DZ CompliancePartner

Point of Compliance

Das Risikomanagement-Magazin für unsere Kunden und Geschäftspartner

AUSGABE 1/2021

Innehalten

IMPRESSUM

Point of Compliance
Das Risikomanagement-Magazin für unsere Kunden und Geschäftspartner, Ausgabe 25, 1/2021
ISSN: 2194-9514
Herausgeber: DZ CompliancePartner GmbH, Wilhelm-Haas-Platz, 63263 Neu-Isenburg, Telefon 069 6978-3324, Telefax 069 6978-3322, www.dz-cp.de
Handelsregister HRB 11105, Amtsgericht Offenbach, USt.-IdNr.: DE201150917
Geschäftsführung: Jens Saenger (Sprecher), Andreas Marbeiter, Norbert Schäfer

Verantwortlich i. S. d. P.: Jens Saenger
Redaktion: Gabriele Seifert, Leitung (red.), Vanessa Lanskoy (red.)
Redaktionsanschrift: DZ Compliance-Partner GmbH, Redaktion Point of Compliance, Wilhelm-Haas-Platz, 63263 Neu-Isenburg, Telefon 069 6978-3188, Telefax 069 6978-3322, E-Mail: poc@dz-cp.de
Weitere Autoren dieser Ausgabe:
Christine Bartsch, Thomas Grebe, Axel Hofmeister, Alexander Lorenz, Michael Maier, Martin Reglinski, Jens Saenger, Jörg Scharditzky, Lars Schinnerling, Thorsten Schmeil, Michael Switalla, Thomas Wagener

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

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

Corona hält uns im Bann.

Das viel beschworene New Normal lässt weiter auf sich warten. Unterdessen geht das Leben weiter.

Jens Saenger
Sprecher der Geschäftsführung

Im regulativen Beauftragtenwesen sehen wir, dass sowohl auf europäischer als auch auf nationaler Ebene die Gesetzgebung wie auch die Aufsicht ihre Ziele mit einem hohen (wohl zu hohen) Ambitionsniveau verfolgen. Das Thema Nachhaltigkeit nimmt mit der Taxonomie- und der Offenlegungsverordnung deutlich an Fahrt auf. Die neuen MaRisk und mit ihnen die BAIT stehen kurz vor der Veröffentlichung und werden im Risikomanagement weitere Schwerpunktthemen setzen. In der Geldwäscheprävention wird der § 261 StGB in Verbindung mit dem Gesetz zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche einen erheblichen Mehraufwand generieren.

Eine aufsichtsrechtliche Schonfrist ist nicht in Sicht. Zeit, innezuhalten und eigene Strukturen und Stärken neu zu betrachten.

Wir sehen es als unsere Aufgabe, Sie in Ihrem Tun zu unterstützen – allen Viren zum Trotz und den aufsichtsrechtlichen Anforderungen entsprechend.

In diesem Sinne wünsche ich eine anregende Lektüre.

Ihr Jens Saenger

WpHG-Compliance

Nachhaltigkeit in der Anlageberatung

Bereits seit 2013 sind Unternehmen mit mehr als 500 Mitarbeitern verpflichtet, einen nichtfinanziellen Bericht, den Nachhaltigkeitsbericht, zu erstellen. Mit dem Inkrafttreten der Taxonomie- und der Offenlegungsverordnung gewinnt die Nachhaltigkeitsregulierung nochmal an Schwung.

In den letzten Jahren verging nicht ein Branchentreffen, in dem nicht auf das kommende Thema Nachhaltigkeit in der Anlageberatung hingewiesen wurde. Mit der Taxonomie- und der Offenlegungsverordnung (siehe Kasten S. 6) erhält die Regulierung zu Nachhaltigkeitsaspekten eine neue Dimension in der Finanzdienstleistungsbranche. Die jetzt anstehenden Regelungen gehen weit über die Anlageberatung hinaus. Sie betreffen die Banken selbst und insbesondere die Durchführung ihres Wertpapiergeschäfts.

Die Regelungen gelten für den Großteil der Genossenschaftsbanken, als

- Finanzmarktteilnehmer, sofern sie die Finanzportfolioverwaltung (MeinInvest, VermögenPlus) anbieten, und/oder
- Finanzberater, bei Angebot der Anlageberatung,
- Banken, die verpflichtet sind, einen Nachhaltigkeitsbericht zu erstellen.

Offenlegung der Nachhaltigkeitsstrategie

Als Erstes steht die Offenlegung von Nachhaltigkeitsstrategien an. Auf diesem Wege soll transparent gemacht werden, wie Banken Nachhaltigkeitskriterien in ihren Investitionsentscheidungs- und Beratungsprozessen berücksichtigen.

Diese Pflicht gilt seit dem 10. März 2021 und sieht die Veröffentlichung auf den Internetseiten der Banken zu folgenden Nachhaltigkeitsstrategien vor:

- Transparenz der Strategien (bei der Finanzportfolioverwaltung und Anlageberatung) für den Umgang mit Nachhaltigkeitsrisiken (Art. 3)
- Transparenz nachteiliger Nachhaltigkeitsauswirkungen auf Ebene des Unternehmens (Art. 4)
- Transparenz der Vergütungspolitik im Zusammenhang mit der Berücksichtigung von Nachhaltigkeitsrisiken (Art. 5)
- Transparenz in vorvertraglichen Informationen zur Berücksichtigung von Nachhaltigkeitsrisiken (Art. 6)
- Transparenz bei Werbung zu einem Finanzprodukt mit ökologischen oder sozialen Merkmalen in vorvertraglichen Informationen (Art. 8)
- Transparenz in vorvertraglichen Informationen bei nachhaltigen Investitionen (Art. 9)
- Transparenz bei der Bewerbung ökologischer oder sozialer Merkmale auf Internetseiten (Art. 10)

Inhaltlich konkret können diese Darstellungen im Moment nicht sein, da bisher die dazu erforderlichen technischen Regulierungsstandards der Offenlegungsverordnung nicht vorliegen. Daher wird die Darstellung der Strategien derzeit nur prinzipienorientiert erfolgen.

Der BVR hat in Aussicht gestellt, den Genossenschaftsbanken eine Umsetzungshilfe zur Verfügung zu stellen (siehe BVR-Intranet, dort: „Regulatorische Vorgaben für den Vertrieb nachhaltiger Anlagen"). Diese soll auch eine vorläufige Lösung für die Nachhaltigkeitspräferenzabfrage bereitstellen. Sie wird voraussichtlich unmittelbar in der Anlageberatung einsetzbar sein, um so für die verpflichtende Umstellung des Beratungsprozesses zeitlichen Vorlauf zu haben.

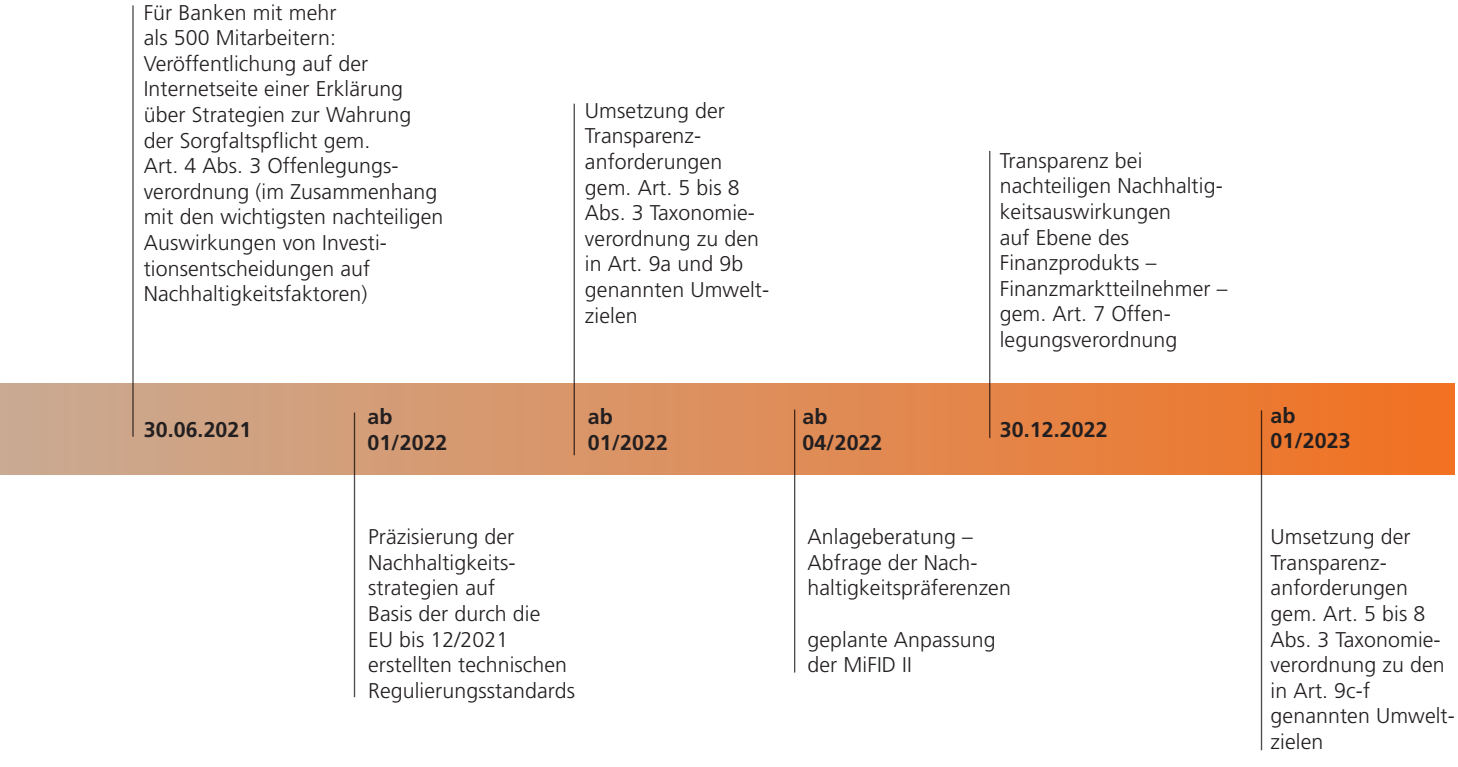
Nachhaltigkeit in der Anlageberatung

Das Thema Nachhaltigkeit hat bereits vollen Einzug in die Anlageberatung der Banken gehalten. Spätestens seit dem letzten Jahr sind die Weichen gestellt.

Die Kunden fragen zunehmend nachhaltige Anlageformen nach. Die Union Investment stellt einen rasanten Anstieg der in nachhaltigen Investmentprodukten investierten Anlagegelder fest. Waren es von 2009 bis 2019 noch 5 % der zufließenden Gelder, so betrug diese Summe in 2020 50 % bei Privatanlegern.

Die institutionellen Anleger der Union Investment sind schon längere Zeit nachhaltig orientiert. Von 2009 bis 2019 waren es 30 % der investierten Summen, 2020 ca. 60 %.

Für 2020 berichtet die Union Investment auf ihrer Internetseite von einem deutschlandweiten Rekordwert bei institutionellen Anlegern, die nachhaltig investieren: 80 % der Anleger haben danach nachhaltig investiert.



Banken sind bereits seit 2018 verpflichtet, im Rahmen der Anlageberatung Präferenzen und Anlageziele ihrer Kunden in der Geeignetheitserklärung darzustellen und Empfehlungen entsprechend darauf abzustimmen. Als explizites Beispiel für spezielle Kundenwünsche führt die BaFin die „Nachhaltigkeit" auf (vgl. auch BVR-Rundschreiben vom 15.04.2020 „Geeignetheitserklärung – Ergänzung der Begründung der Geeignetheit").

Dieser Aspekt der Geldanlage wird in der Anlageberatung nun Pflichtbestandteil: Berater werden Kunden explizit nach deren Wünschen zur Nachhaltigkeit befragen.

Der BVR geht davon aus, dass diese Pflicht ab ca. April 2022 einschlägig wird. Zuvor bedarf es weiterer regulatorischer Anpassungen. Insbesondere wird dem eine Änderung der Delegierten Verordnung zu MiFID II vorausgehen.

Der weitere Zeitplan zur Umsetzung von Taxonomie- und Offenlegungsverordnung

Die EU-Kommission hat sowohl sich als auch den Banken zeitliche Ziele für die Umsetzung der einzelnen Anforderungen gestellt.

Das erste Ziel, bis Ende 2020 technische Regulierungsstandards zu den ersten beiden Klimazielen Klimaschutz und Anpassung an den Klimawandel zu erstellen, konnte zeitlich nicht eingehalten werden. Hintergrund ist zum einen die enorme Anzahl an Rückmeldungen, die die Europäische Kommission im Rahmen der Konsultationen erhalten hat, zum anderen ist es die Diskussion um die Einstufung von Kohle in Bezug auf ihre Auswirkungen auf die ersten beiden Klimaziele.

Trotz der fehlenden technischen Standards wird die Offenlegungsverordnung umgesetzt, womit es ein klares Zeichen gibt, dass Nachhaltigkeit in das Finanzsystem integriert werden soll.

Taxonomie- und Offenlegungsverordnung

Die Taxonomieverordnung ist eine EU-Verordnung (2020/852), die Vorgaben für nachhaltige Investitionen definiert. Sie gilt für Banken, die Finanzportfolioverwaltung anbieten und/oder verpflichtet sind, eine nichtfinanzielle Erklärung (Nachhaltigkeitsbericht) zu erstellen.

Die Offenlegungsverordnung ist ebenfalls eine EU-Verordnung (2019/2088), die die Veröffentlichung von Informationen der Finanzmarktteilnehmer zur Nachhaltigkeit ihrer Investitionsentscheidungen regelt. Sie gilt für Banken, die Anlageberatung oder auch Finanzportfolioverwaltung anbieten.

AUTORIN UND ANSPRECHPARTNERIN

Christine Bartsch
Beauftragte WpHG-Compliance,
E-Mail: christine.bartsch@dz-cp.de

Die BaFin geht in ihrem aktuellen Journal (Februar 2021, S. 13) davon aus, dass die Europäische Kommission die technischen Regulierungsstandards innerhalb von drei Monaten verabschiedet. Diese sollen laut Vorschlag der ESAs (European Supervisory Authorities) im finalen Bericht ab dem 1. Januar 2022 gelten.

Die neue Regulierung und WpHG-Compliance

In den Erwägungsgründen für die Taxonomieverordnung zeigt die Europäische Kommission klar auf, dass das Ziel der Verlagerung von Kapitalflüssen hin zu nachhaltigeren Tätigkeiten angestrebt wird.

Im Fokus steht somit die Durchführung des Wertpapiergeschäfts der Banken: Anlageberatung, Finanzprodukte, das Vergütungssystem – die Themen von WpHG-Compliance.

WpHG-Compliance ist vor diesem Hintergrund in der breiten Umsetzung dieser neuen Verordnungen zentral.

Die Beauftragten für WpHG-Compliance werden ihre Mandate konkret unterstützen und bei Vorliegen weiterer Informationen direkt den Handlungsbedarf aufzeigen. ▬

MaRisk-Compliance

Nachhaltigkeitstransparenz

Seit dem 10. März 2021 tritt stufenweise die Verordnung (EU) 2019/2088 „über nachhaltigkeitsbezogene Offenlegungspflichten im Finanzdienstleistungssektor" (Offenlegungsverordnung) in Kraft. Sie ist Teil des EU-Aktionsplans für ein nachhaltiges Finanzwesen, mit dem unter anderem die Ziele des Pariser Klimaabkommens erreicht werden sollen.

Die Offenlegungsverordnung ist mit 19 Seiten nicht besonders umfangreich. Doch in Kombination mit anderen Regulierungen wie der Verordnung (EU) 2020/852 Taxonomieverordnung und der kurzfristig verschobenen Veröffentlichung der technischen Regulierungsstandards (RTS) steht die gesamte Finanzdienstleistungsbranche vor großen Herausforderungen (siehe auch S. 4).

Finanzmarktteilnehmer und Finanzberater betroffen

In erster Linie verfolgt die Offenlegungsverordnung das Ziel, für mehr Transparenz im Finanzdienstleistungssektor zu sorgen. Konkrete Aussagen darüber, was der Regulator als ökologische oder soziale Merkmale definiert, sucht man in der Offenlegungsverordnung vergebens. Nichtsdestotrotz gilt dieses Regelwerk als programmatisch für den Umgang mit Nachhaltigkeit in der Finanzdienstleistungsbranche.

Finanzmarktteilnehmer und Finanzberater treffen umfassende Offenlegungspflichten zu Nachhaltigkeitsrisiken. Unter die Begriffe Finanzmarktteilnehmer und Finanzberater fallen explizit Kreditinstitute, die Anlageberatung oder Portfolioverwaltung anbieten, und Versicherungsvermittler, die Versicherungsanlageprodukte vermitteln. Als Erfüllungsgehilfen von Organismen für gemeinsame Anlagen in Wertpapieren (OGAW) und Verwaltungsgesellschaften für Alternative Investmentfonds, Kreditinstituten und Wertpapierfirmen sind auch vertraglich gebundene Vermittler und Wertpapiervermittler zumindest mittelbar von den Vorschriften des Regelwerks betroffen.

Grundsätzlich verlangt die Offenlegungsverordnung, dass Finanzmarktteilnehmer und Finanzberater, die unter die Verordnung fallen, z. B. gegenüber ihren Endkunden ihre Strategien zur Einbeziehung von Nachhaltigkeitsrisiken offenlegen müssen. Eine Ausnahme für die Anwendung der Regelungen der Offenlegungsverordnung besteht nur für sehr kleine Unternehmen, die weniger als drei Personen beschäftigen (Art. 17 Abs. 1 EU-Offenlegungsverordnung).

Mehr Transparenz

Folgende Offenlegungspflichten müssen Finanzmarktteilnehmer und Finanzberater seit dem 10. März 2021 zwingend beachten:

- Für Finanzmarktteilnehmer und Finanzberater besteht die Pflicht, auf ihrer Internetseite zu veröffentlichen, ob und wie sie Nachhaltigkeitsrisiken bei ihren Investitionsentscheidungsprozessen bzw. ihren Anlageberatungs- oder Versicherungsberatungstätigkeiten berücksichtigen. Ein Nachhaltigkeitsrisiko ist ein Ereignis in den Bereichen Umwelt, Soziales oder Unternehmensführung, dessen Eintreten wesentliche negative Auswirkungen auf den Wert einer Investition haben könnte (Art. 2 Nr. 22 EU-Offenlegungsverordnung).
- Für Finanzmarktteilnehmer und Finanzberater besteht ebenfalls die Pflicht, entsprechende Angaben zu nachteiligen Nachhaltigkeitsauswirkungen auf Ebene des Unternehmens (sog. „Principal adverse sustainability impacts statement") auf ihrer Internetseite zu veröffentlichen.
- Darüber hinaus besteht die Pflicht, die veröffentlichten Informationen auf der Internetseite stets auf dem aktuellen Stand zu halten und Änderungen klar zu erläutern (Art. 12 Abs. 1 Offenlegungsverordnung).
- Marketingmitteilungen müssen im Einklang mit den veröffentlichten Informationen stehen.
- Und nicht zuletzt besteht die Pflicht zur Angabe der Einbeziehung von Nachhaltigkeitsauswirkungen in die Vergütungspolitik (sog. „Principal adverse sustainability impacts statement").

>

Für Finanzmarktteilnehmer bestehen über die oben aufgeführten Pflichten hinaus noch weitere Offenlegungspflichten. Eine umfangreiche Tabelle mit den relevanten Offenlegungspflichten kann seit dem 15. Februar 2021 auf der Internetseite der BaFin eingesehen werden.

Durch die Offenlegungsverordnung wird sich für Primärbanken der Genossenschaftlichen FinanzGruppe aktuell (noch) nichts am eigentlichen Beratungsprozess für Finanzinstrumente i.S.d. WpHG ändern.

Jedoch werden im kommenden Jahr Nachhaltigkeitsaspekte verpflichtend im Beratungsprozess berücksichtigt werden müssen. Für die Primärinstitute bedeutet dies, dass Anlageberater ihre Kunden im Rahmen einer Anlageberatung vorab fragen müssen, ob sie bei ihrer Geldanlage sog. Nachhaltigkeitspräferenzen berücksichtigt wissen möchten. Diese Vorgabe sieht eine Änderungsverordnung der Delegierten Verordnung (EU) 2017/565 (MiFID II) vor, die im ersten Quartal 2021 veröffentlicht wurde.

Es ist davon auszugehen, dass sich durch die Offenlegungsverordnung im Zusammenspiel mit der EU-Taxonomieverordnung sowie durch die Änderungsverordnung zur MiFID II Auswirkungen auf das gesamte Institut, einschließlich der Compliance-Funktion, ergeben werden. ▬

AUTOREN UND ANSPRECHPARTNER

Axel Hofmeister
Beauftragter MaRisk-Compliance/Sustainable Finance Manager,
E-Mail: axel.hofmeister@dz-cp.de

Jörg Scharditzky
Beauftragter MaRisk-Compliance/Certified Expert in Sustainable Finance,
E-Mail: joerg.scharditzky@dz-cp.de

Geldwäsche- und Betrugsprävention

Stärken innerhalb des Verbundes nutzen

Die aktuellen Entwicklungen auf nationaler und europäischer Ebene in der Geldwäsche- und Betrugsprävention sowie zur Bekämpfung der Terrorismusfinanzierung führen in immer kürzeren Abständen dazu, dass das Geldwäschegesetz und das Kreditwesengesetz regelmäßig aktualisiert und angepasst werden. Diese Entwicklungen führen schlussendlich zu stetig steigendem Aufwand bei den Verpflichteten.

Umso wichtiger ist es, einen verlässlichen Partner an seiner Seite zu haben. Unser Ziel ist es, Sie bei der ordnungsgemäßen Erledigung der gesetzlichen und aufsichtsrechtlichen Themengebiete zu entlasten, Synergien als Mehrmandantendienstleister zu heben, Sie qualifiziert durch unsere Fachexpertise zu beraten und dabei im partnerschaftlichen Dialog mit Ihnen zu stehen.

Gesetz zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche

Am 18. März 2021 trat das Gesetz zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche in Kraft.

Kernstück des Gesetzes ist der Verzicht auf einen selektiven Vortatenkatalog. Künftig kann somit jede Straftat Vortat der Geldwäsche sein. Delikte wie Diebstahl, Unterschlagung, Raub, Betrug oder Untreue kamen bisher als Vortaten der Geldwäsche nur dann in Betracht, wenn diese gewerbsmäßig oder von einem Mitglied einer Bande, die sich zur fortgesetzten Begehung solcher Straftaten verbunden hat, begangen wurden. Dadurch wird eine deutliche Zunahme der Verdachtsmeldungen nach § 43 GwG an die Financial Intelligence Unit (FIU) erwartet.

Transparenzregister- und Finanzinformationsgesetz

Des Weiteren wurde am 10. Februar 2021 der Entwurf eines Gesetzes zur europäischen Vernetzung der Transparenzregister und zur Umsetzung der Richtlinie 2019/1153 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Nutzung von Finanzinformationen für die Bekämpfung von Geldwäsche, Terrorismusfinanzierung und sonstigen schweren Straftaten (Transparenz-Finanzinformationsgesetz) durch die Bundesregierung verabschiedet. Der Gesetzesentwurf sieht insbesondere folgende Neuregelungen des Transparenzregisters vor:

- Transparenzregister wird Vollregister
- Rechtsformabhängige Übergangsfristen für die Nachmeldung des wirtschaftlich Berechtigten
- Vernetzung der europäischen Transparenzregister
- Erweiterung der Eintragungsinhalte im Transparenzregister
- Erleichterung bei der Überprüfung der Angaben für den wirtschaftlich Berechtigten

Die sich daraus ergebenden Folgen für die Arbeitspraxis Ihres Hauses stellen wir Ihnen in einem Online-Seminar im zweiten Quartal 2021 detailliert vor.

Anforderungen mit Mehrmandantenansatz begegnen

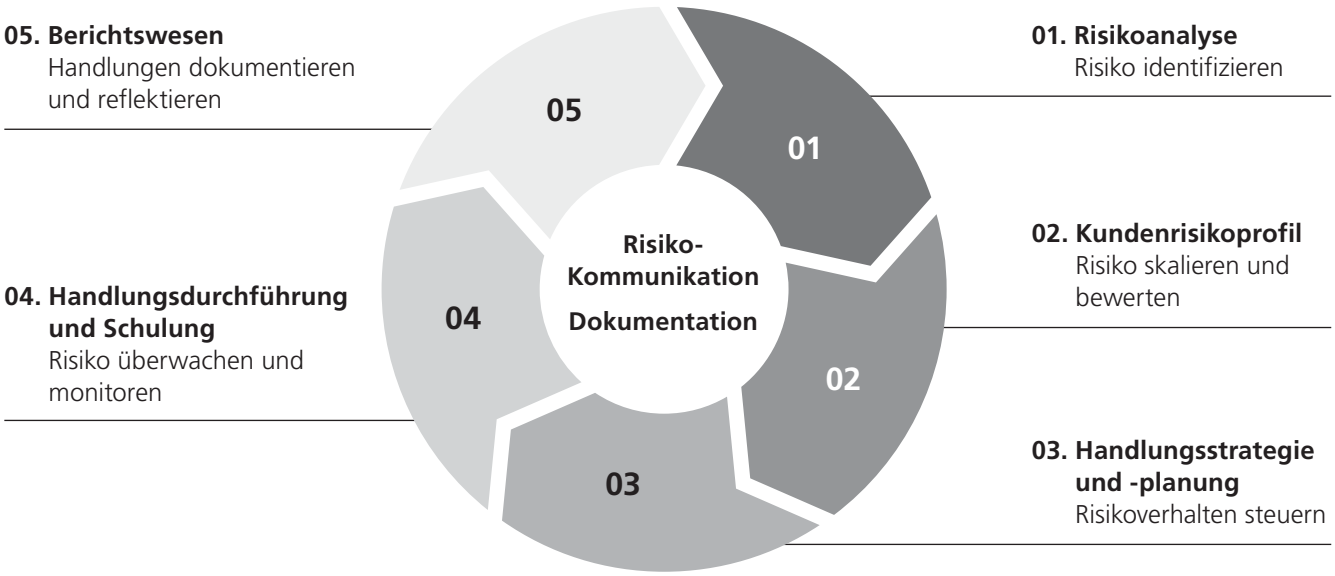
Auch vor dem Hintergrund der steigenden Anforderungen sehen wir die durch uns betreuten Institute gut aufgestellt.

Die DZ CompliancePartner hat für mehr als 400 Institute die Funktion und die Aufgaben des Geldwäschebeauftragten übernommen. Diese Banken profitieren einerseits von dem Mehrmandantenansatz, der eine Verteilung der Last ermöglicht. Andererseits ist die Vollauslagerung in der Geldwäsche- und Betrugsprävention in ein skalierbares und auch anpassungsfähiges Compliance Management System eingebunden und folgt dem dargestellten Risikomanagementprozess (vgl. Abbildung 1).

Mit der Übernahme der Funktion und der Aufgaben des Geldwäschebeauftragten bieten wir Ihnen somit ein integriertes Gesamtkonzept an. Das Institut wird den steigenden gesetzlichen und aufsichtsrechtlichen Anforderungen gerecht und gleichzeitig finanziell wie personell entlastet.

Institute, die das Modell der Vollauslagerung nicht in Anspruch nehmen möchten, können ebenfalls von dem System profitieren, beispielsweise in Form einer Teilauslagerung. Dabei ist eine Übernahme einzelner Tätigkeiten ebenso möglich wie die Übernahme der Trefferbearbeitung im Rahmen des >

ABB. 1 RISIKOMANAGEMENTPROZESS



EDV-Monitorings mittels Geno-SONAR.

Darüber hinaus bieten wir im Detail folgende Beratungsleistungen an:

- **Fachlich / konzeptionell**
  - Erstellung und Aktualisierung der Risikoanalysen und Arbeitsanweisungen
  - Prozessanpassungen aufgrund gesetzlicher oder aufsichtsrechtlicher Änderungen
  - Prozessoptimierung bei der Erfüllung der Sorgfaltspflichten
  - Überprüfung und Stärkung Ihres internen Kontrollsystems, z. B. durch individuelle Unterstützungen und Beratungen vor Ort in Form von zusätzlichen Kontrollen, Prozessanalysen oder Praxis-Workshops in enger Abstimmung mit den Erfordernissen Ihres Hauses
  - Beratung Ihrer Tochterunternehmen bei der Erfüllung aller Pflichten nach dem GwG
- **Technisch**
  - Adjustierung von Geno-SONAR und Überprüfung der vorgenommenen Einstellungen
  - Web-Based-Trainings zu den geldwäscherechtlichen Sorgfaltspflichten

Spezifische Unterstützungsangebote

Aufgrund der aktuellen Gesetzesänderungen bieten wir Ihnen folgende Unterstützungsleistungen an:

Im Hinblick auf die Umgestaltung des Transparenzregisters stellen wir Ihnen die Änderungen, deren Auswirkungen auf die Prozesse Ihres Hauses sowie unsere damit zusammenhängenden Unterstützungsleistungen in einem (in der Vollauslagerung kostenfreien) Online-Seminar vor. Über die im zweiten Quartal 2021 vorgesehenen Termine werden wir zeitnah informieren.

Die Nationale Risikoanalyse weist auf ein hohes Geldwäscherisiko im Bereich des Immobiliensektors hin. Auch in der am 31. August 2020 in Kraft getretenen Rechtsverordnung des Bundesministeriums der Finanzen werden Sachverhalte bei Immobilientransaktionen (Erwerbsvorgänge nach § 1 des Grunderwerbssteuergesetzes) aufgegriffen, die von Verpflichteten der rechtsberatenden Berufe an die FIU zu melden sind. Sachlich bestimmt diese Verordnung damit einzelne typisierte Sachverhalte bei Immobilientransaktionen, die aufgrund bestimmter Auffälligkeiten einen möglichen Zusammenhang zu Geldwäsche aufweisen, als meldepflichtig. Wird dieses typische Geldwäscherisiko durch hinzutretende Tatsachen entkräftet, greift eine Ausnahme von der Meldepflicht.

Sofern Sie selbst oder über Tochtergesellschaften das Immobilienmaklergeschäft betreiben, stehen wir Ihnen sehr gerne auch in diesem Kontext zur Erfüllung der geldwäscherelevanten Sorgfaltspflichten beratend zur Seite.

Fazit

Ob Vollauslagerung, Teilauslagerung oder Beratung – mit unseren Dienstleistungen bieten wir Ihnen eine breite Produktpalette im Bereich der Geldwäsche- und Betrugsprävention an. Gerade vor dem Hintergrund der nun zu erwartenden Mehrbelastung bewährt sich einmal mehr das gemeinsame Vorgehen innerhalb der Genossenschaftlichen FinanzGruppe. ▬

AUTOREN UND ANSPRECHPARTNER

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

Thorsten Schmeil
Leiter Geldwäsche- und Betrugsprävention,
E-Mail: thorsten.schmeil@dz-cp.de

Unsere Compliance-Grundsätze

1. Qualifizierte Spezialisten – für Kunden engagiert
2. Lösungs-Finder
3. Die Risikosituation und Komplexität des Kunden im Blick
4. Handlungen transparent und nachvollziehbar
5. Verantwortlichkeiten verabredet
6. Definierte Arbeitsanweisungen, umfangreiche Kontrollplanung
7. Dokumentation aller Kontrollhandlungen
8. Stringente interne Kontrollen
9. Verbindliche Kommunikation
10. Geprüfte Prozesse

▶ **IT-Audit**

Robotic Process Automation und Chatbot

Robotic Process Automation und Chatbots sind zwei interessante, technische Möglichkeiten, im Zuge der digitalen Transformation Prozesse neu zu gestalten. Erste Erfahrungen aus dem Beratungsbetrieb zeigen, wie wichtig es ist, diese neuen Prozesse sorgfältig vorzubereiten.

Die Herausforderung für die IT-Revision im Rahmen der digitalen Transformation nimmt inzwischen immer mehr Gestalt an – u. a. in Form von Bots.

Nach Wikipedia ist ein Bot (aus dem Englischen robot – Roboter – abgeleitet) ein Computerprogramm, das „weitgehend automatisch sich wiederholende Aufgaben abarbeitet, ohne dabei auf eine Interaktion mit einem menschlichen Benutzer angewiesen zu sein". Bots sind elektronische Servicekräfte, die untereinander kommunizieren (Bot-Netz oder Botnet) und in die Kategorien Good Bots und Bad Bots eingeteilt werden können.

Bad Bots werden z. B. als Spambots zum Sammeln von E-Mail-Adressen für Werbezwecke oder zum Ausspionieren von Software-Lücken bei Servern eingesetzt. Ein Good Bot ist beispielsweise ein von Suchmaschinen eingesetzter Webcrawler, der sich an definierte Standards, die sogenannten Robot Exclusion Standards, hält. Mit diesen Standards können Server- bzw. Webseiten-Betreiber das Verhalten von Webcrawlern oder Suchmaschinen-Bots auf ihren Webseiten beeinflussen.

Bots können automatisiert mit Menschen kommunizieren (Chatbots) oder interne Geschäftsprozesse optimiert ausführen (Robotic Process Automation). Doch was will man mit einem Bot in seinem Unternehmen erreichen? Bevor man einen Bot einsetzt, muss man genau wissen, wie man ihn nutzen und in welchem Bereich man ihn einsetzen will.

Robotic Process Automation (RPA)

Software-Roboter erledigen automatisiert betriebsinterne Routinen bzw. Prozesse. Mittels eines zuvor definierten Workflows (z. B. Process-Mining) werden ihnen Schritte und Anwendungen beigebracht, damit sie programmgesteuert menschliches Verhalten nachahmen können. Häufig wiederkehrende Aufgaben, die eindeutig identifizierbar sind, können somit äußerst effizient gelöst werden.

Chatbot

Unter einem Chatbot versteht man eine Software, die automatisiert mit Menschen über das Internet kommuniziert. Es findet eine Mensch-Maschine-Interaktion statt, bei der ein Chatbot versucht, durch Menschen gestellte Fragen auf persönliche Art und Weise zu beantworten, quasi ein digitaler Kundensupport. Er erledigt ganz bestimmte Aufgaben, wie z. B. das Beantworten von Fragen rund um das Bankgeschäft. Dabei ist sein Wissen allerdings beschränkt, denn der Chatbot analysiert die menschliche Sprache und Absicht des Kunden immer bezogen auf die vorgegebene Programmierung. Er erkennt diese Absichten und ruft die passende Antwort aus den ihm verfügbaren Ressourcen entsprechend ab.

Ein Bot benötigt somit Daten. Datenmenge und Datenqualität sind ausschlaggebend für die Performance. In der Regel liegen die Daten im Unternehmen bereits vor oder werden ggf. in der Pilotphase generiert. Unter Umständen ist es erforderlich, vorhandene Daten aufzubereiten. Dies wird umso wichtiger, je komplexer der Sachverhalt ist, den der Bot verarbeiten soll. Ein Chatbot beispielsweise benötigt eine Wissensdatenbank mit entsprechenden Schlüsselwörtern, auf die er reagieren kann.

Die DZ CompliancePartner GmbH konnte bereits einige Banken bei der Einführung eines Chatbots oder einer RPA-Lösung begleiten. Hierbei zeigte sich, dass es bei aller Euphorie für die beiden Technologien Herausforderungen gibt, die es zu meistern gilt.

Erfahrungsbericht

Anwendungsentwicklung

Grundsätzlich sind Chatbot und Robotic Process Automation als Eigenentwicklung zu betrachten bzw. bei Einschaltung von Dienstleistern als Fremdentwicklung. Herangezogen werden die

in der Bank bereits existierenden Regelungen zur Anwendungsentwicklung gemäß der „Interpretation der genossenschaftlichen FinanzGruppe zu den BAIT“ wie auch gemäß dem „SOIT der Fiducia & GAD – Teil 1“. Kernaspekte sind dabei:

- Risikoanalyse
- Tests und Freigaben
- Rechte und Rollen
- Releasemanagement (Updates)
- Datensicherung
- Pläne zur Rückabwicklung oder zum Ausfall

Prozessdefinition

Welche Prozesse sollen abgebildet werden? Hierfür liegen die Definitionen zum bisherigen Prozess oft bereits vor. In der Praxis zeigt sich, dass diese Vorlage regelmäßig granular ausgearbeitet werden muss, damit die Technik die Definitionen auch verstehen kann. Das heißt: Bisher übliche konkludente Handlungsstränge müssen aufgebrochen und präzise ausformuliert werden. Ergebnis ist dann ein umfassendes, fein aufgegliedertes Konzept.

Projekt Robotic Process Automation

Grundlage sind Server- und Client-Installationen. An bzw. auf dem Client arbeitet der Roboter mit seiner Anmeldung in agree®BAP und anderen notwendigen Systemen, auf die im Prozess zugegriffen werden muss. Die Aktionen des Roboters werden dabei in Dateien (Logs) gespeichert.

Auf dem Server werden die abzuarbeitenden Prozesse initial abgelegt und im weiteren Verlauf überwacht. Teilprozesse, Fortschritte wie auch Fehler des Bots werden dokumentiert. Hier findet das Prozess-Controlling statt.

Client und Server bilden ein geschlossenes System in der Infrastruktur der Bank und so auch bei der Robotic Process Automation.

Projekt Chatbot

Der Kunde startet meist über eine Website den dort integrierten Chatbot, manchmal auch implizit mit dem Aufruf der Site. Ähnlich wie beim Chat mit einem Mitarbeiter werden Fragen gestellt und Antworten gegeben. Allerdings „will“ der Chatbot möglichst in einem der definierten Prozesse münden. Falls noch kein passender Prozess definiert sein sollte, wird der Chatverlauf direkt an einen Mitarbeiter zur weiteren Bearbeitung übergeben.

Die Kunst oder vielmehr die Künstliche Intelligenz (KI) besteht also insbesondere in der Interpretation der Kundeneingaben und einer fortlaufenden Spezifizierung der hinterlegten Prozesse.

Die Pflege der Prozesse bzw. die eigentliche Programmierung des Chatbots erfolgt über ein Webinterface, oft softwareseitig an naher Stelle wie der Aufruf des Chatbots. Daher wird der Bot auch gern direkt bei dem Dienstleister der Wahl belassen, ohne eigene Hardware betreiben zu müssen.

Eine Betrachtung der Dienstleistung wie auch der genutzten (Cloud-)Dienstleister unter IT-Sicherheits- und Datenschutzgesichtspunkten ist dabei unabdingbar.

Datenschutz

Werden beim Einsatz von Robotic Process Automation oder Chatbots auch personenbezogene Daten verarbeitet, so sind die EU-DSGVO sowie das Bundesdatenschutzgesetz (BDSG) zu beachten. Die jeweilige Verarbeitung muss dann über einen der Erlaubnistatbestände des Art. 6 DSGVO legitimiert sein und die Betroffenen müssen in einer Datenschutzerklärung im Sinne des Art. 13 DSGVO über die Verarbeitung informiert werden. Weitere Probleme könnten auftreten, wenn das Verhalten von Mitarbeitern überwacht wird oder besonders sensitive personenbezogene Daten, wie z. B. Gesundheitsdaten, miteinbezogen werden. Bei der Einbindung von Dienstleistern muss in der Regel eine Auftragsverarbeitungsvereinbarung abgeschlossen werden, insbesondere bei Cloud-Lösungen.

Wird z. B. in einer Robotic Process Automation eine ausschließlich prozessautomatisierte Entscheidung getroffen, die unmittelbar eine rechtliche Wirkung gegenüber einem Menschen entfaltet, hat nach Art. 22 DSGVO eine betroffene Person das Recht, durch diese nicht beeinträchtigt zu werden. Das Verbot einer automatisierten Entscheidung kann somit einem RPA-Prozess entgegenstehen. Verboten sind danach Systeme, die automatisch Verträge ablehnen, wenn bestimmte Parameter nicht erfüllt sind.

Personenbezogene Daten sollten nur verarbeitet werden, soweit dies für den jeweiligen Verarbeitungszweck erforderlich ist und entsprechende technische Anforderungen die jeweils notwendige Datensicherheit erfüllen. Zudem sind Datenschutzhinweise zu Verarbeitungsvorgängen innerhalb des Bots sowie eine transparente Darlegung zur Löschung gespeicherter Chatverläufe anzupassen bzw. zu erstellen.

Zu beachten wird auch das zukünftige TTDSG (Telekommunikation-Telemedien-Datenschutzgesetz) und hier insbesondere der § 24 sein. Das Bundeskabinett hat den Gesetzentwurf zum TTDSG am 10. Februar 2021 beschlossen. Weitere >

Veränderungen sind bezüglich der noch ausstehenden ePrivacy-Verordnung zu erwarten.

Nachfolgende Artikel der DSGVO sind ggf. zu beachten:

- Einholung der Einwilligung des Kunden vor Beginn des Chats (Art. 6 Abs. 1 lit. a DSGVO)
- Datenschutzhinweise (Art. 5 DSGVO)
- Löschung (Art. 17 DSGVO)
- Verschlüsselung (Art. 32 DSGVO)
- Abschluss einer Auftragsverarbeitungsvereinbarung (Art. 28 DSGVO)
- Aufnahme des Verfahrens in das Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO)
- Durchführung einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO)
- Vertragliche Regelungen – SDK unter Berücksichtigung der Empfehlungen der DSK (Schrems-II-Urteil) bzw. von Art. 46 DSGVO

Gaia X

Nach dem US CLOUD Act können US-Behörden auch ohne richterlichen Beschluss auf Daten zugreifen, die bei US-Providern – mit Muttersitz in den USA und Tochtersitz in Europa – gespeichert sind. Nachdem der Europäische Gerichtshof im sogenannten „Schrems-II-Urteil" das Privacy-Shield-Abkommen als unwirksam erklärt hat, sind Alternativlösungen umso wichtiger.

Bereits im Herbst 2019 wurde das Projekt Gaia X begründet. Mit dem Projekt soll eine vertrauenswürdige Dateninfrastruktur in Europa geschaffen werden. Hierzu soll ein Rahmen für Anbieter von Rechenzentren, Cloud-Lösungen, High Performance Computing (HPC) etc. geschaffen werden, um verschiedene Services und Systeme in Form von Komponenten einbinden zu können. An dem Projekt sind Unternehmen, Organisationen und Verbände aus mehreren europäischen Ländern beteiligt.

AUTOREN UND ANSPRECHPARTNER

Thomas Grebe
Leiter IT-Audit,
E-Mail: thomas.grebe@dz-cp.de

Alexander Lorenz
Beauftragter IT-Audit,
E-Mail: alexander.lorenz@dz-cp.de

Ausblick

Der Einsatz von Robotic Process Automation oder Chatbots bietet Unternehmen ein hohes Potenzial, ihre Prozesse zu optimieren. Mitarbeiter können entlastet und Aufgaben schnell, zuverlässig und unter Einhaltung rechtlicher Voraussetzungen ausgeführt werden.

Um dies zu gewährleisten, müssen die einschlägigen rechtlichen Voraussetzungen vorab erkannt und in den Prozess-Workflow integriert werden. Mit Blick auf die Zukunft bleibt weiterhin zu beobachten, wie sich Robotic Process Automation oder Chatbots im Hinblick auf eine erweiterte KI-Implementierung und die damit einhergehenden rechtlichen Anforderungen weiterentwickeln.

Wir werden die Entwicklung im Auge behalten, die gewonnenen Erkenntnisse aus unseren Beratungsprojekten bewerten und zur Unterstützung unserer Kunden gezielt einsetzen. ▬

Datenschutz

Übersicht zur Rechtsprechung in 2020: Digitalisierung

Ob Pandemie, Brexit oder Digitalisierung – ab einem gewissen Punkt ist es unerlässlich, sich kritisch, aber auch konstruktiv mit dem Datenschutz zu beschäftigen. Nachfolgend eine Zusammenstellung der wichtigsten Rechtsprechungen in 2020 aus Sicht des Datenschutzbeauftragten.

Das Jahr 2020 stellte die genossenschaftlichen Banken vor gewaltige Herausforderungen. Die globale Verbreitung des Coronavirus SARS-CoV-2 (COVID-19) und die Maßnahmen zu dessen Eindämmung zwingen auch die Banken zur Aufgabe bisheriger Gewohnheiten und Verhaltensweisen. Die ungewöhnliche Situation verlangt ein Umdenken in allen Bereichen und die Bereitschaft, neue Wege zu gehen, sei es in der Organisation, Produktion oder im Vertrieb.

Der Pandemie selbst lässt sich nichts Positives abgewinnen. Die durch sie erzwungene Intensivierung des Innovationswettbewerbs bietet gleichwohl die Chance, die Digitalisierung zu fördern und neue Technologien zu erschließen. Hierbei ist freilich auf die gesetzlichen Anforderungen Rücksicht zu nehmen, deren Neuerungen im Nachfolgenden skizziert werden sollen.

Brexit und Datenschutz

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) hat klargestellt, dass Datenübermittlungen in das Vereinigte Königreich Großbritannien und Nordirland auf Basis des Brexit-Abkommens auch nach dem 1. Januar 2021 möglich sind.

Nach dem Entwurf des Brexit-Abkommens besteht zunächst eine Übergangsfrist von vier Monaten, in der Übermittlungen von personenbezogenen Daten in das Vereinigte Königreich wie bisher stattfinden dürfen. Hierbei müssen also weiter alle Anforderungen der DSGVO direkt erfüllt sein.

Die EU-Kommission soll in dieser Zeit tragfähige Adäquanzentscheidungen vorlegen, die insbesondere die aktuelle Rechtsprechung des Europäischen Gerichtshofs (EuGH) berücksichtigen. Die Frist kann nach dem Entwurf des Brexit-Abkommens höchstens um zwei Monate verlängert werden.

Ungültigkeit des „EU-US Privacy Shield"

Noch am 23. Oktober 2019 bestätigte die EU-Kommission den EU-US Privacy Shield als Basis für den Datenverkehr zwischen der EU und den USA. Das Vorgehen stieß auf heftige Kritik. Nicht einmal ein Jahr später, am 16. Juli 2020, hat der EuGH in der Schrems-II-Entscheidung das Abkommen für nichtig erklärt. Die Übermittlung von personenbezogenen Daten muss daher immer auf Rechtsgrundlagen der DSGVO gestützt werden.

Jedoch hat der EuGH auch festgestellt, dass internationale Übermittlungen personenbezogener Daten weiterhin auf die EU-Standardvertragsklauseln gestützt werden können. Unternehmen müssen hierbei sicherstellen, dass die EU-Standardvertragsklauseln ein angemessenes Schutzniveau herstellen. Dies müssen Unternehmen und öffentliche Stellen für jeden Einzelfall gesondert prüfen.

ePrivacy-Verordnung

Die Verhandlungen über die „Verordnung über Privatsphäre und elektronische Kommunikation" führten im Jahr 2019 zu keinem Erfolg. Die Zukunft der ePrivacy-Verordnung bleibt auch nach dem Jahr 2020 ungewiss. Zwar hat die EU unter der deutschen Ratspräsidentschaft einen neuen Anlauf gewagt und einen überarbeiteten Verordnungsvorschlag vorgestellt. Eine Einigung zwischen den Mitgliedstaaten konnte jedoch nicht erzielt werden.

Mit dem Wechsel der EU-Ratspräsidentschaft zum Jahresende liegt es nun an der portugiesischen EU-Ratspräsidentschaft, eine Einigung bezüglich der ePrivacy-Verordnung innerhalb des EU-Ministerrats herbeizuführen. Die Erfolgsaussichten sind weiter unklar. >

Patientendatenschutzgesetz (PDSG)

Auch wenn dieser Teil für die Banken keine Relevanz hat, soll auch das Thema Patientendatenschutzgesetz zumindest eine kurze Erwähnung finden. 2020 ist das Patientendatenschutzgesetz in Kraft getreten. Es dient dem Schutz sensibler Gesundheitsdaten und soll die Nutzung digitaler Angebote, wie das E-Rezept oder die elektronische Patientenakte, sicherstellen. Vor dem Hintergrund des Datenschutzrechts stehen bereits jetzt die Zugriffsrechte auf die elektronische Patientenakte in der Kritik, da der Patient dem behandelnden Arzt nur nach dem Alles-oder-nichts-Prinzip Zugang zu seiner elektronischen Patientenakte gewähren kann. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat bereits angekündigt, aufsichtsrechtliche Maßnahmen gegen die Krankenkassen, die die Regelungen des PDSG umsetzen, zu ergreifen.

IT-Sicherheitsgesetz 2.0

2020 hat zudem das Bundesinnenministerium einen neuen Referentenentwurf zum IT-Sicherheitsgesetz 2.0 vorgelegt. Der Entwurf sieht u. a. Änderungen des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik, des Telekommunikationsgesetzes, des Telemediengesetzes und der Außenwirtschaftsverordnung vor.

Gegenüber dem Referentenentwurf von 2019 wurde der Adressatenkreis des BSIG um „Unternehmen im besonderen öffentlichen Interesse“ erweitert.

Kritisch gesehen wird vor allem die Umsetzung des EU Cybersecurity Act und die damit verbundene Ausweitung der Befugnisse des BSI. So kann das BSI beispielsweise die Kommunikationstechnik des Bundes kontrollieren und Betreibern kritischer Infrastrukturen, wie Telekommunikationsnetzbetreibern, den Einsatz kritischer Komponenten untersagen.

Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG)

Das Bundesministerium für Wirtschaft und Energie arbeitete 2020 an dem Entwurf eines Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien sowie zur Änderung des Telekommunikationsgesetzes, des Telemediengesetzes und weiterer Gesetze. Am 10. Februar 2021 wurde der Gesetzentwurf zum TTDSG beschlossen.

AUTOR UND ANSPRECHPARTNER

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

Der Entwurf führt Datenschutzregelungen aus dem Telekommunikationsgesetz (TKG) und dem Telemediengesetz (TMG) zusammen.

Anlass des Entwurfs war auch die richtlinienkonforme Umsetzung der ePrivacy-Richtlinie sowie die jüngste Rechtsprechung des EuGH und des BGH, die eine Anpassung des § 15 TMG notwendig machten. Das Gesetzesvorhaben gewann vor allem nach dem Scheitern der ePrivacy-Verordnung an Bedeutung.

Aussichten

Auch das Jahr 2021 wird gerade im Bereich Datenschutz zahlreiche Neurungen für die genossenschaftlichen Banken bringen. Insbesondere die sich nun neu bildende Rechtsprechung wird zeigen, welche der aktuellen Maßnahmen einer Anpassung bedürfen und welche Lösungen bereits als rechtssicher bezeichnet werden können. ▬

Datenschutz

Bußgeldverfahren

Das Landgericht Bonn hat ein entscheidendes Urteil gegen den Telekommunikationsdienstleister 1&1 Telecom GmbH in der noch jungen Geschichte der Datenschutzgrundverordnung (DSGVO) gesprochen. Das Urteil stellt insbesondere die Frage nach einer angemessenen Bußgeldfestsetzung.

Im Dezember 2019 verhängte der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) ein Bußgeld in Höhe von 9,55 Millionen Euro gegen 1&1 wegen eines Verstoßes gegen die DSGVO. Daraufhin legte das Telekommunikationsunternehmen Einspruch gegen den Bußgeldbescheid ein. Schließlich bestätigte das LG Bonn den Datenschutzverstoß aufgrund unzureichender Sicherheitsmaßnahmen und folgte außerdem der Auffassung, dass das Unternehmen nach den Maßstäben der DSGVO dafür zu haften hat. Allerdings empfand das LG Bonn das ursprüngliche Bußgeld als unangemessen hoch und setzte es auf 900.000 Euro herab.

Das Urteil bildet einen Meilenstein in der Rechtsprechung zu den DSGVO-relevanten Bußgeldern. Einerseits wird deutlich, welche Maßstäbe die Gerichte an die erforderlichen Schutzmaßnahmen stellen. Andererseits wird ersichtlich, welche Maßgaben bei der Bemessung von Bußgeldern berücksichtigt werden.

Solch unmittelbare Haftung des Unternehmens stellt bis dato ein Novum im deutschen Sanktionsrecht dar. Nach § 41 des Bundesdatenschutzgesetzes (BDSG) gelten die Vorschriften des Gesetzes über Ordnungswidrigkeiten (OWiG) sinngemäß. Für Ordnungswidrigkeitentatbestände in Art. 83 Abs. 4 bis 6 DSGVO gelten wiederum die Grundsätze des supranationalen Kartellrechts. Dieses geht bei Verstößen gegen Art. 101 und 102 AEUV von einer unmittelbaren Verantwortlichkeit der Unternehmen aus.

Der zugrundeliegende Sachverhalt

2018 reichte ein Kunde des Telekommunikationsunternehmens Beschwerde ein. Seine ehemalige Lebensgefährtin gab sich gegenüber dem 1&1-Callcenter als dessen Ehefrau aus und konnte so die neue Telefonnummer erfragen. Mit bloßer Angabe des Namens und des Geburtsdatums des Kunden konnte sich die Anruferin als Berechtigte authentifizieren und personenbezogene Daten in Erfahrung bringen. Dem Kunden wurde daraufhin durch seine Ex-Lebensgefährtin in strafrechtlich relevanter Weise nachgestellt.

1&1 reagierte auf die Beschwerde unmittelbar mit der Einführung einer angepassten Authentifizierungsmethode – bestehend aus Kunden-/Vertrags- oder Auftragsnummer, Geburtsdatum bzw. E-Mail-Adresse und den letzten vier Ziffern der IBAN. Ende 2019 stellte 1&1 auf eine fünfstellige Service-PIN zur Authentifizierung um.

Der Bußgeldbescheid des BfDI

Als der Bundesdatenschutzbeauftragte (BfDI) von dem Vorfall Kenntnis erlangte, warf er 1&1 einen Verstoß gegen Art. 32 DSGVO vor. Die Abfrage von Name und Geburtsdatum zur Authentifizierung gewährleiste keinen ausreichenden Schutz der Kundendaten. Deshalb handele es sich in diesem Fall um einen schwerwiegenden Verstoß.

Diesen Datenschutzverstoß ahndete der BfDI mit einer Geldbuße in Höhe von 9,55 Millionen Euro. Bei der Bemessung des Bußgeldes sieht Art. 83 DSGVO Abs. 4 Geldbußen von bis zu 2 % des Jahresumsatzes des vorangegangenen Geschäftsjahrs vor. Im Falle von 1&1 wäre somit bei einem Umsatz von 3,63 Milliarden Euro im Jahr 2018 eine Geldbuße von bis zu 72,6 Millionen Euro möglich. Aufgrund des kooperativen Verhaltens von 1&1 blieb der BfDI im unteren Bereich des möglichen Bußgeldrahmens.

1&1 erhob Einspruch mit der Begründung, das Bußgeld sei unverhältnismäßig und verstoße gegen das Grundgesetz.

Die Entscheidung des Landgerichts Bonn

Im November 2020 erklärte das LG Bonn 1&1 für schuldig im Sinne einer Ordnungswidrigkeit nach Art. 83 Abs. 4a DSGVO. Der Bußgeldbescheid wurde somit als berechtigt eingestuft. Aber das Bußgeld ist nach Ansicht des Landgerichts unverhältnismäßig hoch bemessen. >

Schuldhafter Verstoß gegen Art. 32 DSGVO

Das LG Bonn bestätigte den Verstoß gegen Art. 32 Abs. 1 DSGVO, wonach die Datenverantwortlichen keine geeigneten technischen und organisatorischen Maßnahmen zum Schutz von personenbezogenen Daten ergriffen hatten.

Die Abfrage von Name und Geburtsdatum reichte sogar aus, wenn offensichtlich nicht der Vertragsinhaber, sondern eine dritte, möglicherweise nicht berechtigte Person in dessen Namen anrief. Besonders da sich Callcenter-MitarbeiterInnen und KundInnen in der Regel nicht persönlich kennen, muss eine sichere Authentifizierungsmethode zum Schutz der Kundendaten gewährleistet sein. Das Schutzniveau muss an die Eintrittswahrscheinlichkeit, die Schwere der Folgen und den Stand der Technik angepasst sein.

Es bestand somit ein erhebliches und reales Risiko für die Kunden, Opfer von Straftaten zu werden oder durch unberechtigten Datengebrauch geschädigt zu werden. Besonders die Daten Name und Geburtsdatum sind leicht von Dritten zu ermitteln. Daher eignen sich diese auch nicht zur Authentifizierung von Berechtigten und/oder Bevollmächtigten. Die Gefahr des Datenmissbrauchs ist somit deutlich erhöht und einfach möglich gewesen.

Mit geringem – personellem und finanziellem – Aufwand hätte, so das Gericht in seiner Urteilsbegründung, das Schutzniveau erhöht werden können. Schon die Abfrage von spezifischeren Daten hätte das Schutzniveau maßgeblich verbessert.

Das LG Bonn geht indes nicht davon aus, dass die Callcenter-Mitarbeiterin vorsätzlich gehandelt hat und sich über den Tatbestand bewusst war. Sie folgte dabei allen Vorschriften der damals gültigen Sicherheitsmaßnahmen. Ebenso ist zu berücksichtigen, dass die Callcenter-Mitarbeiterin keinen Zugriff auf besonders sensible oder schützenswerte Kundendaten hatte. Schlussendlich lag auch kein Massendiebstahl von Kundendaten vor und ein solcher sei auf diese Weise auch nicht möglich gewesen. Bis zu dem Zeitpunkt des Verstoßes war die Authentifizierungsstrategie des Callcenters nicht bemängelt worden. Zudem gibt es keine einheitlichen Richtlinien und Anforderungen an Authentifizierungsprozesse in Callcentern seitens des BfDI.

Nichtsdestotrotz ist der Datenverstoß vermeidbar gewesen. So ist es nötig, die Sicherheitsmaßnahmen der Datenverarbeitungsprozesse regelmäßig zu prüfen und an den Stand der Technik und etwaige Risiken anzupassen. Bei der Einführung der DSGVO hat die Rechtsabteilung des Unternehmens es versäumt, entsprechende Evaluierungen durchzuführen.

Eine Kernfrage war, ob eine Verbandshaftung in einem derartigen Fall überhaupt zulässig sei. § 41 BDSG verweist bei Bußgeldverfahren auf das Ordnungswidrigkeitengesetz (OWiG). Nach §§ 30 und 130 OWiG ist eine Verbandsgeldbuße nur dann möglich, wenn Betriebsinhaber, juristische Personen oder Personenvereinigungen eine Straftat oder Ordnungswidrigkeit ausüben. Das LG Bonn definiert den funktionalen Unternehmensbegriff des europäischen Kartellrechts nach Erwägungsgrund 150 DSGVO. Somit haftet das Unternehmen, woraus sich wiederum höhere Bußgelder ergeben.

Bemessung des Bußgeldes

Die Bemessung des Bußgeldes richtet sich nach Art. 83 DSGVO nach dem Umsatz des letzten abgeschlossenen Jahres vor Erlass des Bußgeldbescheides. Demnach bemisst sich das Bußgeld an dem Umsatz von 3,63 Milliarden Euro aus dem Kalenderjahr 2018, woraus sich eine zweiprozentige Obergrenze von 72,6 Millionen Euro ergibt. Diese Grenze gilt dabei lediglich als erste

AUTOR UND ANSPRECHPARTNER

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

In 2020

283 Bußgelder

mit einem Gesamtbetrag von ca. 48 Mio. Euro

Anstieg um ca. 50 Prozent gegenüber dem Vorjahr*

Orientierung, denn eine Geldbuße muss stets wirksam, verhältnismäßig und abschreckend sein.

Bei leichten Datenschutzverstößen umsatzstarker Unternehmen muss daher besonders auf die Verhältnismäßigkeit der Buße geachtet werden. Dementsprechend sind Zumessungskriterien zu berücksichtigen wie „Art, Schwere und Dauer des Verstoßes, die Zahl der von der Verarbeitung betroffenen Personen, das Ausmaß des Schadens, die Kategorie der betroffenen personenbezogenen Daten, das Bemühen des Unternehmens, den Schaden zu begrenzen, Art und Umfang der Kooperation mit den Datenschutzbehörden und der Grad der Verantwortlichkeit".

In dem konkreten Fall sind nach Ansicht des LG Bonn mildernde Umstände zu berücksichtigen.

- Es waren keine sensiblen Daten betroffen. Es hat nur einen Fall gegeben und es handelte sich um die erste Geldbuße gegen 1&1 wegen eines Datenschutzverstoßes.
- Der Datenschutzverstoß wurde nicht bewusst oder vorsätzlich begangen. 1&1 empfand den Authentifizierungsprozess als rechtlich unbedenklich, zumal es bezüglich der Authentifizierung im Callcenter keine Vorgaben des BfDI gab. Außerdem bestand dieses niedrige Schutzniveau, um den Kunden die Kontaktaufnahme zu erleichtern.
- Schließlich zeigte sich das Unternehmen äußerst kooperativ, erhöhte umgehend das Schutzniveau und stellte letztendlich auf eine Service-PIN um.
- Theoretisch waren 7,4 Millionen Kunden betroffen; relativ betrachtet bestand das Risiko allerdings nur für eine geringe Kundenzahl.

Infolge des öffentlichkeitswirksamen Verfahrens ist ein Reputationsverlust entstanden, der aufgrund der vergleichsweise geringfügigen Straftat unbegründet ist. In Anbetracht der mildernden Gesichtspunkte reduzierte das LG Bonn das Bußgeld schließlich auf 900.000 Euro.

Fazit

Das Urteil des LG Bonn gegen den Telekommunikationsdienstleister 1&1 zeigt einmal mehr auf, dass Datenschutzverstöße nicht ohne Folgen bleiben.

Der Bundesdatenschutzbeauftragte Ulrich Kelber stellt klar: „Datenschutz ist Grundrechtschutz. Die ausgesprochenen Geldbußen sind ein klares Zeichen, dass wir diesen Grundrechtschutz durchsetzen werden. Die europäische Datenschutzgrundverordnung (DSGVO) gibt uns die Möglichkeit, die unzureichende Sicherung von personenbezogenen Daten entscheidend zu ahnden. Wir wenden diese Befugnisse unter Berücksichtigung der gebotenen Angemessenheit an."

Angesichts der unmittelbaren Verbandshaftung von Unternehmen bei Datenschutzverstößen einzelner Mitarbeiterinnen und Mitarbeiter wird die Notwendigkeit deutlich, sämtliche Prozesse der Datenverarbeitung an ein solch erhöhtes Haftungsrisiko anzupassen. ▬

*Quelle: https://dsgvo-portal.de/news/rueckblick_dsgvo_bussgelder_datenpannen_2020.php

WpHG-Compliance

Sachkunde kompakt – von Praktikern für Praktiker

AUTOR UND ANSPRECHPARTNER

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

Die Sachkunde ist gemäß § 87 WpHG/WpHGMaAnzV kontinuierlich zu wahren, jährlich zu überprüfen und regelmäßig auf den neuesten Stand zu bringen (§ 1 Abs. 1 Satz 2 WpHGMaAnzV).

Die Sachkundeanforderungen bestehen in der Regel aus zwei Komponenten:

1. die fachliche und praktische Seite der jeweiligen Tätigkeit und
2. die rechtliche Seite der Tätigkeit.

Während in den Banken eine hohe Expertise bezüglich der fachlichen und praktischen Seite vorherrscht und damit diese Schulungen selbst durchgeführt werden können, bestehen zu den rechtlichen Komponenten der Sachkunde oft Unsicherheiten.

Damit Sie ein eigenes Schulungskonzept effizient und kostengünstig umsetzen können, übernehmen wir den rechtlichen Teil der Schulungen.

Wir haben unser Schulungsangebot erweitert und noch weiter ausdifferenziert. Für alle relevanten Zielgruppen haben wir Grundlagen- und Zielgruppenschulungen erstellt. Darüber hinaus bieten wir ab sofort auch Schulungen für einzelne Fachthemen an. Neu ist auch, dass fortan alle Schulungen sowohl in Präsenz als auch als dozentengeführtes Online-Seminar durchgeführt werden können. Besonders Online-Seminare bieten einen finanziellen und organisatorischen Vorteil für Sie und Ihre MitarbeiterInnen.

Unsere fachkompetenten und praxiserfahrenen DozentInnen vermitteln mit unseren Schulungen die für die Zielgruppen relevante rechtliche Sachkunde zusammen mit Tipps zum Umgang mit Herausforderungen im beruflichen Alltag.

Ihre Vorteile im Überblick:

- Fachmännische Expertise mit hohem Praxisbezug
- Nachhaltige Aus- und Weiterbildungsangebote
- Passende Bausteine zur Ergänzung Ihres eigenen Schulungskonzepts
- Freie Wahl der Schulungsform
- Transparente und kalkulierbare Preisstruktur

Grundlagenschulung	Zielgruppenschulung	Fachthemen
WpHG-Compliance Grundlagen 30 Min. ▶ Auszubildende ▶ Neueinstellung ▶ Stellenwechsel in Bereich WpHG ▶ Auffrischungsschulung **MAR-Marktmissbrauch** 30 Min. ▶ Jährliche Pflichtschulung für ausgewählten Mitarbeiterkreis	**Verantwortlichkeitsbereiche** ▶ Vertriebsmitarbeiter 1,0 Std. ▶ Vertriebsbeauftragte 1,5 Std. ▶ Anlageberater 3,5 Std. ▶ Product Governance 1,5 Std. ▶ Compliance-Funktion 2,5 Std. ▶ Beschwerdemanagement 1,0 Std.	**Spezialwissen** jew. 60 Min. ▶ Professionelle Kunden/ Geeignete Gegenparteien ▶ Vertriebsvorgaben/Soll-Ist-Analyse ▶ Telefonische Orderannahme/ Anlageberatung ▶ Zu- und Verwendungsverzeichnis ▶ Eigene Vermögensverwaltung
Verfügbar als WBT, Online-Seminar und als Präsenzschulung	Verfügbar als Online-Seminar und als Präsenzschulung	Verfügbar als Online-Seminar und als Präsenzschulung
Teilnehmerzahlen: Präsenzschulung: max. 25 Personen – Online-Seminar: mind. 3 Personen – WBT: Online-Schulung einzeln		

MaRisk-Novelle: Veröffentlichung steht unmittelbar bevor

AUTOR UND ANSPRECHPARTNER

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

Am 26. Oktober 2020 hat die BaFin den Entwurf zur Änderung der Mindestanforderungen an das Risikomanagement (MaRisk) konsultiert. Wesentliche Inhalte betreffen dabei insbesondere die Umsetzung der EBA-Leitlinien zu

- notleidenden und gestundeten Risikopositionen,
- Auslagerungen sowie
- IKT- und Sicherheitsrisiken.

Stellungnahmen konnten bis zum 4. Dezember 2020 eingereicht werden. Die BaFin hatte bereits angekündigt, die MaRisk-Novelle im ersten Quartal 2021 veröffentlichen zu wollen. Wir gehen aktuell jedoch davon aus, dass die Novelle voraussichtlich erst im zweiten Quartal 2021 veröffentlicht wird, um Anmerkungen aus der Sondersitzung des Fachgremiums MaRisk im Februar 2021 noch berücksichtigen zu können.

Zu geplanten Umsetzungsfristen gibt es bislang keine offiziellen Angaben. Es ist jedoch zu erwarten, dass analog der Vorgehensweise bei der letzten MaRisk-Novelle (2017) Änderungen, die lediglich klarstellender Natur sind, unmittelbar nach Veröffentlichung von den Instituten anzuwenden sind, wohingegen neue Anforderungen mit einer Umsetzungsfrist umzusetzen sein werden.

Selbstverständlich werden wir Sie über die Veröffentlichung und die darin enthaltenen Umsetzungsfristen in unserem MaRisk-Rechtsmonitoring informieren. Voraussichtlich werden Sie zu diesem Zeitpunkt als Abonnent unseres Rechtsmonitorings auch schon von dem technisch-systemischen Upgrade profitieren können: Durch eine automatisierte Workflow-Steuerung werden Sie Umsetzungsfristen – auch die der MaRisk – künftig noch besser im Blick behalten und steuern können. ▬

Interne Revision

Regelmäßig berichten wir an dieser Stelle über die Interne Revision der DZ CompliancePartner GmbH. Wir möchten Ihnen damit einen Überblick über die Qualität der unterschiedlichen Auslagerungsdienstleistungen geben und Sie in Ihrem Auslagerungscontrolling unterstützen. Die Internen Revisionen unserer Kunden können von daher auf eigene Prüfungshandlungen verzichten: 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 (3/2020, S. 19) wurde entsprechend der Jahresprüfungsplanung 2020 der Bericht zu den Prüffeldern „Informationssicherheit & Datenschutz“ sowie „IT & Projekte/IT-Sicherheit“ abgeschlossen und veröffentlicht. Damit wurde der Jahresprüfungsplan der Internen Revision vollumfänglich erfüllt.

Beide oben genannten Berichte wurden als dienstleistungsbezogene Berichte an unsere Kunden versandt.

Aus dem von der Geschäftsführung der DZ CompliancePartner GmbH genehmigten Jahresprüfungsplan für 2021 wurden bereits zwei Prüfungen abgeschlossen und die Berichte veröffentlicht. Hierbei handelt es sich um den Bericht „Kommunikation und Bildung“, der nur intern veröffentlicht wurde, und den Bericht „Hinweisgebersystem“, der als dienstleistungsbezogener Bericht Kunden mit der entsprechenden Auslagerung zur Verfügung gestellt wurde.

Der Quartalsbericht zum vierten Quartal 2020 und der Jahresbericht der Internen Revision wurden fristgerecht erstellt und ebenfalls unserer Mandantschaft zur Verfügung gestellt.

Darüber hinaus wurde turnusgemäß ein Follow-up-Quartalsbericht für das vierte Quartal 2020 erstellt und der Geschäftsführung der DZ CompliancePartner GmbH vorgelegt. In den Follow-up-Berichten wird die Abarbeitung der von internen und externen Prüfern getroffenen Maßnahmen/Empfehlungen dokumentiert. Offene Punkte werden durch die Interne Revision konsequent nachgehalten.

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

Die externe Prüfung der Geschäftsbereiche Geldwäsche- und Betrugsprävention, MaRisk-Compliance und WpHG-Compliance nach IDW PS 951 (Typ 2) wurde wiederum von der AWADO GmbH Wirtschaftsprüfungsgesellschaft Steuerberatungsgesellschaft vorgenommen. Erstmalig wurde auch der Geschäftsbereich Informationssicherheit & Datenschutz nach IDW PS 951 (Typ 2) geprüft. Für alle Bereiche wurde jeweils ein Testat ohne wesentliche Einschränkung erteilt. Die Endfassungen der Berichte zur externen Prüfung wurden bereits an die Kunden der jeweiligen Dienstleistung versandt.

Die externe Prüfung der Funktion Hinweisgebersystem nach IDW PS 331 erfolgte ebenfalls durch die AWADO GmbH Wirtschaftsprüfungsgesellschaft Steuerberatungsgesellschaft. Es wurde die Funktionsfähigkeit testiert und auch hier wurde der Prüfungsbericht bereits an die Kunden versandt.

Für die Dienstleistung „Notfall-Management“ haben wir erneut eine TÜV-Zertifizierung vom TÜV Saarland erhalten. Die Zertifizierung testiert jährlich – seit 2008 – die Konformität des Notfallkonzepts nach MaRisk AT 7.3. ▬

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

Wirtschaftliche Lage

Die DZ CompliancePartner konnte im Jahr 2020 trotz pandemiebedingter Schwankungen die selbst gesteckten Ziele erreichen, teilweise sogar leicht übertreffen. Das Jahresergebnis lag mit 1.699 T€ mit 11,9 % über Plan (1.518 T€). Die Umsatzerlöse lagen zum Jahresende mit 16.552 T€ (Plan: 16.012 T€) insgesamt 3,4 % über Plan. Die Personal- und Sachkosten zuzüglich der Abschreibungen wuchsen mit 14.832 T€ nur leicht zum Plan (Plan: 14.494 T€, +2,3 %).

Der Geschäftsbereich Geldwäsche- und Betrugsprävention weist einen Umsatzerlös von 9.529 T€ (Vorjahr: 8.359 T€) aus, die Bereiche Informationssicherheit & Datenschutz von 3.086 T€ (Vorjahr: 2.647 T€), WpHG-Compliance von 2.032 T€ (Vorjahr: 2.110 T€), IT-Revision von 1.023 T€ (Vorjahr: 953 T€) und MaRisk-Compliance von 683 T€ (Vorjahr: 611 T€). Weiterhin konnten sonstige Erlöse i.H.v. 199 T€ (Vorjahr: 60 T€), getragen insbesondere durch Beratungs- und Schulungsleistungen, erzielt werden.

Die Erlössteigerungen im Geschäftsbereich Geldwäsche- und Betrugsprävention beruhen im Wesentlichen auf der in 2020 erstmalig ganzjährigen Ergebniswirkung der Übernahme des Bereichs CMI im April 2019. Hingegen konnten die Erlössteigerungen im Bereich des Datenschutzes und der Informationssicherheit durch eine Ausweitung der Mitarbeiter- und Kundenbasis erzielt werden.

Der Personalaufwand ist auf 10.514 T€ gestiegen (Vorjahr: 8.907 T€). Durch die Eingliederung der Abteilung Insourcing Finanzkriminalität der DZ BANK zum 1. April 2019 realisierte sich in 2020 erstmalig das volle Jahr in den Personalkosten der ehemaligen CMI-Mitarbeiter. Das erzielte Wachstum und die regulativen Neuerungen in den Bereichen Informationssicherheit und Datenschutz erforderten eine Aufstockung der Personalressourcen in diesem Bereich, so dass diese Aufstockung einen wesentlichen weiteren Treiber der Personalkostensteigerung darstellt.

Die DZ CompliancePartner hat einen Beherrschungs- und Gewinnabführungsvertrag mit der DZ BANK geschlossen, der in 2020 erstmals wirksam wurde.

Die DZ CompliancePartner wird ihre Wettbewerbsposition mit Hilfe einer konsequenten Kundenorientierung und durchgehenden Prozessorientierung stärken und damit ihr Produktportfolio weiter an den speziellen Bedürfnissen ihrer Kunden ausrichten. In dem in 2020 aufgelegten Projekt „Agenda_2024“ hat die Gesellschaft diese Kundenorientierung festgeschrieben und wird sie weiter intensiv verfolgen. ▬

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