NEWSletter

Ausgabe 2/2016

CASIS

WIRTSCHAFTSPRÜFUNG

We proudly present:

CASIS Heimann Espinoza
Partnerschaft
Steuerberatungsgesellschaft

CASIS
STEUERBERATUNG

Am 17. Juni 2016 haben wir die CASIS Heimann Espinoza Partnerschaft Steuerberatungsgesellschaft in Kiel gegründet.

Die CASIS Steuerberatung bietet Ihnen leistungsstarke Steuerberatung und löst selbst komplexeste Aufgabenstellungen. Die Steuerberater und fachlichen Mitarbeiter der Gesellschaft stehen Ihnen als kompetente Partner in allen Fragen zum Bilanz- und Steuerrecht zur Seite. Neben den laufend anfallenden Tätigkeiten, wie die Lohn- und Finanzbuchhaltung, liegen unsere Kernkompetenzen bei der Erstellung des Jahresabschlusses, der Erstellung der Steuererklärung sowie der steuerlichen Gestaltungsberatung.

Die CASIS Steuerberatung bietet Ihnen persönliche Betreuung, volle Zuverlässigkeit und höchste Qualität.

Inhalt

I. Schwerpunktthema

Nachhaltige IT-Strukturen in Banken

Empfängerkreis

- Geschäftsleiter, Aufsichtsorgane, Informatik, Rechnungswesen, Marketing

1. Einleitung

Eine nachhaltige Geschäftsstrategie, wie in AT 4.2 der MaRisk gefordert, hat sich an der zukünftigen Entwicklung relevanter Einflussfaktoren auszurichten. Die bankenaufsichtliche Perspektive zielt hierbei primär auf die wirtschaftliche Nachhaltigkeit, d. h. den Fortbestand des Instituts ab, da eine Existenzgefährdung von Kreditinstituten stets auch Vertrauensverluste des gesamten Finanzsektors nach sich ziehen könnte. Die breite Öffentlichkeit hingegen setzt den Begriff der Nachhaltigkeit dagegen weitestgehend noch immer mit einer ökologischen Verantwortung der Institute gleich. So verwundert es nicht, dass in Internetforen und sozialen Medien die Nachhaltigkeitsberichterstattung und –zertifizierung großer Banken im Hinblick auf eine gute Unternehmensführung, die Unterstützung sozialer Projekte und der Entwicklungsförderung sowie den Umgang mit den eigenen Mitarbeitern kaum Beachtung findet, solange durch die Institute Atomkraftwerke und Massentierhaltung finanziert werden.

Die isolierte Betrachtung jeweils einer Dimension der Nachhaltigkeit ist hinsichtlich der Ausrichtung und Wahrnehmung der Banken jedoch nicht zielführend. Es ist hervorzuheben, dass es nicht Aufgabe der Finanzinstitute ist, durch ihre finanzwirtschaftliche Funktion ökologische, ökonomische und soziale Belange einer Gesellschaft bewusst zu steuern. Das gilt für Spekulationen mit Nahrungsmitteln ebenso wie für regulierende Eingriffe in die Fremdkapitalfinanzierung einzelner Branchen oder Industrien, sofern keine staatlichen Sanktionen in Bezug auf diese vorliegen. Dem Finanzsektor kommt vor dem Hintergrund der staatlichen Allokationspolitik jedoch eine wichtige Unterstützungsfunktion zu, der aktiv Rechnung zu tragen ist. Eine reputationswirksame Vermarktung der „Nachhaltigkeitsstrategie“ gelingt aus oben angeführten Gründen dennoch bislang primär den kleinen „grünen“ Instituten, deren Anteil am Finanzierungsvolumen, z. B. der erneuerbaren Energien, deutlich hinter dem der großen Banken zurückliegt.

Zudem ist in Zeiten von Terror und Cyberkriminalität die **Gatekeeper-Funktion**, insbesondere der größeren Banken, im Rahmen ihrer **Verantwortung als „Corporate Citizen“** von zentraler Bedeutung. Letztlich zum Schutz unserer Gesellschaft haben die Institute durch geeignete IT-Strukturen und IT-Sicherheitsmaßnahmen zu gewährleisten, dass terroristische und andere kriminelle Vereinigungen keinen Zugriff auf ihre Zahlungsverkehrskanäle und Datenspeicher erhalten. Digitalisierung, Vernetzung und Automatisierung stellen die Banken dabei vor große Herausforderungen. Die IT steht u. a. über die BAIT und die fünfte MaRisk-Novelle im Fokus der Aufsicht. Der Gesetzgeber hat die Risiken z. B. durch Cyberangriffe ebenfalls erkannt und mit dem IT-Sicherheitsgesetz eine Melde- und Informationspflicht sowie die Umsetzung von (branchenspezifischen) Standards für sogenannte **kritische Infrastrukturen** (KRITIS) auf den Weg gebracht. Banken befinden sich dabei im zweiten Korb, dessen Umsetzung ab 2017 geplant ist. Obgleich eine hohe IT-Sicherheit im Bankensektor für die nachhaltige Entwicklung unserer Gesellschaft essentiell ist und für die Kreditinstitute mit hohen finanziellen Konsequenzen verbunden ist, findet diese Mammutaufgabe in der Nachhaltigkeitsberichterstattung der Institute und der öffentlichen Wahrnehmung bislang noch nicht ausreichend Niederschlag. Darüber hinaus sollten die Banken den **Trend zur Digitalisierung und Automatisierung** ebenso nutzen, um die eigene wirtschaftliche Stabilität zu sichern.

2. Digitale Bedrohung

Distributed Denial of Service (DDoS), Advanced Persistent Threat (APT), Spear-Phishing und Fake President Fraud sind Begriffe, die nicht nur dem IT-Sicherheitsbeauftragten geläufig sein sollten, sondern auch der Geschäftsleitung, den Mitarbeitern und Kunden. Insbesondere bei den beiden zuletzt genannten Bedrohungen stehen Kunden und Mitarbeiter im Fokus, denn durch diese Angriffe wird kein IT-System attackiert. Diese zielen vielmehr auf den menschlichen Schwachpunkt im System ab. So helfen die sichersten Firewalls und die besten kryptografischen Verfahren wenig, wenn persönliche Anmeldedaten für das Online-Banking quasi freiwillig an die Angreifer übermittelt werden oder der Mitarbeiter in der Buchhaltung aufgrund einer vermeidlichen E-Mail vom Vorstand Millionenbeträge überweist.

Verhindern lassen sich derartige Angriffe nur in beschränktem Maße. Umso wichtiger sind hier Business Impact Analysen und Schutzbedarfsfeststellungen mit einer angemessenen Abwägung der Bedrohungslage, dem daraus resultierenden Risiko und letztendlich dem möglichen Schaden. Darüber hinaus lässt sich mit einfachen Mitteln der mögliche Schaden abwenden oder minimieren:

- Durchführung von regelmäßigen und anlassbezogenen Penetrationstest zur Prüfung der Sicherheit der IT-Systeme
- Verwendung einer digitalen Signatur zur Sicherstellung der Integrität und Authentizität von E-Mails
- Ein möglichst langfristiges und funktionierendes Backup-Konzept
- Monitoring der IT-Systeme und Auswertung der Protokolle
- Die Verantwortlichen und Mitarbeiter auf aktuellem Stand halten
- Sichere Prozesse und Freigabeverfahren

3. Digitalisierung

Wer im digitalen Zeitalter ein nachhaltiges profitables Bankgeschäft betreiben möchte, kommt an einer Strategie zur Digitalisierung nicht vorbei. So fordert Herr Dr. Andreas Dombret, Mitglied des Vorstands der Deutschen Bundesbank, in einer Rede vor Fachpublikum eine vorrangige Behandlung der Digitalisierung durch die Geschäftsleitung. Insbesondere muss die IT-Struktur in der Lage sein, sowohl die Rahmenbedingungen für die Digitalisierung als auch die IT-Sicherheit sicherzustellen. Netzwerkpläne, mehrstufige Sicherheitssysteme (Firewalls, Demilitarized Zone), Notfallpläne und ein funktionierendes Patch-Management sind dabei Grundvoraussetzungen für jede Bank. Auch im Rahmen von Auslagerungslösungen bleibt die Bank am Ende **für jede Störung und Fehlfunktion verantwortlich.**

Es ist abzusehen, dass sich das klassische Filialgeschäft mehr und mehr ins Netz verlagern wird. Sowohl für Kreditangebote als auch für Kapitalanlagen können die potenziellen Kunden mittlerweile Konditionsvergleiche über eine Vielzahl von Vergleichsportalen abfragen. Zudem drängen zunehmend **Konkurrenten aus dem Nichtbankensektor** auf den Bankenmarkt. Die sogenannten FinTechs bieten schnelle und unkomplizierte Dienstleistungen, z. B. im Bereich Crowdfunding oder Robo Advisory. Um auf diesen Trend reagieren zu können und gegebenenfalls auch auf mögliche Kooperationen mit den FinTechs vorbereitet zu sein, muss die IT-Struktur der Bank flexibilisiert und dynamisch gestaltet werden.

So reicht die bisherige Ausrichtung an gängigen Standards (ISO, BSI, ITIL) nicht mehr aus. Agile Managementmethoden, wie z. B. Scrum oder Kanban, können zu einer Veränderung der Unternehmenskultur beitragen. Doch nicht nur die IT-Strukturen unterliegen hierbei einem Wandel. Auch die **Mitarbeiter benötigen** auf mittelfristige Sicht **mehr IT-Knowhow.**

Wenn nicht bereits vorhanden, wird der Vertriebsmitarbeiter zukünftig Aufgaben eines Social Media Engineers übernehmen, der Anlageberater gegebenenfalls Algorithmen für den Robo-Advisor mitentwickeln und die Marketingabteilung mit SEO-Managern (Search Engine Optimization) besetzt werden, die dafür sorgen, dass die eigene Bank möglichst einen hohen Platz bei Suchanfragen in Suchmaschinen erobert. Eine Umqualifizierung der Mitarbeiter bleibt da nicht aus. Somit ist die Digitalisierung **nicht allein ein Thema für die IT**, sondern für die gesamte Bank.

4. Vernetzung

Ob die Bezahlung mit dem Smartphone per Fingerabdruck an der Kasse im Supermarkt oder das Zusammenstellen seines Aktienportfolio per Robo-Advice, die Möglichkeiten scheinen im Internet keine Grenzen zu kennen. Besonders die Blockchain-Technologie macht aktuell von sich reden. Im gleichen Atemzug wird schon von Banken ohne Mitarbeiter gesprochen. Die **dezentrale und transparente Speicherung von Transaktionen** in einem verteilten System verhindert eine Manipulation bzw. macht diese nur mit erheblichen Aufwand möglich. Clearinghäuser werden somit für Transaktionen nicht mehr benötigt. Bitcoin ist dabei wohl der prominenteste Vertreter für die Blockchain. Aber auch andere Unternehmen bauen auf diese Technologie, wie z. B. die Decentralized Autonomous Organization (The DAO).

Ein funktionierendes Patch- und Changemanagement können der IT dabei helfen, solche Fehler bei der Entwicklung im vornherein zu vermeiden und zeitnah Sicherheitslücken zu schließen. Wer dann noch Synergien beim Change-Prozess realisieren möchte, führt ein durchdachtes **Release-Management** ein.

Dennoch darf nicht vernachlässigt werden, dass mit steigendem Digitalisierungsgrad auch die Risiken im Bereich der IT steigen. So wurde The DAO kürzlich Opfer eines Hackerangriffs auf im Vorfeld bekannte Schwachstellen und verlor etwa 50 Mio. US-Dollar, die das Unternehmen nun nur durch menschliches Eingreifen zum Rückgängigmachen der Transaktionen und damit das Aushebeln des Prinzips der Blockchain zurückgewinnen könnte.

5. Automatisierung

Nicht nur die Prozesse zum Kunden stehen aus Kostengründen im Fokus einer Automatisierung. Die zunehmenden Anforderungen an die **Verfügbarkeit von geschäftsrelevanten Daten** durch die Aufsicht stellen die Banken und besonders die IT-Landschaft vor weitere Herausforderungen.

AnaCredit oder BCS239 zielen darauf ab, sich ein umfängliches Bild von einer Bank zu machen. Dabei liegen die Informationen oft gar nicht im geforderten Umfang oder in der Detailtiefe vor. Und auch die bei Banken häufig anzutreffende heterogene Systemlandschaft begünstigt eine schnelle und automatisierte Lieferung und Analyse der gewünschten Daten nicht. Individuelle Daten Verarbeitung (IDV) zeigt hier ihre Schwächen, da diese meist in den Fachbereichen entwickelt wird, ohne dass dort die Datenstrukturen bekannt oder fundierte Entwicklerkenntnisse vorhanden sind.

Die Idee, dass ein **selbstgestrickter Excel-Report** ziemlich sicher mit geeigneten Anwendungen auch automatisiert von der IT geliefert werden kann, scheint für manchen Fachbereich und auch einige IT-Abteilungen nicht vorstellbar. Wird der Weg zur Quelle der Daten zurückverfolgt und die Datentöpfe identifiziert, ist festzustellen, dass in den meisten Fällen durchaus Schnittstellen bestehen, die es ermöglichen, die Daten **in einer Datenbank zusammenzufassen** oder direkt an ein Empfängersystem weiterzuleiten. Bei einer richtigen Verknüpfung der Daten ist das **Data Warehouse** schon beinahe **fertiggestellt**.

Bei richtiger Umsetzung ist dafür gegebenfalls in Abhängigkeit zum Datenvolumen bereits eine einfache Access-Datenbank ausreichend, der als Frontend zur Zufriedenstellung des Fachbereich die gewohnte Tabellenkalkulationsumgebung vorgeschaltet ist.

6. Fazit

Eine nachhaltige IT-Struktur im Zuge der Digitalisierung in Banken kann nicht alleine Aufgabe der IT sein. Vielmehr muss ein Umdenken in der gesamten Bank und in allen Fachbereichen stattfinden. **Vorrangiges Ziel** muss hierbei **die Wahrung der Informationssicherheit** sein. Sowohl Geschäftsdaten als auch im besonderen Maße die Kundendaten müssen trotz Digitalisierung stets geschützt sein. Eine Sensibilisierung der Kunden und Mitarbeiter für das Thema IT-Sicherheit ist dabei genauso die Aufgabe der Bank, wie auch das Vertrauen in die eingesetzten Technologien und neuen Produkte zu schaffen. Eine gewachsene IT einer Bank dabei auf das dynamische Level einer IT wie z. B. in einem FinTech zu transformieren, scheint schwierig bis unmöglich. Stattdessen bietet sich gegebenenfalls eine Partnerschaft mit FinTech-Unternehmen an, der gegenüber die jungen Unternehmen oftmals positiv gestimmt sind.

> *„Das einzig sichere System müsste ausgeschaltet, in einem versiegelten und von Stahlbeton ummantelten Raum und von bewaffneten Schutztruppen umstellt sein."*
>
> Gene Spafford, Professor an der Purdue Univerity (USA)

Handlungsbedarf

- Beobachtung von digitalen Trends und Berücksichtigung in der Geschäfts -und IT-Strategie
- Umsetzung von gängigen Standards (ISO, BSI) im Bereich der IT-Sicherheit
- Durchführung einer Business-Impact- und Schutzbedarfs-Analyse und Umsetzung der daraus abgeleiteten Maßnahmen
- Prüfen, in wieweit Agile Methoden die Innovationskraft und Entwicklungszyklen positiv beeinflussen können
- Sensibilisierung von Mitarbeitern für IT-Sicherheit durch Fortbildung und Schulung
- Berücksichtig von **drei Kernthesen** bei der Gestaltung von (IT-)Prozessen:
  - Alles, was sich digitalisieren lässt, wird auch digitalisiert werden.
  - Alles, was sich vernetzen lässt, wird auch vernetzt werden.
  - Wenn es digitalisiert und vernetzt ist, dann kann es auch automatisiert werden.
- Stärkere Betonung der Wahrnehmung der Gatekeeper-Funktion der Banken zur Verhinderung von Terrorismusfinanzierung und Datenausspähung in der Nachhaltigkeitsberichterstattung und Öffentlichkeitsarbeit

CASIS bietet Ihnen in diesem Zusammenhang:

- Unterstützung bei der strategischen Ausrichtung der IT-Infrastruktur
- Automatisierung und Optimierung von Prozessen
- Erstellung von IT-Sicherheitskonzepten
- Durchführung von IT-Revision

Kontakt: Stephan Trümper Tel. 0160/2552708 oder s.truemper@casis-wp.de

Aktuelle aufsichtsrechtliche Anforderungen an FinTechs

Empfängerkreis

- Geschäftsführer und Führungskräfte in FinTechs

Hintergrund

Während klassische Banken mit einer Vielzahl von aufsichtsrechtlichen Regulatorien der Bankenaufsicht konfrontiert sind, bewegen sich FinTechs aktuell oftmals noch in einer nichtregulierten Grauzone. Mit zunehmender Anzahl und Geschäftstätigkeit der FinTechs ist die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) inzwischen dazu übergegangen, auch den Markt der FinTechs in den aufsichtsrechtlichen Fokus zu rücken. Hierbei gilt der Grundsatz „same business, same risk, same rules“, wonach die rechtlichen Anforderungen an Banken bei gleichartigen Geschäftsmodellen auch auf FinTechs anzuwenden sind.

Anforderungen

Der Umfang der geltenden rechtlichen Anforderungen macht eine Analyse des eigenen Geschäftsmodells unumgänglich, um beurteilen zu können, welche dieser Anforderungen einschlägig sind.

Als zwei aktuelle Regelungen mit hoher Relevanz für eine Vielzahl von FinTechs im Umfeld der Finanzbranche sind hierbei jedoch die zweite Zahlungsdiensterichtlinie (Payment Service Directive II, kurz: PSD II) und das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (kurz: IT-Sicherheitsgesetz) hervorzuheben.

Die **PSD II** umfasst im Gegensatz zur Vorgängerregelung auch „dritte Zahlungsdienstleister“. Dritte Zahlungsdienstleister sind nach der PSD II Zahlungsauslösedienste, Kontoinformationsdienste sowie weitere Drittdienste. Als Zahlungsauslösedienste gelten Dienste, die im Auftrag des Zahlungsdienstnutzers in Bezug auf ein bei einem anderen Zahlungsdienstleister geführtes Zahlungskonto einen Zahlungsauftrag auslösen. Kontoinformationsdienste werden definiert als Online-Dienste zur Bereitstellung konsolidierter Informationen über eines oder mehrere Zahlungskonten, das bzw. die entweder bei einem oder mehreren anderen Zahlungsdienstleister(n) geführt wird bzw. werden. Für die Anbieter dieser Dienstleistungen gelten im Wesentlichen erhöhte Anforderungen an vorzuhaltende Sicherheitsmaßnahmen sowie Kommunikations– und Authentifizierungsstandards.

Das **IT-Sicherheitsgesetz** verpflichtet die Betreiber besonders gefährdeter Infrastrukturen (sogenannte kritische Infrastrukturen), u. a. auch das Finanz– und Versicherungswesen, ihre Netze besser vor Hacker-Angriffen zu schützen. Neben der obligatorischen Meldung von IT-Sicherheitsvorfällen werden zudem Mindeststandards für die IT-Sicherheit bei den Betreibern der IT -Infrastrukturen branchenweit festgelegt. Zudem haben die Branchen selbst brancheneigene Standards zu entwickeln, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zu genehmigen sind. Alle zwei Jahre ist nachzuweisen, dass die Anforderungen weiterhin erfüllt werden.

Für die Bemessung der Einschlägigkeit der PSD II sowie des IT-Sicherheitsgesetzes sind neben dem eigenen Geschäftsmodell auch die Anforderungen, die an die Auftraggeber und Geschäftspartner der FinTechs gestellt werden, heranzuziehen.

Handlungsbedarf

- Analyse des eigenen Geschäftsmodells
- Prüfung, ob für das eigene Geschäftsmodell eine Erlaubnis der BaFin erfordert
- Prüfung, welche aufsichtsrechtlichen Anforderungen für das eigene Geschäftsmodell einschlägig sind
- Prüfung des Umsetzungsaufwands und möglicherweise bestehender Meldepflichten gegenüber der Aufsicht

BCBS 368: Veröffentlichung der finalen Standards zu Zinsänderungen im Bankbuch

Empfängerkreis:

- Risikocontrolling, Geschäftsführung, Banksteuerung

Zinsänderungsrisiken sind Teil des Basel Säule II Überwachungsprozesses (Supervisory Review Process). Mit den im April 2016 veröffentlichten Standards „Interest rate risk in the banking book“ (IRRBB, BCBS 368) hat das Baseler Committee on Banking Supervision (BCBS) die „Principles for the management and supervision of interest rate risk“ aus dem Jahr 2004 überarbeitet. Der Standard war im Juni 2015 zur Konsultation gegeben worden.

Der Standard enthält die Erwartungen der Aufsicht zur Identifikation, Messung, Überwachung und Kontrolle der Zinsänderungsrisiken im Bankbuch. Die Überarbeitung berücksichtigt die Änderungen im Markt und in der Aufsichtspraxis seit der Veröffentlichung des Standards in 2004 — insbesondere im Hinblick auf die derzeitige außergewöhnliche Zinssituation. Die Anwendung des Standards wird für 2018 erwartet. Konsistent zum gesamten Baseler Rahmenwerk richtet sich der Standard an international tätige Banken auf konsolidierter Basis. Es steht im Ermessen der nationalen Aufsicht, den Standard auch auf andere Institute anzuwenden.

Die wesentlichen Änderungen im Vergleich zum Papier von 2004 sind:

- Eine ausführlichere Beschreibung der Erwartung der Aufsicht an den IRRBB-Management-Prozess (z. B. die Entwicklung von Zinsschock-Szenarien, Modellannahmen bei der Messung des IRRBB, Interner Validierungsprozess)
- Erweiterte Offenlegungsanforderungen zur Schaffung von mehr Konsistenz, Transparenz und Vergleichbarkeit bei der Messung und des Managements des IRRBB
- Die Anwendung des Standardansatzes kann Banken durch die Aufsicht angeordnet werden.
- Der Grenzwert zur Identifizierung von „Ausreißerbanken“, (outlier banks) wurde von 20 % des Gesamtkapital auf 15 % des TIER 1 Capital geändert.

Handlungsbedarf

- Prüfen Sie, in wie weit Sie die Anforderungen an Identifikation, Messung, Überwachung und Kontrolle der Zinsänderungsrisiken im Bankbuch bereits erfüllen.
- Prüfen Sie, inwieweit gegebenenfalls Anpassungen erforderlich sind.

Geldwäscheprävention: Gesteigerte Anforderungen an die Videoidentifikation?

Empfängerkreis

- Geldwäschebeauftragte, Organisation, Geschäftsleitung, Auslagerungscontrolling

Bereits mit dem Rundschreiben 1/2014, welches im April 2015 um ein Schreiben des BMF zu datenschutzrechtlichen Fragen ergänzt wurde, hatte die BaFin erläutert, welche Anforderung sie an eine Videoidentifikation stellt.

Am 10. Juni 2016 veröffentlichte die BaFin das Rundschreiben 4/2016, das erhöhte Anforderungen enthielt. Am 11. Juli 2016 setzte sie dieses bis zum 31. Dezember 2016 aus. Über diesen ungewöhnlichen Vorgang wollen wir Sie informieren.

Was enthielt das (bis 31. Dezember 2016 ausgesetzte) Rundschreiben 4/2016?

Zunächst stellte die Aufsicht klar, dass die Videoidentifizierung eine Identifizierung unter Anwesenden darstellt, auf die die allgemeinen Identifizierungspflichten nach § 3 Abs. 1 Nr. 1 i. V. m. § 4 Abs. 1, Abs. 3 Nr. 1 und Abs. 4 Nr. 1 GwG anzuwenden sind.

Ferner konkretisierte das Rundschreiben bestehende Anforderungen bei der Videoidentifizierung, z. B. seien alle wesentlichen Identifizierungsschritte dabei durch eine zweite Ebene im Unternehmen auf ihre korrekte Durchführung hin zu überprüfen.

Weiterhin erfolgte eine wesentliche Anhebung der Anforderungen/des Sicherheitsniveaus dadurch, dass

- „sich das verpflichtete Kreditinstitut vom Kunden, dessen Konto unter Zugrundelegung des Videoidentifizierungsverfahrens eröffnet worden ist, **bei Kontoeröffnung** einen – in der Höhe unbestimmten – **Geldbetrag** von einem auf den Namen des Kunden lautenden Konto bei einem Kreditinstitut in der europäischen Union **überweisen** zu lassen“ hat.
- „das verpflichtete Kreditinstitut auf der Grundlage von zusätzlichen öffentlich zugänglichen Daten und Informationen (etwa im Internet oder in sozialen Netzwerken), wie dies § 9b Abs. 2 Nr. 2 GwG bereits für andere Verpflichtete des GwG vorsieht, eine **erneute Überprüfung der Identität** und der vom Kunden gemachten Angaben vorzunehmen“ hat.

Das Videoidentifizierungsverfahren hätte damit nur noch durch Kreditinstitute i. S. d. § 1 Absatz 1 des KWG und nur noch von Kunden, die bereits ein Konto bei einem Kreditinstitut der europäischen Union unterhalten, genutzt werden können.

Was gilt aktuell?

Aktuell gilt das Rundschreiben 1/2014 (interimsweise bis zum 31. Dezember 2016) fort. Die Übergangsfrist soll gemäß BaFin den betroffenen Marktteilnehmern Zeit geben, sich auf die höheren Sicherheitsstandards einzustellen und verweist darauf, dem Gesetzgeber zur Umsetzung der 4. EU-Geldwäscherichtlinie entsprechende Hinweise für eine gesetzliche Verankerung von Anforderungen in Bezug auf die Datensicherheit und Digitalisierung an alle Verfahren der Kundenidentifizierung zu geben.

Handlungsempfehlungen

- Verfolgen Sie das Gesetzgebungsverfahren zur Umsetzung der 4. EU-Geldwäscherichtlinie.
- Beschäftigen Sie sich als „worst-case-Szenario“ damit, inwieweit bei einer inhaltlichen Beibehaltung des RS 4/2016 ihre Kundenannahmeprozesse angepasst werden müssten und welche Konsequenzen sich hieraus für sie und Ihre Kunde ergeben werden.

Überblick zur Datenschutzgrundverordnung (DSGVO)

Empfängerkreis:

- Datenschutzbeauftragte (intern/extern), Compliance-Beauftragte, externe Datenverarbeiter, IT-Abteilungen, Vorstände

Am 6. Mai 2016 wurde die DSGVO im Amtsblatt der EU veröffentlicht. Sie gilt ab dem 25. Mai 2018 und schafft ein einheitliches Datenschutzniveau in der EU. Bis 2018 müssen auch Banken und Finanzdienstleister ihre DV-Prozesse, Verträge, Webseiten, Einwilligungserklärungen u. a. stufenweise den veränderten Anforderungen anpassen.

Am 9. Juni 2016 stellte das BMI auf der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) seinen Zwei-Stufen-Zeitplan für die Umsetzung in nationales Recht vor: Anfang 2017 soll zuerst ein „BDSG-Ablösegesetz“ in Kraft treten; Anfang/Mitte 2018 folgen u. a. Änderungen des TKG und TMG. Nachfolgend finden Sie **in Kürze einige Einzelheiten**, die eine eingehende Analyse der eigenen Situation und der zu ziehenden Schlüsse jedoch nicht ersetzen können:

- Die Datenerhebung/-verarbeitung bleibt verboten, es sei denn, sie ist durch Gesetz oder **Einwilligung** des Betroffenen erlaubt (Verbot mit Erlaubnisvorbehalt). Der Betroffene muss **freiwillig** (Art.7 i.V.m. Art. 32 u. 34 DSGVO) sowie **erkennbar, ausführlich und bestimmt in einfacher, klarer Sprache informiert** in die Datenverarbeitung für einen **bestimmten Zweck** (Art.7 Nr. 2, Art. 6 I a, Art. 25 DSGVO) einwilligen. Die Einwilligungserklärungen sind entsprechend anzupassen und dürften künftig eher länger als kürzer ausfallen. Die **Abgabe der Einwilligung** kann dagegen anders als in § 4a BDSG, elektronisch erfolgen, Art. 7 Nr.1 DSGVO.
- **Datenschutz bleibt Unternehmensaufgabe**. Ein betrieblicher Datenschutzbeauftragter muss weiterhin bestellt werden. Es ist aber laut BMI noch offen, ob der Grenzwert bei „mehr als 9 Personen“ oder „mehr als 20 Personen“ liegen wird, da die DSGVO nicht zwischen automatisierter und nicht automatisierter Verarbeitung unterscheidet.
- Art. 30 DGSVO zählt diverse **IT-Sicherheitsverfahren** auf, die erfüllt und **konkret dokumentiert**/regelmäßig überprüft werden müssen. Hohe Bußgelder (bis 20 Mio. € oder 4 % des weltweiten Jahresumsatzes) und Sanktionen sollen darüber hinaus das Bewusstsein für den Datenschutz schärfen.
- Art. 4 DSGVO definiert einen **einheitlichen Datenverarbeitungsbegriff**: Aufgehoben wird die Unterscheidung von Erhebung, Verarbeitung oder Nutzung von Daten.
- **Auftragsdatenverarbeitung:** Art.28 ff. DSGVO (bisher: § 11 BDSG) bestimmen, welche Maßstäbe Verantwortliche an „Datenverarbeiter“ stellen müssen. Neu ist, dass der Verarbeiter selbst zum „Verantwortlichen“ wird, wenn er selbst den Zweck der Datenverarbeitung bestimmt und sich damit bei Verstößen den Bußgeldern von bis zu 10 Mio. € oder bis zu 2 % des weltweiten Jahresumsatzes aussetzt.
- Auch die Gestaltung und Erklärungen bezüglich Cookies, Big Data, Social Media auf **Webseiten** wird nun in Art. 12 - 14 DSGVO, anstelle von §§ 11 ff. TMG, abstrakt geregelt. Sie nehmen Bezug auf die DS-RL 95/46/EG.
- Die **Aufsichtsbehörden** haben künftig mehr Aufgaben. Art. 57 DSGVO zählt **22 Aufgaben** auf, zuzüglich in anderen Artikeln zugewiesene Aufgaben. Insbesondere klassifizieren sie **Datenverarbeitungsprozesse mit** oder ohne zwingende **Datenschutz-Folgeabwägung.** Dieser Begriff ist zentral in der DSGVO und gilt wohl auch für die Videoüberwachung, die — abstrakt geregelt — nun ein geringeres Datenschutzniveau hat (§ 32 BDSG soll laut BMI erhalten bleiben).

Handlungsbedarf

- Überprüfung der IT-Sicherheitskonzepte, der internen technischen u. organisatorischen Datenschutz-Maßnahmen (auch Videoüberwachung, Datenschutz-Folgeabwägung) für IT-Abteilungen, Datenschutzbeauftragte bis 01/2017
- Überprüfung/Anpassung der Auftragsdatenverarbeitungsverträge durch Recht und IT bis 01/2017
- Überprüfung/Anpassung der Einwilligungserklärungen der Kunden, der Webseiten-Gestaltung durch Recht u.v.m.

Whistle-Blowing aus arbeitsgerichtlicher Sicht

Empfängerkreis:

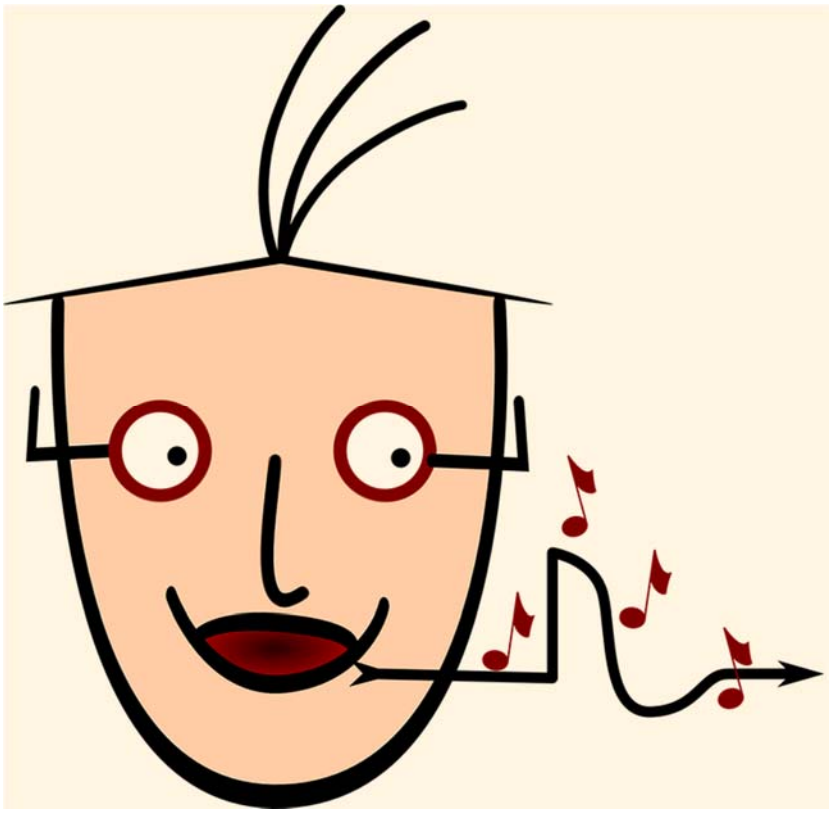
- Personalabteilung, Führungskräfte von Banken und Finanzdienstleistern

Spätestens seit „Snowden“ und den „Panama-Papers“ stellt sich die Frage, welche Auswirkungen Meldungen von Mitarbeitern über (vermeintliche) Missstände haben können. Solchen Meldungen stehen verschiedene Interessen gegenüber: Das bekundete Interesse des meldenden Arbeitnehmers an der Beseitigung von Missständen, das öffentliche Interesse an solchen Informationen sowie das Interesse des Arbeitgebers an der Wahrung seines Rufs und von Geschäftsgeheimnissen sowie an der Loyalitätspflicht des Arbeitnehmers.

1. Meldungen an einen betriebsfremden Empfänger: (Fristlose) Kündigung? — Interessenabwägung im Einzelfall

Bei Meldungen an externe Empfänger legte das Bundesarbeitsgericht (BAG) schon früh fest (Urteil v. 5.2.1959, 2 AZR 60/56), dass es stets einer **Interessenabwägung im Einzelfall** bedarf, ob der Arbeitgeber einem Arbeitnehmer kündigen darf, wenn letzterer Mängel/Missstände bei den Strafverfolgungs- oder anderen zuständigen Behörden anzeigt.

Dabei können **auch zutreffende Angaben** des Arbeitnehmers gegenüber Behörden den Arbeitgeber zur (fristlosen) Kündigung berechtigen, wenn sie ausschließlich aus **Schädigungsabsicht** erfolgen (BAG v. 3.7.2003, 2 AZR 235/02) oder die Anzeige eine **unverhältnismäßige Reaktion** auf das Verhalten des Arbeitgebers oder seines Repräsentanten darstellt (BAG NZA 2013, 808). Selbst der tatsächliche Ausgang eines Strafverfahrens gegen den Arbeitgeber, dem eine Anzeige des Arbeitnehmers voranging, ist nicht ausschlaggebend dafür, ob eine daraufhin ausgesprochene Kündigung rechtmäßig war oder nicht (BAG v. 7.12.2006, NZA 2007, 502). Der Ausgang des Strafverfahrens sei nur „ein Indiz dafür, dass die Anzeige nicht leichtfertig erhoben wurde (...)“.



Der Europäische Gerichtshof für Menschenrechte (EGMR) fordert in Fällen, in denen der Arbeitnehmer zuvor interne Hinweise gegeben hat und nicht wissentlich falsch/leichtfertig gehandelt hat, ergänzend die **Bedeutung eines angemessenen Ausgleichs zwischen den Interessen** des Arbeitgebers und der **Freiheit der Meinungsäußerung** des Arbeitnehmers sowie dem **„zweifellos“ öffentlichen Interesse** an den Mängeln/Missständen (hier: Pflege-Missstände in staatlichem Unternehmen) zu berücksichtigen.

Der „Whistle-Blower“ habe wiederum eine **sorgfältige Prüfungspflicht in Bezug auf den Wahrheitsgehalt** der Informationen, die er nach außen gibt (LAG Köln mit Urteil vom 2.2.2012, AA 12/93).

2. Innerbetriebliche Information — Abmahnung oder Kündigung?

Wie verhält es sich dagegen mit Meldungen an interne Stellen, die hierfür nicht gemäß § 25a Abs. 1 Satz 6 Nr. 3 KWG vorgesehen sind?

Der Arbeitnehmer hat dabei darauf zu achten, dass eine solche innerbetriebliche Anzeige **keine unverhältnismäßige Reaktion** sein darf und er seine **Pflicht zur Diskretion** wahrt. In dem Fall einer Privatkundenbetreuerin, die der „Zentralen Revision" einen Verstoß gegen die Sicherheitsrichtlinie meldete, hielt das BAG (Urteil v. 27.9.2012, 2 AZR 646/11) die Diskretion für gewahrt und sah daher eine Abmahnung für ausreichend an.

Als unverhältnismäßig bewertete dagegen das Landesarbeitsgericht Rheinland-Pfalz (Urteil v. 5.5.2014, 5 Sa 60/14) die neben der internen Anzeige ausgesprochene zusätzliche Drohung eines Arbeitnehmers, den Medien und einem örtlichen Politiker belastendes Material zuzusenden.

In jedem Fall sind das Grundrecht der **Meinungsfreiheit,** Art. 5 Abs. GG, des Arbeitnehmers und die wirtschaftliche **Betätigungsfreiheit** des Arbeitgebers, Art. 12 GG, in ein ausgewogenes Verhältnis zu bringen. Während bewusste und falsche Tatsachen nicht von Art. 5 Abs. 1 GG gedeckt sind, sind es dagegen überzogene Äußerungen, so dass hierbei wiederum eine Interessenabwägung vorzunehmen sei (BAG, Urteil v. 1.7.2014, 2 AZR 505/13).

3. EU-Geschäftsgeheimnisse-Richtlinie

An diesen Grundsätzen wird die seit April 2016 geltende, bis 2018 umzusetzende **EU-Richtlinie 2013/0402** „über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung" nach jetziger Einschätzung nichts ändern.

Handlungsbedarf

- Umsetzung von geeigneten Maßnahmen bei bekannten/durch Mitarbeiter angezeigten Missständen/Verstößen gegen eigene Richtlinien
- Erforschung des Sachverhalts: Je nach Wahrheitsgehalt/Verstoß des eigenen Unternehmens/Einzelfalls abgestufte Maßnahmen: Abmahnung, Kündigung, fristlose Kündigung des Arbeitnehmers und/oder Abstellen des Verstoßes
- Einrichtung einer „Whistle-Blower"-Beschwerdestelle (intern/extern je nach Betriebskultur), die den Arbeitnehmer schützen kann und dem Unternehmen den Anreiz gibt, Missstände/Verstöße gegen Gesetze abzustellen.

  Vorteil: Der Betrieb verliert nicht erst den guten Ruf! Hierbei sind Vorstand/Geschäftsführung, Personal, Recht und Betriebsrat (soweit vorhanden) einzubinden.

Änderung der Definition „Umsatzerlöse“ durch das BilRuG

Empfängerkreis

- Geschäftsführung, Rechnungswesen

Durch das BilRuG (Bilanzrichtlinie-Umsetzungsgesetz), das auf der Grundlage der Richtlinie 2013/34/EU erlassen wurde, ergeben sich u. a. Änderungen bei der Definition von Umsatzerlösen (§ 277 HGB). Die Umsatzerlöse werden nun weiter gefasst als bisher.

In der Vergangenheit waren die Umsatzerlöse auf die „gewöhnliche Geschäftstätigkeit“ bzw. auf das „typische Leistungsangebot“ begrenzt. Diese Einschränkung entfällt nun, so dass künftig alle Erlöse aus Waren, Erzeugnissen oder Dienstleistungen als Umsatzerlöse angesehen werden. Dies kann zu einer erheblichen Steigerung der ausgewiesenen Umsatzerlöse führen. Weiterhin resultiert daraus eine Reduzierung der sonstigen betrieblichen Erträge sowie der Wegfall der außerordentlichen Aufwendungen und Erträge. Eine detailliertere Erläuterung hat nur noch im Anhang zu erfolgen. Nach § 285 Nr. 31 HGB i.V.m. § 314 Abs. 1 Nr. 23 HGB ist die Aufschlüsselung nach außerordentlichen Aufwendungen und Erträgen nun verpflichtend im Anhang vorzunehmen.

Insbesondere bei der Erstellung des Jahresabschlusses ist darauf zu achten, dass diese neuen Regelungen korrekt umgesetzt werden. Hier sind eine besondere Sorgfalt der betreffenden Mitarbeiter sowie deren fachliche Qualifikation erforderlich.

Notwendig ist auch eine einmalige Erläuterung im Anhang über den „Bruch“ der Ausweisstetigkeit bei den Umsatzerlösen (Art. 5. Abs. 2 EGHGB).

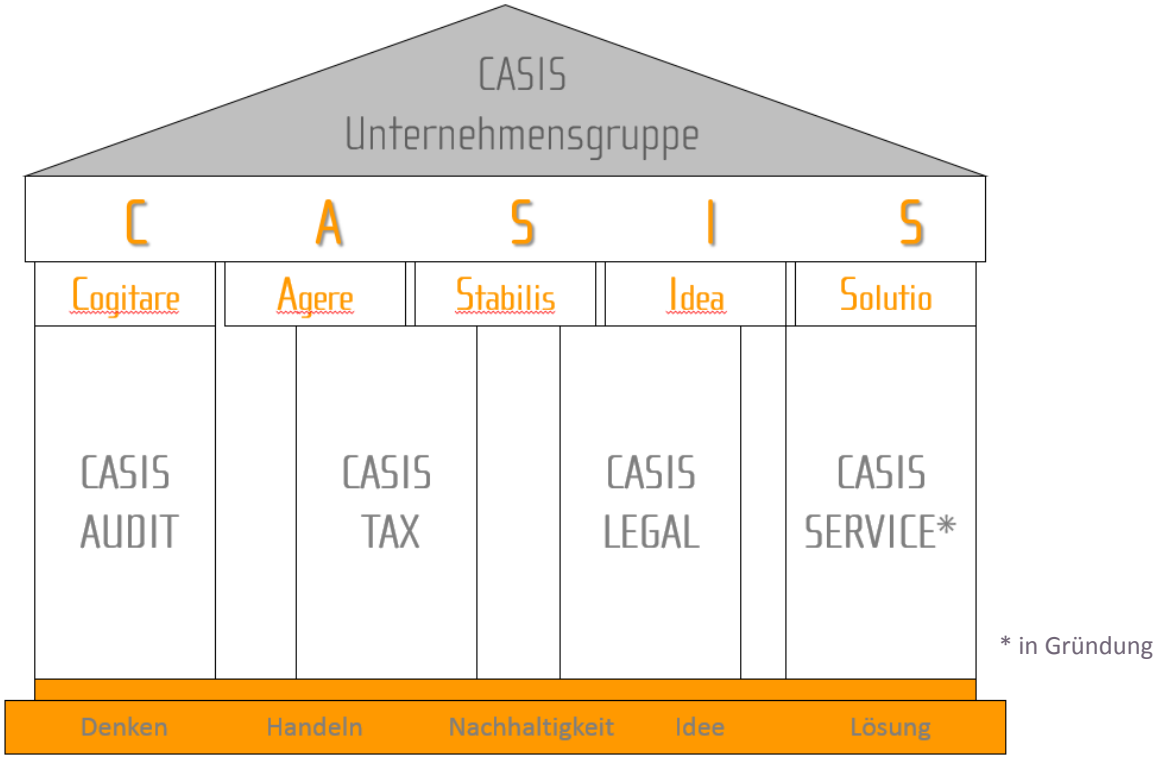
Die Änderungen gelten für nach dem 31. Dezember 2015 beginnende Geschäftsjahre.

Handlungsbedarf

- Besondere Beachtung der Positionen Umsatzerlöse, sonstige betriebliche Erträge sowie außerordentliche Aufwendungen und Erträge bei der Erstellung des Jahresabschlusses
- Schulung der mit der Buchhaltung und Bilanzierung betrauten Mitarbeiter
- Beachtung der erforderlichen Angaben im Anhang

III. CASIS Intern

CASIS Unternehmensgruppe



* in Gründung

- Die CASIS Unternehmensgruppe bietet interdisziplinäre Beratung ohne Schnittstellenverluste und gewährt dadurch ganzheitliche Beratung. Wir sichern unseren Mandanten ein umfassendes Dienstleistungsangebot aus einer Hand zu.
- Unser Team aus Wirtschaftsprüfern, Steuerberatern und Rechtsanwälten steht unseren Mandanten für alle komplexen Fragestellungen in rechtlicher, steuerlicher und betriebs-wirtschaftlicher Hinsicht zur Verfügung. Wir beraten fachübergreifend und lösen Problemstellungen differenziert.
- Die einzelnen Bereiche werden von spezialisierten Mitarbeitern verantwortet.

Aus unserem Seminar- und Workshop-Angebot (Auszug)

- MaRisk 6.0
- Aufsichtsenglisch für nationale/lokale Banken
- § 44 KWG reloaded — SREP, AQR, Challenger Modell in der Bankpraxis
- Gestaltungsansätze und Fallstricke: Wertberichtigungen im Straf-, Handels-, Steuer– und Aufsichtsrecht
- Zielgruppenorientierte Seminare für Aufsichtsrecht, z. B. Aufsichtsrecht für
  - Mitarbeiter in der Organisation
  - Mitarbeiter der IT-Abteilung
  - Mitarbeiter des Personalbereichs
  - Mitarbeiter in Marktbereichen
  - Mitarbeiter in Marktfolgebereichen (Marktfolgen Passiv/Aktiv, Zahlungsverkehr)

V. Impressum

Herausgeber dieser Ausgabe sind:

CASIS Heimann Buchholz Espinoza
Partnerschaft
Wirtschaftsprüfungsgesellschaft
Esplanade 41
20354 Hamburg
T: +49 40 80 80 110 20
F: +49 40 80 80 110 29
E-Mail: info@casis-wp.de

CASIS
Rechtsanwaltsgesellschaft mbH
Esplanade 41
20354 Hamburg
T: +49 40 80 80 110 24
F: +49 40 80 80 110 29
E-Mail: s.beiersdorfer@casis-wp.de

CASIS Heimann Espinoza
Partnerschaft
Steuerberatungsgesellschaft
Bollhörnkai 1
24103 Kiel
T: +49 431 98280330
F: +49 431 98268476
E-Mail: info@casis-wp.de

Wenn Sie Fragen zu unseren Themen haben und weitergehende Hinweise wünschen, freuen wir uns auf Ihre Kontaktaufnahme.

Dr. Antje Buchholz
a.buchholz@casis-wp.de

Redaktionsschluss: 15.07.2016

CASIS Newsletter im Online-Abo unter **www.casis-wp.de/aktuelles**