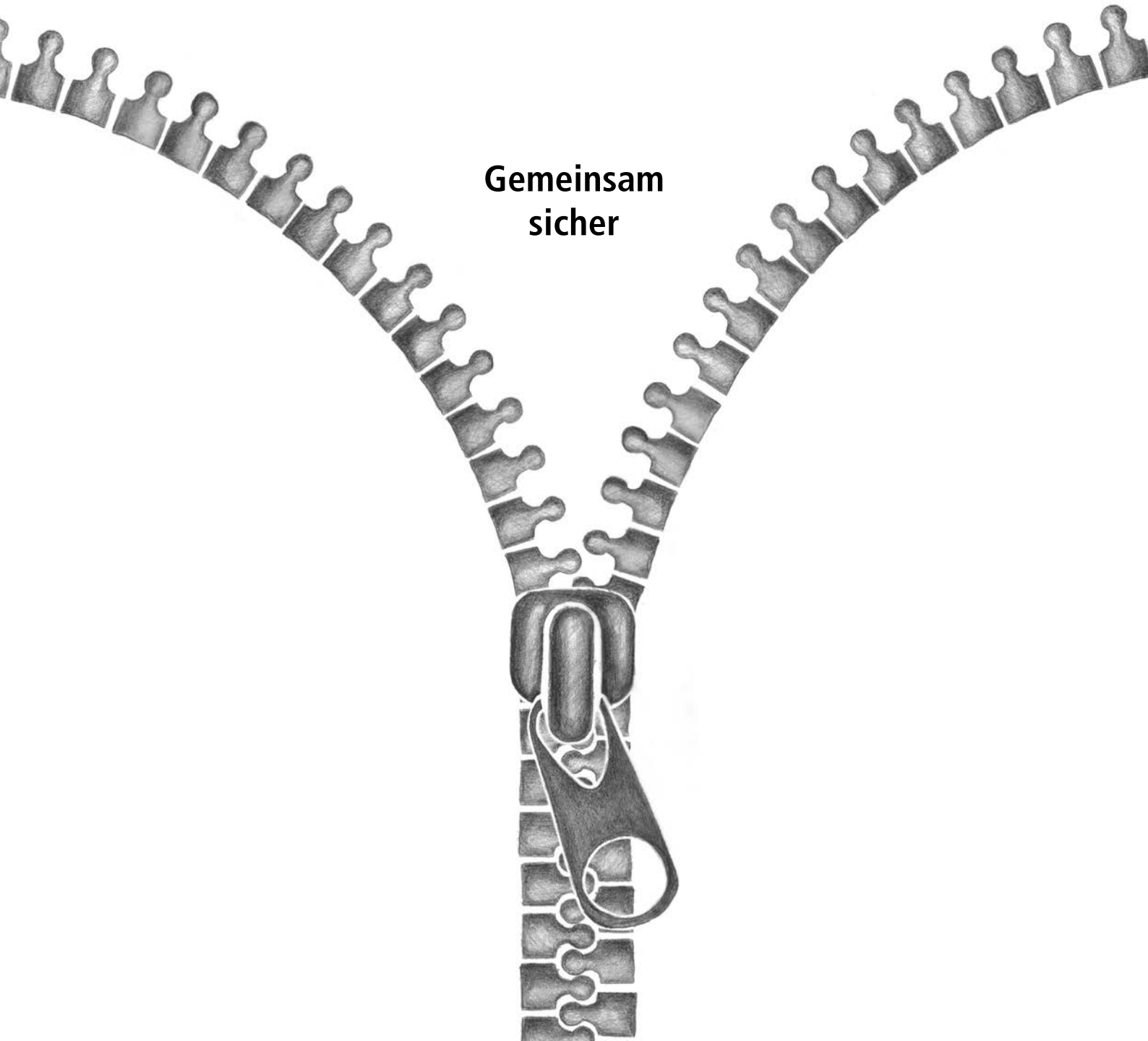
Ausgabe 1 / 2018

GenoTec GmbH

# Point of Compliance

Das Risikomanagement-Magazin
für unsere Kunden und Geschäftspartner





## Gemeinsam sicher

# Termine

| Was | Wann | Wo | Wer |
|---|---|---|---|
| **Fachtagung Datenschutz und Datensicherheit 2018 (GenoAkademie)** | **06. – 07.09.2018** | Rhein-Main-Gebiet | u. a. Thomas Grebe, Leiter IT-Sicherheit & Datenschutz |
| | **13. – 14.09.2018** | Großraum Hannover | |
| | **20. – 21.09.2018** | Großraum Berlin | |
| | **27. – 28.09.2018** | Großraum Bremen | |
| | **11. – 12.10.2018** | Großraum Leipzig | |
| | **29. – 30.10.2018** | Großraum Kassel | |
| | **08. – 09.11.2018** | Genossenschaftsakademie Rendsburg | |

**Weitere Informationen unter https://www.geno-tec.de/termine**


## IMPRESSUM

**Point of Compliance**
Das Risikomanagement-Magazin für unsere Kunden und Geschäftspartner, Ausgabe 18, 1/2018
**ISSN:** 2194-9514
**Herausgeber:** GenoTec GmbH, Wilhelm-Haas-Platz, 63263 Neu-Isenburg, Telefon 069 6978-3324, Telefax 069 6978-3322, www.geno-tec.de
Handelsregister HRB 11105, Amtsgericht Offenbach, USt.-IdNr.: DE201150917
Geschäftsführung: Jens Saenger (Sprecher), Andreas Marbeiter
**Verantwortlich i. S. d. P. :**
Jens Saenger

**Redaktion:** Gabriele Seifert, Leitung (red.)
**Redaktionsanschrift:** GenoTec GmbH, Redaktion Point of Compliance, Wilhelm-Haas-Platz, 63263 Neu-Isenburg, Telefon 069 6978-3188, Telefax 069 6978-3322, E-Mail: poc@geno-tec.de
**Weitere Autoren dieser Ausgabe:**
Florian Fuhrig, Dr. Indranil Ganguli, Thomas Grebe, Martin Hierlemann, Marc Linnebach, Michael Maier, Jens Saenger, RA Jörg Scharditzky, Lars Schinnerling, Sandra Sitter, Dominik Tiburtius, Peter Uherr
**Bildnachweise:** GenoTec GmbH, ©istockphoto

**Gestaltung und Titelillustration:**
EGENOLF DESIGN, Wiesbaden
studio@egenolf-design.de
**Druck:** odd GmbH & Co. KG · Print und Medien
www.odd.de



**Redaktionsschluss:** 9. März 2018
**Auflage:** 2.600 Exemplare
Die aktuellen Mediadaten finden Sie im Internet unter www.geno-tec.de/poc

**Jens Saenger**
Sprecher der Geschäftsführung

Zum 200. Geburtstag von Friedrich Wilhelm Raiffeisen hat das Prinzip „Was einer allein nicht schafft, das schaffen viele" nicht an Kraft verloren. Unverändert bietet es Chancen, die es sonst nicht gäbe. Gleichzeitig ist das Prinzip der Garant für die Eigenständigkeit jeder einzelnen Genossenschaftsbank vor Ort und, wie Uwe Fröhlich es ausdrückt, der „Resilienz" der Gruppe insgesamt.

Heute stehen die Volksbanken Raiffeisenbanken vor vielfältigen Herausforderungen am Markt, sei es die Digitalisierung, die Zinspolitik oder seien es die sich ändernden Kundenbedürfnisse. Umso wichtiger ist es, marktferne Themen effizient zu steuern.

Effizienz in der Regulatorik heißt, die Anforderungen unter Wahrung der Wirtschaftlichkeit umzusetzen. Der Königsweg ist eine zentrale Lösung für die gesamte Gruppe nach dem Motto: **eine Aufgabe, ein starker Partner.**

Ein zentrales, banken- und optimalerweise auch themenübergreifendes Beauftragtenwesen stärkt die Position der Primärbank, weil

– es die Basis für eine systematische Vernetzung, Prozessautomatisierung und auch für Big Data schafft und das Beauftragtenwesen damit **einfacher,**
– es über Lernkurveneffekte das Beauftragtenwesen **sicherer** und
– es über Synergien das Beauftragtenwesen **günstiger** macht.

Nur der gemeinsame Antritt hat die Kraft, die einzelne Genossenschaftsbank signifikant im marktfernen Bereich zu entlasten und sie gegenüber künftigen regulatorischen Anforderungen zu wappnen.

Gemeinsam sicher – in diesem Sinne wünsche ich Ihnen eine anregende Lektüre.

Ihr Jens Saenger

MaRisk

# MaRisk 6.0 – ein erster Erfahrungsbericht

Die Umsetzung der neuen MaRisk setzt insbesondere kleinere Institute unter Druck. Es fehlt häufig die Zeit, um sich im notwendigen Umfang mit dem Thema auseinanderzusetzen. Oft mangelt es aber auch an Vergleichen bzw. dem Austausch mit anderen Häusern.

Die vergangenen Monate bescherten den Banken erheblichen Umsetzungsaufwand. Von

- PSD II über
- MiFID II,
- AnaCredit,
- EU-DSGVO, BAIT,
- EU-Geldwäscherichtlinie

bis hin zur am 27. Oktober 2017 veröffentlichten

- **fünften MaRisk-Novelle.**

Quasi das gesamte Beauftragtenwesen erfährt eine Neuregelung – mit massiven Auswirkungen auf sämtliche Bereiche der Banken. An eine „Verschnaufpause" ist derzeit jedoch leider nicht zu denken. Wir möchten Ihnen daher bezüglich der Umsetzung der MaRisk-Novelle einen ersten Erfahrungsbericht aus der Betreuung zahlreicher Genossenschafts- und Privatbanken geben.

Nach einer öffentlichen Konsultationsphase zu Beginn des Jahres 2016 wurden von unterschiedlichen Anbietern sehr zeitnah die ersten Seminare zur MaRisk-Novelle angeboten. In Vorbereitung auf die zeitnah vermutete Finalisierung der Novelle wurden Seminare gebucht und umfangreiche Unterlagen studiert. Doch dann wurde es ziemlich still um die neuen MaRisk. Als diese am 27. Oktober 2017 nunmehr finalisiert veröffentlicht wurden, waren die offensichtlichen Änderungen allen hinreichend bekannt. Gegenüber der Konsultationsfassung waren zwar einige Anpassungen aufgenommen worden, um den berechtigten Interessen der kleineren Institute besser gerecht zu werden sowie die Zielrichtung der Aufsicht besser zum Ausdruck zu bringen. Größere Überraschungen blieben allerdings aus.

## Umsetzungsfristen

Bezüglich der Umsetzungsfristen unterscheidet die BaFin zwischen Regelungen mit klarstellendem Charakter und neuen Regelungen. Regelungen mit klarstellendem Charakter waren sofort nach der Veröffentlichung der MaRisk-Novelle umzusetzen, neue Regelungen sind bis zum 31. Oktober 2018 umzusetzen.

Jedoch bereits bei der Einstufung als „neue Regelung" bzw. „Regelung mit klarstellendem Charakter" beginnen die Schwierigkeiten. Die Aufsicht hat keine Aussage getroffen, welche Regelungen „neu" sind und welche „lediglich klarstellender Natur" sind. Hier sind die Verbände eingesprungen und haben zur Unterstützung entsprechende Übersichten veröffentlicht. Auch anderweitig wurden derartige Übersichten veröffentlicht. Vergleicht man diese jedoch untereinander, lassen sich schnell diverse Abweichungen erkennen.

Dieser Umstand stellt die Banken vor ein erhebliches Problem: Wenn bereits bei der Einstufung als „neue" oder „klarstellende" Regelung Uneinigkeit herrscht, wie soll dann eine aufsichtskonforme Umsetzung der MaRisk-Novelle erfolgen?

AUTOREN UND ANSPRECHPARTNER

**Michael Maier**
MaRisk-Compliance,
E-Mail: michael.maier@geno-tec.de

**Peter Uherr**
Leiter MaRisk-Compliance,
E-Mail: peter.uherr@geno-tec.de

## Umsetzungsstände

Doch nicht nur die einzelnen Fachbereiche stehen bei der Umsetzung vor dieser Problemstellung. Im Mittelpunkt steht insbesondere auch die MaRisk-Compliance-Funktion. Diese hat gemäß AT 4.4.2 Tz. 1 MaRisk auf die Implementierung wirksamer Verfahren zur Einhaltung der für das Institut wesentlichen Regelungen und Vorgaben sowie entsprechender Kontrollen hinzuwirken. Darüber hinaus hat sie die Geschäftsleitung hinsichtlich der Einhaltung dieser rechtlichen Regelungen und Vorgaben zu unterstützen und zu beraten.

Erfahrungsgemäß tut sich ein nicht unerheblicher Teil der Banken etwas schwer, die Vorgaben aufsichtskonform umzusetzen. Zwar erfahren sie durch die jeweiligen Verbände Unterstützung in Form von Umsetzungsleitfaden usw. Jedoch fehlt häufig die Zeit, um sich ausreichend mit dem Thema, der Umsetzung und insbesondere mit den Problemstellungen auseinanderzusetzen. Darüber hinaus fehlt einer einzelnen Bank vor Ort häufig auch die Vergleichsmöglichkeit bzw. der Austausch mit anderen Instituten.

Als Mehrmandantendienstleister mit langjähriger Erfahrung sind wir daher ein kompetenter Ansprechpartner für unsere Mandanten. Im Rahmen unserer Beauftragtenfunktion kommen wir mit zahlreichen (zum Teil) unterschiedlichen Herausforderungen und Problemstellungen der einzelnen Genossenschafts- und Privatbanken in Berührung und tragen zu der Herbeiführung von bankindividuellen Lösungsansätzen bei.

## Fazit

Es lässt sich feststellen, dass sich die etwas größeren Institute überwiegend bereits mitten in der Umsetzung befinden. Kleinere Institute haben dagegen zum Teil mit der Umsetzung noch nicht begonnen, obwohl die Klarstellungen schon seit dem 27. Oktober 2017 umgesetzt sein sollten. Die Verantwortung für die zeitgerechte und aufsichtskonforme Umsetzung der MaRisk-Novelle trägt dabei die Geschäftsleitung. Jedoch ist insbesondere der Compliance-Beauftragte für die Planung und Vorbereitung der Umsetzung in koordinierender Weise zuständig.

Gerne **beraten** wir Sie bei der **Optimierung** der Umsetzung, um Sie vor aufsichtsrechtlichen Konsequenzen zu **schützen,**

- als Berater,
- als Beauftragter oder
- durch unsere wertvollen Hinweise im rechtlichen Monitoring.

**MaRisk**

# Auslagerungsmanagement kompakt

Auslagerungsmanagement ist nicht trivial. Aber sie macht Sinn, hilft sie doch, die zunehmende Vernetzung – auch innerhalb der Genossenschaftlichen FinanzGruppe – ins rechte Lot zu bringen. Entscheidend ist ein flexibler, übersichtlicher und sicherer Prozess, der die Zusammenarbeit im Haus revisionssicher unterstützt.

Darf ich vorstellen? Harald Steiner – ein fiktiver, doch typischer Auslagerungsmanager in einer Genossenschaftsbank. Er ist Teamleiter in der Organisationsabteilung und seit kurzem auch zum zentralen Auslagerungsmanager befördert worden. Ganz so, wie es die MaRisk-Novelle in AT 9 erwartet. Herr Steiner ist nun auf der Suche nach einem Instrument, das ihn bei dieser Arbeit wirkungsvoll unterstützt. Dabei hat er genaue Vorstellungen, was er von einer geeigneten Unterstützungsleistung erwartet:

- Er will keine Papierlösung, sondern ein IT-gestütztes Instrument.
- Das Tool sollte kollaborationsfähig sein, da der Prozess der Auslagerungssteuerung nur arbeitsteilig bewältigt werden kann.
- Die Arbeitsschritte müssen transparent und selbsterklärend aufgebaut sein und der Status quo muss jederzeit erkennbar sein.
- Das Instrument sollte einfach zu bedienen sein und ihn und seine Kollegen mit einem Hilfesystem punktgenau unterstützen.
- Das Berichts- und Archivierungssystem sollte integrativer Bestandteil der Lösung und revisionssicher ausgestaltet sein.

## Technische Anforderungen

Genau diese Punkte waren die Vorgaben bei der Weiterentwicklung des Tools „Auslagerungsmanagement kompakt“. Schon die erste Version, ein Excel-Tool, konnte viele der genannten Anforderungen erfüllen. Die Kollaborationsfähigkeit und die Revisionssicherheit setzten jedoch eine Datenbanklösung voraus. Die nun verfügbare Version vereint drei entscheidende Vorteile:

**1. Datenhaushalt**
Die effiziente Verwaltung großer Datenmengen ist realisierbar. Beim Auslagerungsmanagement kommen schnell über einhundert Dienstleister zusammen. Das über ein paar Jahre fortgeschrieben, lässt die Menge der Daten erahnen. Da sorgt ein redundanzfreier Datenbestand mit wirkungsvollen Such- und Änderungsmechanismen und einem zügigen Antwortverhalten für Produktivitätssprünge.

**2. Datenqualität**
Die Korrektheit der Daten ist gewährleistet. Bei arbeitsteiligen Vorgängen, wie sie im Auslagerungsmanagement vorliegen, werden Konflikte beim Mehrnutzerbetrieb bzw. gleichzeitigen Datenzugriff durch Konsistenzregeln vermieden. „Falsche“ Daten haben so weniger Chancen.

**3. Datensicherheit**
Die Sicherheit der Daten wird erhöht. Sensible Daten können durch Kompetenzsteuerung vor unbefugtem Zugriff geschützt werden. Änderungen, durch wen auch immer, sind nachvollziehbar und zuordenbar. Dadurch können die Entscheidungsprozesse im Auslagerungsmanagement jederzeit klar und sauber rekapituliert werden.

## Prozessführung

Die Einzelprozesse, die bei der Auslagerungssteuerung zu durchlaufen sind, sind deutlich erkennbar voneinander abgegrenzt. Insgesamt sechs Kernprozesse werden unterschieden, die wiederum mit entsprechenden Teilprozessen unterlegt sind. Abbildung 1 veranschaulicht die Kern- und Teilprozesse. Dabei wurde besonders auf Prozesssparsamkeit und damit auf eine Aufwandsminimierung geachtet. Es müssen immer nur die Prozesse bearbeitet werden, die für die jeweilige Auslagerungsart vorgesehen sind.

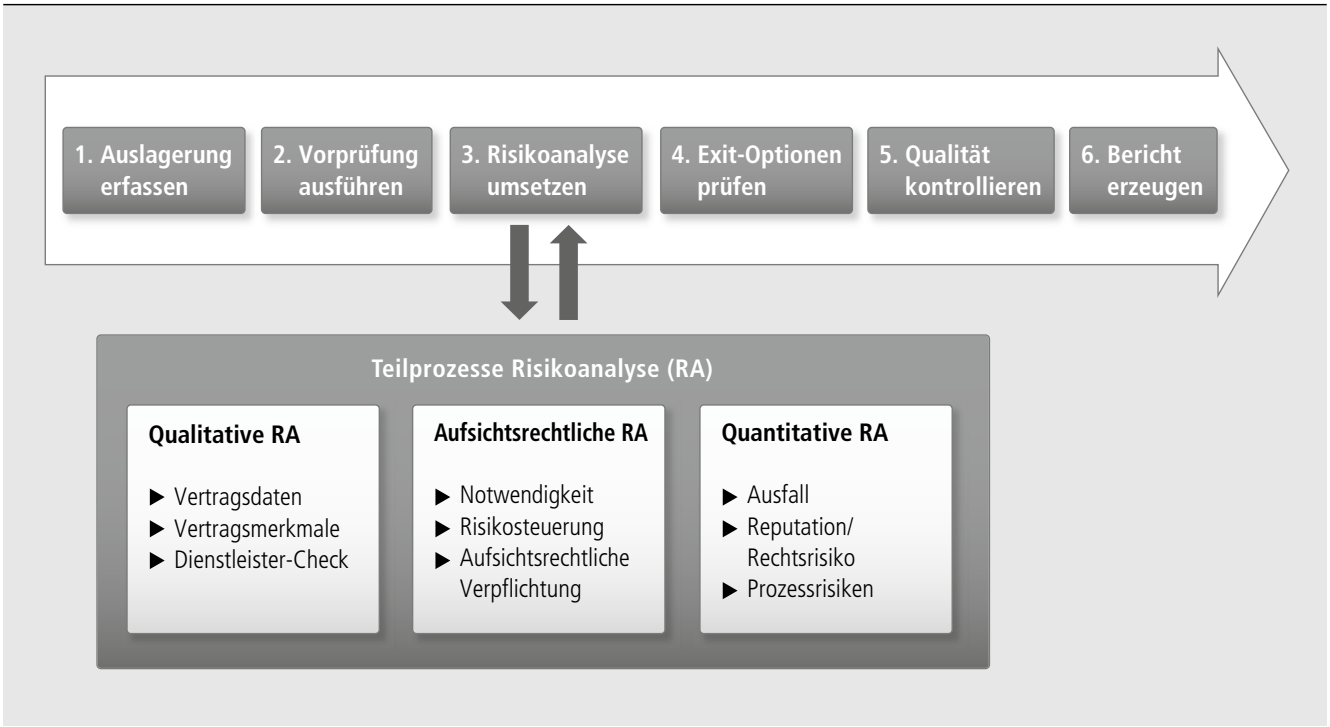
Die MaRisk unterscheiden drei Auslagerungsarten bzw. -stufen:

- sonstiger Fremdbezug,
- unwesentliche Auslagerung,
- wesentliche Auslagerung.

Strenggenommen ist nach den MaRisk der „sonstige Fremdbezug“ keine Auslagerung. Aber auch der „sonstige Fremdbezug“ muss nachvollziehbar identifiziert werden.

Vom „sonstigen Fremdbezug“ über „unwesentliche Auslagerungen“ bis zur „wesentlichen Auslagerung“ steigt das Auslagerungsrisiko und damit auch die Anforderungen an die Auslagerungssteuerung. Deshalb macht es Sinn, anfänglich zu prüfen, welche Auslagerungsart vorliegt, um den Umfang seiner Arbeitsprozesse daran auszurichten. Kann ein „sonstiger Fremdbezug“ bejaht werden, sind das Risiko und der daraus resultierende Arbeitsaufwand relativ klein. Umgekehrt verhält es sich bei der höchsten Stufe, der „wesentlichen Auslagerung“. Das Tool Auslagerungsmanagement kompakt reagiert mit ihren Arbeitsprozessen sehr sensibel auf das Auslagerungsniveau. >

Abb. 1 KERNPROZESSE IM AUSLAGERUNGSMANAGEMENT



## Fallbeispiele

**1. Sonstiger Fremdbezug**

Bei dieser Form der Auslagerung genügen drei Kernprozesse. Zuerst werden die wichtigsten Eckdaten der Dienstleistung erfasst. Der nächste Schritt beinhaltet die Vorprüfung. Sie stellt fest, ob ein „sonstiger Fremdbezug" vorliegt oder nicht. Wenn ja, ist die Arbeit beendet. Es folgt noch ein letzter – automatischer – Arbeitsschritt „Bericht erzeugen", der das Ergebnis der Vorprüfung dokumentiert. Im folgenden Jahr werden dann nur noch die genannten Arbeitsschritte wiederholt und eventuelle Änderungen eingepflegt. Beim sonstigen Fremdbezug werden nur drei von sechs möglichen Kernprozessen des Auslagerungsmanagements aufgerufen.

**2. Unwesentliche Auslagerung**

Die Vorprüfung fiel negativ aus, es liegt kein „sonstiger Fremdbezug" vor. Handelt es sich nun um eine unwesentliche oder wesentliche Auslagerung?

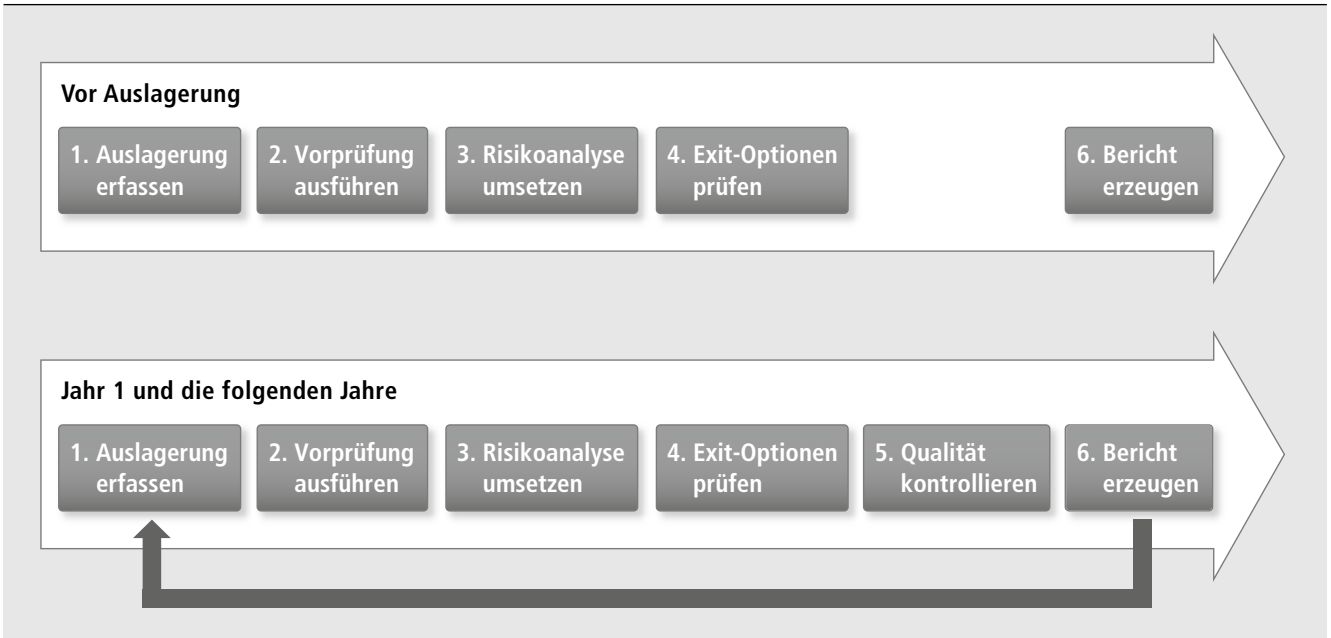
Diese Frage beantwortet der Kernprozess „Risikoanalyse", der Königsprozess des Auslagerungsmanagements kompakt. Er trennt die Spreu vom Weizen bzw. die unwesentlichen von den wesentlichen Auslagerungen in drei Prüfsegmenten bzw. Teilprozessen. Im Ergebnis der qualitativen, aufsichtsrechtlichen und quantitativen Risikoanalyse wird eindeutig beurteilt, welche Form der Auslagerung vorliegt.

Bei einer unwesentlichen Auslagerung ist die Arbeit nach der Risikoanalyse beendet. Als letzter Schritt wird, wie beim „sonstigen Fremdbezug", noch ein – automatischer – Bericht erzeugt, der den Entscheidungsprozess dokumentiert. Bei der unwesentlichen Auslagerung werden also nur vier der sechs Kernprozesse durchlaufen.

**3. Wesentliche Auslagerung**

Das Ergebnis der Risikoanalyse heißt „wesentliche Auslagerung". Das erfordert einen weiteren Arbeitsschritt, nämlich die Exit-Optionen zu prüfen. Für den geplanten oder ungeplanten Ausfall des Dienstleisters müssen Handlungsalternativen untersucht werden. Auch hier unterstützt das Tool Auslagerungsmanagement kompakt mit entsprechenden Prüffragen und Hilfsmitteln. Zum Schluss wird, wie in den beiden vorangegangenen Fällen, der Bericht automatisch erzeugt.

Abb. 2 WESENTLICHE AUSLAGERUNG



AUTOR UND ANSPRECHPARTNER

**Martin Hierlemann**
Leiter Vertrieb,
E-Mail: martin.hierlemann@geno-tec.de

Im Folgejahr werden die identifizierten wesentlichen Auslagerungen hinsichtlich eines eventuellen Anpassungsbedarfs geprüft und durchlaufen mit der Qualitätskontrolle einen zusätzlichen Kernprozess. Dort werden die Erfahrungen mit der Dienstleistungserbringung im vergangenen Jahr bewertet. Die Zusammenhänge veranschaulicht Abbildung 2.

Das Auslagerungsmanagement schrumpft oder wächst mit der Auslagerungsart bzw. dem damit verknüpften Risiko. Atmende Prozesse auf Basis einer Datenbank kennzeichnen ein neues, kompaktes Auslagerungsmanagement.

## aufsichtskonform, verbundkonform, aktuell

Das Tool Auslagerungsmanagement kompakt bezieht selbstverständlich alle neuen aufsichtsrechtlichen bzw. gesetzlichen Anforderungen ein. Die Anforderungen und mit ihnen die Prozesse werden zentral gepflegt und soweit notwendig aktualisiert.

Das Auslagerungsmanagement-Tool in der jetzigen Version berücksichtigt (u. a.)

- die Mindestanforderungen an das Risikomanagement – MaRisk, Rundschreiben 09/2017 (BA) vom 27. Oktober 2017, TZ AT9 Auslagerungen,
- die Bankaufsichtlichen Anforderungen an die IT (BAIT), Rundschreiben 10/2017 (BA) vom 3. November 2017, Kapitel II.8 Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen sowie
- die Datenschutz-Grundverordnung (EU-DSGVO).

Darüber hinaus sind sowohl die Inhalte als auch die integrierten Prozesse an die generelle Vorgehensweisen und die Musterdokumentationen des BVR angepasst. Schlussendlich wird das Tool und dessen aufsichtsrechtlich indizierte Überarbeitung

- mit einer Primärbank entwickelt bzw. verprobt und
- im Rahmen des Fachbeirates Beauftragtenwesen abgestimmt.

Zusammengefasst: Das Tool erfasst alle Auslagerungen, geht aber nur dort in die Tiefe, wo es notwendig ist. Es entspricht den Ausarbeitungen der Arbeitskreise zur Auslagerung beim BVR und DGRV und wurde von den Regionalverbänden abgenommen. Die Bank profitiert von einem objektiven mit den Verbänden abgestimmten Auslagerungsmanangement, das sich praxisorientiert präsentiert, das einfach bedienbar ist und den Aufwand signifikant senkt. ▬

**Der Fachbeirat Beauftragtenwesen** ist eine Initiative der GenoTec. Er setzt sich aus jeweils einem Vertreter der Regionalverbände sowie der Geschäftsführung der GenoTec zusammen. Der Fachbeirat will verbandsübergreifend Sicherheit für Banken, Prüfer 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.

## WpHG-Compliance

# MaComp-Konsultation

Was bringen die neuen MaComp? Änderungen zeichnen sich hinsichtlich der Wertpapiergeschäfte relevanter Personen, der Geeignetheitserklärung, der Staffelprovisionen, des Zuwendungs- und Verwendungsverzeichnisses sowie des Beschwerdemanagements ab.

Seit 2010 informiert die BaFin über ihre Verwaltungspraxis im Zusammenhang mit der Aufsicht über das Depot- und Wertpapier(neben)dienstleistungsgeschäft durch das Rundschreiben „Mindestanforderungen an die Compliance-Funktion und die weiteren Verhaltens-, Organisations- und Transparenzpflichten nach §§ 31 ff. WpHG für Wertpapierdienstleistungsunternehmen“ (MaComp).

Am 2. November 2017 veröffentlichte die BaFin nun eine geplante Anpassung, die sie für die neuen Module AT 3.1, BT 2, 6, 9, 10 und 12.2 zur Konsultation stellt.

Es gab eine ganze Reihe von – teilweise kritischen – Stellungnahmen, und das Konsultationsverfahren ist bis zum Redaktionsschluss immer noch nicht abgeschlossen. Es bleibt daher abzuwarten, ob es noch wesentliche Änderungen für die finale Version geben wird. In dem folgenden Beitrag soll dennoch auf einige geplante Änderungen kurz eingegangen werden und sollen einige Hinweise auf die anstehenden Änderungen gegeben werden.

### BT 2 Wertpapiergeschäfte relevanter Personen

Die bisher im § 33b WpHG geregelte Überwachung von Mitarbeitergeschäften wurde durch das 2. FiMaNoG dort gestrichen und wird nun durch die Art. 28 und 29 der Durchführungsverordnung zur MiFID II 2017/565 geregelt. Im Modul BT 2 wurden daher die Gesetzesgrundlagen und die Begrifflichkeiten entsprechend angepasst.

Von den bisher beispielhaft aufgeführten „geeigneten und bewährten“ Überwachungsvarianten für Geschäfte von Compliance-relevanten Mitarbeitern wurde die dritte Variante – die stichprobenhafte Überwachung – gestrichen.
Als geeignete Verfahren verbleiben damit:

1. die Vereinbarung eines automatischen Zweitschriftenversandes durch das depotführende Institut oder
2. die unaufgeforderte Anzeige von Geschäften durch den Mitarbeiter in Verbindung mit einer regelmäßigen Vollständigkeitserklärung oder
3. die Vereinbarung eines Zustimmungsvorbehalts für jedes einzelne Mitarbeitergeschäft.

Bei den Volksbanken Raiffeisenbanken wird in der Praxis die Variante 1 oder 2 durch die MOA eingesetzt, so dass die Banken durch diese Änderung nicht betroffen sein dürften.

### BT 6 Geeignetheitserklärung

Das Modul BT 6, das bisher das Anlageberatungsprotokoll behandelte, wurde ersetzt durch Hinweise auf die neuen Anforderungen der Geeignetheitserklärung (§ 64 Abs. 4 WpHG und Art. 54 Abs.12 delVO).

Wie schon beim Anlageberatungsprotokoll ist die Geeignetheitserklärung dem Kunden spätestens vor einem Vertragsschluss zur Verfügung zu stellen.

Eine Klarstellung erfolgt in BT 6 Nr. 3 für die Fälle, in denen auf eine Anlageberatung kein Vertragsschluss folgt, z. B. bei einer Halteempfehlung. In diesen Fällen ist die Geeignetheitserklärung dem Kunden zeitnah, spätestens fünf Tage nach der Beratung zur Verfügung zu stellen.

Vor diesem Hintergrund empfiehlt sich, an der bisherigen Regelung festzuhalten und dem Kunden – unabhängig von der konkreten Art der Empfehlung – nach jeder Anlageberatung zeitnah die Geeignetheitserklärung zur Verfügung zu stellen.

### BT 9 Staffelprovisionen

Im neuen Modul BT 9 wird die Aufnahme von potenziellen Interessenkonflikten beim Vorliegen von Staffelprovisionen in den Interessenkonfliktgrundsätzen gefordert.

Sollte das Modul BT 9 unverändert in der finalen Fassung umgesetzt werden, sind die Analyse der potenziellen Interessenkonflikte und die Informationen über den Umgang mit Interessenkonflikten ggf. anzupassen.

AUTOR UND ANSPRECHPARTNER

**Marc Linnebach**
Leiter WpHG-Compliance,
E-Mail: marc.linnebach@geno-tec.de

### BT 10 Zuwendungs- und Verwendungsverzeichnis

Neben dem Bezug auf die neuen Gesetzesgrundlagen formuliert die BaFin zum Thema Dokumentationspflichten bei Zuwendungen eine Reihe neuer Anforderungen.
Dies sind insbesondere:

1. Ein „fortlaufendes“ Führen des Zuwendungs- und Verwendungsverzeichnisses.
   Gegenüber der bisherigen jährlichen Dokumentation sollen Zuwendungen und deren Verwendung zukünftig „fortlaufend“ zu führen sein.
2. Im Zuwendungsverzeichnis ist eine aufzuschlüsselnde Gegenüberstellung der Zuwendungen nach betroffenen Wertpapierdienstleistungen und dem qualitätsverbessernden Einsatz für einzelne Kunden oder homogene Kundengruppen aufzunehmen. Eine zusammenfassende Gegenüberstellung soll nicht mehr ausreichen.
3. Im Zuwendungsverzeichnis ist ein Abschnitt aufzunehmen, in dem dokumentiert wird, wie zukünftige (im kommenden Geschäftsjahr) erwartete Zuwendungen die Qualität verbessern sollen.
4. Die Einführung eines Maßnahmenverzeichnisses.
   In einem fortlaufend zu führenden Verzeichnis ist die Beschreibung der einzelnen Maßnahmen bezogen auf die jeweilige Wertpapierdienstleistung oder Wertpapiernebendienstleistung aufzunehmen, die dazu dienen, Interessenkonflikte im Zusammenhang mit Zuwendungen zu verhindern.

Gegen diese neuen Anforderungen richtet sich eine ganze Reihe von Stellungnahmen zur Konsultation. In welchem Umfang diese in der finalen Fassung umgesetzt werden, bleibt abzuwarten.

Diese Änderungen können im laufenden Jahr erheblichen Handlungsbedarf mit sich bringen. Daher sollte hierauf direkt nach Veröffentlichung der finalen Version der MaComp geachtet werden.

### BT 12 Beschwerdemanagement

Im Modul BT 12.1 verweist die BaFin auf die noch nicht abgeschlossene Konsultation 06/2017 zum gemeinsamen Rundschreibug zur Umsetzung der ESMA/EBA-Leitlinien zur Beschwerdeabwicklung und kündigt hierzu die Ergänzung des Moduls an.

Darüber hinaus werden im Modul BT 12.2 die Anforderungen an einen neuen Beschwerdebericht formuliert. Dieser soll jeweils am 1. März eines Jahres – erstmalig in 2019 – die Beschwerden des vorangegangenen Kalenderjahres nach einem vorgegebenen Muster (MaComp Anlage zu BT 12.2) aufführen und elektronisch an die BaFin eingereicht werden.

Die Beschwerden sind u. a. den betroffenen Wertpapier(neben)dienstleistungen zuzuordnen und nach vorgegebenen Beschwerdegründen zu sortieren. Darüber hinaus soll angegeben werden, ob die Beschwerde erledigt ist, ob sie „erfolgreich“ war und ob sie vor Gericht oder dem Schlichtungsverfahren verhandelt wurde.

Gegen diese Anforderungen äußern die Stellungnahmen ihre Bedenken bezüglich der grundsätzlichen Notwendigkeit, der rechtlichen Zulässigkeit, des geforderten Detailgrades und des Zeitpunkts.

Wie schon beim Modul BT 10 ist auch hier bei Veröffentlichung der finalen Fassung der MaComp darauf zu achten, welche Regelungen umgesetzt wurden, da sich hieraus sofortiger Umsetzungsbedarf ergeben kann. ▬

## Datenschutz

# EU-DSGVO: Die Zeit läuft

Mit der EU-Datenschutz-Grundverordnung (DSGVO) wird der Datenschutz zu einem festen Bestandteil des Risikomanagements. Verfahren und Prozesse müssen bis zum 25. Mai 2018 überprüft und angepasst werden. Nachfolgend Hinweise zur Umsetzung.

Die EU-DSGVO tritt am 25. Mai 2018 in Kraft. Im Gegensatz zur Richtlinie 95/46/EG, die von den EU-Mitgliedstaaten erst in nationales Recht umgesetzt werden musste, gilt die DSGVO ab diesem Zeitpunkt unmittelbar in allen EU-Mitgliedstaaten.

Eine aus der Verordnung heraus mögliche Nutzung von Öffnungsklauseln wurde in einem Datenschutz-Anpassungsgesetz beschlossen und am 31. Juli 2017 im Bundesgesetzblatt veröffentlicht.

Unternehmen sollten nunmehr, bis zum Inkrafttreten der DSGVO, ihre Verfahren und Prozesse überprüfen und an die neuen Vorgaben anpassen. Der Datenschutz wird damit auch zu einem festen Bestandteil des eigenen Risikomanagementsystems.

### Wichtige Umsetzungsschritte

Im Hinblick auf die bereits bestehende Richtlinie 95/46/EG und das daraus auf nationaler Ebene bestehende BDSG ist davon auszugehen, dass Datenschutz in den meisten Häusern bereits gelebt wird und damit – im Vergleich zu anderen europäischen Mitgliedstaaten – in der Unternehmenskultur angekommen ist. Somit dürften bereits grundsätzliche Maßnahmen zum Schutz der personenbezogenen Daten etabliert sein.

Die Herausforderung besteht nun darin, den derzeitigen Ist-Stand im Datenschutz an die neue Verordnung anzupassen. Hierzu ergeben sich zwangsläufig verschiedene praktische Aufgabenstellungen. Diesen müssen sich die Unternehmen widmen, um den Anforderungen der DSGVO gerecht werden zu können. Im Folgenden werden einige wesentliche Aspekte der DSGVO aufgegriffen sowie wichtige Umsetzungsschritte dargestellt:

1. **Haben Sie einen Datenschutzbeauftragten benannt?**
   Art. 37 der DSGVO nennt die Kriterien, wann ein Datenschutzbeauftragter nach neuem Recht „benannt“ werden muss. Der § 38 des neuen Nachfolgegesetzes des alten BDSG, des Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU (DSAnpUG-EU), konkretisiert dies in bewährter Form: ab mindestens zehn Personen, die mit einer ständigen automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

   Aber Achtung: Auch wer keinen Datenschutzbeauftragten nach neuem Recht benennen muss, ist gut beraten, sich mit dem Datenschutz in seinem Unternehmen zu beschäftigen.
2. **Haben Sie ein Verzeichnis von Verarbeitungstätigkeiten erstellt?**
   Bislang musste der Verantwortliche in Ihrem Unternehmen nach dem BDSG ein internes und ein öffentliches Verfahrensverzeichnis führen. Das öffentliche Verzeichnis entfällt künftig. Gemäß DSGVO sind das Unternehmen (Verantwortlicher) und nunmehr auch Auftragsverarbeiter verpflichtet, ein Verzeichnis von Verarbeitungstätigkeiten zu erstellen und zu führen. Als datenverarbeitendes Unternehmen sollten Sie prüfen, welche inhaltlichen Anforderungen Art. 30 DSGVO an das neue Verzeichnis stellt, diese mit Ihrem alten Verzeichnis abgleichen und ggf. ergänzende Veränderungen vornehmen.

   Sinnvollerweise sollten Sie den Prozess der Risiko- und Datenschutz-Folgenabschätzung nach Art. 35 DSGVO für die Betroffenen mit in die Dokumentation einbinden. Sie kommen so gleichzeitig der notwendigen Nachweispflicht nach.
3. **Haben Sie eine Übersicht Ihrer Auftragsverarbeiter?**
   Auftragsverarbeiter kann eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle sein, die personenbezogene Daten im Auftrag des Verantwortlichen (Ihr Unternehmen) verarbeitet. Die bisherigen vertraglichen Regelungen basierten auf dem § 11 BDSG und gestalten sich nunmehr weitgehend über den Art. 28, der

DSGVO und nach § 62 DSAnpUG-EU. Die Analyse Ihrer Vertragsdatenbank (Vertragsspiegel) nach vorhandenen Verträgen mit Auftragsverarbeitern sowie die Anpassung der Verträge entsprechend den neuen gesetzlichen Vorgaben ist dringend anzuraten.

4. **Haben Sie Ihre technischen und organisatorischen Maßnahmen (TOMs) neu dokumentiert?**
   Der Art. 32 DSGVO gibt vor, dass geeignete technische und organisatorische Maßnahmen vorzuhalten sind, um den Risiken für die Rechte und Freiheiten natürlicher Personen mit einem angemessenen Schutzniveau begegnen zu können. Diese sollten sich nicht nur in der bereits erwähnten Verarbeitungsübersicht wiederfinden, sondern auch separat dokumentiert werden: Dies empfiehlt sich mit Blick auf eine verbundene Risikobetrachtung und Maßnahmenbeschreibung unter Berücksichtigung des Technikstands und der Implementierungskosten. Ein Verfahren zur Überprüfung der Wirksamkeit der TOMs sollte gemäß Art. 32 Abs. 1 lit. d DSGVO implementiert werden. Dies kann auch über ein bestehendes Informationssicherheitsmanagementsystem und den dort bereits integrierten PDCA-Kreislauf (Plan – Do – Check – Act) mit abgebildet werden.
5. **Weitere Schritte, die umgesetzt und beachtet werden sollten**

- Interner Prozess zur Gestaltung der Meldepflichten bei Datenpannen gemäß Art. 33 und 34 DSGVO
- Interner Prozess zur Umsetzung des „Rechts auf Löschung“ und des „Rechts auf Vergessenwerden“ gemäß Art. 17 DSGVO und § 58 DSAnpUG-EU
- Interner Prozess zur Umsetzung des „Auskunftsrechts“ gemäß Art. 15 DSGVO und § 57 DSAnpUG-EU
- Umsetzungsprozess zur Erfüllung der Informationspflichten bei der Erhebung von personenbezogenen Daten (hier auch Ihren Internetauftritt beachten) gemäß Art. 12, 13, 14 DSGVO und § 55 DSAnpUG-EU
- Prüfung eingesetzter Einwilligungen nach Art. 7 DSGVO und § 51 DSAnpUG-EU

Und nicht zuletzt ist auch daran zu denken, die Mitarbeiter/-innen entsprechend den neuen gesetzlichen Normen zu sensibilisieren und zu schulen.

### … und wenn wir versuchen, es auszusitzen?

Verstöße gegen die Europäische Datenschutz-Grundverordnung können in Zukunft hohe Strafen nach sich ziehen. Es drohen Bußgelder von bis zu 20 Millionen Euro oder bis zu 4 % des globalen Unternehmensumsatzes (Art. 83 DSGVO). Der Bußgeldrahmen soll wirksam und abschreckend sein. Vielleicht sind kleinere Unternehmen in der Höhe nicht vollständig betroffen, aber auch kleinere Bußgelder können schmerzlich sein und ggf. die eigene Reputation schwächen.

Sollten Sie sich die Frage stellen, ob Sie in Ihrem Unternehmen die DSGVO beachten müssen, so sei hier angemerkt, dass die Gültigkeit der Verordnung alle in der EU ansässigen Unternehmen betrifft. Verarbeiten Sie personenbezogene Daten im Sinne von Art. 2 und 3 der DSGVO, so müssen Sie in Ihrer betrieblichen Praxis die Regelungen der Verordnung entsprechend beachten.

AUTOR UND ANSPRECHPARTNER

**Thomas Grebe**
Leiter IT-Sicherheit und Datenschutz,
E-Mail: thomas.grebe@geno-tec.de

### Fazit

Wenn man sich die grundlegenden Maßnahmen, wie vor beschrieben, vergegenwärtigt hat und umsetzt, so sind die wichtigsten Meilensteine für den Start der neuen DSGVO gelegt.

Der ab dem 25. Mai 2018 beginnende öffentliche Diskussionsprozess um die richtige Auslegung strittiger Datenschutzfragen im Inland und in der EU wird die Basis in verschiedenen Punkten verändern, so dass an den bisher gesetzten Eckpunkten nachjustiert werden muss.

Wem die Umsetzung der datenschutzrechtlichen Aufgaben im Moment lästig erscheint, sollte der wirtschaftliche Mehrwert als Anreiz dienen. Er ergibt sich durch die Prozessprüfung, in dessen Folge die Datenqualität verbessert bzw. die Datenquantität entsprechend reduziert werden kann. Nicht zu vergessen sei darüber hinaus die Rechenschaftspflicht („Accountability“, Art. 5 Abs. 2 DSGVO), verbunden mit zahlreichen Dokumentations- und Nachweispflichten zur Einhaltung der Datenschutzvorgaben gegenüber den zuständigen Aufsichtsbehörden. Hier gilt, mit Aristoteles gesprochen: „Wer schreibt, der bleibt“! ▬

## Informationssicherheit

# Kompetenzen und Rezertifizierung: Fluch oder Segen?

Mit den MaRisk 6.0 und den BAIT wurden Ende 2017 neue Regelungen zur Umsetzung des Risikomanagements getroffen. Ein Punkt, der nahezu unverändert einen hohen Stellenwert einnimmt, ist die Überprüfung von Berechtigungen und Kompetenzen.

Da fragt man sich: Was sollen diese vielen Vorschriften? Bedarf es ihrer wirklich? Oder ist es nur eine weitere Übersicht, die viel Arbeit macht von der Bestandsaufnahme bis hin zur regelmäßigen Überprüfung und schlussendlich doch nur wieder ungenutzt in einer Schublade verschwindet? Reichen denn nicht die Kontrollen der Revision, ob Kompetenzen richtig vergeben wurden? Die Frage sei erlaubt: Was bringt eine weitere Übersicht über alle vergebenen Berechtigungen nach MaRisk AT 4.3.1?

### Aufwand

Ist es ein Fluch? Eine „Schikane“ der Behörden? Auf den ersten Blick scheint es so: Der Aufwand ist in der Praxis enorm.

Zunächst muss ein Überblick darüber erlangt werden, welche Kompetenzen es im Unternehmen überhaupt gibt. Und schon dort liegen die ersten Fallstricke. Die gängige Software fällt jedem auf Anhieb ein. Aber ist das wirklich alles, was zum Thema Kompetenzen gehört? Wie sieht es mit Schlüsseln aus? Sind diese im Sinne der MaRisk eine Kompetenz? Die Frage ist mit „ja“ zu beantworten: Physische Schlüssel fallen ebenso wie elektronische Zugangssysteme darunter. Auch an Unterschriften denkt nicht jeder sofort, und doch werden sie direkt in den MaRisk aufgeführt.

Dann die Frage nach der Verwaltung: Wie verwaltet man beispielsweise MaRisk-konform Online-Zugänge, bei denen sich ein Mitarbeiter einfach registrieren kann? Wie kommt die Information zu einer zentralen Stelle, die die Kompetenz erfasst und bei Bedarf auch wieder sperren kann? Um hier eine Antwort geben zu können, müssen Prozesse im Unternehmen eingeführt werden, die zuverlässig solche Informationen transportieren und verarbeiten. Sicher ist: Das kostet ein Unternehmen nicht nur Geld, sondern auch Ressourcen.

Und damit nicht genug: Auch für die Rezertifizierung ist ein erheblicher Aufwand zu betreiben. So muss die zentral verortete Dokumentation laufend aktualisiert werden, und das von vielen Stellen im Unternehmen.

Treiber ist dabei nicht nur die aufsichtsrechtliche Anforderung, sondern auch die Prüfung. Denn am Ende muss der aufgestellte Prozess vor der Prüfung Bestand haben.

Viele Unternehmen beschränken sich deshalb auf die Pflicht. Sie führen nur die wesentlichen Kompetenzen und Berechtigungen in Registern und überprüfen auch nur diese regelmäßig. Die Regelungen aus der MaRisk werden als Bürde gesehen: Der ganze Aufwand ist im Prinzip ein bürokratischer Akt, der Zeit und Ressourcen verschwendet.

Doch ist das wirklich so? Kann das Thema Kompetenz- und Berechtigungsmanagement mit Rezertifizierung nicht auch ein Segen sein?

### Nutzen

Bei der vollständigen Aufstellung der Kompetenzen stößt man meist auf Systeme, die eigentlich gar nicht mehr benutzt werden. Wer sich intensiv mit der Rezertifizierung beschäftigt, wird auch die Gelegenheit nutzen, veraltete Kompetenzen zu entfernen. In diesem Sinne ist die Aufstellung die Basis für eine Inventur.

AUTORIN UND ANSPRECHPARTNERIN

**Sandra Sitter**
Leiterin IT & Projekte,
E-Mail: sandra.sitter@geno-tec.de

Wenn man keine Übersicht über alle Kompetenzen hat, kann beim Ausscheiden eines Mitarbeiters leicht vergessen werden, Zugänge zu sperren. Und ist es nicht auch für neue Mitarbeiter gut zu wissen, in welchen Systemen sie überall registriert sind? Worauf sie Zugriff haben und welche Verantwortung sie haben? Nicht zuletzt: Die Aufstellung wird auch helfen, bei der Neueinstellung von Mitarbeitern relevante Berechtigungsanträge zu identifizieren. Bei eingeführten Standards, Berechtigungen nach Stellen, gibt es klare Regelungen.

Schlussendlich ist die Überprüfung der Kompetenzen eine gute Gelegenheit, Berechtigungen zu hinterfragen und Prozesse zu optimieren. Wer kennt nicht die Antwort: „Ich mache das, weil es schon immer so war“? Wenn Kompetenzen strikt nach dem „Need-to-know-Prinzip“ vergeben werden, hat man im Rahmen der Überprüfung die Gelegenheit, Arbeitsabläufe oder Aufgaben klarer bzw. neu zu regeln.

Eine weitere Chance besteht darin, klare Strukturen zu schaffen: Wer benötigt für einen schlanken Prozess beispielsweise eine Vollmacht, um Verträge unterzeichnen zu können? Oder: Brauchen wirklich viele Mitarbeiter im Unternehmen rund um die Uhr Zutrittsrechte? Das Risiko des Schlüsselverlustes steigt mit jedem Zugriffsberechtigten. Oft besteht hier eine Möglichkeit, Geld und andere Ressourcen einzusparen.

Ein weiterer Pluspunkt: Klare Strukturen und Standards geben Orientierung und schaffen die Basis für eine höhere Mitarbeiterzufriedenheit. Berechtigungen und Kompetenzen werden seit den detailliert aufgeführten Anforderungen in den MaRisk mehr stellen- als personenbezogen vergeben. Sie sorgen für Arbeitsentlastung, definieren die Rahmenbedingungen eindeutig und wirken sich auch positiv auf die innerbetriebliche Gleichbehandlung aus.

Die Überprüfung der Kompetenzen führt eben nicht nur zur eingesetzten Software und Hardware. Sie stößt vielmehr eine regelmäßige Inventur der Prozesse und Geschäftsverbindungen an.

Unternehmen sollten sich deshalb überlegen, ob sie wirklich nur die wesentlichen, in den MaRisk geforderten Berechtigungen und Kompetenzen dokumentieren und regelmäßig überprüfen. Eine vollständige Übersicht hilft bei der Umsetzung und Optimierung der Standards. Dabei sind durchaus (auch MaRisk-konforme) Erleichterungen denkbar, z. B. indem Überprüfungsabstände großzügiger gestaltet werden.

## Fazit

Die Umsetzung der Normierung ist mehr Segen als Fluch. Sie bietet Unternehmen die Chance, Kosten zu sparen, Prozesse zu optimieren und Risiken zu minimieren.

Wenn man sich auf dem Weg zur Erfüllung gesetzlicher Anforderungen mit dem Unternehmensziel und der Strategie auseinandersetzt, fragt, wie man es erreichen oder auch halten kann, und lieb gewonnene Arbeitsabläufe in Frage stellt, dann ist es eindeutig ein Segen. Die Dokumentation hilft, sich auf wertschöpfende Tätigkeiten zu konzentrieren. Und jedes „Warum“ enthält die Aussicht, Bestehendes zu optimieren und Neues zu denken. ▬

Geldwäscheprävention

# Gruppenweite Pflichten: Gilt das etwa auch für uns?

Gut ein Drittel der von uns betreuten Banken haben Tochtergesellschaften, die in den Anwendungsbereich des § 9 GwG fallen. Das kann einen erheblichen Mehraufwand bedeuten. Es gibt jedoch auch Erleichterungen und Hilfestellungen.

Im Rahmen der Novellierung des Geldwäschegesetzes (GwG) 2017 wurde auch die Anwendbarkeit der „gruppenweiten Pflichten" im Sinne des § 9 GwG geändert. Entgegen der alten Regelung im § 251 Kreditwesengesetz (KWG) in Verbindung mit § 10 KWG fordert die neue Regelung die Einbeziehung aller Tochterunternehmen, die sich mehrheitlich im Besitz des Instituts befinden und selbst Verpflichtete nach § 2 GwG sind. In Kombination mit der Ausweitung der besagten Verpflichteten führt dies zu einem signifikanten Anstieg der Anwendungsfälle des § 9 GwG: der gruppenweiten Pflichten.

Ob ein Kreditinstitut als übergeordnetes Institut tätig werden muss, lässt sich grundsätzlich anhand von zwei einfachen Fragen feststellen:

1. Besteht an einem nachgelagerten Unternehmen eine Mehrheitsbeteiligung (> 50 %)?
2. Ist das nachgelagerte Unternehmen selbst Verpflichteter nach § 2 GwG?

Sofern beide Fragen positiv beantwortet werden, ist die Anwendung der gruppenweiten Pflichten unumgänglich.

### Wer ist in der Praxis davon betroffen?

Nach § 2 Abs. 16 GwG zählen nun auch sogenannte Güterhändler zu den Verpflichteten. Nach der GwG-eigenen Definition ist jede Person ein Güterhändler, die gewerblich Güter veräußert. Die Gesetzesbegründung führt hierzu aus:

„… Güterhändler erfasst zunächst einen weiten Personenkreis. So ist jede Person, die gewerblich mit Gütern handelt, Güterhändler nach Absatz 9. Güter sind alle beweglichen und nicht beweglichen Sachen, unabhängig von ihrem Aggregatzustand, die einen wirtschaftlichen Wert haben und deshalb Gegenstand einer Transaktion sein können …"

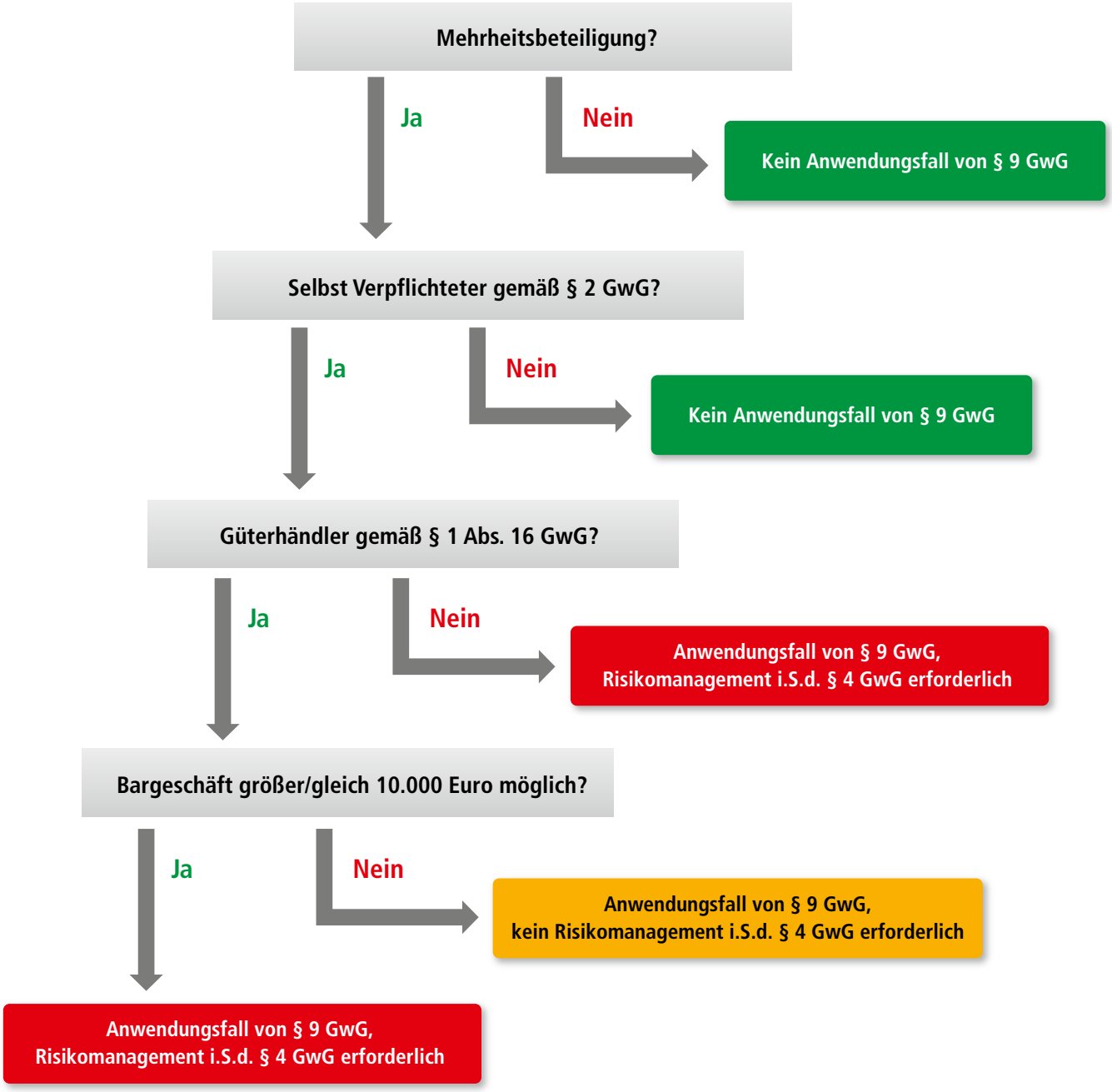
Diese Ausweitung hat zur Folge, dass beispielsweise Genossenschaften zur Energieerzeugung, Tankstellen oder auch klassische Warengenossenschaften nicht nur selbst Verpflichtete nach GwG sind, sondern auch in die gruppenweiten Pflichten einbezogen werden müssen.

Die Güterhändler erwartet zumindest eine Erleichterung bei der Umsetzung der geldwäscherechtlichen Vorschriften, sofern sie auf Bartransaktionen größer als 9.999,99 Euro verzichten. Dies gilt auch, wenn kleinere, in einem Zusammenhang stehende Beträge zusammen diesen Wert nicht überschreiten. In diesen Fällen kann auf ein Risikomanagement im Sinne des § 4 GwG verzichtet werden. Da das Risikomanagement eine Risikoanalyse (§ 5 GwG) und die internen Sicherungsmaßnahmen (§ 6 GwG) umfasst, entfällt somit bereits ein großer Teil der geldwäscherechtlichen Verpflichtungen.

Bei der Einschätzung, ob und in welchem Umfang die gruppenweiten Sorgfaltspflichten angewandt werden müssen, kann nebenstehendes Prüfschema als Unterstützung herangezogen werden.

Ähnlich verhält es sich mit der Pflicht, einen eigenen Geldwäschebeauftragten für das jeweilige Tochterunternehmen zu bestellen. Dies ist beispielsweise bei Güterhändlern und Immobilienmaklern von einer etwaigen Anordnung der jeweiligen Aufsichtsbehörde abhängig. >

Abb. 1 PRÜFSCHEMA ZUR IDENTIFIZIERUNG VON GRUPPENWEITEN PFLICHTEN



AUTOREN UND ANSPRECHPARTNER

**Florian Fuhrig**
Beauftragter Zentrale Stelle,
E-Mail: florian.fuhrig@geno-tec.de

**Dominik Tiburtius**
Leiter Überwachung & Kontrolle,
E-Mail: dominik.tiburtius@geno-tec.de

### Welche Aufgaben hat der Gruppen-Geldwäschebeauftragte?

Die Aufgaben des sogenannten Gruppen-Geldwäschebeauftragten sind losgelöst von den Verpflichtungen des Tochterunternehmens und damit eines etwaigen Geldwäschebeauftragten zu betrachten. Grundsätzlich ist davon auszugehen, dass der Gruppen-Geldwäschebeauftragte regelmäßig der Geldwäschebeauftragte des übergeordneten Instituts ist (vgl. DK-Hinweise Zeile 86).

Der Gruppen-Geldwäschebeauftragte hat im Rahmen des globalen Risikomanagements für die gesamte Gruppe eine einheitliche Strategie zur Prävention von Geldwäsche und Terrorismusfinanzierung zu schaffen, die Umsetzung zu koordinieren und gruppenweit zu überwachen. Sofern das nachgeordnete Unternehmen auch dem KWG unterliegt, gilt dies auch in Bezug auf „sonstige strafbare Handlungen" im Sinne des § 25h Abs. 1 KWG.

Ebenso ist es erforderlich, dass der Gruppen-Geldwäschebeauftragte sich laufend über die nachgeordneten Unternehmen und über deren Einhaltung der geldwäscherechtlichen Pflichten informiert. Gemäß BaFin-Rundschreiben 17/2009 (GW) hat der Gruppen-Geldwäschebeauftragte „… sich in regelmäßigen Abständen – auch durch Besuche vor Ort – insbesondere davon zu überzeugen, dass die Pflichten gemäß § 25l Abs. 1 KWG (neu: § 9 GwG) eingehalten bzw. die notwendigen Maßnahmen getroffen werden …"

### Welche Aufgaben übernimmt die GenoTec?

Die GenoTec übernimmt die Funktion des Gruppen-Geldwäschebeauftragten. Damit verbunden werden ebenfalls die im BaFin-Rundschreiben 17/2009 (GW) geforderten Maßnahmen, inklusive der Vor-Ort-Besuche, durchgeführt. Des Weiteren werden die Ergebnisse in die Risikoanalyse für das übergeordnete Institut reflektiert.
Hinsichtlich der geldwäscherechtlichen Verpflichtungen der Tochterunternehmen bieten wir folgende, modular buchbare, Unterstützungsleistungen an:

- Unterstützung bei der Erstellung einer eigenen Risikoanalyse
- Unterstützung bei der Erstellung von Arbeitsanweisungen
- Unterstützung bei der Einrichtung eines Kontrollkonzeptes
- Unterstützung bei der Durchführung der Kontrollhandlungen
- Schulung der Mitarbeiter
- Überprüfung des Prozesses zum Verdachtsmeldewesen
- Unterstützung bei der Erstellung eines Jahresberichts

## Zentrale Stelle

# EU-Finanzsanktionen und Namenslisten

Banken werden als wichtige Knotenpunkte im großen neuronalen Netz des internationalen Finanzsystems gesehen. Die Umsetzung von EU-Finanzsanktionen erfordert deshalb auch eine besonders sorgsame und nachvollziehbare Vorgehensweise.

### Politische und rechtliche Hintergründe

Seit den 1990er Jahren setzt die EU verstärkt das Instrument gezielter „smarter" Finanzsanktionen im Rahmen ihrer „Gemeinsamen Außen- und Sicherheitspolitik" (GASP) ein.[1] Sie tut dies im Einklang mit den Beschlüssen des Sicherheitsrates der Vereinten Nationen (VNSR) und auf Grundlage entsprechender VNSR-Sanktionsresolutionen. Die Intention ist, sich völkerrechtswidrig verhaltende Staaten und ihre Regierungen, die der Verletzung der Menschenrechte oder der Bedrohung des globalen Friedens und der internationalen Sicherheit bezichtigt werden, einerseits zu bestrafen und andererseits zu einer rechtskonformen Haltung bzw. einem Politikwechsel zu bewegen.[2] Der aktuelle Fall Nordkoreas bietet hierzu reichlich Anschauungsmaterial.[3]

### Banken als wichtige Normadressaten der Finanzsanktionen

Nun wird die Bedeutung von EU-Finanzsanktionsmaßnahmen von den wirtschaftlichen Akteuren regelmäßig unterschätzt. So fragen sich Mitarbeiter und Vorstände von Genossenschaftsbanken im Zusammenhang mit der Durchführung von EU-Finanzsanktionsmaßnahmen oft Folgendes: „ … und was hat das bitte mit uns zu tun?!" Die Antwort bzw. die Erwartungshaltung der EU und ihrer Mitgliedstaaten dazu ist verhältnismäßig klar:

a) Bei der Durchführung der außen- und sicherheitspolitisch sehr bedeutsamen Finanzsanktionsmaßnahmen wird den in geschäftlicher Hinsicht überwiegend universal ausgerichteten Banken in der EU – so auch den Genossenschaftsbanken in Deutschland – bewusst eine überaus wichtige politische Verantwortung als drittbetroffene Unternehmen aufgebürdet.[4]

b) Ferner werden Banken als am Massenzahlungsverkehr teilnehmende Finanzintermediäre und Synapsen im großen neuronalen Netz des internationalen Finanzsystems als Erfüllungsgehilfen der EU-Mitgliedstaaten gesehen. >

[1] Initiiert wurde diese Entwicklung durch den Vertrag von Maastricht aus dem Jahre 1992 (http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=URISERV%3Axy0026 – Stand: 06.03.2018).

[2] Vgl. Ganguli, Indranil, Smarte Finanzsanktionen der EU – Eine politikwissenschaftliche und bankpraktische Effektivitätsanalyse ausgewählter Maßnahmen, Baden-Baden 2013, S. 23 u. 29 sowie Hufbauer, Gary Clyde u. Oegg, Barbara, The European Union as an Emerging Sender of Economic Sanctions, in: Aussenwirtschaft, 58. Jg. (2003), Heft IV, Zürich: Rüegger, S. 560.

[3] Siehe u. a. Spiegel Online, Atomkonflikt mit Nordkorea – Alle Artikel und Hintergründe (http://www.spiegel.de/thema/nordkorea_atomkonflikt/ – Stand 06.03.2018).

[4] Vgl. Dahme, Gudrun, Terrorismusbekämpfung durch Wirtschaftssanktionen, Dissertation der Rechtswissenschaftlichen Fakultät der Westfälischen Wilhelms-Universität Münster, Witten 2007, S. 514 ff.

c) Insoweit werden Banken von der EU dazu verpflichtet, Geldströme und wirtschaftliche Ressourcen sanktionierter Personen zu überprüfen, einzufrieren bzw. zu verwalten und damit im Auftrag der EU und ihrer GASP zu kontrollieren. Dies hat in Übereinstimmung mit den Vorgaben des EU-Rechts und des nationalen Rechts der EU-Mitgliedstaaten, in denen die Banken tätig sind, zu erfolgen.

Hervorzuheben ist ferner, dass Finanzsanktionen der EU aufgrund ihrer außen- und sicherheitspolitisch herausgehobenen Stellung in Form von EU-Rechtsverordnungen erlassen werden. Diese Verordnungen haben unmittelbare Geltung in den EU-Mitgliedstaaten im Bereich des Kapital- und Zahlungsverkehrs. Zur Erreichung der erwähnten außen- und sicherheitspolitischen Ziele enthalten die Maßnahmen einen Katalog von zwischenzeitlich fast durchgängig standardisierten und besonders die Banken betreffenden rechtlichen Vorgaben wie folgt:[5]

a) Gebot der Einfrierung von auf Bankkonten unterhaltenen Geldern und Vermögenswerten gelisteter Personen (Einfrierungsgebot)
b) Verbot der direkten oder indirekten Bereitstellung von Geldern und wirtschaftlichen Ressourcen an gelistete Personen (Bereitstellungsverbot)
c) Umgehungsverbot
d) Ausnahmen
e) bankübliche Verwaltung von Konten sanktionierter Personen
f) Genehmigungsverfahren
g) Meldepflichten der Normadressaten
h) Haftungsfreistellung der Normadressaten

Hinsichtlich der zu sanktionierenden Personen werden seit Verabschiedung z. B. der ersten „Taliban-Verordnung“ der EU[6] die Namen aller Mitglieder und Unterstützer der Taliban, al-Qaidas und Osama bin Ladens in einer dazugehörigen Sanktionsliste aufgeführt und im Rahmen von Folge- bzw. Änderungsverordnungen fortlaufend durch die Organe der EU aktualisiert. Hierdurch wird eine gezielte Ausrichtung von politischen Zwangsmaßnahmen der EU gegen natürliche und juristische Personen ermöglicht.[7] Seitdem enthalten fast alle „smarten“ Finanzsanktionsmaßnahmen der EU solche Listen sanktionierter Personen. Diese werden mit Rundschreiben des Servicezentrums Finanzsanktionen der Deutschen Bundesbank (BBk) regelmäßig an alle Kreditinstitute übermittelt.[8] Die Rundschreiben enthalten u. a. auch Berichtspflichten der Kreditinstitute gegenüber der BBk. Hervorzuheben sind die fristgebundenen Rückmeldungen an die BBk, ob und welche Gelder von EU-gelisteten Personen im Kundenbestand der Kreditinstitute von den Finanzsanktionsmaßnahmen der EU betroffen sind.

Ein verpflichtetes Institut, das im Rahmen seines institutsinternen Monitorings keinen oder einen mangelhaften Abgleich mit den EU-Listen durchführt und somit nicht auskunftsfähig ist, ob EU-gelistete Personen sich in seinem Kundenbestand befinden bzw. welche Vermögenswerte solcher Personen u. a. auf Konten und Depots unterhalten werden, begeht einen klaren Verstoß gegen den erwähnten sanktionsrechtlichen Vorgabenkatalog. Verstöße gegen diese Vorgaben werden beispielsweise im EU-Mitgliedstaat Deutschland insbesondere nach dem Außenwirtschaftsgesetz hart (u. a. mit bis zu zehn Jahren Freiheitsentzug) bestraft. Dahinter ist der Wille des EU-Verordnungsgebers erkennbar, die Maßnahmen wirksam, verhältnismäßig und abschreckend zu gestalten.[9]

---

[5] Vgl. de Vries, Anthonius W., European Union Sanctions against the Federal Republic of Yugoslavia from 1998 to 2000: A Special Exercise in Targeting, in: Cortright, David u. Lopez, George A. (Hrsg.), Smart Sanctions: Targeting Economic Statecraft, Lanham (Maryland) Oxford 2002, S. 96 ff. u. Ziff. 70 ff. Council-EU, Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy, 15114/05, PESC 1084, FIN 475, Brussels, 2 December 2005.

[6] Verordnung (EG) Nr. 467/2001 des Rates v. 06.03.2001 über das Verbot der Ausfuhr bestimmter Waren und Dienstleistungen nach Afghanistan, über die Ausweitung des Flugverbots und des Einfrierens von Geldern und anderen Finanzmitteln betreffend die Taliban von Afghanistan und zur Aufhebung der Verordnung (EG) Nr. 337/2000, in: EG-Amtsblatt L 67 v. 09.03.2001, S. 1 ff.

[7] Zu den problematischen Aspekten der (z. T. auch irrtümlichen) Listung von Personen und den Implikationen für die Menschen- und Freiheitsrechte siehe Feinäugle, Clemens A., Die Terroristenlisten des Sicherheitsrates – Endlich Rechtsschutz des Einzelnen gegen die Vereinten Nationen? ZRP 3/2007, S. 76 u. Ganguli, S. 93 ff., 175 ff. u. 270 ff.

[8] BBk, Servicezentrum Finanzsanktionen, https://www.bundesbank.de/Navigation/DE/Service/Finanzsanktionen/finanzsanktionen.html (Stand: 06.03.2018).

[9] Beispielhaft wird auf Erwägungsgrund 12 der Verordnung (EG) Nr. 2580/2001 des Rates v. 27.12.2001 über spezifische, gegen bestimmte Personen und Organisationen gerichtete restriktive Maßnahmen zur Bekämpfung des Terrorismus, in: EG-Amtsblatt Nr. L 344 v. 28.12.2001, S. 70 ff., verwiesen.

### Maßnahmendurchführung in der Genossenschaftlichen FinanzGruppe

Um sich gegen die erwähnten Risiken und Gefahren aus Normverstößen abzusichern, werden Zahlungsausgänge/-eingänge der Genossenschaftsbanken bzw. ihrer Kunden in das Ausland bzw. aus dem Ausland im Rahmen des Zahlungsverkehrs von der DZ BANK AG systemgestützt gegen die EU-Listen auf Sanktionsrelevanz und Terrorismusfinanzierungsverdacht überprüft.[10] Es wird dabei sichergestellt, dass a) die Maßnahmen des Sanktionsregimes der EU beachtet werden und b) die erbrachte Dienstleistung den rechtlichen Anforderungen entspricht.

Anzumerken ist, dass die DZ BANK AG mit der eingesetzten Prüfsoftware nur die von den Genossenschaftsbanken veranlassten Transaktionen auf Sanktionsrelevanz prüft. Die Kundenbestände sind dagegen von den Genossenschaftsbanken durch den Einsatz von Geno-SONAR zu überwachen bzw. beim Auftreten von Treffern zu überprüfen. Abgesehen von Geno-SONAR bietet das Bankenverfahren „agree“ der Fiducia & GAD IT AG eine Online-Embargoprüfung an, die bereits bei der Personenanlage ggf. einen entsprechenden Hinweis auf eine mögliche Namensübereinstimmung ausgibt. Die Online-Embargoprüfung muss über den Institutskennsatz der Bank aktiviert werden. Wenn der Mitarbeiter den Hinweis im Dialog bestätigt, wird dies im Hinweisprotokoll dokumentiert und kann jederzeit nachvollzogen werden. Insoweit liegen Kundenbestandsprüfungen und ggf. eine Positiv-/Negativmeldung an das zuständige BBk-Servicezentrum Finanzsanktionen sanktions- und außenwirtschaftsrechtlich im Verantwortungsbereich der Genossenschaftsbanken und nicht der DZ BANK AG.

Hinsichtlich der Überprüfung der Transaktionsströme ist noch Folgendes zu beachten: Sofern zu einem späteren Zeitpunkt weitere Rahmenbedingungen oder Listen für die Prüfung der Zahlungsverkehrsaufträge im Hinblick auf Verstöße gegen EU-Finanzsanktionen allgemein verpflichtend werden, behält sich die DZ BANK AG das Recht vor, a) unverzüglich die hierfür erforderlichen Maßnahmen zu treffen und b) die erforderlichen Prüfungen vorzunehmen.[11] Zahlungsverkehrsaufträge, bei denen ein Verdacht auf einen Finanzsanktionsverstoß besteht, werden von der DZ BANK AG zunächst angehalten und unverzüglich an die Genossenschaftsbank zur Entscheidung weitergeleitet. Die finale Entscheidungskompetenz, ob ein Verdacht auf einen Verstoß gegen EU-Finanzsanktionen im jeweiligen Einzelfall besteht, liegt bei der DZ BANK AG.

Derart betroffene Zahlungsverkehrsaufträge führt die DZ BANK AG ohne Erstellung von Buchungsdaten für die Dauer der Bearbeitung (auch über die Tagesgrenze hinaus) nicht aus, sondern bearbeitet die Aufträge nach Weisung der Personen, die die Genossenschaftsbank als Ansprechpartner gegenüber der DZ BANK AG benannt hat. Der weitere Prozess ist wie folgt:

a) Die DZ BANK AG informiert die Genossenschaftsbank zeitnah innerhalb der vereinbarten Fristen über einen Verdacht.
b) Die Genossenschaftsbank informiert die DZ BANK AG innerhalb der vereinbarten Fristen, wie mit den nicht ausgeführten Zahlungsverkehrsaufträgen weiter verfahren werden soll.
c) Bei ausbleibender Rückmeldung der Genossenschaftsbank an die DZ BANK AG innerhalb der vereinbarten Fristen behält sich die DZ BANK AG vor, die betreffenden Aufträge endgültig nicht auszuführen.

### Die besondere Rolle der GenoTec als Auslagerungsdienstleister

Als Auslagerungsdienstleister übernimmt die GenoTec für ihre Kunden (zumeist Genossenschaftsbanken) die vorgenannte und sanktionsrechtlich bedeutsame Kundenbestandsprüfung. Die dazugehörigen Prozesse zur Bearbeitung der BBk-Sanktionsrundschreiben sind in der GenoTec arbeitsanweislich geregelt und setzen bei allen beteiligten Personen ein umsichtiges Handeln voraus. Schließlich gilt es, die bereits erwähnten Compliance- und Strafbar- >

[10] Die nachfolgenden Ausführungen beruhen auf Erkenntnissen, die aus der Zahlungsverkehrspraxis und Maßnahmendurchführung in der Genossenschaftlichen FinanzGruppe stammen. Eine Gewähr für inhaltliche Vollständigkeit wird nicht übernommen. Zweifels- bzw. Klärungsfragen in Zusammenhang mit dem Zahlungsverkehr sollten daher direkt an die DZ BANK AG als Zahlungsverkehrsdienstleister gemäß Geldtransfer-Verordnung (Verordnung (EU) 2015/847 des Europäischen Parlaments und des Rates vom 20.05.2015 über die Übermittlung von Angaben bei Geldtransfers und zur Aufhebung der Verordnung (EU) Nr. 1781/2006, in: EU-Amtsblatt L 141 v. 05.06.2015, S. 1 ff.) adressiert werden.

[11] Wie bereits oben ausgeführt findet dabei keine Prüfung der Kunden- oder Kontenbestände der Primärbank statt.

keitsrisiken zu vermeiden und damit Schaden von der auslagernden Bank und ihren Mitarbeitern sowie auch von der GenoTec und ihren Mitarbeitern abzuwenden. Durch Einrichtung entsprechender Bearbeitungsprozesse in diesem Aufgabenbereich leistet die GenoTec für ihre Kunden einen wertvollen Beitrag zur rechtssicheren Durchführung der von der EU erlassenen Zwangsmaßnahmen.

Im Einzelnen geht die GenoTec wie folgt vor: Die Prüfung der Namenslisten erfolgt jeweils zentral für alle an einem Standort tätigen Beauftragten der Zentralen Stelle. Anzumerken ist, dass die in den Anlagen der einzelnen Rundschreiben veröffentlichten Personen und Institutionen (Sanktionslisten) spätestens mit Veröffentlichung in der Presse durch die Firma World-Check in die World-Check-Listen eingestellt[12] und dann von den Rechenzentralen nach Geno-SONAR übernommen werden. Durch die World-Check-Listen werden die Daten aus den EU-Finanzsanktionslisten nochmals angereichert, um eine zielgenauere Erkennung sanktionierter Personen im Kundenbestand im Rahmen des Listenabgleichs zu ermöglichen.

Kommt es im Zuge des Listenabgleichs zu einer eindeutigen Namensübereinstimmung oder einer nicht eindeutig zu klärenden Namensübereinstimmung, wird der zuständige Beauftragte der Zentralen Stelle umgehend intern informiert. Diese Fakten und die weiteren Maßnahmen des Beauftragten werden von ihm mit einer entsprechenden Meldung im System dokumentiert. Bei der weiteren Bearbeitung wird so disponiert, dass den Banken spätestens vier Arbeitstage vor Ablauf der von der BBk im Rundschreiben genannten Meldefrist eine Nachricht/Meldung zugestellt wird.[13] Damit ist die rechtzeitige Beantwortung an die BBk gewährleistet.Die Meldung an die jeweiligen Banken erfolgt grundsätzlich per Mail. Dabei wird die Mail systemisch generiert und von dem zuständigen Beauftragten an die jeweilige Bank versandt. Über die Übermittlung einer Nachricht an die BBk durch die Bank, die daraufhin zu erfolgen hat, wird der zuständige Bearbeiter in der GenoTec ebenfalls per Mail informiert. Damit ist der Informationskreislauf rechts- und prüfungssicher geschlossen.

Diese Vorgänge werden im Jahresbericht des Beauftragten der Zentralen Stelle ausgewertet. Hierdurch kann die Bank im Berichtszeitraum auf eine zusätzliche wertvolle Informationsquelle über die BBk-Rundschreiben zurückgreifen. Gleichzeitig erhält sie Kenntnis über potenzielle sanktionsrelevante Vorgänge und damit auch über den Stand der institutsinternen Sicherungsmaßnahmen in diesem Bereich.

Ferner bedeutsam ist der Umstand, dass die Finanzsanktionsverordnungen der EU selber keine Vorgaben zur Aufbewahrung der Unterlagen enthalten. Durch analoge Anwendung der gesetzlichen Aufbewahrungsfristen gemäß § 8 Geldwäschegesetz (fünf Jahre) wurde diese vom EU-Verordnungsgeber zu verantwortende „Rechtslücke“ jedoch geschlossen.

## Fazit

Mit der beschriebenen Vorgehensweise bzw. dem erläuterten Standard leistet die GenoTec einen Beitrag zur rechtskonformen und prüfungssicheren Durchführung der EU-Finanzsanktionsmaßnahmen. Sie dokumentiert damit zugleich ein verantwortungsvolles Handeln als Auslagerungs- und Mehrmandantendienstleister im Bereich Finanzsanktionen und Zentrale Stelle innerhalb der Genossenschaftlichen FinanzGruppe. ■

**AUTOR UND ANSPRECHPARTNER**

**Dr. Indranil Ganguli**
Leiter Zentrale Stelle,
E-Mail: indranil.ganguli@geno-tec.de

[12] Thomson Reuters World-Check, http://risksolutions.thomsonreuters.com/world-check-global?utm_source=RiskPortal&utm_medium=PPC&utm_campaign=00010YR_Risk-PPCLandingPages_Digital&utm_term=world%20check&elqCampaignId=998&gclid=EAIaIQobChMIjqrmh7Dk2QIVRl4ZCh1OlgyyEAAYASAAEgKu6PD_BwE&ef_id=WDBtngAABauWEw3d:20180311133147:s (Stand: 06.03.2018).

[13] Dies gilt grundsätzlich, sofern der Eingangszeitpunkt des BBk-Rundschreibens sowie die klärungsrelevanten Zuarbeiten durch weitere Dritte die Einhaltung der Frist möglich machen.

Geldwäscheprävention

# Bitcoin – Mythos und Realität


In letzter Zeit häufen sich in der Presse Artikel über Bitcoins und das Für und Wider dieser Kryptowährung. Was ist passiert?

Bitcoins – englisch sinngemäß für „digitale Münze“ – sind keineswegs neu. Vielmehr wurde das Zahlungssystem bereits vor fast einem Jahrzehnt, am 3. Januar 2009, eingeführt. Die Erfindung des Bitcoins stand im Zeichen eines wachsenden Misstrauens im Zuge der letzten Finanzkrise, die mit dem Zusammenbruch der US-amerikanischen Großbank Lehman Brothers am 15. September 2008 ihren Höhepunkt erreichte und die größte Wirtschaftskrise seit Generationen auslöste.

Der Bitcoin sollte dagegen ein Zahlungsmittel darstellen, das knapp war und das nicht von – fehlbaren – Notenbankern garantiert, sondern von – objektiven – Algorithmen gesteuert wurde.

Neben dem Bitcoin entstand eine Vielzahl an weiteren Kryptowährungen, derzeit ca. 600 an der Zahl. Diese tragen Namen wie Ethereum, Ripple, NEO, Stellar, Dash, IOTA oder Tether, um nur die größeren zu nennen. Den meisten Lesern werden diese Namen jedoch weitgehend unbekannt sein, was auch Ausdruck des Marktanteils von Bitcoin ist, der bei nahezu 90 % liegt.

Bevor die neuesten Entwicklungen und steuerlichen Auswirkungen des Bitcoin-Handels zur Sprache kommen, sollte ein Blick darauf gerichtet sein, wie überhaupt Bitcoins entstehen und welches die wichtigsten Begrifflichkeiten bei virtuellen Währungen sind.

## Funktionsweise

Sogenannte „Miner“ „schürfen“ im „Mining Pool“ neue Bitcoins, indem mit Hilfe von Computern kyptographische Aufgaben gelöst werden. In der Anfangsphase wurde weitgehend für den Eigenbedarf geschürft. Aufgrund der zunehmenden Komplexität und des damit verbundenen Energiebedarfs schürfen heute nur noch professionelle Miner. Sie bieten die Bitcoins auf einer Handelsplattform an und verdienen durch das „Mining“ gleichzeitig eine kleine Provision. Für diese hochkomplexen Aufgaben werden riesige Computerkapazitäten, meist lokalisiert in China, und enormer Speicherplatz benötigt. Durch den hohen Rechenaufwand werden unglaublich hohe Energiekosten produziert. Um dies annähernd zu verdeutlichen: Laut Berechnungen verbraucht das „Schürfen“ mehr Strom als die US-Großstädte Chicago und San Francisco im gleichen Zeitraum zusammen.

Die „Miner“ zeichnen validierte Transaktionen in einem „Block“ auf und transferieren diesen anschließend chronologisch in eine aufeinander aufbauende Kette von Blöcken, die, mit kryptographischen Hashes, verbunden die sog. „Blockchain“ bilden. In der Blockchain werden alle Bezahlvorgänge der Digitalwährung verschlüsselt und fälschungssicher dokumentiert. Die Blockchain ist ein kollektives, sicheres und dezentrales Buchhaltungssystem, englisch „Distributed Ledger Technology“ (DLT), aller Bitcoin-Transaktionen, die jemals getätigt wurden. Die Datenkette verlängert sich mit jeder Transaktion um ein weiteres Datenpaket und aktualisiert sich laufend selbst.

Der jeweilige Geldschöpfungsprozess ist allerdings limitiert. Die maximale Geldmenge bei Bitcoins ist durch das Netzwerkprotokoll auf 21 Millionen Einheiten festgelegt und ist nicht durch einzelne Teilnehmer beeinflussbar. Diese Obergrenze soll im Jahr 2130 erreicht sein.

Die „Wallets“ (elektronische Geldbörsen) dienen der Aufbewahrung der virtuellen Währung und werden auf dem Computer oder auch auf dem Smartphone gespeichert. >


Die Währung besteht aus Zahlencodes, die sich mit jeder Transaktion neu verschlüsseln und dadurch sehr fälschungssicher sind. Eine Wallet kann z. B. eine App für ein Smartphone sein, die aus einem App-Store heruntergeladen werden kann.

### Nicht dasselbe, aber das Gleiche

Die erläuterte Funktionsweise verdeutlicht, dass der Bitcoin von keiner Zentralbank oder öffentlichen Stelle emittiert wird und an keine traditionelle Währung geknüpft ist. Das Bitcoin-System unterliegt auch keiner geographischen Beschränkung – ein Internetzugang genügt – und kann länderübergreifend als Zahlungssystem mit Hilfe einer Open-Source-Software eingesetzt werden.

Der Bitcoin wird von natürlichen oder juristischen Personen als Zahlungsmittel akzeptiert und kann auf elektronischem Wege übertragen, gespeichert und gehandelt werden. Weitere Vorteile sind die sehr niedrigen Gebühren, gepaart mit irreversiblen und schnellen Transaktionen.

Dieser Entwicklung folgend stellte das BMF-Schreiben vom 7. Februar 2018 – III C 3 – S 7433/15/10001 (2018/0108025) unter Berücksichtigung des Gleichbehandlungsgrundsatzes klar: „Sog. virtuelle Währungen (Kryptowährungen, z. B. Bitcoin) werden den gesetzlichen Zahlungsmitteln gleichgestellt, soweit diese sog. virtuellen Währungen von den an der Transaktion Beteiligten als alternatives vertragliches und unmittelbares Zahlungsmittel akzeptiert worden sind und keinem anderen Zweck als der Verwendung als Zahlungsmittel dienen.“ Dementsprechend ist der Umtausch von virtuellen Währungen in gesetzliche Zahlungsmittel und umgekehrt steuerbefreit.

Zusammenfassend liegen die Vorteile der Bitcoins in der Technologie. Sie bietet bis zu einem gewissen Grad Anonymität sowie Schutz vor Inflation, vor Währungszusammenbrüchen und vor Bankpleiten.

### Bitcoin – Eldorado für krumme Geschäfte?

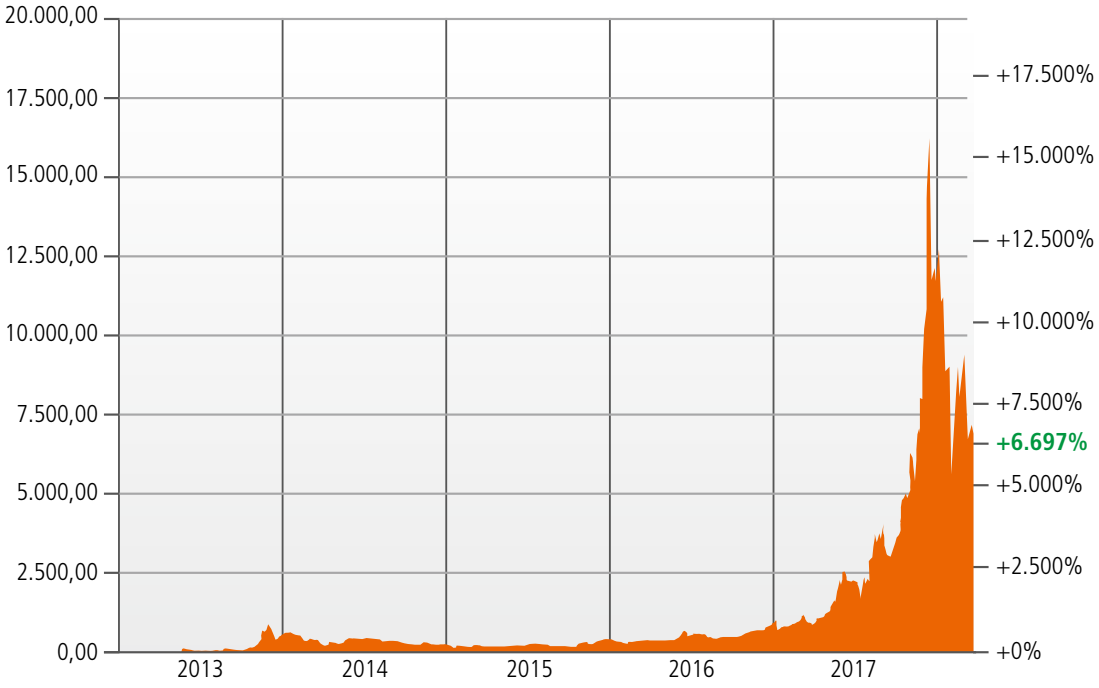
Ungeachtet der Vorteile werden von den Aufsichtsorganen weltweit in einem lauter werdenden Chor Maßnahmen zur Regulierung der Kryptowährung gefordert. Eine mögliche Verwendung von Bitcoins für kriminelle Machenschaften soll unterbunden werden.

Tatsächlich dienen Bitcoins der Bezahlung krimineller Produkte und Dienste im Darknet, wie z. B. für Waffen, illegale Drogen, Terrorismus, Pornografie und auch Erpressertrojaner. Die Politik und die Finanzaufsicht bereiten daher Maßnahmen vor, um sowohl Verbraucher als auch Anleger zu schützen.

### Trotzdem eine attraktive Anlagemöglichkeit?

Aber der Bitcoin wird auch ganz anders genutzt, z. B. für Spekulationsgeschäfte. Geld sucht sich – zumal in einer langanhaltenden Niedrigzinsphase – immer neue, möglichst lukrative Anlagemöglichkeiten. Nach Aktien, Immobilien, Schiffscontainern etc. folgt der Bitcoin als vermeintlicher Star am Börsenfirmament. Nachdem einige Terminbörsen den Handel für Futures auf Bitcoin öffneten, wurde dieser auch für den Massenmarkt attraktiv. Der Bitcoin wurde zum Straßengespräch unter Laien – oft genug ein Hinweis, die Finger davon zu lassen.

Abb. 1 CHART BITCOIN – EURO IN DEN LETZTEN 5 JAHREN




Quelle: www.finanzen.net, Stand 31. Januar 2018

Die Warner jedoch mehren sich. Unlängst hat Bundesbankpräsident Jens Weidmann seine Warnung vor solchen Investments nochmals verschärft: „Wer sie kauft, riskiert Verluste, möglicherweise sogar den Totalverlust", da eine Wertbasis fehle. Der Einstieg von Spekulanten, die Bitcoin nicht als Zahlungsmittel erwerben, führte bereits zu erheblichen Kursschwankungen und Blasen, vergleichbar mit anderen hochvolatilen und risikoreichen Finanzinstrumenten. Dies kann erhebliche Gewinne, aber auch Verluste nach sich ziehen.

Die steuerlichen Konsequenzen werden nachfolgend ausgeführt.

**Auswirkungen bei Veräußerungsgewinnen**

Im Gegensatz zu heutigen Anlagen in Wertpapieren, die grundsätzlich der Abgeltungssteuer von 25 % unterliegen, gilt für Cyber-Währungen wie für Gold, Fremdwährungen oder Oldtimer die Besteuerung privater Veräußerungsgeschäfte gemäß § 23 EStG, auch Spekulationsgeschäfte genannt. Wer Bitcoins u. Ä. über eine Handelsplattform kauft und später wieder in Euro umtauscht und einen Veräußerungsgewinn erzielt, unterliegt bisher den gleichen steuerlichen Anforderungen wie beispielsweise ein Goldbesitzer. Einen Gewinn, der über der Freigrenze von 599,99 Euro liegt, müssen Käufer daher nur dann mit dem individuellen Steuersatz versteuern, sofern dieser binnen Jahresfrist anfällt. Nach der Jahresfrist können sämtliche Veräußerungsgewinne komplett steuerfrei vereinnahmt werden.

Wer beispielsweise im Oktober 2015 drei Bitcoins im Wert von je 300 Euro gekauft hatte und diese im Dezember 2017 für 18.000 Euro wieder verkaufte, konnte 53.100 Euro steuerfrei vereinnahmen. Wäre dieser Gewinn binnen Jahresfrist angefallen, hätte der Fiskus je nach persönlichem Einkommenssteuersatz bis zu 22.302 Euro Steuern verlangt plus Solidaritätszuschlag und ggf. Kirchensteuer.

>


**Auswirkungen bei Veräußerungsverlusten**

Angesichts des Hypes um die virtuellen Währungen sind jedoch viele Anleger zu spät, oft über Handelsplattformen im Ausland, in den Kryptomarkt eingestiegen. Nach dem Kurssturz im Dezember 2017 ist die Veräußerung derzeit mit hohen Verlusten verbunden. Die Abbildung 1 verdeutlicht auf einer 5-Jahres-Basis, welche exorbitante Wertentwicklung, gepaart mit einer äußerst hohen Volatilität, der Bitcoin gerade seit 2017 hinter sich gelegt hat.

Der Fiskus akzeptiert jedoch auch Verluste innerhalb der Jahresfrist, die, genauso wie die Gewinne, in der Einkommenssteuererklärung in der Anlage „Sonstige Einkünfte“ anzugeben sind. Damit lassen sich die Verluste aus dem Bitcoin-Handel mit anderen Gewinnen gegenrechnen, entweder mit Gewinnen aus dem Vorjahr oder als Verlustvortrag mit künftigen Gewinnen. Dies greift aber nur, wenn Gewinne und Verluste jeweils ebenfalls aus privaten Veräußerungsgeschäften stammen.

Damit sind Spekulationsverluste aus Bitcoin-Käufen nur mit Gewinnen aus Bitcoin-Verkäufen oder anderen Spekulationsgeschäften verrechenbar (z. B. Immobilien, Edelmetalle), nicht aber beispielsweise mit Gewinnen aus Aktiengeschäften. Ein automatisches Vorgehen wie bei der Abgeltungssteuer, die bei Zinseinkünften oder Wertpapiergeschäften greift, gibt es hier nicht.

**Ausblick**

Der gesamte Marktwert von Kryptowährungen liegt nach Einschätzung von Experten in der Spitze bislang bei weniger als einem Prozent des Volumens der Weltwirtschaft. Folglich erachteten die G20-Finanzminister und -Notenbankchefs im März 2018 bei ihrem Treffen in Buenos Aires Bitcoin & Co als nicht bedeutend genug, um die Finanzmärkte zu gefährden.

Trotzdem reagieren Regulierungsbehörden weltweit: Die Anforderungen an Kryptowährungen steigen, was sich u. a. an bereits umgesetzten oder geplanten Regularien abzeichnet.

So könnten Plattformen, auf denen sie gehandelt werden, unter die Finanzaufsicht fallen. Die Nutzer müssten dann, wie beim Eröffnen eines Bankkontos per Post- oder Videoident, ihre Identität offenlegen. Die EU hat bereits eine Richtlinie verabschiedet, die genau das vorsieht. Nun ist es an den Mitgliedstaaten, sie umzusetzen. Eindämmen wird man Geldwäsche und Terrorfinanzierung durch Kryptowährungen aber nur, wenn diese Regeln auch international gelten. ▬

AUTOR UND ANSPRECHPARTNER

**Lars Schinnerling**
Stv. Leiter Interne Revision,
E-Mail: lars.schinnerling@geno-tec.de

## Berichterstattung der GenoTec

# Interne Revision

Der Jahresprüfungsplan 2017 wurde erfüllt. Seit der letzten Berichterstattung in der Point of Compliance (3/2017, S. 31) wurden der IT-Revisionsbericht, der Revisionsbericht zur Zentralen Stelle sowie der Jahresrevisionsbericht 2017 und der Revisions-Quartalsbericht 4/2017 erstellt und an die jeweiligen Kunden verschickt.

Die Revisionsberichte zum Vertriebsmanagement und zum Hinweisgebersystem sind fertig und liegen der Geschäftsführung vor. Der Revisionsbericht zum Hinweisgebersystem wird ebenfalls den jeweiligen Kunden übermittelt werden.

Des Weiteren wurde quartalsmäßig ein Follow-up-Bericht erstellt, in dem die Abarbeitung der getroffenen Maßnahmen/Empfehlungen dokumentiert wird. In vorausgegangenen Prüfungen getroffene Feststellungen wurden weitestgehend abgearbeitet. Der Follow-up-Bericht wird regelmäßig mit der Geschäftsführung besprochen. Darüber hinaus erfolgte im Dezember 2017 eine persönliche Information der Gesellschafterversammlung über den Status quo sowie eine Information des Kundenbeirates im März 2018 über den Stand der Prüfungen und deren Ergebnisse.

Die Entscheidung über die Auswahl einer externen Prüfungsgesellschaft zur Prüfung unseres DIKS nach IDW PS 951 bzw. PS 331 ist gefallen. Es ist eine der „Big Four" der Prüfungsgesellschaften; das Auftaktgespräch ist bereits erfolgt. Nach Abschluss der Prüfungen wird den jeweiligen Kunden der externe Prüfungsbericht unaufgefordert zugesandt. ▬

*Ansprechpartner:* ***RA Jörg Scharditzky,*** *Leiter Interne Revision, E-Mail: joerg.scharditzky@geno-tec.de*

# Wirtschaftliche Lage

Wie erwartet ist die Geschäftsentwicklung der GenoTec in 2017 positiv verlaufen. Mit einem Betriebsergebnis von +563 TEUR wurde sowohl das Vorjahresergebnis (+171 TEUR) als auch das Planergebnis (+18 TEUR) überschritten.

Der Trend setzte sich zu Beginn des Jahres 2018 fort: Die ersten beiden Monate sind im Vergleich zum Plan und zum Vorjahr positiv verlaufen. Das kumulative Ergebnis liegt im Februar deutlich über dem Plan. Die Planüberschreitungen resultieren insbesondere aus einer deutlich gestiegenen Nachfrage in den Bereichen Informationssicherheit und Datenschutz sowie Zentrale Stelle.

Die Liquiditätssituation ist unverändert entspannt und liegt deutlich über dem eingezahlten Kapital, die wirtschaftliche Lage der GenoTec ist stabil.

Die regulativen Änderungen im Zuge der neuen MaRisk, MiFID II und der 4. Geldwäscherichtlinie sind in die Prozesse und Systeme eingearbeitet. Die diesjährigen Risikoanalysen und Kontrollen sind vollumfänglich auf die neuen Anforderungen angepasst. Gleichermaßen werden derzeit die Prozesse und Systeme bzgl. der EU-DSGVO angepasst, so dass auch hier die ausgelagerten Prozesse zeitgerecht auf die neuen Anforderungen umgestellt sind.

▬

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