

Point of Compliance

Das Risikomanagement-Magazin für unsere Kunden und Geschäftspartner

AUSGABE 2/2019

Anlegerschutz- und Funktionsverbesserungsgesetz (AnsFuG) · Auslegungs- und Anwendungshinweise zum Geldwäschegesetz (BaFin) · BaFin-Auslegungshinweise, -Konsultationen, -Merkblätter und -Rundschreiben · Bankaufsichtliche Anforderungen an die IT (BAIT) · Bundesdatenschutzgesetz · Derivateverordnung · DK-Hinweise zu Gw-Gesetzen · EBA Guideline on outsourcing arrangements · EBA-Richtlinien und -Empfehlungen · ESMA-Leitlinien und -Verordnungen · EU-Datenschutz-Grundverordnung · EU-Datenschutzrichtlinie 2016/680 · EU-Geldtransferverordnung · Finanz- und Risikotragfähigkeitsinformationenverordnung · Geldwäschegesetz · Hinweisgebersystem nach § 25a KWG · ISO-Standards 27001 und 27002 · Kleinanlegerschutzgesetz · Kreditwesengesetz · Markets in Financial Instruments Directive · Markets in Financial Instruments Regulation · Marktmissbrauchsverordnung (Market Abuse Regulation) an das Risikomanagement – MaRisk · Mir die Compliance-Funktion und weitere Verhaltenstransparenzpflichten – MaComp · Musterorganisation DGRV · Prüfungsberichtsverordnung · Standardisierung der IT-Verfahren · Transparenzrichtlinie-Durchführung · Umsetzungsgesetz zur Transparenzrichtlinie Wertpapierdienstleistungs-Verhaltensverordnung · Wertpapierhandelsanzeigengesetz · WertpapierwPHG-Mitarbeiteranzeigeverordnung · Zahlungsdienstleistungsgesetz · Zahlungsdienstleistungsrichtlinie (Payment Services Directive)

ab Seite 4

Auslagerung im Zeichen der neuen EBA-Richtlinien

ab Seite 6

Auftragsverarbeitung im Visier der Aufsicht

ab Seite 14

Auslegungs- und Anwendungshinweise zum Geldwäschegesetz

STARTPUNKT 3

SCHWERPUNKT

Auslagerung im Zeichen der neuen Richtlinien	4
Auftragsverarbeitung im Visier der Aufsicht	6
Beschwerdemanagement	8
Analyse nach MaRisk AT 8.2	11
Auslegungs- und Anwendungshinweise zum Geldwäschegesetz	14

STANDPUNKT

Compliance trifft Unternehmenskultur	18
---	----

ECKPUNKT

DZ CompliancePartner im Überblick	20
--------------------------------------	----

PUNKTUM

Norbert Schäfer ergänzt Geschäftsführungsteam	22
Wir gratulieren ...	22
Impressum	22
Interne Revision	23
Wirtschaftliche Lage	23
Auslagerungsmanagement – in eigener Sache	27

Mark Zuckerberg sieht in der DSGVO ein Vorbild für das Internet von morgen. Wie das? Mal ganz abgesehen davon, dass damit sicherlich eine breit angelegte Imagekampagne verbunden ist: Was treibt ihn um? Warum will er, der vom vergleichsweise freiem Datenzugriff profitiert, nun die Regeln verschärfen?

Seine Antwort ist: Weil er das „Gute“ am Internet bewahren möchte. Das Gute bewahren? Ist das der Kern der DSGVO?

- ▶ 16 Landesdatenschutzbehörden mit 16, häufig sehr unterschiedlichen Blickwinkeln und Auslegungen.
- ▶ Einige der Vorgaben erfordern nicht nur einen hohen Aufwand, sondern auch hohe Investitionen.
- ▶ Manchmal dienen die Regeln nur der eigenen Absicherung, wie beispielsweise bei den Hinweisen, dass Cookies genutzt oder Räume überwacht werden. Die Frage, wie da ein Schutzmechanismus greifen soll, ist berechtigt.

Aber alles in allem: Der Schutz persönlicher Daten hat eine hohe Relevanz. Unsere persönliche Autonomie, unsere Integrität und unsere Würde sind heute mehr denn je vom Schutz unserer Daten – sowohl vor Wirtschaftsunternehmen als auch vor staatlichen Institutionen – abhängig. Es ist deshalb richtig, dass sich der Staat lenkend in die Erhebung und Verarbeitung unserer Daten einmischt.

Auch wenn das „Gute“ im Internet wohl erst einmal geformt werden müsste, bevor es bewahrt werden kann: Regulierung ist vom Grunde her zu befürworten. Zu unserem eigenen Schutz und zum Schutz unserer Kunden.

In diesem Sinne wünsche ich Ihnen eine anregende Lektüre.

Ihr Jens Saenger



Jens Saenger
Sprecher der Geschäftsführung

► European Banking Authority

Auslagerung im Zeichen der n Mehr Chance als Risiko!

Am 25. Februar 2019 hat die European Banking Authority (EBA, EBA/GL/2019/02) den finalen Bericht zur künftigen Empfehlung der „EBA Guideline on outsourcing arrangements“ veröffentlicht. Die nationalen Aufsichtsbehörden haben nun zu entscheiden, ob und welche Regelungen sie im Rahmen des „comply or explain“-Vorgehens in ihre Aufsichtspraxis übernehmen werden. Erst dann sind die Regelungen bindend.

1. Aktuell verfolgt die BaFin das Ziel, sich bis Juni zu erklären, welche Inhalte sie übernehmen und zu welchen Punkten sie Anpassungen in den geltenden MaRisk vornehmen wird. Speziell Themen im Zusammenhang mit einem Risikomanagement dürften hier noch einmal besonders kritisch beleuchtet werden. Einer ersten Einschätzung nach sind viele Inhalte mit den bereits geltenden Vorgaben in Einklang. Es gibt jedoch einige Anforderungen, die zu einer Anpassung des Auslagerungsmanagements führen dürften. Vorneweg: Die Richtlinie bestätigt die Wichtigkeit der Beibehaltung der Auslagerungsoptionen.

2. Sie bestätigt zugleich die Auslagerungsfähigkeit auch kritischer Funktionen.

Die Auslagerungen „kritischer“ Funktionen werden jedoch künftig einen höheren Einfluss auf das Risikoprofil der auslagernden Institute haben. Dadurch kommt dem Auslagerungsmanagement insgesamt eine größere Bedeutung zu.

Auslagerungsfähigkeit auch kritischer Funktionen bestätigt

Dabei darf es nicht zu einer völligen Aufzehrung der Vorteile einer Auslagerung durch den Aufwand für das Auslagerungsmanagement selbst kommen.

Die fortschreitende Komplexität der regulatorischen Anforderungen bringt viele Institute an den Rand fachlicher Machbarkeit. Einzig mit eigenen Mitteln und ohne das professionelle,

fachliche Management eines Spezialisten sind die Herausforderungen oft genug nur noch mit so hohen Aufwendungen zu bewältigen, dass es betriebswirtschaftlich nicht mehr sinnvoll ist. Auch der BVR bekräftigt immer wieder seinen Grundsatz bei der Beurteilung einer Auslagerung aus Managementsicht¹: Der fachliche Nutzen – die geforderte Qualität immer vorausgesetzt – ist so lange nicht zu hinterfragen, wie sich die betriebswirtschaftlichen Aspekte in Summe nicht zu Ungunsten des auslagernden Instituts verkehren. Erst wenn diese Ratio sich in einen finanziell negativen Beitrag verkehrt, ist über den qualitativen oder machbaren Aspekt gesondert zu urteilen.

Die gute Nachricht ist: Auch im Zeitalter nach der Auslagerungsrichtlinie der EBA kann ein effizient strukturiertes Auslagerungsmanagement eines Instituts mit den Dienstleistungsunternehmen optimal Hand in Hand arbeiten und somit

- unnötige Aufwände auf Seiten des Instituts vermeiden,
- damit verbundene Kosten reduzieren,
- aufsichtsrechtliche Anforderungen mängelfrei abdecken.

Einen zusätzlichen Aufwand bei der Steuerung laufender Auslagerungen durch die neue Richtlinie dürfte insbesondere die Forderung nach sich ziehen, dass die Institute ein detailliertes und vollständiges Register mit allen Auslagerungsvereinbarungen führen müssen. Die Bestandteile dieses Registers werden zwingend vorgegeben und das Registers muss auf Nachfrage kurzfristig zur Verfügung stehen. Dabei findet eine Erweiterung der Informationen zu den einzelnen Auslagerungen gegenüber den bislang erforderlichen Inhalten statt.

¹ BVR-Bankenreihe Band 41 (Outsourcing in Genossenschaftsbanken)

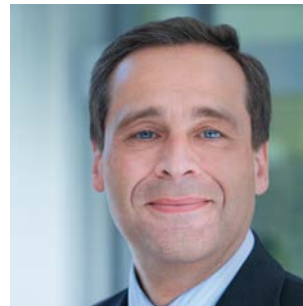
neuen Richtlinien:

Ferner wird wohl zusätzlich eine Anzeigepflicht für Auslagerungen definiert. In Verbindung mit den qualitativen Forderungen zur Kontrolle und Steuerung der bestehenden Auslagerungen lauten die Kernbotschaften für ein gleichermaßen effektives wie effizientes Auslagerungsmanagement:

- ▶ Zusammenfassung aller Auslagerungen mit allen „Muss-Informationen“ in einer zentralen Datei
- ▶ Ergänzung dieser Datei durch alle erforderlichen Maßnahmen, Daten und Schritte, die zur Steuerung und Kontrolle der Auslagerungen erforderlich sind – inklusive notwendiger Service Levels
- ▶ Möglichkeit einer Exportfunktion zur Wahrnehmung der Anzeigepflichten
- ▶ Revisions sichere Dokumentation des Workflows zur unterjährigen Kontrolle und deren Aufgabenerledigungen in dieser zentralen Datei
- ▶ Speicherung externer Prüfungs- und Kontrollberichte zu den jeweiligen Dienstleistern
- ▶ Abstimmung mit den Dienstleistungsunternehmen, dass die erforderlichen Informationen und Dokumentationen in den geforderten Formaten und Fristen geliefert werden können

Härtere, aber auch klarere Vorgaben

Einige Häuser haben bereits mit der Einrichtung einer Funktion für das Auslagerungsmanagement begonnen. Eine Unterstützung dieser Aufgabe durch geeignete Arbeitsmittel und eine Abstimmung mit den betroffenen Dienstleistungsunternehmen –



AUTOR UND ANSPRECHPARTNER

Andreas Marbeiter

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

beispielsweise über die künftigen Dokumentationen, Service Levels und deren Lieferformate – werden den administrativen Aufwand begrenzen können. Durch eine ganze Reihe von Präzisierungen und Klarstellungen der EBA-Guideline wird es den Instituten zudem möglich sein, zielgenau und fokussiert genau das Wesentliche im Rahmen des Auslagerungsmanagements zu berücksichtigen.

Die DZ CompliancePartner unterstützt diese Prozesse bereits inhaltlich für die von ihr selbst angebotenen Auslagerungsdienstleistungen. Ferner stellen wir auch Arbeitsmittel für das Auslagerungsmanagement zur Verfügung, damit Ihr Haus das Auslagerungsmanagement in dem geforderten Umfang und betriebswirtschaftlich sinnvoll erfüllen kann. Bitte sprechen Sie uns an. ■

► **Datenschutz**

Auftragsverarbeitung im Visier der Aufsicht

Mitte Dezember wurde das erste Bußgeld in Höhe von EUR 5.000,00 wegen eines fehlenden Auftragsverarbeitungsvertrages in Hamburg ausgesprochen.

Begründet wurde das Bußgeld gegen das Versandunternehmen Kolibri Image mit einem Verstoß gegen Art. 28 III DSGVO. Nach dieser Vorschrift muss bei jeder Verarbeitung von personenbezogenen Daten durch einen Dritten ein zusätzlicher (Auftragsdatenverarbeitungs-)Vertrag zum Datenschutz geschlossen werden, der unter anderem Details zu den getroffenen technischen und organisatorischen Maßnahmen zum Schutz der Daten enthält.

Zuvor hatte Kolibri Image die Aufsichtsbehörde selbst um Rat gefragt, welche Maßnahmen zu ergreifen sind. Trotz der konkreten Empfehlung der Behörde wurde eine solche Vereinbarung zwischen den Parteien nicht geschlossen. Kolibri Image hat angekündigt, Widerspruch einzulegen.

Auftragsverarbeiter/Auftragsverarbeitung

Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 4 Nr. 8 DSGVO).

Auftragsverarbeitung im datenschutzrechtlichen Sinne liegt nur in Fällen vor, in denen eine Stelle von einer anderen Stelle im Schwerpunkt mit der Verarbeitung personenbezogener Daten beauftragt wird.

Auftragsdatenverarbeitungen sind somit nicht

- Aufträge, welche die Inanspruchnahme fremder Fachleistungen bei einem eigenständig Verantwortlichen regeln;
- Aufträge, welche als Schwerpunkt nicht die Verarbeitung personenbezogener Daten, sondern eine sonstige Tätigkeit haben.

Wann liegt eine Auftragsverarbeitung vor?

Kriterien für die Beurteilung, ob eine Auftragsverarbeitung vorliegt, sind z. B.:

AUTOREN UND ANSPRECHPARTNER

Michael Switalla

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

Björn Veith

Analyst Informationssicherheit & Datenschutz,
E-Mail: bjoern.veith@dz-cp.de

- Der Auftragnehmer verfolgt mit der Verarbeitung keine eigenen Zwecke.
- Der Auftragnehmer hat keine Entscheidungsbefugnis über die Daten.
- Der Auftragnehmer unterliegt einem Nutzungsverbot hinsichtlich der Daten.
- Der Auftragnehmer tritt nach außen nicht in Erscheinung, die Verarbeitung erfolgt unter Verantwortung des Verantwortlichen.
- Der Auftragnehmer steht im Zusammenhang mit der Auftragsverarbeitung in keiner vertraglichen Beziehung zu den von der Datenverarbeitung Betroffenen.

Beispiele können Sie der folgenden Übersicht entnehmen.

Unsere Empfehlung

Bei Verarbeitung der Daten durch Dritte sollte grundsätzlich der Datenschutzbeauftragte mit eingebunden werden. Dieser prüft die Datenweitergabe und etwaige vertragliche Anforderungen. Auch bei der Kommunikation mit der Aufsichtsbehörde bei der Abstimmung bestimmter, datenschutzrelevanter Sachverhalte sollte der Datenschutzbeauftragte eingebunden werden. ■

BEISPIELE FÜR DAS VORLIEGEN UND NICHT-VORLIEGEN EINER AUFTRAGSVERARBEITUNG

AUFTRAGSVERARBEITUNG	KEINE AUFTRAGSVERARBEITUNG	
Regelmäßig mit Schwerpunkt in der Verarbeitung personenbezogener Daten	Inanspruchnahme fremder Fachleistungen bei einem eigenständig Verantwortlichen	Im Kern keine beauftragte Verarbeitung personenbezogener Daten, sondern der Auftrag zielt auf eine andere Tätigkeit
<ul style="list-style-type: none"> ▶ DV-technische Arbeiten für die Lohn- und Gehaltsabrechnung oder die Finanzbuchhaltung durch Rechenzentren ▶ Outsourcing personenbezogener Datenverarbeitung im Rahmen von Cloud-Computing, ohne dass ein inhaltlicher Datenzugriff des Cloud-Betreibers erforderlich ist ▶ Werbeadressenverarbeitung in einem Lettershop ▶ Verarbeitung von Kundendaten durch ein Callcenter ohne wesentliche eigene Entscheidungsspielräume dort ▶ Auslagerung der E-Mail-Verwaltung oder von sonstigen Datendiensten zu Webseiten (z. B. Betreuung von Kontaktformularen oder Nutzeranfragen) ▶ Datenerfassung, Datenkonvertierung oder Einscannen von Dokumenten ▶ Auslagerung der Backup-Sicherheitspeicherung und anderer Archivierungen ▶ Datenträgerentsorgung durch Dienstleister ▶ Prüfung oder Wartung (z. B. Fernwartung, externer Support) automatisierter Verfahren oder von Datenverarbeitungsanlagen, wenn bei diesen Tätigkeiten ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann ▶ ... 	<ul style="list-style-type: none"> ▶ Tätigkeiten der Berufsheimnisträger (Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer) ▶ Inkassobüros mit Forderungsübertragung ▶ Bankinstitute für den Geldtransfer ▶ Postdienste für den Brief- oder Pakettransport ▶ Tätigkeit als WEG-Verwalter ▶ Detektive bei ihrer Observierungs-/Überwachungs-/Ausforschungstätigkeit ▶ Hersteller und Großhändler, die von Einzelhändlern für mit Endkunden vereinbarte Direktlieferungen die Endkundenadressen erhalten (beauftragte Warensendung) ▶ Blumen- oder Weinversender, die eine Liste mit Adressdaten zur Versendung der Blumen- bzw. Weingeschenke an dritte Personen erhalten (beauftragte Warensendung) ▶ Insolvenzverwalter ▶ Personalvermittlung nach Auftrag von Stellensuchenden oder Arbeitgebern ▶ Internet-Platförmbetreiber zur Vermittlung zwischen Anbietern und Nachfragern, die sich auf der Plattform treffen können ▶ TKG-Dienstleistungen, es sei denn, darüber hinausgehende Zusatzdienste wie Auslagerung einer betrieblichen Telefonanlage oder Cloud-Speicherlösungen sind vereinbart ▶ Versicherungs-/Finanzmakler, -vermittler im Rahmen des Kundenvertrags ▶ ... 	<ul style="list-style-type: none"> ▶ vom Vermieter beauftragte Handwerker, die dazu die nötigen Mieterdaten erhalten ▶ Sachverständige zur Begutachtung eines Kfz-Schadens ▶ Personenbeförderung, Krankentransportleistungen ▶ Bewachungsdienstleistungen ▶ Reinigungsdienstleistungen und Handwerkereinsätze in Unternehmen ▶ Reinigung von Berufskleidung mit Namensschildern ▶ Druck von Prospekten, Katalogen, mit Bildern von Beschäftigten oder Fotomodellen ▶ Transport von ausreichend geschreddertem Papiermaterial ▶ Transport von Unterlagen und Waren durch Kurierdienste, Speditionen, Zeitungsausträger ▶ Übersetzung von Texten in/aus Fremdsprachen ▶ ...

► Beschwerdemanagement

Immer umfassendere Anforderungen

In den vergangenen zweieinhalb Jahren sind zahlreiche neue Regelungen zum Beschwerdemanagement in Kraft getreten, die insbesondere den Schutz des Verbrauchers zum Ziel haben. Damit einhergehend sind aber auch die Anforderungen an den Compliance-Beauftragten gestiegen. Es drohen empfindliche Bußgelder, Abmahnungen oder auch Feststellungen in Prüfungshandlungen.

Zu den Neuerungen gehören neben der gesetzlichen Informationspflicht nach der ODR-Verordnung (OS-Plattform) und dem Verbraucherstreitbeilegungsgesetz vor allem auch die Regelungen nach MiFID II, MaComp und den von der BaFin veröffentlichten Mindestanforderungen an das Beschwerdemanagement (MaBeMa). Aufgrund der Vielzahl an Vorgaben in den unterschiedlichen Regelwerken ist es schwer, den Überblick über die umzusetzenden Maßnahmen zu behalten. Werden die Vorgaben nicht oder nicht ausreichend umgesetzt, drohen Bußgelder, Abmahnungen und zum Teil wesentliche Feststellungen in Prüfungshandlungen. Im Ergebnis führen diese Regelungen nicht nur zu einem Umsetzungsaufwand im Institut, sondern auch zu einem gesteigerten Aufwand für die Compliance-Funktionen (insbesondere WpHG- und MaRisk-Compliance).

Beschwerdebegriff und zentrales Beschwerdemanagement

Nach BT 12.1.1 Tz. 1 MaComp und Tz.8 MaBeMa ist jede Äußerung der Unzufriedenheit, die ein Beschwerdeführer an ein beaufsichtigtes Institut in Zusammenhang mit der Erbringung einer Dienstleistung richtet, als Beschwerde zu werten. Das bedeutet, dass Institute den Beschwerdebegriff nicht mehr (z.B. betragsabhängig) selbst definieren können.

BT 12.1.2 Tz. 6 und 7 MaComp sowie Tz. 14 MaBeMa sehen vor, dass jedes Institut eine Beschwerdemanagementfunktion einrichtet. Diese hat dafür zu sorgen, dass alle Beschwerden objektiv untersucht und Interessenkonflikte bei der Beschwerdebearbeitung vermieden werden. Eine entsprechende Funktion war bislang nur für Beschwerden mit Wertpapierrelevanz vorgesehen und wird nunmehr durch die MaBeMa auf alle Beschwerden ausgeweitet.

Grundsätze zum Beschwerdemanagement und Veröffentlichungspflichten

Für eine ordnungsgemäße Geschäftsorganisation ist auch die Aufnahme und Auswertung von Beschwerden erforderlich (Tz. 9 MaBeMa). Die daraus gewonnenen Erkenntnisse müssen in das Risikomanagement einbezogen und von der Internen Revision berücksichtigt werden. Zu diesem Zweck haben Institute Grundsätze sowie wirksame und transparente Verfahren einer angemessenen Beschwerdebearbeitung zu implementieren (BT 12.1.2 Tz. 1 bis 4 MaComp und Tz. 10 bis 14 MaBeMa). Darin müssen festgelegt sein:

- die Beschwerdeeinreichung,
- die Beschwerdebearbeitung inklusive der Zuständigkeiten,
- die Weiterverfolgung von Maßnahmen zur Einhaltung der Grundsätze und Verfahren sowie
- das interne Berichtswesen.

Neben diesen internen Pflichten bestehen jedoch auch zahlreiche Veröffentlichungspflichten gegenüber dem Kunden. So ist auf leicht zugängliche Weise über das Verfahren zur Beschwerdebearbeitung zu informieren (BT 12.1.3 Tz. 6 MaComp und Tz. 19 MaBeMa). Erfahrungsgemäß erfolgt dies am einfachsten über die jeweilige Homepage des Instituts. Es ist allerdings darauf zu achten, dass die vorgeschriebenen Mindestinhalte enthalten sind.

Über das Verfahren zur Beschwerdebearbeitung muss darüber hinaus bei der Eingangsbestätigung der Beschwerde oder auf Verlangen des Beschwerdeführers informiert werden (BT 12.1.3 Tz. 7 MaComp und Tz. 20 MaBeMa).

Kann innerhalb der intern festgelegten Frist dem Beschwerdeführer keine Antwort gegeben werden, muss der Beschwerdeführer über die Gründe der Verzögerung und die voraussichtliche Dauer der Beantwortung informiert werden (BT 12.1.3 Tz. 10 MaComp und Tz. 22 MaBeMa).

Im Rahmen der Veröffentlichungspflichten in Zusammenhang mit dem Beschwerdemanagement müssen jedoch auch die Vorgaben nach dem Verbraucherstreitbeilegungsgesetz (VSBG) und der ODR-Verordnung (OS-Plattform) erwähnt werden. Gemäß § 36 Abs. 1 und 2 VSBG müssen Institute auf deren Homepage und zusammen mit den Allgemeinen Geschäftsbedingungen darüber informieren, inwieweit sie bereit oder verpflichtet sind, an einem Streitbeilegungsverfahren teilzunehmen. Überdies müssen sie auf die zuständige Verbraucherschlichtungsstelle hinweisen. Hinzu kommt, dass nach § 37 VSBG der Verbraucher in Textform auf eine für das Institut zuständige Verbraucherschlichtungsstelle hingewiesen werden muss, sofern eine Streitigkeit über einen Verbrauchervertrag nicht beigelegt werden konnte.

Nach Artikel 14 Abs. 1 der Verordnung (EU) Nr. 524/2013 (sog. OS-Plattform) muss jedes Institut auf der Homepage einen Link zur OS-Plattform bereitstellen. Nach ständiger Rechtsprechung muss der Link auf „<https://www.ec.europa.eu/consumers/odr>“ leicht zugänglich und anklickbar sein. Die nicht anklickbare Gestaltung des Links ist häufiger Bestandteil von Abmahnungen. Sofern Verträge auch über E-Mail abgeschlossen oder angeboten werden, muss in der E-Mail ebenfalls der Link auf die OS-Plattform aufgeführt werden (Abs. 2). Zudem sollte der Link in den Allgemeinen Geschäftsbedingungen aufgenommen werden.

Internes Beschwerderegister

Aufgrund der Vorgaben gemäß BT 12.1.3 Tz. 2 MaComp und Tz. 15 MaBeMa sind alle Beschwerden sowie deren Bearbeitung, getroffene Maßnahmen und die abschließende Entscheidung ohne unnötige Verzögerung in einem internen Beschwerderegister zu dokumentieren. Die Formulierung „alle Beschwerden“ hat für die Institute die Folge, dass auch diejenigen Beschwerden, die bereits direkt mit dem Kunden geklärt werden konnten, in dem Beschwerderegister zu dokumentieren sind. Die konsequente Einhaltung dieser Vorgabe wird regelmäßig eine besondere Herausforderung für das Institut und die Compliance-Beauftragten sein.

An das interne Beschwerderegister werden darüber hinaus durch Tz. 16 MaBeMa zahlreiche Anforderungen gestellt. So ist das Beschwerderegister elektronisch oder in einer anderen Form so zu führen, dass es

- ▶ eine systematische Auswertung ermöglicht,
- ▶ gegen sachlich nicht gebotene Änderungen geschützt ist,
- ▶ nachträgliche Änderungen erkennen lässt und
- ▶ eine ungehinderte Einsichtnahme für die zuständigen Mitarbeiter des Instituts, die zuständigen Prüfer und die Aufsicht gewährleistet.

AUTOREN UND ANSPRECHPARTNER



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



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

Besonders die Kenntlichmachung nachträglicher Änderungen zwingt die Institute, die weitverbreitete Beschwerdebearbeitung in Excel aufzugeben und auf ein aufsichtskonformes Beschwerderegister umzustellen. Da Beschwerden noch immer häufig als etwas (ausschließlich) Schlechtes gesehen werden und die im Beschwerderegister dokumentierte Anzahl an Beschwerden der vergangenen Jahre zum Teil sehr überschaubar ist, muss von den Compliance-Beauftragten mitunter viel Überzeugungsarbeit geleistet werden, um die Notwendigkeit eines aufsichtskonformen Beschwerderegisters und die dafür benötigten Aufwendungen darzulegen und genehmigt zu bekommen.

Für das Institut ergibt sich weiterhin die Pflicht, die Daten zur Beschwerdebearbeitung fortlaufend zu analysieren (siehe Tz. 18 MaBeMa). Dadurch soll sichergestellt werden, dass wiederholt auftretende oder systematische Probleme und daraus resultierende rechtliche sowie operationelle Risiken festgestellt und behoben werden. Hierzu sind jeweils auch die Beauftragten WpHG- und MaRisk-Compliance einzubinden.

Besonderheiten bei Wertpapierbeschwerden

Beschwerden mit Bezug zum Wertpapiergeschäft können als ein spezieller Teil des Gesamt-Beschwerdemanagements des Instituts verstanden werden. In den MaComp wurden mit dem BT 12 hierzu im März 2018 von der BaFin Konkretisierungen veröffentlicht.

Nicht verändert hat sich die Meldepflicht von Beschwerden im Zusammenhang mit einer Anlageberatung. Weiterhin sind nur einschlägige Beschwerden von Privatkunden meldepflichtig. >

Neu ist jedoch, dass die Erfassung und Bearbeitung von Beschwerden nun alle Kundengruppen einschließt (auch professionelle Kunden und geeignete Gegenparteien). Neu ist weiterhin, dass erstmalig im März 2019 ein Beschwerdebericht über das elektronische Meldeportal der BaFin (MVP) abzugeben war.

Der erste Beschwerdebericht durfte verkürzt eingereicht werden und hatte lediglich die Gesamtzahl der Beschwerden aufzuführen (siehe gelb markierte Zeile im Musterbeschwerdebericht unten).

Abschnitt A									
Kategorie	Bearbeitungsstand (Stand der Beschwerden)			Erfolgreiche Beschwerden (nach Status, Anzahl der Anträge)		Gerichts- und Schlichtungsverfahren (Anzahl der Anträge)			
	Anzahl der eingegangenen Beschwerden	Anzahl der erledigten Beschwerden	Anzahl der zum Bericht offenen Beschwerden	Gesamtanzahl erfolgreicher Beschwerden	davon: Rückzahlungen	Gesamtanzahl der Verfahren	Gerichtsverfahren	Schlichtungsverfahren	davon:
Wertpapier- & Wertpapiere (§ 2 Abs. 9 WpHG)									
Anlageberatung (§ 2 Abs. 1)									
Markt-Making (§ 2 Buchstabe a)									
Kollektives Investment (§ 2 Buchstabe b)									
Eigenhandel (§ 2 Buchstabe c)									
Hochfrequenzhandel (§ 2 Buchstabe d)									
Abschlussanfertigung (§ 2)									
Anlagevermittlung (§ 2)									
Anlagegeschäft (§ 2)									
Kleinanlagegeschäft (§ 2)									
Kleinanlagevermittlung (§ 2)									
Handelsplattformvermittlung (§ 2)									
Betrieb eines multilateralen Handelssystems (§ 2)									
Betrieb eines organisierten Handelssystems (§ 2)									
Anlageberatung (§ 2)									
Zusammenfassung									
Wertpapierdienstleistungen § 2 Abs. 9 WpHG									
Handelsplatz (§ 2)									
Übrige Wertpapierdienstleistungen nach § 2 Abs. 9 WpHG									
Handelsplatz									
Sonstige									
Gesamtsumme									

Ab dem kommenden Bericht zum 1. März 2020 sind die Beschwerden auch nach den Wertpapier(neben)dienstleistungen zu gruppieren:

- ▶ MaComp BT 12.2 Nr. 3 Abschnitt A
„Die Anzahl der Beschwerden, gesamt und aufgeschlüsselt nach den einzelnen Wertpapierdienstleistungen nach § 2 Abs. 8 WpHG, dem Depotgeschäft nach § 2 Abs. 9 Nr. 1 WpHG, den übrigen Wertpapiernebenleistungen nach § 2 Abs. 9 WpHG und ‚Sonstige‘; die Zuordnung einer Beschwerde zu einer Kategorie erfolgt dabei nach dem Schwerpunkt der Beschwerde, d. h. Beschwerden sind einfach und nicht mehrfach zu zählen;“
- ▶ MaComp BT 12.2 Nr. 3 Abschnitt B
„Übersicht über die Beschwerdegründe unter Angabe der jeweiligen Fallzahlen aufgeschlüsselt nach den nachfolgenden Beschwerdegründen:

- (1) ‚Auftragsausführung (Erfassung, Durchführung einschließlich Best Execution, Abrechnung)‘;
- (2) ‚Aufzeichnungspflichten (z. B. Geeignetheitserklärung)‘;
- (3) ‚Einholung von Kundeninformationen‘;
- (4) ‚Empfehlung (Geeignetheit)‘;
- (5) ‚Entgelte, Gebühren, Kosten, Zuwendungen‘;
- (6) ‚Interessenkonflikte (Vermeidung, Management, Offenlegung)‘;
- (7) ‚Risikoauflklärung‘;
- (8) ‚Sekundärmarkt (Preisstellung, Quotierung)‘;
- (9) ‚Verwahrung, Verwaltung‘ und
- (10) ‚Sonstiges‘;

die Zuordnung einer Beschwerde zu einem Beschwerdegrund erfolgt dabei nach dem Schwerpunkt der Beschwerde, d. h. Beschwerden sind einfach und nicht mehrfach zu zählen;“

Wichtig ist, dass diese Informationen schon im laufenden Jahr entsprechend bei Eingang und Bearbeitung von Beschwerden dokumentiert werden, um nicht kurz vor dem nächsten Beschwerdebericht alle eingegangenen Beschwerden noch einmal durchgehen zu müssen.

Laut dem Rahmenkonzept „Qualität im Kundengeschäft“ des BVR (Seite 127) kann in agree21 im Vorgang „Beschwerde erfassen“ mit dem Untervorgang „Beschwerde im wertpapieraufsichtsrechtlichen Sinn erfassen“ ein Teil der für den Beschwerdebericht notwendigen Daten sofort unterjährig erfasst werden.

Fazit

In relativ kurzer Zeit wurden viele Regelungen über unterschiedliche Rahmenwerke zum Schutz des Verbrauchers verabschiedet. Der Abgleich der Anforderungen, die teilweise inhaltlich identisch sind, sich jedoch zum Teil gegenseitig ergänzen, stellt die Institute vor große Herausforderungen. Um mögliche Sanktionen abzuwenden, sind insbesondere die Beauftragten WpHG- und MaRisk-Compliance gefragt, auf die Implementierung aller Vorgaben hinzuwirken und die Geschäftsleitung bei deren Umsetzung zu beraten. ■

► IT-Organisation

Analyse „wesentlicher Veränderungen“ nach MaRisk AT 8.2

Aufgrund der MaRisk AT 8.2 sind wesentliche Veränderungen in der IT-Organisation gesondert zu beachten und zu dokumentieren. Doch wie kann der Nachweis erfolgen, dass nicht-wesentliche Veränderungen tatsächlich nicht wesentlich sind?

Die Norm des AT 8.2 MaRisk besagt, dass vor wesentlichen Änderungen in der IT-Organisation die Auswirkungen der geplanten Änderungen zu prüfen sind: „Vor wesentlichen Veränderungen in der Aufbau- und Ablauforganisation sowie in den IT-Systemen hat das Institut die Auswirkungen der geplanten Veränderungen auf die Kontrollverfahren und die Kontrollintensität zu analysieren. In diese Analysen sind die später in die Arbeitsabläufe eingebundenen Organisationseinheiten einzuschalten.“

Im Rahmen ihrer Aufgaben sind auch die Risikocontrolling-Funktion, die Compliance-Funktion und die Interne Revision zu beteiligen.¹

Doch was lässt sich unter einer „wesentlichen Veränderung“ in der IT-Organisation verstehen und wie lässt sich die Norm in der Praxis umsetzen?

Eine „wesentliche Veränderung“ setzt i.S. der MaRisk AT 8.2 voraus, dass die Veränderung unter anderem

- einen oder mehrere wesentliche Prozesse direkt betrifft,
- erhebliche Auswirkungen auf die Aufbau- und Ablauforganisation/das Gesamtunternehmen haben wird,
- erhebliche finanzielle sowie rechtliche Auswirkungen haben wird und folglich
- entsprechende Auswirkungen auf das interne Kontrollverfahren und die Kontrollintensität der Bank zu erwarten sind.

Des Weiteren sind zunächst grundlegende inhaltliche Fragen (Zeitpunkt, Aufbau und Inhalte der Analyse) zu klären.

Zeitpunkt und Ablage der Analyse

Die Analyse ist – wie in den MaRisk AT 8.2 deklariert – vor jeder Veränderung vorzunehmen. Doch was heißt das in der Praxis?

Die Analyse sollte zu Beginn eines jeden Projektes oder Einführungsprozesses erfolgen und kann idealerweise dort auch hinterlegt sein. Danach können weitere Schritte wie z. B. die Test- und Freigabephase erfolgen.

Dabei sind nicht nur die Fachabteilungen neben dem IT-Management involviert. Auch das Risikocontrolling, das Compliance-Beauftragtenwesen und die Interne Revision sind einzubinden und die Analyse/Dokumentation ist zur Kenntnis vorzulegen.

Aufbau und Inhalte der Analyse

Eine aussagekräftige Analyse setzt zunächst die Klärung der Analyse-Inhalte und des Analyse-Aufbaus voraus. Es empfiehlt sich, ein Musterformular zu erstellen bzw. zu verwenden, um eine einheitliche, standardisierte Vorgehensweise und Dokumentation sicherzustellen. Beispielhaft soll an dieser Stelle auf die Möglichkeit zur Nutzung einer Standard-Arbeitsanweisung des Genossenschaftsverbands (z. B. 100.04.07. Rahmenbedingungen zu wesentlichen Änderungen der IT und Organisation) hingewiesen werden. Folgende Inhalte sind in der Analyse zu empfehlen:

- Welche Fachbereiche sind betroffen?
- Wer ist für die Analyse verantwortlich?
- Welche Veränderungen sind mit welchen Anwendungen geplant?
- Zu welchem Zeitpunkt ist die Veränderung geplant?
- Welche Zielsetzung ist mit der Veränderung verbunden?
- Welche Kriterien sprechen für eine wesentliche Veränderung nach MaRisk AT 8.2?
- Wird die Anwendung erstmalig eingesetzt? >

¹ BaFin – Bundesanstalt für Finanzdienstleistungsaufsicht, https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs0917_marisk_Endfassung_2017_pdf_ba.pdf?__blob=publicationFile&v=5 (Stand: 03.04.2019)



- ▶ Sind wesentliche und/oder unwesentliche Geschäftsprozesse betroffen?
- ▶ Liegt eine wesentliche oder nicht-wesentliche Veränderung vor? (mit kurzer Begründung)

Damit die Analyse den Anforderungen der MaRisk AT 8.2 entspricht, ist diese durch den Auftraggeber, den Freigeber sowie zur Kenntnis durch das Risikocontrolling, das Compliance-Beauftragtenwesen und durch die Interne Revision (digital) unterzeichnen zu lassen.

Kriterien der Wesentlichkeit und Auswirkungsanalyse

Zu den Kriterien der Wesentlichkeit zählt, ob sich die wesentlichen Veränderungen in der IT-Organisation auf die Stabilität/Funktionsfähigkeit des wesentlichen Geschäftsprozesses auswirken. Wenn beispielsweise die Einführung einer neuen Anwendung lediglich unterstützenden Charakter hat und bei einem möglichen Ausfall der Geschäftsprozess weiter nahezu uneingeschränkt fortgeführt werden kann, wäre dies ein Begründungsansatz für eine nicht-wesentliche Veränderung.

Darüber hinaus sind die Einhaltung der rechtlichen Anforderungen der Bank sowie mögliche finanzielle Risiken, aber auch

der Schutzbedarf der Daten und die Gesamtauswirkung auf das Unternehmens in der Wesentlichkeitsprüfung einzubeziehen.

Kontrollverfahren und Kontrollintensität in der Praxis

Was ist mit Auswirkungen auf Kontrollverfahren und Kontrollintensität in den MaRisk AT 8.2 gemeint?

Gemäß MaRisk AT 1 Ziffer 1 setzt sich das interne Kontrollverfahren aus dem internen Kontrollsystem (kurz IKS) und der Internen Revision zusammen. In der Praxis können im Bereich der Informationssicherheit/des IT-Managements beispielsweise wiederkehrende Kontrollaufgaben (Rezertifizierung der Zugriffs- und Zutrittsberechtigungen, Überprüfung der IT-Arbeitsanweisungen, Test-Freigabe-Verfahren von Releases etc.) zu dem in der Bank implementierten Kontrollsystem zählen.

Die Kontrollintensität legt dabei fest, wie das Kontrollverfahren bzw. das interne Kontrollsystem konkret umgesetzt wird (z. B. Kontrollzeitpunkte/-intervalle).

Das Ergebnis der Wesentlichkeitsprüfung kann unter anderem sein, dass das IKS und somit auch das Kontrollverfahren der Bank nicht direkt betroffen sind. Dieses wäre ein weiteres Argument für eine nicht-wesentliche Veränderung.

**AUTOR UND
ANSPRECHPARTNER****Benjamin Wellnitz**

Beauftragter Informationssicherheit & Datenschutz,
E-Mail: benjamin.wellnitz@dz-cp.de



Folglich ist immer die Analyse nach MaRisk AT 8.2 voranzustellen, um entsprechende Prüfungsergebnisse herleitbar aufbauen zu können.

Sofern eine wesentliche Veränderung festgestellt wurde, sollte eine detaillierte Auswirkungsanalyse erstellt werden. Die Auswirkungsanalyse sollte

- ▶ die Auswirkungsintensität (Grad der Betroffenheit),
- ▶ Auswirkungen auf die Verfügbarkeit von IT-Systemen,
- ▶ Auswirkungen auf die Risikosituation (z. B. Adressausfallrisiko, Marktpreisrisiko, Liquiditätsrisiko) sowie
- ▶ erhöhte Auswirkungen auf operationelle Risiken darstellen.

Zu empfehlen ist, dass die genannten Dimensionen in der Beurteilung über eine Skalierung/Klassifizierung (z.B. 1 = unwesentlich bis 4 = wesentlich) beantwortet werden.²

Die detaillierte Auswirkungsanalyse braucht beim Ergebnis einer nicht-wesentlichen Veränderung nicht vorgenommen zu werden.

Weitere Schritte nach der Analyse

Nach der Analyse sollte in der nächsten Phase die Konzeption und Implementierung der erforderlichen organisatorischen Maßnahmen festgelegt und umgesetzt werden.

In der Regel wird eine Risikoanalyse gemäß MaRisk AT 7.2 losgelöst vom Ergebnis der Analyse nach MaRisk AT 8.2 vorgenommen. Hierbei werden mögliche Bedrohungsszenarien durch die identifizierten Risiken betrachtet. Um die Risiken (Bruttorisiko) zu minimieren, sind entsprechend Maßnahmen umzusetzen (z. B. Schulungen, um die Risiken einer fehlerhaften Erfassung/Konfiguration des neuen Systems zu minimieren). Dabei ist der Anpassungsbedarf an das interne Kontrollsystem, aber auch der Veränderungsbedarf in der Aufbau- und Ablauforganisation (z. B. Stellenbeschreibungen, Arbeitsanweisungen, Kompetenzen, Prozesse) zu überprüfen.

Im Anschluss erfolgt eine für Dritte nachvollziehbare Dokumentation.

Fazit

Grundsätzlich sind alle Veränderungen in der IT-Organisation auf die Wesentlichkeit vor der geplanten Veränderung in der IT-Organisation zu überprüfen. Das Ergebnis kann sowohl eine wesentliche als auch eine nicht-wesentliche Veränderung sein.

Bei einer fundiert begründeten Feststellung einer nicht-wesentlichen Veränderung kann auf eine Detailanalyse verzichtet werden.

Zu beachten ist, dass eine Wesentlichkeitsfeststellung einen erhöhten Maßnahmen- sowie Dokumentationsaufwand nach sich zieht und gut überlegt sein sollte. ■

² vgl. Geiersbach, Karsten, Prüfungserfahrung zu AT 8.2 MaRisk, <https://www.fc-heidelberg.de/pruefungserfahrungen-zu-8-2-marisk-2/> (Stand: 03.04.2019)

► Geldwäscheprävention

Auslegungs- und Anwendungshinweise zum Geldwäschegesetz

Am 11. Dezember 2018 hat die BaFin ihre Auslegungs- und Anwendungshinweise (AuA) zum Geldwäschegesetz (GwG) auf ihrer Homepage veröffentlicht. Durch diese werden nun die Anforderungen aus dem Gesetz zur Umsetzung der 4. EU-Geldwäscherichtlinie aus 2017 konkretisiert.

Im Vergleich zu der im März 2018 vorgelegten Entwurfsfassung gibt es nun einige Veränderungen und zum Teil erfreulicherweise auch Vereinfachungen. Ein „besonderer Teil für Kreditinstitute“ ist bereits avisiert und wird noch folgen. Die in 2014 veröffentlichten Auslegungs- und Anwendungshinweise der DK gelten bei vergleichbarer Rechtslage weiterhin fort (vgl. auch Rundschreiben des BVR zu den AuA vom 07.02.2019).

Nach eingehender Analyse und Erörterung haben wir unseren Mandanten bereits im Januar bzw. zum 1. April 2019 eine aktualisierte Arbeitsanweisung zur Prävention von Geldwäsche, Terrorismusfinanzierung und sonstigen strafbaren Handlungen, nebst übersichtlicher Information zu den Veränderungen, zur Verfügung gestellt. Weitere Veröffentlichungen, wie beispielsweise eine angepasste Musterarbeitsanweisung des DGRV, sind in Arbeit. Nach Veröffentlichung werden wir diese ebenfalls analysieren und die notwendigen Umsetzungsmaßnahmen vornehmen. Gerne stehen wir hierfür auch im Rahmen von Beratungsmandaten zur Verfügung.

Hinsichtlich der Veränderungen lässt sich im Wesentlichen festhalten, dass die Anforderungen an die Risikoanalyse und organisatorische Gestaltung des Beauftragtenwesens erweitert werden und die Rolle des Geldwäschebeauftragten wichtiger und anspruchsvoller denn je ist. Verstärkt wird dies insbesondere durch die Bezugnahme auf den Beschluss des OLG Frankfurt

vom 10. April 2018, 2 Ss-OWi 1059/17, der auch die Verantwortlichkeit des Geldwäschebeauftragten nochmals verdeutlicht. Nicht zu vernachlässigen sind die Aussagen zu den Kundensorgfaltspflichten, insbesondere zur Identifizierung, und das viel diskutierte Thema (fiktiver) wirtschaftlich Berechtigter. Trotz einiger Erleichterungen dürfte sich hier für alle Institute gesamthaft ein weiterer Aufwand bei der Erfüllung sämtlicher aufsichtsrechtlicher Anforderungen ergeben. ■

AUTOREN UND ANSPRECHPARTNER**Florian Fuhrig**

Beauftragter Geldwäsche- und Betrugsprävention,
E-Mail: florian.fuhrig@dz-cp.de

Michael Müller

Beauftragter Geldwäsche- und Betrugsprävention,
E-Mail: michael.mueller@dz-cp.de

Tabelle 1 WAS ÄNDERT SICH IM WESENTLICHEN?*

Themengebiet	Änderungen im Sinne der AuA
Verantwortlichkeit eines Mitglieds der Leitungsebene	Die Verantwortlichkeit muss eindeutig dokumentiert sein (eine Information an die BaFin ist jedoch nicht notwendig). Die Risikoanalyse sowie die Ersteinrichtung/wesentliche Änderungen der internen Sicherungsmaßnahmen bedürfen der Genehmigung dieser benannten Person.
Risikoanalyse	Eine nationale Risikoanalyse ist für den Sommer 2019 avisiert. Die gemeinsamen Leitlinien nach Artikel 17 und Artikel 18 Absatz 4 der Richtlinie (EU) 2015/849 sind zu berücksichtigen. Die mindestens jährlich vorzunehmende Aktualisierung der Risikoanalyse soll Änderungen nachvollziehbar aufzeigen.
Bestellung eines Geldwäschebeauftragten	Es können, sofern arbeitsteilig sinnvoll, auch mehrere Stellvertreter gegenüber der Aufsicht benannt werden. Im Rahmen der rechtzeitigen BaFin-Anzeige müssen auch die Kontaktdaten übermittelt werden.
Verantwortlichkeit des Geldwäschebeauftragten	Der Geldwäschebeauftragte trifft die Entscheidung über die Beendigung einer Geschäftsbeziehung im Rahmen einer Verdachtsmeldung.
Zuverlässigkeitsprüfung	Die Überprüfung der Zuverlässigkeit in ihrer Intensität und Häufigkeit ist risikoorientiert bei allen Beschäftigten, die in für Geldwäsche und Terrorismusfinanzierung relevanten Arbeitsbereichen tätig sind oder unmittelbaren Zugang zu Geschäftsräumen haben (z. B. Sicherheitspersonal), vorzunehmen. Bei der Auswahl der für die Kontrolle der Zuverlässigkeit einzusetzenden Instrumente sowie hinsichtlich der Kontrolldichte besteht aus Gründen der Verhältnismäßigkeit und unter Berücksichtigung des risikoorientierten Ansatzes die Möglichkeit eines Beurteilungsspielraums (z. B. Nutzung vorhandener Personalbeurteilungssysteme oder eines „Negativtestats“).
Prüfungshandlungen der Internen Revision	Die Innenrevision bzw. die interne/externe Prüfungsstelle hat die Einhaltung aller geldwäscherechtlichen Pflichten zu überprüfen. Es ist regelmäßig ausreichend, wenn jedes Jahr risikogemessen Teilbereiche geprüft werden, sofern innerhalb eines Dreijahresrhythmus sämtliche Bereiche einer Prüfung unterzogen werden.
Geschäftsbeziehungen	Auch der Bürge ist als Vertragspartner nach dem GwG zu sehen und fällt somit unter die Anwendungspflicht der Sorgfaltspflichten.

* Aufzählung aus Gründen der Lesbarkeit nicht abschließend



Fortsetzung Tabelle 1 WAS ÄNDERT SICH IM WESENTLICHEN? *

<p>Wirtschaftlich Berechtigter</p>	<p>Erleichterungen ergeben sich unter anderem bei Tochtergesellschaften von börsennotierten Unternehmen, sofern</p> <ul style="list-style-type: none"> ▶ Letztere mehr als 50 % der Kapitalanteile oder Stimmrechte an der Tochtergesellschaft halten und ▶ es, etwa aufgrund anderweitiger Kontrollausübung, keinen anderen wirtschaftlich Berechtigten im Sinne von § 3 Abs. 1 GwG gibt. <p>Dies gilt auch, wenn die Tochtergesellschaften selbst nicht börsennotiert sind. In diesen Fällen müssen weder „echte“ noch „fiktive“ wirtschaftlich Berechtigte erfasst werden.</p> <p>Der Stifter einer rechtsfähigen Stiftung ist nicht automatisch als wirtschaftlich Berechtigter zu erfassen, da er mit der Entstehung der Stiftung seine Einflussmöglichkeiten auf diese verliert. Ist der Stifter nicht gleichzeitig auch in den Organen der Stiftung vertreten, so hat er keine Einflussmöglichkeiten und kommt als wirtschaftlich Berechtigter nicht in Frage.</p> <p>Die Nacherfassung von wirtschaftlich Berechtigten ist auch für Bestandskunden notwendig.</p>
<p>Fiktiver wirtschaftlich Berechtigter</p>	<p>Erfüllen mehrere Personen den Tatbestand des fiktiven wirtschaftlich Berechtigten (z. B. mehrere Vorstandsmitglieder), reicht die Erfassung einer Person. In Ausnahmefällen können Risikoaspekte die Erfassung aller Personen erforderlich machen.</p>
<p>Aktualisierung von Kundendaten</p>	<p>Die Erfüllung der Aktualisierungspflicht hat periodisch und anlassbezogen zu erfolgen. Unterschieden wird bei den Fristen in geringes (alle 15 Jahre), normales (alle zehn Jahre) und hohes Risiko (alle zwei Jahre). Die BaFin stellt klar: „Aktualisierungsmaßnahmen setzen nicht zwingend Kontaktaufnahme mit dem Kunden voraus. Vielmehr kann auch auf anderweitig erhältliche Informationen zurückgegriffen werden, sofern diese aus einer zuverlässigen Quelle stammen.“ Dies könnten beispielsweise Auszüge aus Melderegistern oder Rücksprache mit Verfügungsberechtigten sein.</p>
<p>Übertragung von Sorgfaltspflichten auf vertraglicher Basis</p>	<p>Das PostIdent-Verfahren ist weiterhin ein geeignetes Identifikationsverfahren. Die Deutsche Post AG ist anderes geeignetes Unternehmen i.S.v. § 17 Abs. 5-9 GwG, alle entsprechenden Voraussetzungen müssen auch gegenüber der Deutschen Post AG erfüllt sein. Sofern gültige Rahmenverträge bestehen, ist kein gesonderter neuer Abschluss erforderlich. Sollten die bestehenden Verträge jedoch nicht diesen Auslegungs- und Anwendungshinweisen entsprechen, sind sie an diese anzupassen.</p>
<p>Sub-Auslagerung</p>	<p>Eine Sub-Auslagerung der Durchführung der Sorgfaltspflichten durch vertraglich beauftragte andere Personen und Unternehmen gemäß § 17 Abs. 5-9 GwG ist nur dann gestattet, wenn alle Voraussetzungen des § 17 Abs. 5-7 GwG im Verhältnis des Verpflichteten zum Weiterbeauftragten erfüllt sind.</p> <p>Dies bedeutet, dass sich weiterbeauftragte andere Personen und Unternehmen auch vertraglich gegenüber dem Verpflichteten, z. B. durch Einräumung entsprechender Verpflichtungen zu Gunsten des Verpflichteten in den Dienstleisterverträgen mit den vertraglich beauftragten anderen geeigneten Personen oder Unternehmen, zur Einhaltung der (gesetzlichen) Vorgaben für die Erfüllung der Sorgfaltspflichten und zur Einräumung von Prüf- und Kontrollrechten für den Verpflichteten und dessen Aufsichtsbehörde verpflichten müssen. Die diesbezüglichen Regelungen im Rundschreiben 3/2017 vom 10. April 2017 bleiben unberührt.</p>
<p>Aufzeichnungs- und Aufbewahrungspflichten</p>	<p>Soweit in Bezug auf Bestandskunden, die vor dem 26. Juni 2017 legitimiert wurden, entsprechende Kopien oder digitalisierte Erfassungen nicht vorliegen, brauchen diese – auch im Rahmen der Aktualisierungspflicht nach § 10 Abs. 1 Nr. 5 GwG i.V.m. § 10 Abs. 3 a.E. GwG – nicht nachgeholt zu werden.</p>
<p>Verdachtsmeldewesen</p>	<p>Die AuA stellen klar, dass eine interne Meldung unmittelbar an den zuständigen Beauftragten zu erfolgen hat. Die Meldung an einen Vorgesetzten/eine andere Stelle, die die Meldung nur dann weiterleitet, wenn sie die Einschätzung des Beschäftigten teilt, ist nicht zulässig.</p>

* Aufzählung aus Gründen der Lesbarkeit nicht abschließend

Tabelle 2 ERLEICHTERUNGEN BEI DER IDENTIFIZIERUNG

Rechtsform	Änderungen im Sinne der AuA
GbR	<ul style="list-style-type: none"> ▶ Identifizierung der GbR anhand des Gesellschaftsvertrags. ▶ Soweit tatsächlicher Gesellschaftszweck in Bezug auf Geldwäsche oder Terrorismusfinanzierung kein erhöhtes Risiko erkennen lässt: Identifizierung der hinsichtlich der Geschäftsverbindung verfügungsberechtigten Personen. ▶ Erfassung sämtlicher Mitglieder oder Vorlage von Mitgliederlisten ist nicht erforderlich.
WEG	<ul style="list-style-type: none"> ▶ Identifizierung der WEG anhand eines Protokolls der Eigentümerversammlung. ▶ Identifizierung der hinsichtlich der Geschäftsverbindung verfügungsberechtigten Personen. ▶ Erfassung sämtlicher Miteigentümer oder Vorlage von Miteigentümerlisten und Einstellung in die Datei zum automatisierten Kontoabruf nach § 24c KWG ist nicht erforderlich. ▶ Es ist keine Erfassung eines (fiktiven) wirtschaftlich Berechtigten notwendig.
Nicht rechtsfähiger Verein (Gewerkschaft/Partei, andere vergleichbare nicht rechtsfähige deutsche Vereine)	<ul style="list-style-type: none"> ▶ Identifizierung des nicht rechtsfähigen Vereins anhand der Satzung sowie des Protokolls über die Mitgliederversammlung, in der die Satzung beschlossen wurde. ▶ Soweit tatsächlicher Vereinszweck in Bezug auf Geldwäsche oder Terrorismusfinanzierung kein erhöhtes Risiko erkennen lässt: Identifizierung der hinsichtlich der Geschäftsverbindung verfügungsberechtigten Personen. ▶ Erfassung sämtlicher Mitglieder oder Vorlage von Mitgliederlisten ist nicht erforderlich. ▶ Es ist keine Erfassung eines (fiktiven) wirtschaftlich Berechtigten notwendig.
Juristische Personen des öffentlichen Rechts (öffentlich-rechtliche Körperschaften, Anstalten)	<ul style="list-style-type: none"> ▶ Vorbehaltlich der Umstände des Einzelfalles ist davon auszugehen, dass die Identifizierung eines wirtschaftlich Berechtigten in diesen Fällen nicht erforderlich ist. ▶ Es ist keine Erfassung eines (fiktiven) wirtschaftlich Berechtigten notwendig.

► **Datenschutz**

Compliance trifft Unternehmenskultur

Die Umsetzung von Compliance-Themen ist selten einfach. Wenn sich der Einsatz auszahlen soll, muss jeder Mitarbeiter mitziehen. Spätestens an diesem Punkt treffen Compliance und Unternehmenskultur zusammen.

Compliance meint allgemein die Einhaltung von Gesetzen, Regeln und Normen. Im Bereich Datenschutz und Informationssicherheit gilt es, eine Vielzahl an Anforderungen zu berücksichtigen und zu dokumentieren. Datenschutz und Informationssicherheit sind – im Übrigen ebenso wie alle anderen Beauftragenthemen – voller Fallstricke, die nicht selten als „Vertriebsverhinderung“ wahrgenommen werden.

Diese Zuweisung versuchen wir jeden Tag aufs Neue zu widerlegen. Fakt ist jedoch: Es bedarf für solche Themen einer gewissen Akzeptanz in der Mitarbeiterschaft. Heute reicht es nicht mehr aus, wenn sich nur spezifische Fachbereiche mit den jeweiligen Compliance-Themen beschäftigen. Inzwischen ist faktisch jeder Mitarbeiter in der Bank gefordert, Compliance prozessorientiert umzusetzen. Eine gute und effiziente Compliance ist heute nur noch gemeinsam möglich. Dazu bedarf es einer entsprechenden Unternehmenskultur.

Es stellt sich die Frage, wie genau Compliance und Unternehmenskultur zusammenhängen.

Von inneren Werten und äußerem Verhalten

Regelt die Compliance korrektes rechtliches und ethisches Verhalten, dann geht es bei der Unternehmenskultur um das Regelwerk der inneren Werte: die Entwicklung und die Vereinbarkeit persönlicher und unternehmerischer Ziele und Werte.

Dies betrifft in erster Linie den internen Umgang miteinander. Eine gesunde Unternehmenskultur verfügt aber über eine Strahlkraft, die auch von Außenstehenden positiv wahrgenommen wird. Ziel ist es, ein Klima zu schaffen, in dem jeder gerne arbeitet und sich mit dem Unternehmen identifizieren kann.

Volker Barczynski hat sich des Themas Unternehmenskultur angenommen und reist um den Globus, um Impulse für mehr

Jobzufriedenheit zu sammeln. Er trifft sich mit Prominenten, wie dem Boxweltmeister Henry Maske, oder interviewt in Hollywood eine Starfrisörin. „Wir müssen über den Tellerrand schauen, um eine attraktive Arbeitskultur zu entwickeln“, sagt Barczynski. Dabei ist es egal, ob er mit Großunternehmer Götz Werner, dem Gründer der dm-Drogeriemarkt-Kette, oder mit einer Auszubildenden eines Handwerksunternehmens spricht. „In modernen Unternehmen spielen Hierarchie und Status eine untergeordnete Rolle“, führt der Experte an. Auf seinen Vorträgen, Coachings und Seminaren gibt er die Grundlagen erfolgreicher Unternehmenskultur und seine gesammelten Impulse weiter.

Wir haben den Experten gebeten, uns ein paar Regeln zu nennen, die Firmen beachten sollten, um eine „gute“ Unternehmenskultur zu entwickeln. Herausgekommen sind vier Tipps für ein gesundes Betriebsklima.

1. Kommunikations- und Streitkultur

„Bilden Sie jeden Mitarbeiter in Grundlagen der Kommunikation aus. Diese folgt nämlich klaren Regeln. Zu oft wird es in der Kommunikation persönlich, spielen Sympathie oder Ablehnung einer Person eine Rolle. Beides hat unerwünschte Folgen: Reibungsverluste bei Ablehnung, Verlust des Fokus auf die Sache bei zu großer Übereinstimmung. Die Folge ist nicht selten Jobfrustration oder unternehmerischer Misserfolg. Es gilt daher die Devise: Richtig kommunizieren und kultiviert streiten.“

2. Spiel mit klaren Regeln

„Es geht darum, Leistungsträger zu sichten und zu fördern. Akzeptieren Sie, dass gute Ideen für Ihren geschäftlichen Erfolg von jedem Mitarbeiter kommen können. Eine gute Führungskraft entwickelt eine Atmosphäre, in der sich jeder einbringen kann. Dazu müssen die Spielregeln klar sein, und Barrieren müssen abgebaut werden. Nur ein Mitspieler, der sich auch auf dem Platz beweisen kann, ist auf Dauer motiviert.“



Kultur ist ein Mitarbeiter-Magnet

Eine Investition in die Kultur lohnt sich, sagt Volker Barczynski. Mehr zum Programm von Volker Barczynski finden Sie unter www.volkerbarczynski.com.

3. Ausgeglichene Mitarbeiter liefern weltmeisterliche Leistungen

„Jogi Löw hat es 2014 vorgemacht. Er hat der deutschen Elf nicht nur Unterricht im Kicken gegeben. Er hat jeden Spieler als Individuum betrachtet. Mentale Fitness und Entspannung gehörten genauso zum Programm wie das körperliche Training. Das Ergebnis war weltmeisterlich. Kümmern Sie sich auch darum, wie es Ihren Mitarbeitern geht, damit diese Ihre Fähigkeiten zu 100% einsetzen können. Ausgeglichene Mitarbeiter sind leistungsfreudiger. Aber nicht nur das: Ein Mitarbeiter, der als Mensch im Unternehmen wahrgenommen wird, zahlt dies durch ein Vielfaches an Loyalität zurück.“

4. Lob und Anerkennung

„Leider gilt in vielen Unternehmen noch die Devise ‚Nicht gemeckert ist Lob genug‘. Das motiviert Mitarbeiter nicht. Allerdings will Loben auch gelernt sein. Oft kommen die gut gemeinten Worte falsch beim Gegenüber an. Besonders dann, wenn zuvor nicht oder wenig gelobt wurde. Umschiffen kann man dieses Missverständnis ganz einfach: Loben Sie nicht die Person, sondern bemerken Sie anerkennend die Handlung der Person, die aus Ihrer Sicht zielführend war. Und: Geben Sie ruhig in kurzen Worten den Grund für Ihre anerkennenden Worte an. Das hilft dem Gegenüber, das Lob in die richtige Schublade zu stecken.“

Es wird klar, dass Compliance und Unternehmenskultur vor allem eines gemein haben: Man muss am Ball bleiben und die Prozesse auf dem Laufenden halten. Aber dahinter steckt noch mehr: Mit einer guten Unternehmenskultur wird der Boden für eine gute Compliance gelegt.

Kultiviert im Inneren, glaubwürdig nach außen

Selbstbewusste, orientierte, sich ernst genommen und respektiert führende Mitarbeiter können sich die Notwendigkeit einer Compliance-Maßnahme eher zu eigen machen als Mitarbeiter, die orientierungslos sind. Darüber hinaus zahlt eine gute Unternehmenskultur – die innere „Strahlkraft“ – auf die Glaubwürdigkeit der Unternehmens-Compliance ein.

Unternehmenskultur und Compliance gehen im Optimalfall Hand in Hand: Der innere Zusammenhalt wirkt wie eine Immunisierung gegen diverse Risiken und ist Impulsgeber für das angestrebte „richtige“ Verhalten nach außen – egal ob Datenschutz, Informationssicherheit oder eine anderes Beauftragthema. ■

AUTOR UND ANSPRECHPARTNER

Michael Switalla

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



► **DZ CompliancePartner im Überblick**

Compliance aus einer Hand



1. Sichere Lösungen: Unsere Kunden profitieren von dem Wissen der Gemeinschaft (Knowledge Sourcing)

2. Günstige Lösungen: i.d.R. 30% Kostensenkung zur Eigenfertigung (inkl. MwSt.)

3. Zertifizierte Lösungen: Zertifizierung nach IDW PS 951 Typ II, Prüfung durch Fachbeirat Beauftragtenwesen

4. Kompetente Lösungen: Fokussierung auf das regulatorische Beauftragtenwesen

5. Vernetzte Lösungen: Einbettung in den Verbund, vernetzt mit Gremien und der Aufsicht

Compliance bundesweit

Compliance bedarfsorientiert

	Auslagerung	Teil-Auslagerung	Coaching/ Beratung	Interims- Management	Werkzeug	WBT, Schulung
Geldwäsche-/Betrugsprävention	✓	✓	✓	✓	✗	✓
WpHG-Compliance	✓	✓	✓	✓	MAR kompakt	✓
MaRisk-Compliance	✓	✓	✓	✓	Rechtsmonitoring	✓
Informationssicherheit	✓	✓	✓	✓	Quick-Check	✓
Datenschutz	✓	✓	✓	✓	Quick-Check	✓
Hinweisgebersystem (25a KWG)	✓	✗	✓	✗	✗	✓
Notfallmanagement	✓	✗	✓	✗	✗	✓
Auslagerungsmanagement	?*	?*	✓	✗	AM kompakt	✓
IT-Revision	✓	✗	✓	✓	✗	✓

* in Abstimmung

Compliance: vernetzt und abgesichert

Aufsichtsrat

Am 22. März 2019 fand die konstituierende Sitzung des Aufsichtsrats der DZ CompliancePartner statt.

Zum Vorsitzenden wurde **Herr Michael Speth**, Mitglied des Vorstandes der DZ BANK, zur stellvertretenden Vorsitzenden **Frau Ulrike Brouzi**, Mitglied der Vorstandes der DZ BANK, gewählt.

Als Vertreterin der Regionalverbände wird der Aufsichtsrat komplettiert durch **Frau Monika van Beek**, Mitglied des Vorstandes des Baden-Württembergischen Genossenschaftsverbandes.

Fachbeirat Beauftragtenwesen

Der Fachbeirat Beauftragtenwesen ist eine Initiative der DZ CompliancePartner. Er setzt sich derzeit aus jeweils einem hochrangigen Vertreter der vier Regionalverbände sowie der Geschäftsführung der DZ CompliancePartner zusammen. Der Fachbeirat will verbandsübergreifend Sicherheit für Banken, Prüfer sowie Leiter Compliance und Beauftragte schaffen durch

- die Validierung von Fachvorgaben und
- eine ex ante prüferische Begleitung.

Gleichzeitig werden (praktische) Erkenntnisse aus der Regulatorik und den Prüfungen thematisiert mit dem Ziel, auch gegenüber Ämtern und Behörden eine gemeinsame Auffassung zu festigen.

Mitglieder des Fachbeirats sind derzeit:

- Herr Tino Behrends, Leiter Grundsatzabteilung, Genossenschaftsverband – Verband der Regionen e.V.
- Herr Michael Fritz (Vorsitzender), Leiter Grundsatzabteilung, Baden-Württembergische Genossenschaftsverband e.V.
- Herr Stefan Grueterich, Leiter Grundsatzabteilung, Genossenschaftsverband Weser-Ems e.V.
- Herr Dr. Alexander Leißl, Leiter Grundsatzabteilung, Genossenschaftsverband Bayern e. V.
- Herr Kai-Hendrik Friese, Leiter Bereich Compliance, DZ BANK AG

Kundenbeirat

Der Kundenbeirat bezieht aktiv und regelmäßig die Kunden der DZ CompliancePartner in die Produkt- und Dienstleistungsentwicklung ein. Durch seine beratende Funktion sollen mögliche Entwicklungspotenziale der Gesellschaft aufgezeigt und eine nachhaltige, marktorientierte Positionierung der Gesellschaft sichergestellt werden.

Interne und externe Prüfung/Absicherung

- ▶ Regelmäßige Prüfung/Testierung der Dienstleistungen durch einen unabhängigen Wirtschaftsprüfer nach IDW 951 Typ II
- ▶ Regelmäßige Prüfung/Testierung der Tools bzw. Module (u. a. Gefährdungsanalyse, Kontrollpläne und Kontrolldurchführung) durch einen unabhängigen Wirtschaftsprüfer nach IDW PS 880
- ▶ Abstimmung mit den Regionalverbänden über den Fachbeirat Beauftragtenwesen
- ▶ Eigene Interne Revision
- ▶ Auslagerungsmanagement: bedarfsorientierte Musterrisikoanalysen durch einen unabhängigen Wirtschaftsprüfer, z. B. zum Kauf durch die DZ BANK oder zur Integration des DZ BANK-Angebots in der Geldwäsche- und Betrugsprävention (siehe S. 23)

Norbert Schäfer ergänzt Geschäftsführungsteam



Mit Wirkung zum 1. April 2019 wurde Norbert Schäfer in die Geschäftsführung der DZ CompliancePartner GmbH berufen.

Norbert Schäfer ist ein ausgewiesener Experte in der Geldwäsche- und Betrugsprävention und wird künftig dieses Geschäftsfeld in der DZ CompliancePartner GmbH verantworten. Er ist der Genossenschaftlichen FinanzGruppe seit über 37 Jahren eng verbunden und hat zuletzt die Abteilung Insourcing Finanzkriminalität in der DZ BANK AG Deutsche Zentral-Genossenschaftsbank am Standort Düsseldorf verantwortet.

Hintergrund ist die Integration des Auslagerungsangebotes „Geldwäsche- und Betrugsprävention“ der DZ BANK AG in die DZ CompliancePartner GmbH und die damit verbundene Bündelung der Kräfte im Beauftragtenwesen. Sie ist eine Antwort auf die nach wie vor steigenden Anforderungen im Beauftragtenwesen. Ziel ist, die Position der Genossenschaftsbanken zentral und nachhaltig zu stärken. ■

Wir gratulieren ...

- ▶ Marco Becker zu seiner Beförderung zum Leiter des Bereichs Geldwäsche- und Betrugsprävention (Team I)
- ▶ Michael Maier zu seiner Beförderung zum Leiter des Bereichs MaRisk-Compliance
- ▶ Christoph Menzyk zu seiner Beförderung zum Leiter des Bereichs Geldwäsche- und Betrugsprävention (Team II)
- ▶ Lars Schinnerling zu seiner Beförderung zum Leiter des Bereichs Interne Revision
- ▶ Thorsten Schmeil zu seiner Beförderung zum Leiter des Bereichs Geldwäsche- und Betrugsprävention (Team III)

- ▶ Michael Switalla zu seiner Beförderung zum Leiter des Bereichs Informationssicherheit und Datenschutz
- ▶ Thomas Wagener zu seiner Beförderung zum Leiter des Bereichs Compliance Spezialisten

Wir gratulieren außerdem unseren Mitarbeiterinnen und Mitarbeitern zur erfolgreich bestandenenen Prüfung:

- ▶ Kai-Oliver Bock: Master of Business Administration (MBA), Risk & Fraud Consultant

IMPRESSUM

Point of Compliance

Das Risikomanagement-Magazin für unsere Kunden und Geschäftspartner, Ausgabe 20, 2/2019

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 CompliancePartner 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:

Florian Fuhrig, Marc Linnebach, Michael Maier, Andreas Marbeiter, Michael Müller, Lars Schinnerling, Michael Switalla, Björn Veith, Benjamin Wellnitz

Bildnachweise: DZ CompliancePartner GmbH

Gestaltung: EGENOLF DESIGN, Wiesbaden studio@egenolf-design.de

Druck: odd GmbH & Co. KG · Print und Medien, www.odd.de

Redaktioneller Hinweis: Nachdruck, auch auszugsweise, nur mit ausdrücklicher Genehmigung der Redaktion sowie mit Quellenangabe und gegen Belegexemplar. Die Beiträge sind urheberrechtlich geschützt. Zitate sind mit Quellenangabe zu versehen. Jede darüber hinausgehende Nutzung, wie die Vervielfältigung, Verbreitung, Veröffentlichung und

Onlinezugänglichmachung des Magazins oder einzelner Beiträge aus dem Magazin, stellt eine zustimmungsbedürftige Nutzungshandlung dar. Namentlich gekennzeichnete Beiträge geben nicht in jedem Fall die Meinung des Herausgebers wieder. Die DZ CompliancePartner GmbH übernimmt keinerlei Haftung für die Richtigkeit des Inhalts.

Redaktionsschluss: 4. April 2019

Auflage: 2.600 Exemplare

Die aktuellen Mediadaten finden Sie im Internet unter www.dz-cp.de/poc

Interne Revision

Seit der letzten Berichterstattung in der Point of Compliance (1/2019, S. 27) wurden entsprechend der Jahresprüfungsplanung 2018 die Berichte zu den Prüffeldern Zentrale Stelle, Unternehmenssteuerung, Risikomanagement und Produktentwicklung & -pflege veröffentlicht. Der Bericht zur IT-Revision 2018 wurde ebenfalls veröffentlicht. Der Quartalsbericht zum vierten Quartal 2018 sowie der Jahresbericht 2018 wurden erstellt und an unsere Kunden versandt. Aus der Jahresprüfungsplanung 2019 heraus wurde im Februar 2019 als erster Bericht des Jahres der Bericht zum Prüffeld Hinweisgebersystem („Ombudsstelle“) veröffentlicht.

Die Abarbeitung des internen Jahresprüfungsplanes für 2018 verlief unter Berücksichtigung der in 2018 durch die Geschäftsführung genehmigten Anpassungen planmäßig. Für das Jahr 2019 wurde ein neuer Jahresprüfungsplan basierend auf zwei Vollzeitmitarbeitern erstellt und von der Geschäftsführung genehmigt.

Die aus dem Jahr 2018 übertragenen zwei Prüfungen wurden in die Planung des Jahres 2019 aufgenommen.

Darüber hinaus wurde turnusgemäß ein Follow-up-Quartalsbericht für das vierte Quartal 2018 erstellt, in dem die Abarbeitung der von internen und externen Prüfern getroffenen Maßnahmen/Empfehlungen dokumentiert wird. Gegenüber dem vorherigen Quartal ist die Anzahl der offenen Punkte leicht gestiegen. Jedoch wurden die in vorangegangenen Prüfungen gemachten Feststellungen konsequent abgearbeitet, sodass die Zahl der überfälligen Punkte zurückging. Der Follow-up-Bericht für das vierte Quartal 2018 wurde der Geschäftsführung der DZ CompliancePartner GmbH fristgerecht vorgelegt. Darüber hinaus finden zwischen der Geschäftsführung und der Internen Revision mehrmals monatlich Jours fixes statt. ■

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

Wirtschaftliche Lage

Die Geschäftsentwicklung der DZ CompliancePartner (ehemals GenoTec) in 2018 ist im Vergleich zum Vorjahr und im Vergleich zum Plan positiv verlaufen. Mit einem Betriebsergebnis von +833 T€ und einem Jahresüberschuss von +771 T€ wurden das Betriebsergebnis und der Jahresüberschuss des Vorjahres erneut klar überschritten.

Die Umsatzerlöse konnten insgesamt gegenüber dem Vorjahr um 8,9 % gesteigert werden. Die Steigerung wird insbesondere durch die Produkte Geldwäsche- und Betrugsprävention sowie Datenschutz und Informationssicherheit getragen.

Der Trend setzt sich auch zu Beginn des Jahres 2019 fort: Die beiden ersten Monate liegen – trotz der Integrationsaufwendungen im Bereich der Geldwäsche- und Betrugsprävention und der Neuaufstellung der Bereiche Datenschutz, Informationssicherheit und IT-Revision – über dem Plan. Die Liquiditätssituation ist unverändert entspannt, die wirtschaftliche Lage der DZ CompliancePartner GmbH stabil. ■

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

Auslagerungsmanagement – in eigener Sache

Die AWADO Deutsche Audit GmbH hat zwei Musterrisikoanalysen zur Risikoeinschätzung nach MaRisk AT9 erstellt:

- ▶ Musteranalyse zum Kauf der DZ CompliancePartner (ehemals GenoTec)
- ▶ Musteranalyse zur Integration des DZ BANK-Angebotes in der Geldwäsche- und Betrugsprävention

Beide Analysen kamen zu folgenden Ergebnissen: „Das Risiko, dass ausgelagerte Aktivitäten und Prozesse des Dienstleisters ausfallen oder der Dienstleister insgesamt wegfällt, hat sich durch die beschriebenen Veränderungen nicht wesentlich verändert, dürfte sich durch die Einbindung in den DZ BANK-Konzern sogar eher vermindert haben und ist weiterhin als gering

einzustufen. Die Prüfungen des dienstleistungsbezogenen internen Kontrollsystems (IKS) der Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft im Jahr 2018 sind im Ergebnis ohne Mangel geblieben und haben ein uneingeschränktes Prüfungsurteil erhalten. Die Ausgestaltung des IKS und die Kontrollziele werden als geeignet und sachgerecht beurteilt, die Kontrollen als angemessen und wirksam.“

Die Musteranalysen können bei Bedarf unseren Kunden zur Verfügung gestellt werden. ■

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

