Creditreform Compliance

Compliance & Risk Newsletter

Ausgabe II/2020
Juli 2020

Inhaltsverzeichnis

Covid-19: Nichts wird mehr so sein, wie es war – auch im Management?!

Die aktuelle Corona-Krise hat – obwohl wir uns noch mittendrin befinden und es noch nicht klar ist, welche weiteren sowohl wirtschaftlichen als auch sozialen Auswirkungen sich noch ergeben werden – in ihrer Intensität bei vielen Unternehmen große Änderungen und Maßnahmen hervorgerufen. Und das Ganze in einer nicht geahnten Intensität und in äußerst kurzer Zeit. Manche Unternehmen haben innerhalb kurzer Zeit ihr Geschäftsmodell über den Haufen geworfen und sind nun vornehmlich im E-Business tätig oder sind auf die Produktion von Masken und sonstigem persönlichen Schutzbedarf (PSA) umgestiegen. Fast schon normal ist es geworden, dass alle oder zumindest ein Großteil der Mitarbeiter innerhalb kürzester Zeit vom Homeoffice aus arbeiten. Genauso normal wurden und werden in der Politik die immer größer werdenden Rettungspakete, die schon jetzt die Volumina der Finanzkrise 2008 locker übertroffen haben.

Im Folgenden werden einige Gedankenanstöße hinsichtlich systematischen Fehlern, Verzerrungen und Trugschlüssen in der Entscheidungsfindung und im Management dargestellt, die im aktuellen Marktumfeld erstaunlich häufig wieder auftreten. *Diese Fehler, Verzerrungen und Irrtümer sind dem Buch „Risiko im Management" (Springer 2019, ISBN 978-3-658-25834-4) entnommen, das insgesamt 100 verschiedene Ausprägungsformen darstellt!*

Zu starker Fokus auf historischen Daten

Viel zu oft werden zentrale Zukunftsentscheidungen immer noch rein oder vornehmlich auf Basis von historischen Daten getroffen. Dies mag zielführend sein, wenn die Vergangenheit repräsentativ für die Zukunft ist. In der aktuellen Situation, in der an vielen Ecken und Ecken die Rede ist von Digitalisierung und der Disruption bestehender Geschäftsmodelle, in der es große Unsicherheiten aufgrund des Klimawandels und der wirtschaftlichen Folgen des European Green Deals gibt und Branchen wie der Einzelhandel, die Automobil- und Finanzbranche, aber auch die Unterhaltungs- und Reisebranche vor einer ungewissen Zukunft stehen, sollten auch alternative Zukunftsprojektionen erlaubt sein.

© Adobe Stock / Patrick Daxenbichler

Ein Artikel der Harvard Business Review aus dem Jahr 2017 forderte deshalb, dass Manager mehr Science Fiction lesen sollten (vgl. Peper 2017). Als Beispiel wird aufgeführt, dass die Stadt New York Ende des 19. Jahrhunderts aufgrund der 145.000 Pferde, die wiederum 45.000 Tonnen Dünger pro Monat produzierten, „zum Himmel stank". Stadtplaner und Experten kamen aus aller Welt, um nach einer Lösung für dieses Problem zu suchen. 14 Jahre später löste es sich quasi von allein durch die weite Verbreitung des Automobils. Es scheint zwar aktuell nur schwer denkbar, dass eine Pandemie wie Covid-19 sich vollständig und für immer auflöst, bleibt doch eine latente Gefährdung aufgrund der Globalisierung für ähnliche Konstellationen, selbst wenn ein Impfstoff gefunden wird. Ein wahrer Game Changer – wie im Beispiel des New Yorks des 19. Jahrhunderts – könnte allerdings eine flächendeckende Frühdiagnostik werden, die mögliche Infektionen früh zu erkennen hilft und Ausbreitungen damit verhindert oder zumindest dramatisch verlangsamt, wodurch

wiederum die Notwendigkeit großangelegter Lockdowns drastisch abnimmt.

Inflation der „schwarzen Schwäne“

Durch den Bestseller „Der schwarze Schwan“ von Nassim Taleb hat dieser Begriff speziell im Risikomanagement eine sehr große Bekanntheit erlangt und es wurden viele Ansatzpunkte für den Umgang beziehungsweise die Vermeidung solcher Extremereignisse diskutiert. Gleichzeitig kann man aber auch immer häufiger vernehmen, dass auch „normale“ Probleme schnell als unvorhersehbare „schwarze Schwäne“ klassifiziert werden, um ein mögliches Führungsversagen unter den Teppich zu kehren.

Natürlich gibt es gute Gründe, die Corona-Pandemie als schwarzen Schwan zu klassifizieren. Es kommt aber dabei auf eine sehr genaue Prüfung an. Denn einige Missstände und Fehlentscheidungen wurden auch unabhängig von Corona schlagend – die Krise hat höchstens den Zeitpunkt vorgezogen. Außerdem konnten die Einflussfaktoren der jetzigen Krise nicht nur mit verblüffender Ähnlichkeit bereits in der Phantasie Hollywoods im Film „Contagion“ im Jahr 2011 konstruiert werden, sondern auch in einer Risikoanalyse mit dem Titel „Pandemie durch Virus Modi-Sars“ der Bundesregierung aus dem Jahr 2012.

Viel wichtiger als ein Ereignis wie Covid-19 und die wirtschaftlichen und sozialen Folgen des weltweiten Lockdowns präzise vorherzusagen, ist es aber, darauf vorbereitet zu sein und im Falle eines Schadenseintritts „antifragil“ zu sein, also nicht so leicht verwundbar.

Fehlende Antifragilität und/oder Resilienz

Bei den Ansätzen der Resilienz und der Antifragilität geht es darum, einerseits die Rahmenbedingungen so zu schaffen, dass kein Dominoeffekt entstehen kann beziehungsweise dass keine existenzbedrohenden Schäden durch Dominoeffekte entstehen. Andererseits ist ein weiteres, sicherlich sehr hehres Ziel – speziell bei der Antifragilität im Vergleich zur eher starren Resilienz und Robustheit – mit jedem Schaden und mit jedem Schock noch besser zu werden. Das heißt, der Umgang mit Fehlern und eine gelebte Fehlerkultur spielen hier eine zentrale Rolle.

Wenngleich es für die meisten Unternehmen noch ein größerer Schritt sein dürfte, bis die Ansätze der Antifragilität und Resilienz umgesetzt sind, sollten sie „im Kopf schon einmal umparken“ und sich darauf einstellen, nicht sämtliche Energie darauf zu verwenden, die Prognosen – die ohnehin nie gänzlich korrekt sein können – bis ins Detail zu perfektionieren, sondern vielmehr alternative Maßnahmenpläne im Sinne von Wenn-Dann-Überlegungen vorzubereiten. Denn im Endeffekt ist es für ein Unternehmen egal, ob der Auslöser eines Umsatzeinbruchs und einer möglichen Liquiditätsklemme mit erhöhten Ausfällen der Kunden nun eine weltweite Pandemie, eine Bankenkrise oder ein Terroranschlag ist.

Weitere Beispiele für Fehler und Verzerrungen, die im Buch dargestellt werden, und sehr gut auf die aktuelle Situation übertragen werden können, sind unter anderem:

- Der Volvo-Irrtum: auch bekannt als „anekdotischer Fehlschluss“ und die Tatsache, dass Geschichten stärker wirken als Fakten.

- Mathematisierung der Zukunft: Die Illusion, alles erklären zu können, sobald ein konkreter Zahlenwert verfügbar ist.
- Die Welt als „Random Walk"? Glücksspiel á la Monte Carlo oder doch eher Kausalität?
- Alpha- und Beta-Fehler oder: die Illusion, alle Risiken zu vermeiden sei gut.
- Verfügbarkeitsheuristik: was lange genug wiederholt wird, wird irgendwann als plausibel wahrgenommen.
- Mentale Buchführung: Warum Geldbeträge für uns, subjektiv betrachtet, unterschiedliche Werte einnehmen können.
- Isoliertes Paralleluniversum: Warum Informationen nie in Silos gelagert werden dürfen.
- Umgang mit unangenehmen Wahrheiten: Nichts tut so weh wie die Wahrheit!

Fazit

Systematische Denkfehler führen speziell in der Entscheidungsfindung des Managements zu Verzerrungen und Irrwegen. Es gibt allerdings auch Auswege, wie die zahlreichen Tipps und praktischen Tricks zu den einzelnen Irrtümern und Unschärfen gezeigt haben. Dies ist auch sehr wichtig, wenn man bedenkt, welche strategische Tragweite die meisten unternehmerischen Entscheidungen haben bzw. haben können. Denn die eingangs beschriebene Schnelligkeit in der Entscheidungsfindung und der Anpassung von Strategien und Geschäftsmodellen sorgt auch dafür, dass Fehler besonders teuer oder gar existenzbedrohend werden können.

(Dr. Christian Glaser, Generalbevollmächtigter der Würth Leasing GmbH & Co. KG)

Nachweisbarer Datenschutz ist gar nicht so schwierig mit einem Datenschutz-IKS!

Alle Unternehmen, die personenbezogene Daten verarbeiten, müssen die Einhaltung datenschutzrechtlicher Vorgaben sicherstellen und dafür entsprechende Dokumentation bereitstellen. Dies ist eindeutig aus Art. 5 Abs. 2 der DSGVO zu entnehmen. Allein das Vorhandensein von Regelungen zum Datenschutz und die Benennung eines Datenschutzbeauftragten stellen nicht sicher, dass die Regelungen funktionsfähig sind und die Vorgaben von allen Mitarbeitern wirksam eingehalten werden. Die Geschäftsführung ist zwar per Gesetz verantwortlich für die Einhaltung der datenschutzrechtlichen Vorgaben, kann aber oftmals selber aufgrund fehlender Nachweise keine messbare Einschätzung zum Einhaltungsgrad abgeben. Gerade wenn ein Unternehmen als Dienstleister im Sinn von Art. 28 DSGVO (Auftragsverarbeiter) tätig ist, muss diese Nachweisbarkeit aber auch gegenüber dem Auftraggeber gewährleistet werden. Viele Unternehmen, welche die Verarbeitung von personenbezogenen Daten als Dienstleistungen anbieten, werden inzwischen von ihren Auftraggebern angehalten, qualifizierte Bestätigungen zur Einhaltung des Datenschutzes abzugeben.

Datenschutz-IKS einführen

In der Praxis kann eine solche Nachweisbarkeit gut herbeigeführt werden, wenn Datenschutzkontrollen in tägliche Abläufe integriert werden. Interne Kontrollen für wesentliche Elemente des Datenschutzes können als Datenschutz-Kontrollsystem (Datenschutz-IKS) wirken. Das Datenschutz-IKS beinhaltet Kontrollen, die in alle datenschutzrelevanten (Teil-) Prozesse des Unternehmens integriert werden. Dokumentationen und Nachweise werden zeitnah in Prozessen mitgeführt und sind dann einfach in ihrer Wirksamkeit beurteilbar. Gut zu verdeutlichen ist dies am Beispiel der Einholung von Verschwiegenheitserklärungen für neue Mitarbeiter:

- Wird bereits ein Nachweis durch den Personalbereich über die Einholung einer solchen Verschwiegenheitserklärung geführt, kann sehr einfach die Fehlerquote und damit der Wirkungsgrad der Umsetzung der Vorgaben objektiv gemessen werden.

Welches wichtige Kontrollen sind, kann aus dem Prüfungshinweis des Instituts der Wirtschaftsprüfer in Deutschland e.V. „Prüfung der Grundsätze, Verfahren und Maßnahmen nach der EU-Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz (IDW PH 9.860.1) entnommen werden. Bei Auftragsverarbeitern müssen interne Kontrollen im Hinblick auf die Nachweisbarkeit des Datenschutzes in der Tätigkeit für andere Unternehmen mindestens in Prozessen und Unternehmensbereichen vorhanden sein, die zur Dienstleistungserbringung relevant sind.
Der Mindestumfang des Datenschutz-IKS ist ebenfalls gut aus der Verantwortlichkeitsabgrenzung zwischen Auftraggeber und Auftragnehmer abzuleiten. Regelungen, die typischerweise durch den Auftraggeber umzusetzen sind, sind nicht zwingend Gegenstand des Datenschutz-IKS beim Auftragnehmer. Demnach sind beispielsweise die Umsetzung der Informationspflichten gegenüber den Betroffenen oder die Durchführung von Datenschutz-Folgenabschätzungen direkt beim Auftraggeber anzuordnen und zu beurteilen.
Als Auftragsverarbeiter sollten mindestens die nachfolgenden Kriterien prüfbar als Mindestumfang eines Datenschutz-IKS aufgenommen werden:

- Benennung eines Datenschutzbeauftragten und Erfüllungsgrad der gesetzlich geforderten Tätigkeiten
- Beauftragung und vertragliche Regelungen von Unterauftragnehmern in Bezug auf die relevante Dienstleistung, ggf. einschließlich Datenübermittlung in Drittländer
- Prozesse zum Umgang mit Datenschutzvorfällen und Meldung an den Auftraggeber
- Schulung bzw. Sensibilisierung der Mitarbeiter zum Datenschutz

- Technische und organisatorische Datenschutz-Maßnahmen in Bezug auf die relevante Dienstleistung
- Bei Entwicklungen von Software (als Gegenstand der Dienstleistung): Umsetzung der Prinzipien - Privacy by Design und Privacy by Default
- Datenschutzgerechte Löschung / Vernichtung personenbezogener Daten der Auftragsverarbeitung
- Führung eines Verzeichnisses über Verarbeitungstätigkeiten hinsichtlich der relevanten Dienstleistung

© Adobe Stock / maxkabakov

Wirksamkeit im laufenden Betrieb beurteilen / Einführung unterstützen

Für die Wirksamkeit sind unterschiedliche Nachweise relevant. Die Einholung einer Verschwiegenheitserklärung wird jeweils im Einstellungsprozess nachweisbar sein, ein ausreichender Kenntnisstand des Datenschutzbeauftragten sollte durch Fortbildungsnachweise belegbar sein.

Effizient kann die Einführung eines Kontrollsystems insbesondere durch einen Berater oder Datenschutzauditor unterstützt werden, der aufgrund seiner Erfahrungen hier angemessene Vorgaben für das spezifische Unternehmen mitbringen wird, so dass Regelungen weder überfrachtend und damit ineffizient sind noch notwendige Regelungen vergessen bzw. missachtet werden. Darüber hinaus kann dieser z.B. einmal jährlich bei der internen Wirksamkeitsprüfung unterstützen oder alternativ die Wirksamkeit und Funktionsfähigkeit des internen Datenschutzkontrollsystems im Rahmen eines Audits bestätigen. Da in den meisten Unternehmen die Mitarbeiter zeitlich im Tagesablauf ausgelastet sein dürften, ist der Einsatz eines Beraters oftmals eine gute Möglichkeit den Aufwand und die Belastung für die Mitarbeiter bei der Einführung eines solchen internen Kontrollsystems überschaubar zu halten.

Vorteile eines Datenschutz-IKS

Vorteile eines Datenschutz-IKS ergeben sich in mehrfacher Hinsicht: Die Geschäftsführung eines Unternehmens kann jederzeit die Wirksamkeit des Datenschutzes mittels objektiver Nachweise bewerten und mit überschaubarem Aufwand durch eine (externe) Prüfung bestätigen lassen. Mit dem Nachweis eines „geprüften Datenschutzes“ kann für die Dienstleistungen geworben werden und den häufig vereinbarten vertraglichen Regelungen mühelos nachgekommen werden. Oftmals wird nämlich vom Auftragnehmer eine qualifizierte Prüfungsbestätigung erwartet, um nicht dem eigenen Prüfrecht vor Ort nachkommen zu müssen. Nachweise werden oftmals schon in der Phase der Auswahl eines Dienstleisters erwartet und danach jährlich angefordert, um ein effektives Auslagerungscontrolling sicherzustellen.

Auch im Rahmen von Jahresabschlussprüfungen beim Auftraggeber kann das Vorliegen von qualifizierten Prüfungsbestätigungen die vereinfachte Nachweisführung zum Datenschutz unterstützen und dadurch Kosten sparen.

Skalierbarkeit einer Prüfung des Datenschutz-IKS

Eine Prüfung zur Bestätigung der Datenschutzeinhaltung im Unternehmen kann bei Bedarf auch skaliert, d.h. nach Prüfungsthemen aufgeteilt werden. Zuerst kann die Angemessenheit der Regelungen und danach ihre Wirksamkeit beurteilt werden. Damit ist die finanzielle und aufwandstechnische Belastung im Unternehmen zeitlich verteilt und besser tragbar. Ähnlich der Vorgehensweise von ISO Zertifizierungen kann im Jahr nach der Erstzertifizierung/Erstprüfung mit relativ geringem Aufwand die weitere Wirksamkeit der Maßnahmen bestätigt werden.

Für Auftragsverarbeiter stellt die Einführung eines Datenschutz-IKS eine empfehlenswerte Möglichkeit dar, vorhandene Datenschutzmaßnahmen besser beurteilbar zu gestalten und somit für mögliche bzw. bestehende Auftraggeber die Qualität und die Risiken einer Beauftragung besser einschätzen zu können. Insbesondere bei der nicht delegierbaren Haftung, die sich durch die Verarbeitung von personenbezogenen Daten für den Auftraggeber (Verantwortlichen) ergibt, ist dies ein entscheidendes Kriterium der Risikobeurteilung.

Zur Nachweisbarkeit eines angemessenen Datenschutzniveaus kommt außerdem die Auditierung durch eine unabhängige Stelle in Betracht. Die Creditreform Compliance Services GmbH (CCS) führt Datenschutzaudits zur Erteilung des Compliance-Certs Datenschutz auf Basis der gesetzlichen Vorgaben der EU-Datenschutz-Grundverordnung (DSGVO) sowie des Bundesdatenschutzgesetzes (BDSG) durch und lehnt sich dabei an das von der 98. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 05. bis 07. November 2019 in Trier beschlossenen Standard-Datenschutzmodell Version 2.0 an. Die Auditoren der CCS sind speziell ausgebildete Juristen und verfügen über eine gültige TÜV-Zertifizierung zum Datenschutz-Auditor oder ähnliche Qualifikationen. Des Weiteren beziehen die Auditoren der CCS ihr umfangreiches Fachwissen aus langjähriger Datenschutz-Beratungspraxis und Revisionserfahrung und orientieren sich bei der Prüfung von Datenschutzmanagementsystemen an bewährten Best-Practice Ansätzen.

(Linda Liesum, Sachverständige für Wirtschaftskriminalität und Compliance)

Update zum Verbandssanktionengesetz – Referentenentwurf und erste Stellungnahmen

Am 22.04.2020 veröffentlichte das Bundesministerium der Justiz und für Verbraucherschutz den offiziellen Referentenentwurf zum „Gesetz zur Stärkung der Integrität in der Wirtschaft (Verbandssanktionengesetz – VerSanG)". Bereits hier gab es die erste Änderung, denn die bisherige Bezeichnung „Gesetz zur Bekämpfung der Unternehmenskriminalität" wurde verworfen und durch die Bezeichnung „Gesetz zur Stärkung der Integrität in der Wirtschaft" ersetzt. Eine weitere Änderung von Bezeichnungen durchlief die „Verbandsstraftat". Dieser Begriff wurde durch die „Verbandstat" ersetzt. Beide Änderungen der Begrifflichkeiten ziehen keine inhaltlichen Änderungen nach sich, zeigen jedoch einen durchaus milderen Ton, den auch die nachfolgenden Änderungen weiter unterstreichen.

So wurde darüber hinaus der Anwendungsbereich des Gesetzes beschränkt. Gemäß § 1 VerSanG-RefE sind nur noch Verbände mit einem **wirtschaftlichen Zweck** vom Anwendungsbereich erfasst. Gemeinnützige Organisationen und Unternehmen, die hoheitliche Aufgaben erfüllen, sind demnach vom Anwendungsbereich des VerSanG ausgeschlossen und unterfallen lediglich weiterhin dem Ordnungswidrigkeitengesetz (OWiG). Auch dies stellt eine „Milderung" im Vergleich zum „inoffiziellen" Entwurf aus August 2019 dar. Genau diese Änderung wirft eine ketzerische Frage auf: Sollten nicht gerade gemeinnützige und öffentliche Unternehmen besonderen Wert auf Compliance legen?

Des Weiteren wurde die ultima ratio der **Verbandsauflösung** aus dem Repertoire der Sanktions-möglichkeiten gestrichen. Es verbleibt die sog. Verbandsgeldsanktion, die pauschal oder in Abhängigkeit vom Umsatz festgelegt wird und sich zudem auch auf den Konzernumsatz beziehen kann.

Auf der anderen Seite „soll" das Gericht nun im Fall einer zu verhandelnden Verbandstat von der Möglichkeit der **Milderung der Sanktionen** Gebrauch machen, wenn die Voraussetzungen wie bspw. eine ununterbrochene und uneingeschränkte Zusammenarbeit des beschuldigten Verbandes mit den ermittelnden Behörden gewährleistet wird. Bislang „konnte" das Gericht nach eigenem Ermessen von der Milderungsoption Gebrauch machen.

Nichts desto trotz **kritisieren** bspw. sowohl die Deutsche Kreditwirtschaft (DK), als auch das Deutsche Institut für Compliance (DICO) in vielen Teilen die Schärfe des Referentenentwurfs. So wird u.a. die schuldunabhängige Konzernhaftung aus § 9 Abs. 2 VerSanG-RefE kritisiert. Außerdem ginge die Definition der Verbandstat als eine Straftat, durch die Pflichten, die den Verband treffen, verletzt worden sind oder durch die der Verband bereichert worden ist oder werden sollte [...] zu weit – eine Orientierung am Begriff der Wirtschaftskriminalität sei sinnvoller und verhältnismäßiger. Darüber hinaus wird darauf hingewiesen, dass erst in der Gesetzesbegründung Rolle und Wirkung von Compliance-Management-Systemen mit Blick auf Verbandstaten dargestellt werden. Eine konkrete Benennung als Präventionsmechanismus im Referentenentwurf blieb jedoch aus.

Sicherlich werden noch weitere Verbände zum aktuellen Referentenentwurf Stellung nehmen. Die Einführung eines Unternehmensstrafrechts würde eine große Veränderung der Deutschen Rechtskultur herbeiführen und sollte daher natürlich stark diskutiert und Chancen und Risiken gegeneinander abgewogen werden. Eine Verfolgung der Stellungnahmen, Positionen und des weiteren Gesetzgebungsverfahrens lohnt sich in jedem Fall!

(Carina Bühne, Senior Consultant Compliance & AML, Creditreform Compliance Services GmbH)

Kryptowährungen: Geldwäscherechtliche Regelungen für das Kryptoverwahrgeschäft

Kryptowährungen sind bereits seit einiger Zeit in aller Munde und auch in der Presse wird regelmäßig darüber berichtet. Mit den Änderungen des Geldwäschegesetzes (GwG) und des Kreditwesengesetzes (KWG), die zum 01. Januar 2020 in Kraft getreten sind, fallen auch Unternehmen, die das Kryptoverwahrgeschäft betreiben, als Finanzdienstleister unter die Verpflichteten und müssen daher diverse Punkte beachten. Tauschbörsen fallen hingegen nach Auffassung der BaFin bereits seit 2013 unter die Vorgaben des KWG und des GwG, was vielen Tauschbörsenbetreibern nicht bekannt ist.

Was sind Krypotwährungen und Kryptoverwahrgeschäft?

Kryptowährungen sind einfach gesprochen dezentral herausgegebene, digitale Zahlungsmittel, die auf Basis von sogenannten Blockchains existieren und kryptographisch verschlüsselt sind. Sie sind unabhängig von Ländern, Währungen wie z.B. dem Euro oder sogar Banken. Man kann also auch sagen, dass es sich um eine Art „künstliche Währung" handelt. Die derzeit bekannteste Kryptowährung ist der Bitcoin.

© Adobe Stock / jd-photodesign

Unter Kryptoverwahrgeschäft versteht man die Verwahrung, Verwaltung und Sicherung von Kryptowährungen oder privater kryptographischer Schlüssel für andere.

Kryptoverwahrstellen als Verpflichtete nach dem GwG

Seit dem 01. Januar 2020 unterliegen die Kryptoverwahrstellen als Verpflichtete dem GwG und müssen die gesetzlich definierten Vorgaben erfüllen.

Werden entsprechende Unternehmen erst nach dieser Gesetzesänderung gegründet, dann benötigen diese eine schriftliche Erlaubnis der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) nach § 32 Abs. 1 Kreditwesengesetz (KWG). Für alle Unternehmen, die bereits zum 31. Dezember 2019 das Kryptoverwahrgeschäft erbracht haben, gilt diese Genehmigung als vorläufig erteilt. Allerdings gilt hier die Vorgabe, dass bis zum 31. März 2020 gegenüber der BaFin schriftlich angezeigt werden musste, dass die Absicht besteht, einen Erlaubnisantrag zu stellen. Dieser muss dann bis zum 30. November 2020 schriftlich erfolgen (Übergangsvorschrift nach § 64y KWG).

Betroffene Unternehmen müssen seit dem 01. Januar 2020 die Vorgaben des GwG erfüllen. Bei neuen Marktteilnehmern gilt dies ab dem Stichtag, an dem die Erlaubnis für das Kryptoverwahrgeschäft erteilt wurde. Bei der Umsetzung der geldwäscherechtlichen Vorgaben wird häufig externe Unterstützung benötigt.

Welche Vorgaben müssen durch die Unternehmen erfüllt werden?

Im Grunde sind es drei wesentliche Bereiche, analog zu anderen Verpflichteten, die beachtet werden müssen:

1. Risikomanagement:

Die Unternehmen müssen eine individuelle **Risikoanalyse** erstellen, die insbesondere die spezifischen Risiken darstellt, die sich aus dem Kryptoverwahrgeschäft oder ihrer Tätigkeit als Tauschbörse ergeben und diese regelmäßig aktualisieren. Hierbei sind

insbesondere die Anlagen zum GwG für potentiell höhere Risiken sowie die Ergebnisse der Nationalen Risikoanalyse der Bundesrepublik Deutschland zu beachten.

Aufbauend auf diese Risikoanalyse sind die unternehmensspezifischen **internen Sicherungsmaßnahmen** zu definieren. Das bedeutet unter anderem die Erstellung einer Geldwäscherichtlinie (unternehmensinterne Arbeitsanweisung, Handlungsrichtlinien etc.), die Definition von Kontrollhandlungen sowie regelmäßige Schulungen und Zuverlässigkeitsprüfungen der Mitarbeiter.

Weiterhin besteht die Verpflichtung zur Bestellung eines **Geldwäschebeauftragten**. Diese ist der BaFin rechtzeitig vorab mitzuteilen. Sobald ein Unternehmen mehr als 15 Mitarbeiter (berechnet auf Vollzeitkapazitäten) beschäftigt, ist es nicht mehr zulässig, dass ein Geschäftsführer diese Funktion übernimmt. Grundsätzlich besteht die Option, dass diese Funktion an einen Dienstleister ausgelagert werden kann, wie z. B. die Creditreform Compliance Services GmbH.

2. Kundensorgfaltspflichten

Hier handelt es sich um die bereits aus dem Kontakt mit Banken und Finanzdienstleistern bekannten Vorgaben zur **Identifizierung des Vertragspartners** (inkl. der auftretenden Person) sowie der Abklärung von wirtschaftlich Berechtigten, PEP-Prüfung, Überwachung der Geschäftsbeziehung sowie Aktualisierung der Unterlagen. Ein weiterer relevanter Punkt ist die Einholung und Bewertung von Informationen über den Zweck und die Art der Geschäftsbeziehung.

3. Verdachtsmeldungen

Der dritte Bereich ist das Erkennen und Bewerten von potentiellen **Verdachtsfällen** im Hinblick auf Geldwäsche und Terrorismusfinanzierung sowie die Weiterleitung von Verdachtsmeldungen an die Ermittlungsbehörden. Dieser Aufwand sollte nicht unterschätzt werden, da nicht auszuschließen ist, dass Kryptowährungen durchaus zur Anonymisierungen von Zahlungen genutzt werden können und dadurch ein höheres Risikopotential besteht.

Die BaFin hat am 14. Mai 2020 ein Hinweisblatt für die verpflichteten Unternehmen unter dem Titel „Geldwäscherechtliche Hinweise für Institute, die das Kryptoverwahrgeschäft erbringen, als Neuverpflichtete nach dem Geldwäschegesetz (GwG)“ veröffentlicht. Das Dokument ist auf der Seite der BaFin abrufbar (https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Auslegungsentscheidung/A/ae_200512_krypto_gw.html).

Wie können wir als Creditreform-Gruppe unterstützen?

Im Rahmen der Kundensorgfaltspflichten können wir durch die **Auskunftsprodukte** Unterstützung bei der Identifizierung von juristischen Personen und der Ermittlung von wirtschaftlich Berechtigten leisten. Weiterhin besteht die Option, über CrefoSystem bzw. den Compliance-Check der CCS eine Prüfung gegen **PEP- sowie Sanktionslisten** durchzuführen.

Benötigt das Unternehmen weitergehende Unterstützung, z.B. bei der Erstellung der entsprechenden Unterlagen wie z.B. der Risikoanalyse oder internen Dokumentationen, bis hin zu einer **Vollauslagerung** der Funktion des Geldwäschebeauftragten, dann ist die Creditreform Compliance Services GmbH (CCS) der richtige Ansprechpartner.

Gleiches gilt für **Schulungsmaßnahmen**. Die CCS kann neben der klassischen Präsenzschulung auch Webinare oder E-Learnings anbieten. Insbesondere aufgrund der aktuellen Beschränkungen sind flexible und digitale Schulungsangebote die ideale Lösung.

(Ralf Inderwies, Senior Consultant Compliance & AML, Creditreform Compliance Services GmbH)

Impressum

Herausgeber

Creditreform Compliance Services GmbH

Hellersbergstraße 11

41460 Neuss

Tel: +49 2131 109-1089

Fax: +49 2131 109-81089

www.creditreform-compliance.de

info@creditreform-compliance.de

Amtsgericht Neuss HRB 4213

USt-IdNr.: DE120690803

Geschäftsführung

Silvia Rohe

Redaktion, Layout und Satz

Jasmin Falk

Autoren dieser Ausgabe

Dr. Christian Glaser, Linda Liesum, Carina Bühne, Ralf Inderwies

Bildnachweis

Adobe Stock

Redaktioneller Hinweis