März 2018

Compliance & Finance

Die Zeitschrift für Compliance in der Finanzbranche

Inhalt

Aufmacher

Taylor Wessing

2

IT-Compliance und Cybersecurity halten die Finanzbranche auf Trab
Die zunehmende Digitalisierung bietet Chancen aber auch diverse Risiken für die Finanzbranche. In unserem Interview beschreibt Detlef Klett, mit welchen Bedrohungen Banken im Hinblick auf die Sicherheit ihrer IT-Systeme umgehen müssen und wie sie sich im Spannungsfeld zwischen Datenschutzgrundverordnung und Geldwäsche-Bekämpfung verhalten sollten.

News

cybrain/iStock/Thinkstock

4

BaFin konkretisiert Anforderungen an IT-Sicherheit
Im November 2017 hatte die BaFin die Bankaufsichtlichen Anforderungen an die IT (BAIT) veröffentlicht. Die BAIT seien nunmehr der zentrale Baustein der IT-Aufsicht für alle Kredit- und Finanzdienstleistungsinstitute in Deutschland, erläutert die BaFin.

Personalwechsel

Sebastian Hartrott wurde im Dezember 2017 in die Geschäftsführung der Hannover Leasing Investment GmbH berufen. Dort ist er unter anderem für die Bereiche Recht, Gesellschaftsverwaltung, Compliance, IT und Strukturierung verantwortlich. Hartrott kam bereits im Jahr 2015 zur Hannover Leasing-Gruppe, deren Neuaufstellung als Kapitalverwaltungsgesellschaft er zuvor als externer Berater rechtlich begleitet hatte.

Urs Krapf ist seit November 2017 neuer Leiter Compliance der Glarner Kantonalbank. Krapf war zuvor Compliance Officer und Datenschutzbeauftragter der Raiffeisen Gruppe, St. Gallen.

Frank Kilchenmann ist seit Oktober 2017 Mitglied der Direktion und Leiter Compliance, Geldwäsche und Datenschutz der SwissBanking – Schweizerischen Bankiervereinigung. Kilchenmann kommt von IWB Industrielle Werke Basel, wo er als Chief Compliance Officer tätig war.

Veranstaltungen

11.04.2018 | Frankfurt |
Praxisseminar zum neuen Datenschutzgesetz

18. - 20.04.2018 | Warschau | **TECC 2018 - Europäische Konferenz für Compliance Officer**

19.04.2018 | Frankfurt |
RdF-Workshop zum Frankfurter Kommentar

24.04.2018 | Düsseldorf |
Digitalisierung und Compliance

06.06.2018 | Frankfurt |
Deutsche Compliance Konferenz 2018

IT-Compliance und Cybersecurity halten die Finanzbranche auf Trab

Die zunehmende Digitalisierung bietet Chancen aber auch diverse Risiken für die Finanzbranche. In unserem Interview beschreibt Detlef Klett, mit welchen Bedrohungen Banken im Hinblick auf die Sicherheit ihrer IT-Systeme umgehen müssen und wie sie sich im Spannungsfeld zwischen Datenschutzgrundverordnung und Geldwäsche-Bekämpfung verhalten sollten.

Taylor Wessing

Detlef Klett, Fachanwalt für IT-Recht, ist Partner im Düsseldorfer Büro von Taylor Wessing. Er hat sich auf die rechtliche Beratung in den Bereichen Datenschutz, Cybersecurity und Digitalisierung spezialisiert. Zu seinen Mandanten zählen Unternehmen aus der Finanzbranche und der digitalen Wirtschaft ebenso wie die öffentliche Hand.

» Cybersecurity beschäftigt die Finanzbranche immer wieder aufs Neue. Ist eine Betrugsmasche erkannt, kommt schon die nächste. Was sind derzeit die größten Bedrohungen?
« Die größten Bedrohungen ergeben sich für die Finanzbranche derzeit durch Ransomware und andere Malware. Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf oder die Nutzung von Daten und Programmen verhindern oder einschränken und nur gegen eine Lösegeldzahlung wieder freigeben. Als prominentes Beispiel ist hier die Software WannaCry zu nennen, welche im Mai 2017 etliche IT-Systeme lahmlegte.

» Wie gelangt diese schädliche Software in die Systeme?
« Eingeschleust werden solche Programme regelmäßig über E-Mails oder im Rahmen eines angeblich benötigten Softwareupdates. Auch andere Malware (alle Arten von schädlichen Programmen) wird hauptsächlich über sogenannte Phishing-E-Mails auf die Computer von Bankmitarbeitern geschleust.

» Worin liegen die Gefahren der Malware?
« Diese Schadprogramme können zum Beispiel Kundendaten in den Datenbanken der Bank auslesen. Solche sensiblen Daten werden nach Erlangung verkauft oder es wird versucht, die Konten der Opfer des Datendiebstahls zu übernehmen. Auch das Social Engineering ist eine zunehmende Bedrohung für die Finanzbranche. Bei diesem wird mittels gezielter Einwirkungen auf Bankmitarbeiter versucht, Zahlungsvorgänge zu Gunsten der Täter zu autorisieren oder Zugang zu dem Mitarbeitercomputer zu erlangen. Letzteres erreichen die Täter oft, indem sie sich als Servicemitarbeiter renommierte Hersteller wie Microsoft ausgeben, welche ein IT-Problem beheben sollen.

» Wie problematisch sind aktuell sogenannte „Geisterkonten", die unter falschem Namen eröffnet werden, um damit Online-Betrügereien zu ermöglichen?
« Die Thematik der „Geisterkonten" besteht zwar schon seit längerem, ist aber auch aktuell noch als sehr problematisch einzustufen. Das Problem entsteht dadurch, dass eine Kontoeröffnung selbst mit einem schlecht gefälschten Ausweis in der Regel leicht gelingt. Oft erfolgt die Kontoeröffnung im Rahmen des Postident-Verfahrens, bei welchem der Betrüger zur Kontoeröffnung lediglich seinen gefälschten Personalausweis in einer beliebigen Postfiliale vorlegen muss. Nach der Kontoeröffnung kann der Täter nicht vorhandene Waren im Internet anbieten und diese per Vorkasse auf das „Geisterkonto" bezahlen lassen. Nach erfolgter Zahlung wird das Konto dann leer geräumt. Die Bank wird in der Regel auf das Konto erst aufmerksam, nachdem die Betrogenen sich beschweren, der Schaden also schon entstanden ist.

» Wie können sich die Banken davor schützen?
« Ein effektiver Schutz ist derzeit nur möglich, wenn die Identitätskontrollen sehr sorgfältig durchgeführt werden. Hierzu gehört auch eine Schulung der mit den Identitätskontrollen befassten Mitarbeiter, insbesondere in den Postfilialen. Eine weitere Schutzmöglichkeit kann in der Nutzung digitaler Identifizierungsprozesse bestehen – z.B. der sog. videobasierten Identitätskontrolle.

» Wie funktioniert das?
« Die Identitätskontrolle erfolgt mittels spezieller Softwareanwendungen. Dies hat nicht nur den Vorteil der Erhöhung der Sicherheit, sondern bietet für den Kunden zudem einen deutlich höheren Komfort. So kann er bei Nutzung dieses Verfahrens die Kontoeröffnung bequem von zuhause über seinen Computer durchführen. Dieses Verfahren wird deshalb bereits seit längerem von einigen Onlinebanken eingesetzt.

» Gerade um Geldwäscherisiken frühzeitig zu erkennen, sind Banken zur Erhebung vielfältiger Daten Ihrer Kunden angehalten. Gleichzeitig müssen Sie aber auch den Datenschutzanforderungen der DSGVO gerecht werden. Wie bewerten Sie dieses Spannungsfeld?
« Ab dem 25. Mai 2018 wird die EU-Datenschutzgrundverordnung (DSGVO) Anwendung finden. Damit gilt ab diesem Zeitpunkt in allen Ländern der EU ein relativ hohes Datenschutzniveau. Ziel der DSGVO ist ein umfassender Schutz personenbezogener Daten. Ende 2017 haben sich die notwendigen EU-Institutionen auf die 5. Novelle der Geldwäsche-Richtlinie geeinigt. Ziel der Novelle ist die Verbesserung der Bekämpfung der Terrorismusfinanzierung und die Stärkung der Transparenz von finanziellen Transaktionen. Das zwischen diesen beiden Regelungswerken bestehende Spannungsverhältnis ist evident.

» Wo genau liegen die Schwierigkeiten?
« Die heute schon bestehende Geldwäsche-Richtlinie fordert die Speicherung personenbezogener Daten über einen Zeitraum von mindestens 5 Jahren. Dies hat der nationale Gesetzgeber in § 8 Geldwäschegesetz (GwG) entsprechend umgesetzt. Die Novelle der Geldwäsche-Richtlinie ist deshalb auch unter Datenschützern umstritten. Teilweise wird aufgrund der umfassenden und langen Speicherpflichten ein Vergleich zur Vorratsdatenspeicherung vorgenommen und die Novelle jedenfalls insoweit für unvereinbar mit der Rechtsprechung des EuGH gehalten.

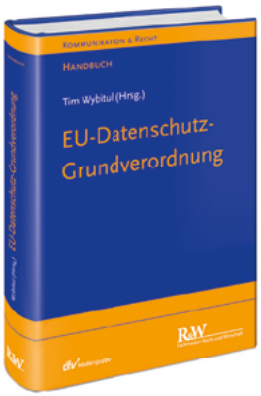
» Was heißt das für die Finanzbranche?
« Für die Banken bedeutet die Erfüllung der Anforderungen aus dem GwG zwar einen großen Aufwand, einen Konflikt mit dem Datenschutzrecht müssen sie allerdings nicht befürchten. Art. 6 Abs. 1 lit. c. DSGVO legt nämlich ausdrücklich fest, dass eine Datenverarbeitung auch dann rechtmäßig ist, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, welcher der Verantwortliche unterliegt. Die Erhebung und Speicherung der personenbezogenen Daten ist also durch das GwG gedeckt. *chk*

Mehr zu IT-Compliance, Cybersecurity und weiteren Compliance-Themen in Zusammenhang mit Digitalisierung erfahren Sie bei der Konferenz „**Digitalisierung & Compliance, Datenschutz 2.0 – Chance und Risiko**" am 24. April 2018 in Düsseldorf.

EU-DatenschutzgrundVO, BundesdatenschutzG (neu)

Auch als E-Book

Das neue Datenschutzrecht 2018



- Unkomplizierter Einstieg und Kurzkommentierung der für die Praxis wichtigsten Vorschriften des ab 2018 geltenden neuen europäischen Datenschutzrechts

Lieferbar!

2017, Handbuch, 833 Seiten, Geb.,
ISBN: 978-3-8005-1623-0

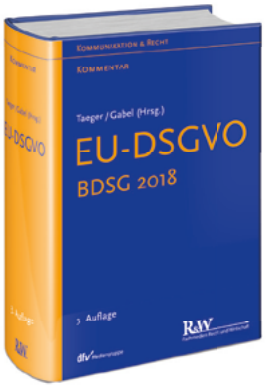
€ 119,-

- Schneller Überblick über die für die Praxis wichtigen Änderungen
- Erläuterung der notwendigen Prozesse zur Implementierung der DSGVO im Unternehmen

Lieferbar!

2016, 280 Seiten, Kt.,
ISBN: 978-3-8005-1634-6

€ 39,-



- Ausführliche, praxisnahe Kommentierung des neuen Datenschutzrechts
- Umfassende Darstellung der EU-DSGVO und des neuen BDSG 2018 mit Handlungsempfehlungen

In Vorbereitung für Mai 2018!

3. Auflage 2018, Kommentar,
ca. 1.800 Seiten, Geb.,
ISBN: 978-3-8005-1659-9

ca. € 298,-

- Kommentierung der Vorschriften des neuen BDSG für Unternehmen und private Stellen
- Der Autor war Sachverständiger im Bundestag

Lieferbar!

2018, Praxiskommentar,
372 Seiten, Kt.,
ISBN: 978-3-8005-1654-4

€ 89,-

Bestellung – per Fax **08581 754** oder auf **www.shop.ruw.de** oder als E-Book unter **e-books.ruw.de**

- ☐ **EU-Datenschutz-Grundverordnung** – Handbuch
- ☐ **EU-Datenschutz-Grundverordnung im Unternehmen**
- ☐ **EU-DSGVO – BDSG 2018** – Kommentar
- ☐ **BDSG** – Praxiskommentar für die Wirtschaft

Name | Firma | Kanzlei

E-Mail

Straße | Postfach

PLZ | Ort

Datum | Unterschrift

Sie haben die K&R noch nicht im Abo?

☐ **Ja,** ich möchte die **K&R** (11 Ausgaben) zum Jahresbezugspreis Inland € 475,- bzw. € 99,- für Studenten und Referendare inkl. aller Gebühren und MwSt. abonnieren. Im Abonnement ist ein Zugang zur Online-Datenbank enthalten. Bitte liefern Sie ab sofort.

Widerrufsrecht: Diese Bestellung kann innerhalb einer Frist von 14 Tagen gegenüber der Deutscher Fachverlag GmbH, Mainzer Landstraße 251, 60326 Frankfurt am Main, widerrufen werden. Zur Wahrung dieser Frist genügt das rechtzeitige Absenden des Widerrufs.

dfv Mediengruppe

Tel 08581 9605-14 | Fax 08581 754 | E-Mail info@suedost-service.de
www.shop.ruw.de | Deutscher Fachverlag GmbH | Frankfurt am Main

R&W Fachmedien Recht und Wirtschaft

BaFin konkretisiert Anforderungen an IT-Sicherheit

Im November 2017 hat die BaFin die Bankaufsichtlichen Anforderungen an die IT (**BAIT**) veröffentlicht. Sie sollen der zentrale Baustein der IT-Aufsicht für alle Kredit- und Finanzdienstleistungsinstitute sein.

cybrain/iStock/Thinkstock

IT-Sicherheit: Mit den BAIT stellt die BaFin vor allem auf Lücken ab, die ihr bei früheren IT-Prüfungen auffielen.

Defacto enthalten die BAIT keine neuen Anforderungen an die Institute beziehungsweise ihre IT-Dienstleister. Die BAIT interpretieren aber – ebenso wie die Mindestanforderungen an das Risikomanagement der Banken (MaRisk) – die gesetzlichen Anforderungen des § 25a Absatz 1 Satz 3 Nummern 4 und 5 Kreditwesengesetz (KWG). Sie konkretisieren, was die Aufsicht unter einer angemessenen technisch-organisatorischen Ausstattung der IT-Systeme versteht. Die BaFin stellt klar, dass die BAIT vor allem Themen adressieren, bei denen sie bei IT-Prüfungen der vergangenen Jahre wesentliche Mängel identifiziert hat.

Die prinzipienorientierten Anforderungen der BAIT seien daher nicht als vollständiger Anforderungskatalog anzusehen. Insoweit bleiben die Banken gemäß AT 7.2 MaRisk in der Pflicht, bei der Umsetzung der BAIT-Anforderungen auf gängige Standards abzustellen.

Die BaFin drängt besonders darauf, dass die Institute das Informationssicherheitsmanagement, den IT-Betrieb und die Anwendungsentwicklung angemessen mit Personal ausstatten. So solle das Risiko einer qualitativen oder quantitativen Unterausstattung dieser Bereiche frühzeitig erkannt und möglichst umgehend behoben werden können. Verantwortlich hierfür ist die Geschäftsleitung. Sie muss auch dafür sorgen, dass unvereinbare Tätigkeiten innerhalb der IT-Aufbau- und -Ablauforganisation vermieden werden.

Dreh- und Angelpunkt der BAIT ist damit auch ein funktionierendes Informationsrisikomanagement. Zentrales Element für die Einhaltung und Überwachung der Informationssicherheit innerhalb des Instituts und gegenüber Dritten ist daher der Informationssicherheitsbeauftragte. Seine Funktion muss organisatorisch und prozessual unabhängig ausgestaltet sein, um Interessenkonflikte zu vermeiden.

Die BaFin dürfte schon bald Anpassungen und weitere Konkretisierungen der BAIT vornehmen. So prüft die Aufsicht derzeit, ob etwa die wesentlichen Elemente der Cybersicherheit, die die G-7-Staaten bereits im Oktober 2016 veröffentlichten, im Regelwerk umgesetzt werden können.

In Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) will die BaFin außerdem ein spezielles Modul für Betreiber Kritischer Infrastrukturen im Sinne des § 2 Absatz 10 BSI-Gesetz in die BAIT aufnehmen. Die Ergänzung der BAIT um das Thema IT-Notfallmanagement inklusive Test- und Wiederherstellungsverfahren sei ebenfalls in Planung. *chk*

IT-Risiko

Unter dem Begriff IT-Risiko versteht die BaFin alle Risiken für die Vermögens- und Ertragslage der Institute, die aufgrund von Mängeln entstehen, die folgende Bereiche betreffen:

- das IT-Management beziehungsweise die IT-Steuerung,
- die Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität der Daten,
- das interne Kontrollsystem der IT-Organisation,
- die IT-Strategie, -Leitlinien und -Aspekte der Geschäftsordnung
- den Einsatz von Informationstechnologie

Kritik an Krypto-Währung

„Neuartige Technologie ist nicht gleichbedeutend mit besserer Technologie oder besserer Wirtschaftlichkeit", sagte Agustín Carstens, Generaldirektor der Bank für Internationalen Zahlungsausgleich (BIZ). Mit dieser Feststellung während eines Vortrags, den Carstens im Februar in Frankfurt hielt, zielte er auf die Ausbreitung von Krypto-Währungen – sogenannten Bitcoins.

Carstens sieht die neuartige Währung kritisch und appellierte an die Behörden, Verbraucher und Investoren vor ihr zu schützen. Damit das Geld seinen Wert behalte, bräuchten wir Institutionen, die das Vertrauen der Öffentlichkeit genießen: „Zentralbanken sind hier der Schlüssel", zeigte sich Carstens überzeugt. Private „digitale Wertmarken", die sich als Währungen ausgeben, dürften dieses Vertrauen nicht untergraben.

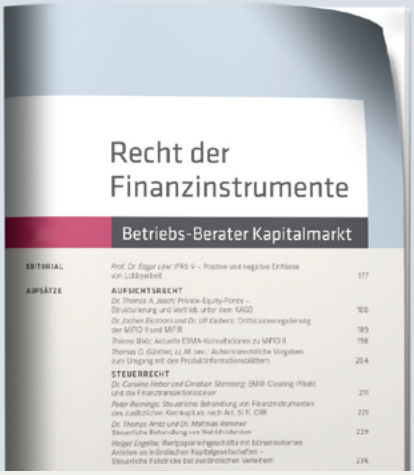
www.bis.org

Agustín Carstens, Generaldirektor der BIZ: Krypto-Währungen sind ihm ein Dorn im Auge.

Carstens sieht vor allem auch die Gefahr, dass Krypto-Währungen zur Verdeckung illegaler Geschäfte genutzt werden und die Finanzstabilität gefährden: „Auch wenn Bitcoin vielleicht ursprünglich als alternatives Zahlungssystem ohne staatliche Beteiligung gedacht war, ist es doch zu einer Kombination aus einer Blase, einer Betrugsmasche und einer Umweltkatastrophe geworden." Große Preisschwankungen, hohe Transaktionskosten und ein Mangel an Verbraucher- und Anlegerschutz machten Kryptowährungen unsicher und ungeeignet, um die Rolle des Geldes zu erfüllen. *chk*

IMPRESSUM
Verlag
Deutscher Fachverlag GmbH, Mainzer Landstraße 251,
60326 Frankfurt am Main
Registergericht AG Frankfurt am Main HRB 8501
USt-IdNr. DE 114139662

Geschäftsführung: Angela Wisken (Sprecherin), Peter Esser, Markus Gotta, Peter Kley, Holger Knapp, Sönke Reimers
Aufsichtsrat: Klaus Kottmeier, Andreas Lorch, Catrin Lorch, Peter Ruß
Redaktion: Christina Kahlen-Pappas (verantwortlich),
Telefon: 069 7595-1153, E-Mail: christina.kahlen-pappas@dfv.de
Verlagsleitung: RA Torsten Kutschke,
Telefon: 069 7595-1151, E-Mail: torsten.kutschke@dfv.de
Anzeigen: Lena Moneck,Telefon: 069 7595-2713, E-Mail: lena.moneck@dfv.de
Fachbeirat der Online-Zeitschrift Compliance & Finance:
Joern-Ulrich Fink, Compliance Regulatory Management Germany, Deutsche Bank AG; James H. Freis, Jr., Chief Compliance Officer, Deutsche Börse AG; Corina Käsler, Head of Regulatory Strategy, UniCredit Bank AG; Stephan Niermann; Hartmut T. Renz, Group Chief Compliance Officer, Landesbank Baden-Württemberg; Eric S. Soong, Group Head Compliance & Corporate Security, Schaeffler Technologies AG & Co. KG
Jahresabonnement: kostenlos
Erscheinungsweise: monatlich (10 Ausgaben pro Jahr)
Layout: Uta Struhalla-Kautz, SK-Grafik



RdF-Workshop zum Frankfurter Kommentar

Aktuelle Fragen des Kapitalanlagerechts

19. April 2018

Frankfurt a. M.

Spannungsfelder zwischen KAGB und MiFID II bei Fondsverwaltung und -vertrieb
Jochen Kindermann, RA/FABKR, Partner, Simmons & Simmons LLP, Frankfurt a. M.

Problempunkte beim Kapitalanlagerundschreiben
Dr. Jens Steinmüller, LL.M., RA, Partner, Pöllath + Partners, Berlin

Dividendenausgleichszahlungen nach dem InvStG 2018
Dr. Marcus Helios, RA/StB, Partner, EY WPG, Düsseldorf/Frankfurt a. M.

Bilanzierung strukturierter Produkte nach IFRS, HGB und Steuerrecht
Prof. Dr. Edgar Löw, Frankfurt School of Finance and Management, Frankfurt a. M., und
Dr. Martin Haisch, RA, Partner, Noerr LLP, Frankfurt a. M.

Genussrechtsbesteuerung im Umbruch aus Sicht der Praxis
Götz Reinhardt, Leiter Steuern, Deutsche Apotheker- und Ärztebank eG, Düsseldorf, und

aus Sicht der Verwaltung
Dr. Alexander Mann, Hessische Finanzverwaltung, Wiesbaden

Firma

Name | Vorname*

Position | Abteilung

Straße*

PLZ | Ort*

Telefon (für Rückfragen)*

Mobil

E-Mail (zur Bestätigung)*

Datum | verbindliche Unterschrift*

Anmeldung

Ja, ich nehme am RdF-Workshop am 19. April 2018 teil.

☐ Ich bin Abonnent der RdF. Ich zahle € 299,–
Meine Abonnement-Nr:

☐ Ich zahle € 399,–

Infos

Veranstaltungszeit: 16.00 – 20.00 Uhr
Veranstaltungsort: Frankfurt am Main
Anmeldung:
E-Mail sonja.poertner@dfv.de
Tel 069 7595-2712
Fax 069 7595-1150

oder unter **http://veranstaltungen.ruw.de**

*Pflichtfelder

dfv Mediengruppe