Rollen und Verantwortlichkeiten in der Datenschutzorganisation: Im Datenschutzbereich fallen zahlreiche strategische und operative Aufgaben an. Eine Aufgabenverteilung hilft dabei, die einer jeden Datenschutzorganisation innewohnenden Risiken zu reduzieren.

Die Datenschutz-Grundverordnung (DSGVO) überträgt Verantwortlichen und Auftragsverarbeitern die Pflicht, ihre innerbetriebliche Datenschutzorganisation derart zu gestalten, dass die Datenverarbeitungen jederzeit im Einklang mit den Anforderungen erfolgen. Werden dabei lediglich die gesetzlichen Mindestanforderungen umgesetzt, geraten Datenschutzorganisationen in der betrieblichen Realität schnell an ihre Grenzen: Sie halten den komplexen regulatorischen und aufsichtsbehördlichen Anforderungen sowie den veränderten Kundenerwartungen nicht stand. Unternehmen, die lediglich einen Datenschutzbeauftragten benennen (egal ob intern oder extern) und damit die Erwartung verbinden, alle ihre Verpflichtungen aus der DSGVO umgesetzt und eine fortlaufende Compliance sichergestellt zu haben, werden für diesen Irrtum häufig abgestraft.

Überforderung und Interessenkollision

Ein durchschnittlich informierter Beschäftigter ist mit den komplexen datenschutzrechtlichen Bestimmungen üblicherweise nicht im Einzelnen vertraut. In zahlreichen Fällen (beispielsweise bei Vertragserstellung, Änderungen von Geschäftsprozessen, Produkteinführungen, Kundenbeschwerden oder im Falle von Datenschutzverletzungen) besteht daher das Bedürfnis nach Beratung und Unterstützung. In Ermangelung einer speziellen Stelle im Unternehmen wird in all diesen Fällen häufig der Datenschutzbeauftragte konsultiert. Dabei wird nicht selten der gesetzliche Beratungsauftrag falsch verstanden und als Unterstützungsauftrag ausgelegt. Es wird erwartet, dass der Datenschutzbeauftragte die Aufgaben in Gänze übernimmt. Aus naheliegenden Gründen können diese Aufgaben aber nicht in vollem Maße an ihn delegiert werden. Der Hauptgrund für diese Limitierung besteht in der gesetzlich geforderten Unabhängigkeit des Datenschutzbeauftragten und der damit zusammenhängenden Problematik von latenten Interessenkonflikten.

Die zwischen der notwendigen Bestellung eines Datenschutzbeauftragten und der Erfüllung operativer Compliance-Pflichten bestehende Lücke muss durch weitere Maßnahmen geschlossen werden. Hierzu sind organisatorische und personelle Aspekte festzulegen. Im Folgenden soll aufgezeigt werden, welche Bereiche, Stellen und Funktionen in eine risikoadäquate Datenschutzorganisation eingebunden werden sollten.

Unternehmensleitung und Supportbereiche

Gesamtverantwortung für den Datenschutz trägt die Unternehmensleitung (Vorstand, Geschäftsführung). Dies umfasst die Verantwortung für die wirksame Umsetzung und regelmäßige Kontrolle aller datenschutzrechtlichen Vorgaben. Sofern die Aufgaben zur Umsetzung der Vorgaben an Mitarbeiter delegiert werden, muss dies in geeigneter Weise dokumentiert werden. Dazu gehört es, dass mittels Anweisungen wie Leitlinien, Richtlinien, Arbeitsanweisungen die einzelnen Stellen und deren Aufgaben in

der Aufbau- und Ablauforganisation festgelegt werden. Die Leitung trägt die Verantwortung für die Bereitstellung der erforderlichen finanziellen, sachlichen wie personellen Ressourcen und muss durch Etablierung eines Reportingsystems sicherstellen, dass sie trotz Delegation von Aufgaben und Zuständigkeiten stets über den Zustand des Datenschutzes im Unternehmen informiert bleibt. Eine regelmäßige (auch unterjährige) Berichterstattung ist daher zwingend erforderlich. Es bietet sich zudem an, dem Datenschutzbeauftragten eine Teilnahme an Vorstandssitzungen zu ermöglichen, soweit dort datenschutzrechtliche Themen vorgestellt und besprochen werden.

Auch einzelnen Supportbereichen (also speziellen Fachbereichen mit Management- und Servicefunktionen, z. B. Organisation, Recht, Informationssicherheit und Revision) können Aufgaben aus der Datenschutzorganisation zugewiesen werden. In Betracht kommen hier etwa die Bearbeitung von Beschwerden mit Datenschutzbezug, Betroffeneneingaben zu Einwilligungen, Widersprüchen, Auskunftsersuchen und Löschersuchen. Häufig werden in Supportbereichen bereits ticketbasierte Lösungen eingesetzt, die für die Bearbeitung von Betroffenenrechten mitgenutzt werden können. Darüber hinaus können sie mit spezifischem Know-how Aufgaben z. B. in der Beschaffung und dem Lieferantenmanagement übernehmen, Vertragsprüfungen durchführen und Sicherheitsmaßnahmen prüfen und bewerten (Informationssicherheit).

Operative Organisationseinheiten

Für die Umsetzung der restlichen datenschutzrechtlichen Vorgaben sind grundsätzlich die operativen Organisationseinheiten (Fachbereiche/Geschäftsbereiche) zuständig. Als Prozess- und Verarbeitungsverantwortliche tragen sie für einen angemessenen Schutz der verarbeiteten personenbezogenen Daten bei der Gestaltung und Durchführung ihrer Datenverarbeitungen Sorge. Dies umfasst insbesondere die Vornahme datenschutzrechtlicher Risikobewertungen, Erstellung von Löschkonzepten und bedarfsweise Durchführung von Datenschutz-Folgenabschätzungen. Um eine Nachweisbarkeit der Maßnahmen zu gewährleisten, haben die Organisationseinheiten eine angemessene Dokumentation anzufertigen und grundsätzlich auch die fortlaufende Pflege des Verzeichnisses der Verarbeitungstätigkeiten zu übernehmen. Ab einer gewissen Größe und Innovationsfreudigkeit sollten Organisationseinheiten als Schnittstelle zum Datenschutzbeauftragten einen eigenen Koordinator benennen.

Möglichkeiten und Grenzen der Aufgabenzuweisung an den Datenschutzbeauftragten

Die Aufgaben des Datenschutzbeauftragten ergeben sich zunächst aus den Artikeln 38 und 39 DSGVO. Danach fungiert er u. a. als Anlaufstelle für betroffene Personen. Ihm obliegt die Unterrichtung und allgemeine Beratung der Organisationseinheiten und die spezielle Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung. Er hat entsprechend im Unternehmen adressatengerecht zu kommunizieren und der höchsten Managementebene zu berichten. Seine Hauptaufgabe liegt jedoch in der Überwachung der Einhaltung der Datenschutzvorschriften im Unternehmen. Die Stelle des Datenschutzbeauftragten ist daher als unabhängiges Überwachungsorgan auszugestalten. Das verantwortliche Unternehmen muss ihm die dazu notwendige Unabhängigkeit gewähren. Führt er Aufgaben bzw. operative Tätigkeiten aus, die er im Rahmen seiner Überwachungstätigkeit kontrollieren sollte, treten schnell Interessenkonflikte zutage.

Es existieren zahlreiche mögliche Fallkonstellationen, in denen es zu einer „kritischen Nähe“ verschiedener Tätigkeiten kommen kann. Für die Frage nach der Zulässigkeit des Tätigwerdens sind oft Details ausschlaggebend. In welchen Fällen der Verantwortliche den Datenschutzbeauftragten als Erfüllungsgehilfen heranziehen kann, soll nachfolgend anhand ausgewählter Pflichten erläutert werden:

1. **Beantwortung von Betroffenenanfragen einschließlich Datenschutzbeschwerden**
   Die Beantwortung von Betroffenenanfragen sollte nach Möglichkeit durch zentrale Servicebereiche erfolgen, da diese ohnehin regelmäßig Kundenkorrespondenz führen. Der Datenschutzbeauftragte kann hier zuarbeiten. Soll die Bearbeitung vollständig an den Datenschutzbeauftragten delegiert werden, ist dies als wesentlicher Faktor bei seiner regelmäßigen Aufwandsabschätzung (Umfang der nötigen Aufwände) zu berücksichtigen.

2. **Erstellung und Pflege des Verzeichnisses von Verarbeitungstätigkeiten**
   Nach Art. 30 DSGVO ist der Verantwortliche (also die Unternehmensleitung oder die Fachbereiche) für die Erstellung und Pflege eines Verarbeitungsverzeichnisses zuständig. In der Praxis kann trotzdem häufig beobachtet werden, dass diese Aufgabe durch den Datenschutzbeauftragten wahrgenommen wird. Dies ist dann pro-

blematisch, wenn der Datenschutzbeauftragte damit nicht ausdrücklich von seiner Unternehmensleitung beauftragt wurde. Es ist zudem sicherzustellen, dass die jeweiligen Prozess- und Verarbeitungsverantwortlichen zur fortlaufenden Bereitstellung der erforderlichen Informationen verpflichtet werden und die Vollständigkeit und Aktualität des Verzeichnisses im Rahmen des Internen Kontrollsystems (IKS) überwacht wird.

3. **Entscheidung über die Meldung von Datenschutzverletzungen**
   Eine Beteiligung des Datenschutzbeauftragten bei Bewertungs- und Dokumentationsvorgängen im Rahmen von Datenschutzverletzungen sollte nach Möglichkeit vermieden werden. Die Vorfälle können durch den Datenschutzbeauftragten begleitet und bedarfsweise nachträglich durch ihn geprüft werden. Entsprechende Prüfungen würden durch eine zu aktive Rolle in den zu prüfenden Vorgängen jedoch entwertet. In keinem Fall darf ihm die Kompetenz zur Entscheidung von Meldungen nach Art. 33 bzw. Benachrichtigungen gemäß Art. 34 DSGVO übertragen werden.

4. **Durchführung einer Datenschutz-Folgenabschätzung**
   Der Datenschutzbeauftragte ist verpflichtet, die Durchführung der Datenschutz-Folgenabschätzung zu überwachen. Daraus folgt, dass er sie nicht selbst durchführen, sondern lediglich eine beratende Funktion einnehmen darf. Folgenabschätzungen sind mitunter komplex und zeitaufwändig. Es bietet sich daher regelmäßig an, einen Dienstleister hinzuzuziehen.

Nicht nur die Zuweisung einzelner operativer Datenschutztätigkeiten, auch die gleichzeitige Wahrnehmung artfremder Aufgaben durch den Datenschutzbeauftragten kann zu Interessenkonflikten führen. Positionen, bei denen über Zwecke und Mittel einer Datenverarbeitung entschieden wird, dürfen Datenschutzbeauftragte nicht innehaben. Mitglieder der Geschäftsführung oder des Vorstandes sowie Beschäftigte mit ausgewählter Leitungsfunktion (Leitung der Personalabteilung, Leitung der IT-Abteilung, Leitung der Rechtsabteilung, Leitung der Marketing- oder Vertriebsabteilung) können daher nicht wirksam als Datenschutzbeauftragte benannt werden.

Unzulässig ist eine Benennung zum Datenschutzbeauftragten laut dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit regelmäßig auch für hierarchisch nachgeordnete Positionen, wie etwa Beschäftigte in der IT oder Personalabteilung sowie für Gesellschafter und Familienangehörige der Geschäftsleitung.

Die Übernahme der Funktion des Datenschutzbeauftragten in Personalunion mit der Tätigkeit des Informationssicherheitsbeauftragten oder Compliance-Beauftragten ist laut dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit ebenfalls in einigen Fällen unzulässig. Ähnlich kritisch äußerten sich dazu in der Vergangenheit bereits die Datenschutz-Aufsicht in Bremen sowie der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit.

Sehr bedenklich ist auch die Wahrnehmung in Personalunion mit dem Amt des Betriebsratsvorsitzenden oder des Revisionsleiters, da es dem Datenschutzbeauftragten auch hier an der notwendigen Unabhängigkeit fehlen könnte. Unternehmen sollten zudem stets einen Vertreter benennen, für den die gleichen Anforderungen gelten. Sofern dies intern nicht abgebildet werden kann, bietet sich eine externe Beauftragtenvertretung an.

Maximilian Schmidt
Beauftragter Informationssicherheit und Datenschutz,
E-Mail: maximilian.schmidt@dz-cp.de

Datenschutzteam

Egal ob sich Verantwortliche dafür entscheiden, dem Datenschutzbeauftragten zur Vermeidung von Interessenkonflikten keine operativen Datenschutzaufgaben zu übertragen oder ob sie ihm in zulässiger Weise begrenzte operative Tätigkeiten delegieren: Es bedarf in jedem Fall einer oder mehrerer weiterer Stellen, die im Rahmen der Datenschutzorganisation die verbleibenden Pflichten übernehmen und insbesondere die Fachbereiche unterstützen. Hierzu sind entsprechende Stellen mit den erforderlichen Kompetenzen einzurichten. Um zu gewährleisten, dass Ausrichtung und Umsetzung des Datenschutzes im gesamten Unternehmen einheitlich erfolgen, können die entsprechenden Stellen in einem Datenschutzteam institutionalisiert werden. Abhängig von der Unternehmenskultur und dem vorherrschenden Management-Commitment bietet es sich an, auch die Unternehmensleitung im Rahmen ihrer Möglichkeiten ins Datenschutzteam einzubinden.

Es handelt sich hierbei um ein Modell, das im Hinblick auf unterschiedliche Einflüsse anzupassen ist, insbesondere Größe der Organisationseinheit, Umfang und Kritikalität der Datenverarbeitung. Gerade in kleineren Unternehmen können mehrere Rollen zusammenfallen oder sind extern zu besetzen.

Es haben sich verschiedene Bezeichnungen für entsprechende Stellen/Rollen etabliert (z. B. Datenschutzmanager, Datenschutzkoordinator, Datenschutzreferent). Wie die Stelle bezeichnet wird und welche Aufgaben ihr letztlich zugewiesen werden, kann jedes Unternehmen selbst entscheiden. Am geläufigsten dürfte der Datenschutzkoordinator sein, der insbesondere bei einer Auslagerung des Datenschutzbeauftragten als dessen Ansprechpartner fungiert, aber nicht zwangsläufig operative Datenschutzaufgaben ausführt. Gerade bei externen Datenschutzbeauftragten ist eine Zuarbeit durch eine operative Einheit jedoch sinnvoll. Entsprechend sollten Aufgabenverteilungen, klare Abgrenzungen zwischen den operativen Datenschutzrollen sowie dem Datenschutzbeauftragten und Fragen der Zusammenarbeit organisatorisch geregelt werden.

Fazit

Wird die Bedeutung einer arbeitsteiligen Datenschutzorganisation verkannt, drohen erhebliche Compliance-Risiken. Die strategische und operative Umsetzung des Datenschutzes muss durch geeignete strukturelle Maßnahmen und Prozesse sichergestellt werden. Der Datenschutzbeauftragte kann wie gezeigt nur in einigen Fällen herangezogen werden, da er laut Gesetz eine Beratungs- und Überwachungsfunktion innehat und insoweit nicht die Rolle eines „Datenschutz-Sachbearbeiters“ für die Fachbereiche übernehmen darf. Mithin verbleiben einige Aufgaben und Pflichten, die entweder geeigneten internen Bereichen oder neu zu schaffenden (internen oder externen) Stellen übertragen werden müssen. ▬

Aktuelle Entwicklungen

Die FATF veröffentlicht ihren Abschlussbericht über die jüngste Deutschlandprüfung.Das BMF stellt die „Eckpunkte für eine schlagkräftigere Bekämpfung der Finanzkriminalität und eine effektivere Durchsetzung von Sanktionen in Deutschland“ vor. Unter anderem sind eine neue „Bundesoberbehörde zur Bekämpfung der Finanzkriminalität“ (BBF) und weitere weitreichende Schritte in der Geldwäschebekämpfung geplant.

Abschlussbericht der FATF

Die Financial Action Task Force (FATF) – das wichtigste internationale Gremium zur Bekämpfung und Verhinderung von Geldwäsche, Terrorismusfinanzierung und Proliferationsfinanzierung – hat am 25. August 2022 ihren Abschlussbericht über die letzte Prüfung Deutschlands veröffentlicht. Die FATF-Mitgliedstaaten, zu denen auch Deutschland gehört, werden regelmäßig auf die Umsetzung der FATF-Standards überprüft. Die Deutschlandprüfung begann im September 2020. Bei der letzten Länderprüfung im Jahr 2010 hatte die FATF Deutschland Verbesserungsbedarf attestiert.

Der Fokus der jüngsten Prüfungen sollte dabei erstmals auf dem Nachweis der Effektivität liegen. Insbesondere wurde evaluiert, ob Verpflichtete im Nichtfinanzsektor ihre Risiken im Hinblick auf Geldwäsche und Terrorismusfinanzierung kennen und die vorgeschriebenen Präventionsmaßnahmen umsetzen. Die FATF hat auch geprüft, ob die zuständigen Behörden die Präventionsmaßnahmen effektiv beaufsichtigen.

Im Ergebnis attestiert die FATF insbesondere der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) eine positive Entwicklung. Die FATF sieht aber nach wie vor ebenso wichtige Herausforderungen und konkreten Handlungsbedarf.

Deutschland hat zwar in den letzten fünf Jahren bedeutende Reformen durchgeführt, um sein System zu stärken und Geldwäsche und Terrorismusfinanzierung wirksamer zu bekämpfen. Es sind allerdings weitere Reformen umzusetzen, um sicherzustellen, dass auf operativer Ebene Ressourcen bereitgestellt und Prioritäten gesetzt werden, um illegale Finanzströme zu bekämpfen.

Nach Feststellung der FATF haben deutsche Behörden zwar ein gutes Verständnis für diese Risiken und arbeiten konstruktiv mit entsprechenden Stellen in anderen Ländern zusammen. Allerdings ist die Koordinierung zwischen den 16 deutschen Bundesländern laut FATF eine Herausforderung. Die Organisation und das Zusammenspiel zwischen den verschiedenen Aufsichtsbehörden – gerade und insbesondere im und für den Nichtfinanzsektor – und den Strafverfolgungsbehörden sollte verbessert werden.

Priorität sollte laut FATF auch der Minderung der Risiken eingeräumt werden, die mit der hohen Verwendung von Bargeld und der Nutzung informeller MVTS-Dienste (Money or Value Transfer Services) verbunden sind. Denn nach wie vor erfreut sich in Deutschland die Verwendung von Bargeld großer Beliebtheit und, damit verbunden, auch die Möglichkeit zur Anonymisierung von Zahlungsströmen.

Weiterhin mahnt die FATF weitere Verbesserungen bei der Ausstattung des Transparenzregisters und bei den über das Register verfügbaren Information an.

Spielraum besteht dem Länderbericht zufolge auch, wenn es um die Stärkung der Rolle der Financial Intelligence Unit (FIU) und die Beschaffung von Finanzinformationen geht.

Eckpunkte des Bundesfinanzministeriums

Quasi als Antwort auf die Deutschlandprüfung der FATF stellte das Bundesfinanzministerium (BMF) bereits einen Tag vor der Veröffentlichung des Berichtsergebnisses seine „Eckpunkte für eine schlagkräftigere Bekämpfung der Finanzkriminalität und eine effektivere Durchsetzung von Sanktionen in Deutschland“ vor.

Die Pläne des BMF sehen insbesondere vor, die wichtigsten Kompetenzen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung unter dem Dach einer neuen Behörde auf Bundesebene zu bündeln. Damit soll die Finanzkriminalität in Deutschland entschieden eingedämmt werden. Die Eckpunkte sehen die folgenden drei Maßnahmen vor.

1. Kernkompetenzen unter einem Dach bündeln
2. Hoch qualifizierte Finanzermittlerinnen und Finanzermittler ausbilden
3. Digitalisierung und Vernetzung von Registern vorantreiben

1. Bündelung der wichtigsten Kompetenzen

Mit der Bündelung der wichtigsten Kompetenzen unter dem Dach einer neuen Behörde, der „Bundesoberbehörde zur Bekämpfung der Finanzkriminalität“ (BBF), sollen alle relevanten Funktionen und Kompetenzen zusammengezogen werden:

Neues Bundesfinanzkriminalamt (BFKA)

„Ein neu geschaffenes Bundesfinanzkriminalamt soll gezielt komplexe Fälle von Finanzkriminalität aufklären und bündelt hierfür die erforderliche Expertise. Es verfolgt den ‚follow-the-money’-Ansatz, fokussiert also auf illegale Finanzströme. Es bietet darüber hinaus die nötige klare Struktur für eine effektive Durchsetzung von Sanktionen.“

Effektivere Zentralstelle für Finanztransaktionsuntersuchungen (Financial Intelligence Unit)

„Anfangspunkt zahlreicher Ermittlungen sind Verdachtsmeldungen, die bei der FIU eingehen. Die FIU ist daher wichtiger Partner des BFKA. Sie wird als zweite Säule unter dem Dach der BBF integriert und als unabhängige Analyseeinheit entsprechend den europäischen und internationalen Vorgaben fortgeführt. Durch gezieltere Steuerung und risikobasierte Ausrichtung soll die FIU weiteres Effizienzpotenzial heben.“

Neue Zentralstelle für Geldwäscheaufsicht

„Neu geschaffen wird als dritte Säule eine Zentralstelle für Geldwäscheaufsicht. Sie koordiniert künftig die Aufsicht über den Nichtfinanzsektor, der neben unterschiedlichsten Gewerbetreibenden z. B. auch Veranstalter von Glücksspiel umfasst. Dabei ist das Ziel, die Zahl der Aufsichtsbehörden der Länder von derzeit über 300 zu reduzieren. Darüber hinaus hat die Zentralstelle die Aufgabe, Leitlinien und Standards für eine risikobasierte Aufsicht aus einem Guss zu erarbeiten, und soll der zukünftigen europäischen Geldwäscheaufsichtsbehörde AMLA als zentraler Ansprechpartner zu Fragen des Nichtfinanzsektors in Deutschland dienen.“

2. Hoch qualifizierte Finanzermittlerinnen und Finanzermittler ausbilden

„Um Expertise in der Bekämpfung von Finanzkriminalität auf- und auszubauen, sollen hoch qualifizierte Finanzermittlerinnen und Finanzermittler ausgebildet werden. Den Ausgangspunkt dafür bildet ein Kern besonders relevanter Trainings. Gemeinsam mit Expertinnen und Experten wird dieses Angebot ausgebaut und konzeptionell weiterentwickelt.“

3. Digitalisierung und Vernetzung von Registern vorantreiben

„Um Eigentumsverhältnisse und wirtschaftlich Berechtigte insbesondere im Ermittlungsfall oder bei Sanktionsdurchsetzung effizient prüfen zu können, sollen alle dafür relevanten Register digital verknüpft werden. Bis zur Umsetzung einer solchen umfassenden Vernetzung sollen einfach zu realisierende Übergangslösungen schnell unmittelbaren Mehrwert bieten.“

Die vom BMF veröffentlichten Eckpunkte finden Sie auch auf der Internetseite des Ministeriums unter https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Schlaglichter/Geldwaesche-bekaempfen/voller-einsatz-gegen-finanzkriminalitaet.html ▬

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

Immobiliensektor – Im Fokus der Aufsicht

In der Genossenschaftlichen FinanzGruppe werden seit jeher Immobilien finanziert. Gerade in Zeiten knapper Margen ist die Immobilienvermittlung ein wachsendes Geschäftsfeld. Nun rückt sie in den Fokus der Aufsicht.

Maklertätigkeiten sind in der Genossenschaftlichen FinanzGruppe überwiegend in zwei Varianten organisatorisch aufgestellt: Entweder sind sie in einer bankinternen Abteilung integriert oder sie werden über Immobilienmakler einer Tochtergesellschaft abgewickelt.

Warum müssen sich Immobilienmakler der Geldwäscheprävention widmen?

Seit Juli 2018 sind auch Immobilienmakler gemäß § 2 Abs. 1 Nr. 14 GwG Verpflichtete im Sinne des Geldwäschegesetzes (GwG). Hierdurch obliegt ihnen die Umsetzung zahlreicher sogenannter „Sorgfaltspflichten“ nach dem GwG.

Im Oktober 2019 wurde in Deutschland die erste Nationale Risikoanalyse (NRA) veröffentlicht, in der das Geldwäscherisiko für den deutschen Immobiliensektor als hoch eingestuft wird. Im Dezember 2020 erfolgte darüber hinaus in der sektorspezifischen Risikoanalyse des Bundesministeriums der Finanzen eine Risikobewertung möglicher spezifischer Anfälligkeiten in Bezug auf juristische Personen und sonstige Rechtsgestaltungen.

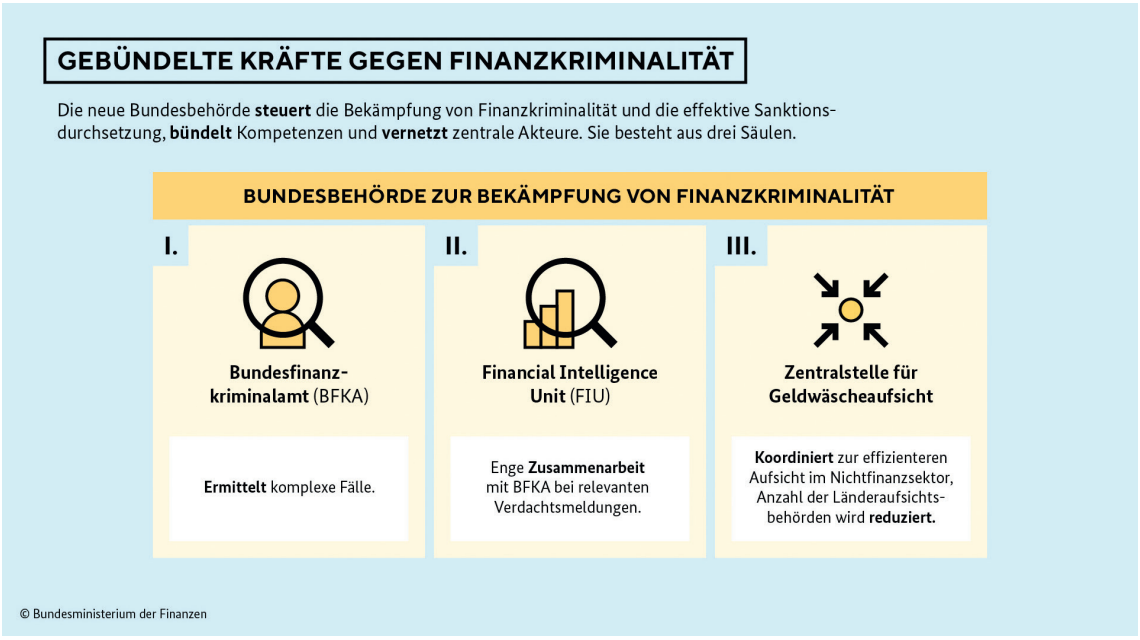
Welche Ausstrahlungswirkungen ergeben sich aus weiteren Verordnungen?

Nicht nur die Immobilienmakler selbst werden insofern stärker in die Pflicht genommen, sondern auch weitere Beteiligte. So ist im Oktober 2020 die Geldwäschegesetzmeldepflichtverordnung-Immobilien (GwGMeldV-Immobilien) in Kraft getreten. Diese verpflichtet Rechtsanwälte, Kammerrechtsbeistände, Patentanwälte, Notare sowie Wirtschaftsprüfer, vereidigte Buchprüfer, Steuerberater, Steuerbevollmächtigte und steuerberatende Vereine (wenn diese am Erwerbsvorgang nach § 1 GrEStG mitwirken) unter bestimmten Voraussetzungen zur Abgabe einer Verdachtsmeldung im Sinne des GwG. Damit soll der geringen Anzahl an Verdachtsmeldungen aus den genannten Berufsgruppen entgegengewirkt werden, die teilweise mit deren Verschwiegenheitspflicht zu begründen war.
Auch wenn Sie in Ihrer Funktion als Makler zunächst nicht Adressat dieser Verordnung sind, können sich durch das veränderte Meldeverhalten aufgrund der GwGMeldV-Immobilien unter Umständen Folgen für Ihre Kunden und somit Ausstrahlungswirkungen auf Ihre Geldwäschepräventionssysteme ergeben.

Die geplante Reorganisation der Aufsicht im Nichtfinanzsektor lässt bereits heute ein stärker vernetztes Vorgehen erkennen. Die Immobilienmakler rücken stärker in den Fokus der Aufsicht.

Wie verhält sich die zuständige Aufsicht?

Die Aufsicht im Nichtfinanzsektor liegt in der Kompetenz der einzelnen Bundesländer. Das heißt, es existiert aktuell ein kaum durchschaubarer Zuständigkeitendschungel und eine nicht einheitliche Aufsicht. Während in einigen Bundesländern eine gewisse Aktivität der Aufsicht zu



Quelle: Bundesministerium der Finanzen

verzeichnen ist, bleibt diese in anderen Bundesländern eher unsichtbar.

Insbesondere durch die nunmehr vorliegenden Erkenntnisse aus der Deutschlandprüfung 2021/2022 der Financial Action Task Force (FATF) hat das Thema „Geldwäscheprävention im Immobiliensektor" erneut an Brisanz gewonnen.

Laut FATF steht in Deutschland der effektiven Bekämpfung von Finanzkriminalität und der erfolgreichen Sanktionsdurchsetzung die zersplitterte Zuständigkeit bei einer Vielzahl von Behörden auf Bundes- und Landesebene im Wege. Zwar legt Deutschland einen starken Fokus auf die Verfolgung der Vortaten (z. B. Bekämpfung von Betrug, Bargeldschmuggel, Menschenhandel, im Ausland begangenen Vortaten) und sei in diesem Bereich auch recht gut aufgestellt. Allerdings werden die illegalen Finanzflüsse laut Bericht der FATF als solche zu wenig untersucht. Zudem erschwerten die große Anzahl an Aufsichtsinstanzen im Nichtfinanzsektor und die dort bestehenden Unterschiede hinsichtlich ihrer risikobasierten Aufsichtstätigkeit eine Priorisierung und Fokussierung auf komplexe Fälle von Finanzkriminalität, eine effektive Sanktionsdurchsetzung und eine effiziente, risikobasierte Aufsicht im Nichtfinanzsektor.

Als sogenannte prioritäre Handlungsempfehlung („Priority Action") nennt die FATF u. a.

- eine stärkere Koordinierung und
- den Ausbau der Aufsicht im Nichtfinanzsektor,

um ein einheitliches Risikoverständnis, verbunden mit einem wesentlichen Ausbau der personellen Ressourcen, zu etablieren.

Auf politischer Ebene wurde dieser Gedanke bereits im August 2022 aufgegriffen. Hiernach soll nunmehr eine Zentralstelle für Geldwäscheaufsicht geschaffen werden. Sie soll künftig die Aufsicht über den sehr breit aufgestellten Nichtfinanzsektor koordinieren, der neben unterschiedlichsten Gewerbetreibenden, z. B. Veranstalter von Glücksspiel, vor allem auch den Immobiliensektor umfasst. Die Zahl der Aufsichtsbehörden der Länder von derzeit über 300 soll hierbei reduziert werden. Diese Zentralstelle soll nicht nur Leitlinien und Standards für eine risikobasierte Aufsicht erarbeiten, sondern auch der zukünftigen europäischen Geldwäscheaufsichtsbehörde Anti-Money-Laundering Authority (AMLA) als zentraler Ansprechpartner zu Fragen des Nichtfinanzsektors in Deutschland dienen.

Was müssen Immobilienmakler tun?

Verpflichtete im Sinne des GwG, also auch Immobilienmakler, müssen über ein wirksames Risikomanagement verfügen. Im Rahmen der zu erstellenden Risikoanalyse

müssen die Verpflichteten die Risiken der Geldwäsche und Terrorismusfinanzierung, welche aus den von ihnen angebotenen Geschäften mit Bezug zu Immobilientransaktionen herrühren können, ermitteln und bewerten. Durch angemessene interne Sicherungsmaßnahmen sind diese festgestellten Risiken zu steuern und zu mindern. Das Risikomanagement umfasst insbesondere die Einhaltung entsprechender Sorgfaltspflichten in Bezug auf die Vertragsparteien, das Aufzeichnen und Aufbewahren von erhobenen Angaben und eingeholten Informationen und auch das Erkennen relevanter, meldepflichtiger Sachverhalte. In Verdachtsfällen ist eine Verdachtsmeldung im Sinne des GwG abzugeben.

Um welche Risiken geht es?

Die Risiken des Missbrauchs für Geldwäsche- und Terrorismusfinanzierung in Deutschland werden u. a. in Gesetzen (z. B. GwG), in Typologienpapieren und sogenannten Whitepapers zusammengefasst. Die dort aufgeführten Risiken sind durch die Immobilienmakler zu berücksichtigen. Beispielhaft seien folgende Risiken erwähnt:

- Barzahlung einer Immobilientransaktion
- Auffälligkeiten im Zusammenhang mit der Finanzierung einer Immobilientransaktion
- Auffälligkeiten im Zusammenhang mit den beteiligten Parteien
- Auffälligkeiten im Zusammenhang mit dem wirtschaftlich Berechtigten

Fazit

Durch den Aufbau einer Zentralstelle für Geldwäscheaufsicht werden Immobilienmakler stärker in den Fokus rücken, Prüfungen werden wahrscheinlicher. Die Ausgestaltung eines wirksamen und funktionierenden Risikomanagements ist daher von großer Bedeutung.

Im Übrigen muss auch eine bankinterne Immobilienabteilung die vorgenannten Sorgfaltspflichten im Rahmen der Immobiliengeschäfte erfüllen. In der Praxis kann es zum einen zu Herausforderungen bei der Identifizierung aller Vertragsparteien kommen und zum anderen können z. B. aufgrund einer fehlenden Schnittstelle der verwendeten Makler-Software zum Bankenverfahren Schwächen in der Dokumentation auftreten.

Wenn Sie Unterstützung brauchen, stehen wir gerne zur Verfügung. ▬

Christina Fiedler
Compliance-Spezialistin,
E-Mail: christina.fiedler@dz-cp.de

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

MaRisk-Konsultation

Am 26. September 2022 hat die BaFin auf ihrer Homepage den Entwurf der Neufassung des Rundschreibens 10/2021 (BA) – Mindestanforderungen an das Risikomanagement – MaRisk zur Konsultation gestellt (7. MaRisk-Novelle).

Bei den Mindestanforderungen an das Risikomanagement (MaRisk) handelt es sich um Verwaltungsanweisungen der BaFin zur Ausgestaltung des Risikomanagements in Kreditinstituten. Sie wurden erstmals mit BaFin RS 18/2005 im Dezember 2005 veröffentlicht und zuletzt durch das RS 10/2021 im August 2021 geändert. Die MaRisk sind normeninterpretierende Verwaltungsvorschriften und stellen eine Selbstbindung der Aufsicht gegenüber den Kreditinstituten dar. Ihr Ziel ist es, den Kreditinstituten Rechts- und Planungssicherheit zu geben, insbesondere im Hinblick auf die Regelung des § 25a Abs. 1 KWG zur ordnungsgemäßen Geschäftsorganisation.

Bei der diesjährigen Konsultation geht es im Wesentlichen um die Umsetzung der Leitlinien der Europäischen Bankenaufsichtsbehörde (EBA) zu Vorgaben der Kreditvergabe und Überwachung. Ferner werden Erkenntnisse aus der Aufsichts- und Prüfungspraxis eingeführt. Dies betrifft insbesondere Regelungen zur Handhabung des Immobiliengeschäftes, Anforderungen an die im Risikomanagement verwendeten Modelle, die Durchführung von Handelsgeschäften im Homeoffice und einzelne überproportionale Regelungen für sehr große Förderbanken.

Im Hinblick auf europäische Initiativen zur Nachhaltigkeit werden nun konkrete Anforderungen an das Risikomanagement von ESG-Risiken – ESG steht dabei für Environmental, Social, and Governance – in die MaRisk aufgenommen werden. Bereits im Dezember 2019 hatte die BaFin das „Merkblatt zum Umgang mit Nachhaltigkeitsrisiken“ veröffentlicht. Es hatte jedoch noch keinen verbindlichen Charakter und stellte lediglich Best-Practice-Ansätze dar.

Konsultation der 7. MaRisk-Novelle

Im Detail sind folgende Themen adressiert:

1. Übernahme der EBA-Leitlinien für

a) Kreditvergabe und Überwachung

Diesbezüglich ist ein differenziertes Vorgehen geplant: Soweit der bisherige Regelungstext die Anforderungen aus den Leitlinien auch heute schon überwiegend abbildet, werden die konkrete Anforderung oder – bei Klarstellungen – die jeweilige Erläuterung zu dieser Anforderung so ergänzt, dass die Vorgabe der Leitlinie (hiernach) vollumfänglich umgesetzt wird. Bei Neuerungen erfolgt ein Verweis auf die EBA-Leitlinien einschließlich deren Proportionalitätsklausel.

b) Governance requirements for credit granting and monitoring (Abschnitt 4 der Leitlinien)

Themen sind hier das Management der Kreditrisiken, der Strategie, des Risikoappetites, der Risikokultur und der Limitierung, jeweils bezogen auf das Kreditrisiko und die Kreditentscheidungsprozesse. Da die MaRisk diesbezüglich schon ausführliche Regelungen enthalten, begnügt sich die BaFin diesbezüglich mit Ergänzungen und Verweisungen.

c) Loan origination procedures (Abschnitt 5 der Leitlinien)

In diesem Abschnitt erfolgt eine Regelung der Kreditvergabe-Prozesse einschließlich der Auskünfte, Unterlagen und Daten, die für die Kreditwürdigkeitsprüfung der Kreditnehmer relevant sind. Ebenfalls werden Verbraucherschutzaspekte erfasst. Das Proportionalitätsprinzip richtet sich nach der Finanzierungsart und nur noch eingeschränkt nach der Größe des kreditgebenden Instituts.

d) Pricing (Abschnitt 6 der Leitlinien)
Geregelt sind hier die aufsichtlichen Erwartungen an die risikobasierte Preisgestaltung von Krediten. Da diese Anforderungen schon heute überwiegend in den MaRisk erhoben werden, wird die bisherige Regelung in BTO 1.2 Tz. 9 nur ergänzt. Danach sind relevante Kosten und angemessene Leistungsindikatoren zu bestimmen. Bei der Kostenermittlung ist u. a. die Einstufung im Risikoklassifizierungsverfahren zu berücksichtigen. Bei den Leistungsindikatoren gilt, dass diese hinsichtlich Größe, Art, Komplexität und Risikoprofil angemessen sein müssen.

e) Valuation of immovable and movable property (Abschnitt 7 der Leitlinien)
Der entsprechende Passus enthält Anforderungen für die Bewertung von Sicherheiten zum Zeitpunkt der Kreditaufnahme sowie die Anforderungen an Überwachung und Neubewertung. Auch gibt es Ausführungen zu unabhängigen Gutachtern. Zum Teil sind die Umsetzungen bereits in der 6. MaRisk-Novelle erfolgt, soweit die Anforderungen auch in den NPE-Leitlinien der EBA enthalten waren. Umzusetzen sind daher nur die darüber hinausgehenden Anforderungen. Insoweit verweist die MaRisk-Novelle auf die entsprechenden Abschnitte der Leitlinien (insbesondere im Bereich der Kreditvergabe).

f) Monitoring framework (Abschnitt 8 der Leitlinien)
Dieser Abschnitt befasst sich mit den Anforderungen an die laufende Überwachung des Kreditrisikos. Die Neuerungen sind nur in einzelnen Abschnitten enthalten, auf die dann ein Verweis erfolgt.

g) Neuer Abschnitt zu Anforderungen an Modelle (Abschnitte 4.3.3 und 4.3.4 der Leitlinien; AT 4.3.5 MaRisk-Entwurf)
Im Allgemeinen Teil der MaRisk wird ein neues Modul 4.3.5 aufgenommen, das die Anwendung, Datenqualität, Validierung und Erklärbarkeit von Modellen regeln soll. Die Anforderungen an die Modelle sind technologieneutral. Sie regeln sowohl den Einsatz einfacher Modelle als auch den von fortgeschrittenen Modellen im Bereich künstlicher Intelligenz und maschinellen Lernens. Sie schließen damit eine weitere Regelungslücke. Im neuen Abschnitt AT 4.3.5 werden grundlegende Anforderungen genannt, so dass bereits heute bestehende Anforderungen, die z. B. zur Sicherstellung der Risikotragfähigkeit gestellt sind, darauf aufbauen können.

h) Besonderheit von Immobiliarförderkrediten
Der deutsche Gesetzgeber hat bei Immobiliar-Verbraucherkrediten, die als Förderkredite vergeben werden, den Umfang der (verbraucherschützenden) Kreditwürdigkeitsprüfung bzw. der vorvertraglichen Informationspflicht stark eingeschränkt. Der Darlehensgeber ist verpflichtet, den Darlehensnehmer rechtzeitig vor Abgabe von dessen Vertragserklärung auf einem dauerhaften Datenträger über die Merkmale der einschlägigen Vorschriften des Einführungsgesetzes zum Bürgerlichen Gesetzbuche (EGBGB) zu informieren. Nach Auffassung der BaFin dürfen weitergehende Anforderungen aus der Wohnimmobilienrichtlinie, die auch in den Abschnitten 5.2.1 und 5.2.2 der EBA-Leitlinien adressiert werden, nicht auf solche Immobiliarförderkredite angewendet werden.

2. Anforderungen an das (eigene) Immobiliengeschäft

Es sollen Mindestanforderungen an das Immobiliengeschäft der Institute eingeführt werden. Hierzu wird ein neues Modul (BTO 3) in den Besonderen Teil der MaRisk aufgenommen. Vorgesehen ist ein Schwellenwert (2 % der Bilanzsumme oder 10 Mio. Euro), unterhalb dessen auf die Einhaltung der Anforderungen verzichtet werden kann.

Neben den direkten Immobiliengeschäften gelten auch Immobiliengeschäfte von Tochterunternehmen des Instituts im Sinne von § 290 HGB als Immobiliengeschäft des Instituts. Den Tochterunternehmen sind insoweit Unternehmen gleichgestellt, auf die Institute gemeinschaftlich einen beherrschenden Einfluss ausüben können. Lediglich Immobiliengeschäfte, die überwiegend dem eigenen Geschäftsbetrieb dienen, sind ausgenommen.

Wie im Kreditgeschäft gilt auch hier als maßgeblicher Grundsatz für die Ausgestaltung der Prozesse die klare aufbauorganisatorische Trennung der Bereiche Markt und Marktfolge einschließlich der Geschäftsleitung. Bei der Entscheidung, ein Immobiliengeschäft einzugehen, sind zwei zustimmende Voten der Bereiche Markt und Marktfolge einzuholen.

Hinsichtlich der Kompetenzen und der Prozesse gelten die Kreditregelungen analog: Es muss eine klare und konsistente Kompetenzordnung für Entscheidungen im Immobiliengeschäft geben. Zudem sind Prozesse und Bearbeitungsgrundsätze für Immobiliengeschäfte zu formulieren. Auch sind Bearbeitungskontrollen einzurichten und die für das Risiko eines Immobiliengeschäfts bedeutsamen Aspekte vor Immobilienerwerb oder -errichtung zu analysieren und zu beurteilen.

3. Geschäftsmodellanalyse

Zu AT 4.2 MaRisk erfolgt die Klarstellung, dass die Institute beurteilen sollen, ob sich das eigene Geschäftsmodell über einen angemessen langen, mehrjährigen Zeitraum aufrechterhalten lässt oder ob Anpassungsbedarf am Geschäftsmodell besteht und strategische Steuerungsmaßnahmen ergriffen werden müssen.

4. Handel im Homeoffice

Handelsaktivitäten im Homeoffice sollen dauerhaft zugelassen werden. Entsprechende interne Vorgaben müssen existieren. Auch wenn das Handelsgeschäft teilweise an häuslichen Arbeitsplätzen vorgenommen wird, ist stets eine ausreichende Präsenz anderer Händler in den Geschäftsräumen zu gewährleisten. Kleine Institute mit nur einem oder zwei Händlern müssen hier zumindest für angemessene Vertretungsregelungen sorgen oder wRegelungen für den Wechsel vom häuslichen Arbeitsplatz in die Geschäftsräume treffen.

5. Berücksichtigung von ESG-Risiken

Die MaRisk-Novelle übernimmt die Leitplanken aus dem Merkblatt zu Nachhaltigkeitsrisiken nunmehr in den Regelungstext und stellt damit prüfungsrelevante Anforderungen auf. Die Unternehmen sollen im Umgang mit Nachhaltigkeitsrisiken einen ihrem Geschäftsmodell und Risikoprofil angemessenen Ansatz entwickeln. Den Instituten wird aufgegeben, bisherige Prozesse anzupassen und neue Mess-, Steuerungs- und Risikominderungsinstrumente zu entwickeln, zumal sich sowohl physische Risiken als auch Transitionsrisiken sehr kurzfristig realisieren können.

ESG-Risiken werden definiert als Ereignisse oder Bedingungen aus den Bereichen Umwelt, Soziales oder Unternehmensführung, deren Eintreten potenziell negative Auswirkungen auf die Vermögens-, Finanz- oder Ertragslage eines Unternehmens haben kann. ESG-Risiken sind kein isoliertes Risiko, sondern wirken als Risikotreiber auf die bekannten Risiken Adressenausfallrisko, Marktpreisrisiken, Liquiditätsrisiken und operationelle Risiken ein.

Bei der Beurteilung der Auswirkungen von ESG-Risiken sind verschiedene plausible, aus wissenschaftlichen Erkenntnissen abgeleitete Szenarien zugrunde zu legen und ist ein angemessen langer Zeitraum zu wählen. Diese Beurteilung erfolgt, soweit sinnvoll und möglich, auch quantitativ.

Den Auswirkungen der durch den Klimawandel und die Transition zu einer nachhaltigen Wirtschaft entstehenden Risiken (z. B. durch soziale Folgen) ist im Rahmen einer zukunftsgerichteten Betrachtung sowohl in der normativen als auch in der ökonomischen Perspektive Rechnung zu tragen. Ein Abstellen auf vorhandene Datenhistorien ist nicht ausreichend.

In BTO 1.2, Anforderungen an die Prozesse im Kreditgeschäft, wird eingefügt, dass die EBA-GL 2022/06 in Bezug auf Umwelt, Soziales und Governance zu beachten sind. Auch soll in den Risikoberichten über die Auswirkung von ESG-Risiken informiert werden, dies gilt insbesondere für den Gesamtrisikobericht nach BT 3.2 Tz. 1, in dem auf die Auswirkungen von ESG-Risiken über einen angemessen langen Zeitraum einzugehen ist.

6. Regelungen für bedeutende Förderbanken

Hinsichtlich der Förderbanken hat die BaFin die Regelungen des AT 4.4.1 Tz. 5 zur Exklusivität der Risikocontrollingfunktion und des AT 4.4.2 Tz. 4 zur eigenständigen Compliance-Einheit identifiziert, die auf große Förderbanken angewendet werden sollen. Aus Sicht der BaFin ist eine Förderbank groß, wenn ihre Bilanzsumme mindestens 70 Mrd. Euro beträgt.

Es bestand die Möglichkeit der Stellungnahme bis zum 28. Oktober 2022. Seitens der Verbände und der Interessenvertretungen wurde die Konsultation kommentiert, so dass jetzt abzuwarten bleibt, welchen finalen Inhalt die MaRisk-Novelle haben wird.

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

Ausblick

Wir gehen davon aus, dass den Instituten hinsichtlich der Neuerungen in der MaRisk-Novelle wieder eine Übergangsfrist zur Umsetzung eingeräumt wird, während Klarstellungen ab Veröffentlichung der neuen MaRisk-Novelle gelten werden.

Wir werden unseren Kunden, wie auch bei der letzten MaRisk-Novelle, wieder einen Quick-Check zur Bearbeitung der MaRisk-Novelle zur Verfügung stellen, nachdem diese final veröffentlicht wurde. ▬

Sachkunde und Sachkundevermittlung

2021 war bei den Schlichtungsstellen – mit insgesamt 409 Eingaben – ein Rekordjahr. Die Mehrzahl der Eingaben betrafen das Wertpapiergeschäft (167), gefolgt von Bankgeschäft (156) und Versicherungsgeschäft (22). Dies bedeutet einen Anstieg von über 40 % gegenüber dem Vorjahr, das mit 279 Eingaben auch schon einen Rekord zu verzeichnen hatte.

Der Anstieg der Eingaben im **Wertpapiergeschäft** steht u. a. im Zusammenhang mit den **stetig** steigenden Anforderungen der aufsichtsrechtlichen Verpflichtungen **und der damit unmittelbar erforderlichen Sachkunde Ihrer Mitarbeiterinnen und Mitarbeiter.** Die Bedeutung der Sachkundevermittlung und damit einhergehend auch des Schulungskonzepts ist hoch: Es trägt erheblich zur Rechtssicherheit eines Unternehmens bei. Zudem zahlt es auf die Mitarbeiterbindung ein, qualifiziertes Personal zu finden ist aktuell schwerer denn je.

Die stetig **steigenden** Anforderungen des Aufsichtsrechts und die damit zusammenhängenden Sachkundeanforderungen stehen jedoch im Spannungsverhältnis zwischen Rechtssicherheit einerseits und Kosten sowie Zeitmanagement andererseits.

Bankeigenes Schulungskonzept

Einige Banken haben sich daher dafür entschieden, ein bankeigenes Schulungskonzept zu erstellen. Die Umstellung auf ein bankinternes Schulungskonzept erfolgt in der Regel aus folgenden Gründen:

- Hohe Kosten durch externe Schulungsangebote können erheblich gesenkt werden.
- Lange Abwesenheiten der Mitarbeiterinnen und Mitarbeiter durch Teilnahme an externen Schulungen inklusive An- und Abreise sowie Übernachtung gehören der Vergangenheit an.
- Hohe Fachkompetenz der eigenen Mitarbeiter, Anlageberater und des Beauftragten WpHG-Compliance kann effektiv genutzt werden.

Um den Aufwand möglichst gering zu halten, bietet es sich an, beim Aufbau, der Durchführung und der fortlaufenden Dokumentation des bankinternen Schulungskonzepts bedarfsorientiert auch auf externe Module/Dienstleister zurückzugreifen.

So bieten wir beispielsweise eine bedarfsorientierte Vermittlung der aufsichtsrechtlichen Sachkunde inklusive Dokumentation an. Die fachlichen und technischen Sachkundeanforderungen vermitteln Sie in diesem Modell bankintern oder durch externe Vertriebspartner.

Dies handhaben wir bereits seit mehreren Jahren erfolgreich bei vielen unserer Kunden. Von unserem Fachwissen, das auf der Erfahrung der Betreuung von einer Vielzahl an Mandaten beruht, profitieren die Banken mehrfach: Komplexe, erklärungsbedürftige Sachverhalte werden kompakt vermittelt. Sie sind aufsichtsrechtlich sicher. Ihr Schutzniveau wird gestärkt und Haftungsrisiken werden minimiert.

Update der Schulungsmodule

Um Sie bei der Herausforderung zur Bewältigung der steigenden Sachkundeanforderungen bei gleichzeitigem Zeit- und Kostendruck noch besser unterstützen zu können, haben wir unsere Dienstleistung für Sie weiter verbessert:

Grundlagenschulung

WpHG-Compliance

- **Auszubildende**
- **Neue Mitarbeiter**
- **Stellenwechsel in den Bereich WpHG**
- **Auffrischungsschulungen**

MAR-Marktmissbrauch

- **Pflichtschulung für einen ausgewählten Mitarbeiterkreis**

Schulungsdauer:
je circa 0,5 Stunden

Zielgruppenschulung

- **Vertriebsmitarbeiter**
- **Vertriebsbeauftragte**
- **Anlageberater**
- **Product Governance**
- **Compliance-Funktion (MF)**
- **Beschwerdemanagement**

Schulungsdauer:
zwischen 1 und 3,5 Stunden

Schulung zu Spezialthemen

- **Geeignete Gegenparteien**
- **Vertriebsvorgaben**
- **Telefonische Orderannahme/-beratung**
- **Zu- und Verwendungsverzeichnis**
- **Eigene Vermögensverwaltung**
- **Kundeninformationen**

Schulungsdauer:
je circa 1,5 Stunden

Web-based Training (WBT)
unbegrenzte Teilnehmeranzahl

Onlineseminar
mit mindestens 4 Teilnehmern

Präsenzschulung
mit maximal 25 Teilnehmern

Martin Reglinski
Beauftragter WpHG-Compliance,
E-Mail: martin.reglinski@dz-cp.de

Update 1:
Vertriebsbeauftragten-Schulung jetzt auch als WBT

Wir haben unser WBT-Angebot um die Schulung für „Vertriebsbeauftragte“ erweitert.

- Für unsere WpHG-Compliance-Auslagerungskunden und Listbanken ist dies eine kostenfreie Erweiterung unseres Angebots und kann jederzeit über die Homepage genutzt werden.
- Banken, die noch keine WpHG-Compliance an uns ausgelagert haben, können das komplette WBT-Angebot (WpHG-Compliance Grundlagenschulung, MAR-Marktmissbrauch und Vertriebsbeauftragte) zu günstigen Konditionen buchen.

Update 2:
Erweiterung der Grundlagen- und Zielgruppenschulungen

Im Bereich der Grundlagen- und Zielgruppenschulungen haben wir weitere Fachthemen und Spezialwissen in dozentengeführten Schulungen aufgegriffen, u. a.

- Kundeninformationen (Marketing und Research) und
- Telefonaufzeichnungen (telefonische Anlageberatung/Order).

Die dozentengeführten Schulungen erfolgen direkt durch die Fachabteilung bzw. praxiserfahrene WpHG-Compliance-Beauftragte. Sie können als Präsenzschulung oder auch als Online-Konferenz durchgeführt werden. Mit der Vermittlung der Sachkunde werden Tipps zum Umgang mit Herausforderungen im beruflichen Alltag gegeben.

Fazit

Die Anforderungen durch Regulatorik und aus den verbraucherschützenden Vorgaben nehmen weiter zu. Mit Blick auf das Schutzinteresse der Bank, aber auch mit Blick auf die drohenden Sanktionen und Schadensersatzansprüche ist es für die Institute entscheidend, die ordnungsgemäße Erbringung der Anlageberatung darlegen zu können. Dazu gehören der richtige Einsatz der IT und die – dokumentierte – Sachkunde des Personals.

Die Banken stehen vor der Herausforderung, diese Anforderungen in Zeiten von Fachkräftemangel sowie verstärktem Kosten- und Zeitdruck zu managen. Hierfür bietet es sich an, modular aufgebaute, bedarfsorientierte Lösungsmöglichkeiten einzubeziehen. ▬

Auslagerungsvertrags-Update 6.0

Vor Kurzem haben wir Ihnen umfangreiche neue Vertragsunterlagen zugeschickt. Was sind die Beweggründe für diese Aktion? Was hat das Ganze für Auswirkungen? Welchen Nutzen haben Sie dadurch?

Die Motivation für die Vertragsanpassung war die Änderung von und Anpassung an aufsichtsrechtliche Vorgaben. Konkret: die Neufassung der Mindestanforderungen an das Risikomanagement (MaRisk), die am 16. August 2021 veröffentlicht und als Rundschreiben versandt wurde. Das war die 6. Novelle der Ursprungsfassung vom September 2017.

Haupttreiber der aktuellen Überarbeitung waren die Änderungen von drei Regelwerken der Europäischen Bankenaufsichtsbehörde (EBA):

- die Leitlinie zu notleidenden und gestundeten Risikopositionen
- die Leitlinie zu Minderung und Management von Informations- und Kommunikationsrisiken
- die Leitlinie zu den Auslagerungsregeln

Die jetzige Vertragsanpassung referiert auf die geänderten Auslagerungsregeln, die in den MaRisk im Abschnitt AT 9 (Auslagerung) dokumentiert werden. Die Neuerungen betreffen drei Themenbereiche:

- die Anforderungen an die Risikoanalyse und die Bestimmung der Wesentlichkeit
- die Ausgestaltung des Auslagerungsvertrages
- die Steuerung und Überwachung der Risiken von Auslagerungsvereinbarungen

In AT 9 Tz. 7 wird aufgezählt, was in einem Auslagerungsvertrag, der wesentliche Auslagerungen betrifft, beinhaltet sein muss. Neu hinzugekommen sind:

- erweiterte Vertragsinhalte
- Informations- und Prüfungsrechte bei nicht wesentlichen Auslagerungen
- Erläuterungen zu Kündigungsrechten, sonstigen Sicherheitsanforderungen und dem Ort der Durchführung der Dienstleistung

Bereits bestehenden oder in Verhandlung befindlichen Auslagerungsverträgen wurde eine Frist bis zum 31. Dezember 2022 für die Anpassung an diese Neuerungen eingeräumt.

Im Verbund abgestimmte Vertragsaktualisierung

Wir haben den Zeitraum genutzt, um alle unsere Auslagerungsverträge auf den Prüfstand zu stellen. Dazu zählen die klassischen Vollauslagerungen von kompletten aufsichtsrechtlichen Beauftragtenfunktionen, wie die Geldwäsche- und Betrugsprävention oder die Informationssicherheit. Aber auch kleinere Auslagerungen wie das Hinweisgebersystem oder der Single Officer zählen dazu. Und die Teilauslagerungen wie die Trefferbearbeitung im Wertpapiergeschäft runden das Ganze ab.

Wir haben alle Auslagerungsverträge nach den Anforderungen an wesentliche Auslagerungen ausgerichtet – unabhängig davon, ob ein Institut vielleicht die eine oder andere Auslagerung oder Teilauslagerung für sich anders einstuft. Alle profitieren von einem höheren vertraglichen Sicherheitslevel, indem wir heute schon die Anforderungen von morgen erfüllen.

Dazu haben wir einen Master-Auslagerungsvertrag für alle Auslagerungen und Auslagerungsvarianten entwickelt und mit dem Arbeitskreis Vertragsprüfung des DGRV abgestimmt. Nachdem der DGRV ihn geprüft hatte (siehe DGRV RS Nr. 10/22/G-BA), haben wir alle Auslagerungsverträge entsprechend angepasst.

Alle profitieren von einem höheren vertraglichen Sicherheitslevel

Über 500 Kunden mit mehr als 1.200 Auslagerungsverträgen wurden angeschrieben. Bei der Rücksendung bzw. Einholung der Unterschriften haben wir auf eine rechtlich geprüfte, pragmatische Vorgehensweise gesetzt: Nur die Unterschriftsseite muss an uns zurückgeschickt werden. Das ressourcenschonende Vorgehen bedingt, dass eine Synopse für jeden einzelnen Vertrag entfällt. Stattdessen haben wir mit der „Anlage Vertragserneuerung" rechtsverbindlich zugesichert, dass die regulatorischen Vorgaben der MaRisk AT 9 umgesetzt sind und dass die bestehenden Regelungen zur Vergütung, zu Laufzeiten/Kündigungsfristen und sonstigen Sondervereinbarungen durch die Aktion nicht verändert werden.

Änderungen im Detail

Insgesamt haben wir an sechs Stellen den Vertrag bzw. seine Anlagen geändert. Folgende Änderungen – bezogen auf unser letztes Vertragswerk – wurden vorgenommen:
Im Punkt „Steuerung und Kontrolle" bestätigen wir, dass unsere Dienstleistungen ausschließlich in Deutschland erbracht werden. Zudem verpflichten wir uns, über einen Standortwechsel rechtzeitig vorab zu informieren. Auch die Speicherung und Verarbeitung von Daten findet nur im EU/EWR-Raum statt. Abgerundet wird dieser Punkt durch die Feststellung, dass wir gegen übliche Dienstleistungsrisiken angemessen versichert sind.

Die Aufzählung unserer Weiterverlagerungen wurde nun in eine Anlage „Auslagerung" gepackt. Das ist praktischen Erwägungen geschuldet. Bei einer Änderung der Sub-Dienstleister müssten wir nur die Anlage tauschen und nicht das gesamte Vertragswerk.

Das Thema Beendigungsunterstützung wurde in den Punkt „Fortwirkung von Rechten und Pflichten" integriert. Bisher war dies extra unter „Rückführung der Outsourcing-Tätigkeiten" geregelt. Die Umsortierung hatte logische Gründe, die Ausführungen wurden zudem sprachlich präzisiert, inhaltlich verändert wurde hingegen nichts.

Im Datenschutz verpflichten wir uns zusätzlich, auch Zugangsbeschränkungen zu Gebäuden und Räumen und Zugriffsberechtigungen auf Software-Lösungen zu berücksichtigen und einzuhalten.

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

Dann gibt es einen neuen letzten Punkt „Einwilligung zu werblicher Ansprache". Um unsere Kundenzufriedenheitsbefragungen durchzuführen, war diese Ergänzung nötig. Wir wollen Ihr Feedback regelmäßig ohne große Formalien einholen. Das hilft sowohl Ihnen, indem Sie uns strukturiert bewerten, als auch uns mit Hinweisen und zielgenauen Aufforderungen, unsere Arbeit zu verbessern.

Die materiellen Regelungen wie Vergütung, Laufzeiten, Kündigung und eventuelle sonstige getroffene Sondervereinbarungen behalten weiterhin ihre Gültigkeit. Dies haben wir in einer Extra-Anlage „Vertragserneuerung" für jeden Auslagerungsvertrag bestätigt.

Fazit

Mit dem Vertrags-Update kommen wir der Pflicht zur Umsetzung der regulatorischen Vorgaben gemäß MaRisk AT 9 nach. ▬

Interne Revision

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

Seit der letzten Berichterstattung in der Point of Compliance (2/2022, S. 27) wurden entsprechend der Jahresprüfungsplanung 2022 vier weitere Prüfungen abgeschlossen. Die Berichte zu den Bereichen „IT & Projekte – IT-Systeme", „Datenschutz" und „Informationssicherheit" wurden als dienstleistungsbezogene Berichte der Mandantschaft mit der entsprechenden Auslagerung zur Verfügung gestellt.

Des Weiteren wurde ein Bericht zum Prüffeld „Unternehmenssteuerung – Personalmanagement" abgeschlossen und, da nicht dienstleistungsbezogen, intern veröffentlicht.

Der Quartalsbericht zum dritten Quartal 2022 der Internen Revision wurde fristgerecht erstellt und unserer Mandantschaft zur Verfügung gestellt.

Darüber hinaus wurde turnusgemäß ein Follow-up-Quartalsbericht für das dritte Quartal 2022 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, *Bereichsleiter Interne Revision,*
E-Mail: lars.schinnerling@dz-cp.de

Wirtschaftliche Lage

Die Ergebnisentwicklung der DZ CompliancePartner GmbH ist auch nach dem dritten Quartal positiv. So konnte ein Ergebnis aus gewöhnlicher Geschäftstätigkeit von +1.287 T€ erreicht werden. Dies sind ca. +299 T€ mehr als geplant. Die Erlöse konnten kumuliert bei +12.788 T€ den Plan leicht überschreiten, der Aufwand lag bei -11.501 T€ leicht unter Plan. Es wird davon ausgegangen, dass die DZ CompliancePartner GmbH den Plan von 1.452 T€ leicht unterschreiten wird.

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

Genossenschaftliche FinanzGruppe
Volksbanken Raiffeisenbanken