Das **Compliance-**Management muss **agiler** werden

Von Sascha Hansen

Bildquelle: thehluediamondgallery.com

Die Regulierung ist dem Tempo des Fortschritts häufig nicht mehr gewachsen. Entsprechend hat sich die Taktung der rechtlichen Anpassungen deutlich erhöht. Wie schwierig es für Banken ist, dies umzusetzen, zeigt Sascha Hansen am Beispiel PSD2 und MaSI auf. Generell rät er dazu, das Compliance-Management weiterzuentwickeln. Dazu gehören Automatisierung und agile Methoden. Damit könnte die Verankerung von Agilität in Banken sogar vom Compliance-Bereich ausgehen. Red.

Der Zahlungsverkehr in Europa hat sich zu einem für Außenstehende schwer greifbaren regulatorischen Mikrokosmos entwickelt, zu dem eine nicht minder komplexe und zudem auch volatile Regulierung gehört. Zentrale Treiber der Regelungsflut sind der technische Fortschritt und die damit einhergehenden veränderten Kundenbedürfnisse. Neue Zahlungsdienstleister, Online-Kontoeröffnungen per Video-Identverfahren, Internetwährungen und 24/7-Auslandsüberweisungen über das Smartphone sind nur einige Eckpunkte, an denen sich ein Umbruch im Zahlungsverkehr festmachen lässt.

Regulatorisch drückt sich dieser Umbruch im Zahlungsverkehr und im Zahlungsverkehrsrecht vor allem in der Payment Services Directive (PSD1 und PSD2) aus. Damit strebt die EU einen einheitlichen, grenzüberschreitenden und gleichzeitig sicheren Zahlungsverkehr an. Als EU-Richtlinie ist die PSD rechtlich betrachtet lediglich ein Rahmenwerk. Erst durch nationale Umsetzungsgesetze werden Vorschriften bindend. In Deutschland zeigt sich der regulatorische Anpassungsbedarf in einschlägigen Regelwerken wie etwa dem Kreditwesengesetz und dem Geldwäschegesetz.

Regulatorischer Mikrokosmos Zahlungsverkehr

Durch die Komplexität des Finanzdienstleistungssektors erfolgt die detaillierte Ausgestaltung der gesetzlichen Anforderungen zuweilen auf einer weiteren Ebene. So bedient sich die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) ihrer Kompetenz, norminterpretierende Verwaltungsanweisungen in Form von Rundschreiben zu erlassen. Mit sogenannten Mindestanforderungen schafft sie hiermit ein zumindest de facto rechtsverbindliches Regime. Für Zahlungsdienstleistungen wurden im November 2015 die Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI) formuliert. Diese Anweisungen sind praktisch ein Abbild der Ende 2014 von der European Banking Authority (EBA) formulierten „Leitlinien zur Sicherheit von Internetzahlungen".

Zum Autor

Sascha Hansen, Sopra Steria GmbH, Hamburg

Laut Anwendungsbereich der MaSI gilt das Rundschreiben „für die Erbringung von über das Internet angebotenen Zahlungsdiensten durch Zahlungsdienstleister, die in Artikel 1 der PSD I definiert sind." Solche vom Anwendungsbereich der Richtlinie erfassten Zahlungsdienstleister müssen beispielsweise eine verschärfte Form der Kundenauthentifizierung sicherstellen. Von diesem Anwendungsbereich explizit ausgenommen wurden mobile Zahlungen und „Überweisungen, bei denen ein Dritter auf das Zahlungskonto des Kunden zugreift". Jedoch bieten gerade dritte Zahlungsauslösedienste wie Paypal bereits etablierte Bezahlmöglichkeiten, die im Alltag der Kunden angekommen sind. Auch der Durchbruch von Mobile Payment lässt sich nicht mehr aufhalten. Die Massentauglichkeit mobiler Bezahlfunktionen – Zahlung im Supermarkt per Smartphone – ist nur noch eine Frage der Zeit.

Missverhältnis zwischen Regulierung und Nutzungsverhalten

Das Missverhältnis zwischen Regulierung und dem veränderten Nutzungsverhalten mit dem Ergebnis, dass neuere Zahlungs-

formen weniger streng reguliert sind, bedeutet ein Risiko, das der EU-Regulator bereits erkannt hat. Das Ergebnis ist die Novellierung der PSD1 zur PSD2 und eine Ausweitung der Pflicht zur starken Kundenauthentifizierung auf Zahlungsauslöse- und Kontoinformationsdienste.

Für alle betroffenen Institute heißt das: Mit der Ankündigung der PSD2 und dem gespannten Blick auf die Umsetzung in nationales Recht bis zum 13. Januar 2018 wurden die MaSI zum Provisorium erklärt. Bedenkt man, dass sich die inhaltlich weitaus weniger umfassenden MaSI bereits auf mehr als 50 Einzelbestimmungen zur internen Organisation und zum Risikomanagement auswirken, sollten die Institute mit einem beachtlichen Umsetzungsaufwand rechnen.

BaFin räumt rechtliches Delta ein

Unklar ist dabei, ob die PSD2 mit ihrem Wirksamwerden nahtlos auf den Mindestanforderungen der MaSI aufsetzt oder andere Akzente setzt. Vermutlich haben die Banken und andere Institute viele, sich aus der Umsetzung der PSD2 ergebende Regelungen bereits umgesetzt. Letztlich bleibt den Instituten auch nichts anderes übrig, als sich durch konsequente Umsetzung der MaSI für die Welt der PSD2 fit zu machen und den nachträglichen Anpassungsbedarf zu minimieren.

Die Details werden sich jedoch erst aus den technischen Regulierungsstandards der EBA ergeben, mit deren Umsetzung nicht vor Oktober 2018 zu rechnen ist. Eine – wenn auch nur vorläufige – Koexistenz von PSD2 und MaSI ist damit nicht ausgeschlossen.

Die BaFin räumt das im Ausmaß unklare rechtliche und technische Delta zwischen aktuell geltenden Mindestanforderungen und der künftig Wirkung entfaltenden PSD2 auch ein. Entsprechend legt sie den Unternehmen nahe, diese Lücke an Klarheit als Risiko zu berücksichtigen. Unternehmen können hier allein auf das Augenmaß der EBA hoffen.

Mit dem Regulierungsrisiko klug umgehen

Derartige Operationen am offenen Regulierungsherzen beschränken sich nicht auf den Zahlungsverkehr. In allen Bereichen, in denen eine hohe Regulierungsdichte auf häufige und zudem technische Innovationen trifft, treibt das Erfordernis einer schnellen, komplexen Regulierung das Regulierungsrisiko aus Compliance-Sicht in die Höhe.

Was den Unternehmen zusetzt, ist zudem die Tatsache, dass selbst relativ simpel anmutende regulatorische Anpassungen oft einen langen Vorlauf für die technische Umsetzung benötigen. Einfach abzuwarten, bis alle Details feststehen und dann loszulegen, ist allein deswegen schon keine adäquate Antwort, weil die Rechtsetzung nie final ist. Gegen ein reaktives abwartendes Handeln spricht auch, dass es selbst mit Vorlaufzeiten, Umsetzungsfristen und Übergangsregelungen für Unternehmen ein enormer Kraftakt bleibt, zum verbindlichen Inkrafttreten einer Vorschrift tatsächlich regelkonform zu arbeiten.

Compliance automatisieren

Die Konsequenz für die Branche kann nur lauten, sich Mechanismen zu überlegen, wie sie schneller und effizienter mit dem Rückgang an Planungssicherheit umgehen kann. In der jüngeren Vergangenheit rückte vermehrt das Thema Industrialisierung und Outsourcing von Compliance in den Fokus. Die Masse der Institute geht dabei allerdings sehr dosiert vor. Nur jeder zehnte Entscheider plant bis 2019 Investitionen, um Tätigkeiten wie die Umsetzung von Regulierung auszulagern. Das zeigt der aktuelle Branchenkompass Banking von Sopra Steria Consulting. Die Zurückhaltung hat Gründe: Compliance ist mittlerweile im obersten Management angekommen, und ein öffentliches Interesse herrscht vor. Ein derart geschäftskritisches Feld steuert jedes Unternehmen bis auf einzelne Prozesse lieber inhouse.

Im Gegensatz zum Outsourcing ist das Thema Automatisierung auf dem Vormarsch. Beispielsweise sind die technischen Möglichkeiten auf dem Gebiet von Robotic Process Automation und künstlicher Intelligenz in den vergangenen zwei Jahren deutlich angewachsen. So haben Banken bereits angefangen, bestimmte Arbeiten, die sonst von Juristen erledigt werden, durch eine Software übernehmen zu lassen. Mittels künstlicher Intelligenz und Robotic Process Automation sichten und interpretieren Compliance-Abteilungen Vertragsunterlagen deutlich schneller. Angesichts tausender Seiten technischer Begleitschreiben und Konkretisierungen sowie Konsultationspapieren durch Branchenverbände könnte diese Form der Automatisierung auch für die Analyse regulatorischer Vorhaben eine echte Erleichterung darstellen und für Zeitersparnis sorgen.

Vorausschauende statt reaktive Compliance

Natürlich werden Institute in Zukunft einen noch größeren Teil in ihre Compliance-Abteilungen investieren müssen – dies ist allein schon dem gestiegenen Stellenwert geschuldet. Ziel sollte dabei allerdings sein, die Regulierungsmaßnahmen – idealtypisch formuliert – schon umgesetzt zu haben, bevor es der Regulator fordert. Dieser Schwenk in Richtung einer vorausschauenden Compliance wäre sogar eine Rückbesinnung hin zur ihrer ursprünglichen Raison, die nicht ausschließlich als Reaktion auf rechtliche Vorgaben verstanden werden sollte, sondern ein aktives und vorausschauendes Handeln erfordert.

Dazu wird es unvermeidbar sein, dass sich Banken mit noch mehr Analysefähigkeiten ausstatten. Über ein Technologieradar sollten sie beispielsweise in der Lage sein, Auswirkungen technologischer Trends auf das Bankgeschäft und die Sicherheit für den Verbraucher vorauszuberechnen und entsprechende Compliance-Maßnahmen im Sinne des Regulators ergreifen. Hierzu wird der Compliance-Bereich deutlich stärker als Berater des oberen Managements und der Fachbereiche sowie der IT auftreten müssen.

Compliance-Management weiterentwickeln

Es steht außer Frage, dass sich das Compliance-Management selbst weiterentwickeln und neue Technologien zu eigen machen muss, um regulatorische Vorhaben frühzeitig zu durchdringen und die Auswirkungen auf all ihren Ebenen und in voller Detailtiefe zu verstehen.

Sicherlich bedeutet der Aufbau einer derartigen Organisation für Banken zunächst zusätzliche Ausgaben für neue Technik, spezielle Fachkräfte sowie für den Umbau der Prozesse – in Abwägung der Kosten für Non-Compliance und unter Berücksichtigung der positiven Wahrnehmung eines funktionierenden Compliance-Managements dürften die erforderlichen Investitionen aber einen nachhaltig positiven Effekt haben.

Agile Methoden

Neben der Betrachtung technischer Entwicklungspotenziale zur Gewährleistung einer vorausschauenden Compliance ist ein weiterer Trend zu beobachten: Agilität. Natürlich ist Regulatory Compliance ein spezielles und hochkomplexes Feld. Allerdings müssen sich auch andere Bereiche den Herausforderungen wie dem Erfordernis vorausschauenden Handelns und schneller Reaktionsfähigkeit stellen. Der zentralen Problematik – komplexe Problemstellungen und unklare, sich verändernde Anforderungen – wird zunehmend mithilfe agiler Modelle aus dem Projektmanagement begegnet.

Entscheidend an der Stelle sind weniger die Ausprägungen bestimmter Modelle wie Scrum und Kanban. Vielmehr könnte es von Mehrwert sein, die Grundgedanken wie zum Beispiel ein rollierendes und iteratives Vorgehen, crossfunktionales Arbeiten und effiziente Kommunikation in das Compliance-Management zu integrieren.

Sanierungsbedarf kommt oft erst dann zum Vorschein, wenn die Nachbarn einmal mit der Modernisierung begonnen haben. Auch für das Compliance-Management ist nicht immer sofort ersichtlich, wo die regulatorische Reise hingeht. Um den Nachbarn nicht an sich vorbeiziehen zu lassen, ist es in Zeiten von Digitalisierung und technischer Innovation umso wichtiger, einen Schritt voraus zu sein.

Spagat zwischen Rechtssicherheit und Aktualität immer schwieriger

Betrachtet man die rechtliche Entwicklung – der Fall von MaSI und PSD2 ist nur ein Beispiel – müssen die Institute akzeptieren, dass die Taktung der Rechtsanpassung schlicht höher geworden ist. Dass das Zahlungsdiensterecht ein Konglomerat ineinander verwobener Regelungen unterschiedlicher Normhierarchien darstellt, erhöht die Schwierigkeit. Mit einer abwartenden und reaktiven Haltung im regulatorischen Umfeld riskieren die Verpflichteten nicht nur Imageschäden. Die jüngste Vergangenheit zeigt, dass Compliance-Verstöße nicht nur medial in den Fokus gerückt sind, auch der Regulator greift mit voller Härte durch.

Ansätze wie Outsourcing bieten sich für standardisierte Compliance-Teilaufgaben an. Eine komplette Auslagerung ist nicht realistisch, denn die benötigte Verände-

rung der Compliance- und Unternehmenskultur wird damit nicht gefördert. Anstelle des Wegschiebens gilt es, eine Kultur der Rechtstreue und des vorausschauenden Compliance-Managements im schnelllebigen Tagesgeschäft zu etablieren.

Zweifellos wird das Compliance-Management von neuen Technologien profitieren (müssen). Je schneller sich die Welt dreht und technische Innovationen den Zahlungsverkehr verändern, desto schneller muss das Compliance-Management reagieren – wenn nicht sogar voraussagen, welche Risiken sich aus einer etwaigen Veränderung ergeben können.

Und dennoch: Die Weiterentwicklung muss zunächst in den Köpfen stattfinden. Hier könnte der im allgemeinen Projektmanagement zu beobachtende Trend der agilen Ansätze auch der Optimierung des Compliance-Managements zuträglich sein. Dass Compliance und Agilität sich nicht ganz fern sind, erschließt sich bereits aus der Gemeinsamkeit, dass sich auch Letztere in der Unternehmenskultur in Form von Vertrauen, Kontrollabgabe, gegenseitiger Motivation, gemeinsamer Übernahme von Verantwortung und somit in einem Wandel des autoritären Führungsstils wiederfinden muss. Auch wenn sich der öffentliche Fokus meist auf Strafzahlungen beschränkt, ist der Kern von Compliance schließlich die Unternehmenskultur.

Vielleicht ist der Compliance-Bereich genau der richtige, um Agilität im Unternehmen zu verankern. Ein Compliance-Management, das über kurze Iterationszyklen anpassungsfähig ist, durch ein inkrementelles Vorgehen eine ständige Analyse der regulatorischen Landschaft vornehmen kann und all dies mithilfe neuer Technologien wie Automatisierung auch schnell versteht und umsetzen kann, ist der erste Schritt, um wirklich vorausschauend zu handeln und reaktionsschnell wenn nicht sogar präventiv Maßnahmen zur Sicherstellung der Regulatory Compliance ergreifen zu können.