4

15. November 2024
Fritz Knapp Verlag
35. Jahrgang
ISSN 0937-597 X
D 25079

KARTEN
cards | cartes

ZEITSCHRIFT FÜR ZAHLUNGSVERKEHR UND PAYMENTS

Digitaler Sonderdruck

STRATEGIEN FÜR DIE DIGITALE WELT

PSD2 und Co. – kosteneffiziente Compliance-Strategien für Banken

Von Matthew Colebourne

ISSUING – REGULIERUNG – INSTANT PAYMENT

PSD2 und Co. – kosteneffiziente Compliance-Strategien für Banken

Von Matthew Colebourne

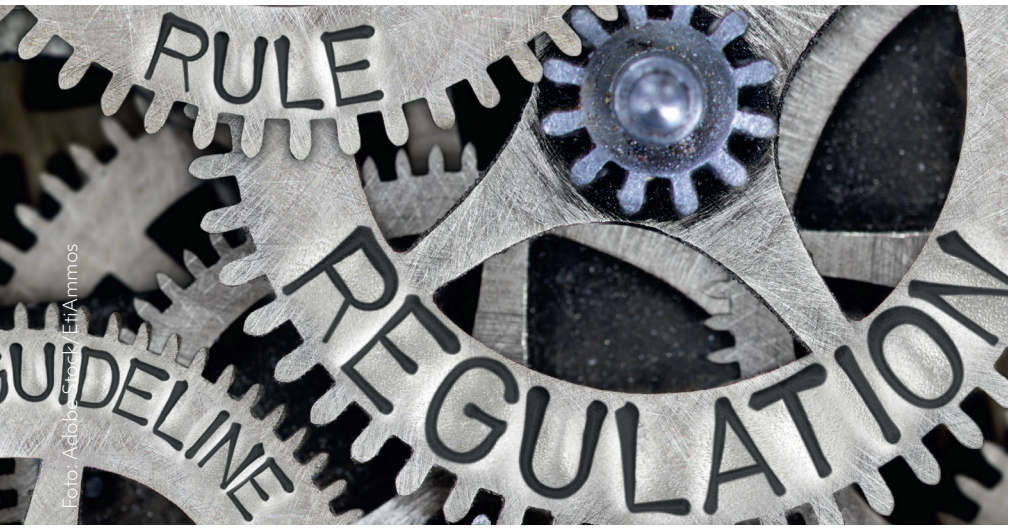

Foto: Adobe Stock / EtiAmmos

Schon die PSD2-Compliance hat erhebliche Kosten für Banken mit sich gebracht. In dem Maße, wie PSD3, PSR und FIDA ihre Schatten voraus werfen, sollten Banken sich deshalb Gedanken über kosteneffiziente Compliance-Strategien machen, sagt Matthew Colebourne. In der Abwägung zwischen Inhouse oder Outsourcing rät er nicht nur kleinen Instituten zum Outsourcing. Denn der hohe Takt bei Regulierungsmaßnahmen macht Anpassungsfähigkeit und Flexibilität zu Kriterien, die immer mehr an Bedeutung gewinnen. So lassen sich vor allem die massiven IT-Investitionen begrenzen. Red.

Seit 2019 begleitet die Zahlungsdiensterichtlinie PSD2 (Payment Services Directive 2) die Finanz- und Bankenwelt. Die Verabschiedung der Nachfolgeregelung steht kurz bevor. Mehr noch: Die PSD3 wird ergänzt werden durch zwei weitere Richtlinien: FIDA und PSR. So weit, so bekannt. Bereits die PSD2 hat viele Finanzinstitute vor eine ganze Reihe von Herausforderungen gestellt. So war es erforderlich, IT-Systeme und Schnittstellen anzupassen, um Drittanbietern den geforderten Zugang zu Kontoinformationen und Zahlungsdiensten zu ermöglichen. Der erleichterte Marktzugang für FinTechs und andere Wettbewerber führte und führt bis heute zu einem verstärkten Konkurrenzdruck und der Gefahr, Kundenbeziehungen und Marktanteile zu verlieren. Schlussendlich mussten die Finanzinstitute ihre Geschäftsmodelle und Strategien überdenken, um in dem neuen Wettbewerbsumfeld bestehen und die Chancen der PSD2, wie neue Kooperationen und datenbasierte Dienste, effektiv nutzen zu können.

Die Implementierung einer PSD2-Compliance mit all ihren neuen Anforderungen und Herausforderungen auf eine sichere und rechtskonforme Art und Weise bedeutet für die Banken unter dem Strich vor allem eins: Personalaufwand und hohe Kosten, insbesondere, wenn in den Finanzinstituten eigene Abteilungen einzig und allein zu diesem Zweck unterhalten werden.

Erhebliche Investitionen in IT-Infrastruktur und Sicherheit

Die in der PDS2 enthaltene Verpflichtung, Kundendaten und Zahlungssysteme für Drittanbieter zugänglich zu machen, bedeutet für die der Regelung unterworfenen Institute vor allem eins: erhebliche Investitionen in IT-Infrastruktur und Sicherheitsmaßnahmen.

Die in der Zahlungsdiensterichtlinie geforderten Schnittstellen (APIs) für Drittanbieter müssen zunächst einmal entwickelt und dann in die IT-Infrastruktur implementiert werden. Neben diesen Implementierungskosten fallen weitere, fortlaufende Kosten für die Wartung und den Betrieb dieser Schnittstellen an. Die PSD2 (und in noch höherem Maße die PSD3 mit ihren Begleitregelungen PSR und FIDA) enthalten umfangreiche Anforderungen an eine starke Kundenauthentifizierung und erfordern folglich zusätzliche Investitionen in Sicherheitstechnologien.

Die Entwicklung robuster und sicherer Schnittstellen erfordert beträchtliche Investitionen nicht nur in die IT-Infrastruktur, sondern auch in Fachpersonal. Denn mit den initialen Entwicklungskosten ist es nicht getan – es fallen zusätzlich kontinuierliche Ausgaben für Wartung, Sicherheits-Updates und Performance-Optimierungen an. Schätzungen zufolge können die Kosten für die API-Entwicklung und -Implementierung für eine mittelgroße Bank mehrere Millionen Euro betra-

Foto: Qwist

Matthew Colebourne,
Managing Director, Qwist GmbH,
Berlin

gen. Zusätzlich müssen Banken Ressourcen für das Monitoring der APIs, die Verwaltung von Drittanbieter-Zugriffen und die Einhaltung sich ändernder regulatorischer Anforderungen bereitstellen. Diese laufenden Betriebskosten können jährlich bis zu 20 Prozent der initialen Implementierungskosten ausmachen.

Da bereits in der PSD2 und in noch höherem Maße in der PSD3 umfangreiche Sicherheitsmaßnahmen und Authentifizierungssysteme gefordert werden, fallen aufseiten der Banken und Finanzdienstleister weitere Kosten an: So erfordert die Einführung der starken Kundenauthentifizierung (SCA) beispielsweise Investitionen in neue Technologien wie biometrische Verfahren, Zwei-Faktor-Authentifizierung und sichere Kommunikationskanäle. Schätzungen zufolge können die Kosten für die Implementierung und Wartung dieser Systeme für große Banken in die Millionen Euro gehen. Kleinere Institute müssen mit Ausgaben im sechsstelligen Bereich rechnen. Zusätzlich fallen laufende Kosten für die Aktualisierung und Anpassung der Sicherheitssysteme an, um mit den sich ständig weiterentwickelnden Bedrohungen Schritt zu halten.

Indirekte Kosten häufig unterschätzt

Trotz des bekannten Bonmots aus dem Administratoren-Umfeld „never touch a running system", ist es nicht empfehlenswert, eine Compliance-Software oder die APIs nach der Implementierung sich selbst zu überlassen. Die indirekten Kosten für Personal und Compliance-Teams stellen einen bedeutenden, oft unterschätzten Faktor bei der Umsetzung von PSD2 und anderen regulatorischen Anforderungen dar.

Diese Kosten umfassen nicht nur die Gehälter und Sozialabgaben für zusätzliche Mitarbeiter in diesem Bereich, sondern auch Ausgaben für Schulungen, Weiterbildungen und die kontinuierliche Aktualisierung von Fachwissen. Darüber hinaus entstehen möglicherweise noch weitere indirekte Kosten durch die Umverteilung von Ressourcen aus anderen Abteilungen, die zur Unterstützung der Compliance-Bemühungen abgezogen werden.

Die Implementierung neuer Prozesse und Kontrollen kann darüber hinaus zu einer vorübergehenden Verringerung der Produktivität führen, während sich Mitarbeiter an neue Abläufe gewöhnen. Zusätzlich müssen Banken mit erhöhten Kosten für externe Beratung, Rechtsbeistände und Audits rechnen, um die Einhaltung der Vorschriften sicherzustellen.

Kostenvergleich Inhouse versus Outsourcing

Wie halten es die Finanzinstitute im DACH-Raum nun mit der PSD2-Compliance? Obwohl genaue Zahlen schwer zu ermitteln sind, lässt sich immerhin ein Trend erkennen: Schätzungsweise regeln etwa 60 bis 70 Prozent der größeren Banken und Finanzinstitute die PSD2-Compliance intern, da sie über die notwendigen Ressourcen und das Fachwissen verfügen. Kleinere und mittlere Banken hingegen greifen häufiger auf externe Partner zurück, um die komplexen Anforderungen der Richtlinie zu erfüllen. Etwa 40 bis 50 Prozent dieser Institute nutzen spezialisierte Dienstleister oder Technologieanbieter, um ihre PSD2-Compliance sicherzustellen und gleichzeitig von deren Expertise und innovativen Lösungen zu profitieren.

Die Personalkosten stellen den größten Posten dar. Dazu gehören nicht nur die Gehälter für qualifizierte Compliance-Experten, sondern auch Nebenkosten wie Sozialabgaben, Versicherungen und Weiterbildungsmaßnahmen. Hinzu kommen Investitionen in spezialisierte rechtskonforme Software und IT-Infrastruktur, die regelmäßig aktualisiert werden müssen. Auch Raumkosten für Büroflächen und Ausstattung sind zu berücksichtigen.

Nicht zu vernachlässigen sind zudem die Opportunitätskosten: Ressourcen, die für Compliance aufgewendet werden, stehen nicht für das Kerngeschäft zur Verfügung. Bei der Berechnung sollten auch potenzielle Kosten für Fehlentscheidungen oder Compliance-Verstöße einkalkuliert werden, die bei mangelnder Expertise entstehen können. Insgesamt können die Kosten für eine interne Compliance-Abteilung je nach Unternehmensgröße und Komplexität der Regulierungen erheblich variieren.

Bei einer ROI-Betrachtung des Einsparungspotenzials durch externe Partner im Compliance-Bereich zeigen sich gleich mehrere Vorteile. Outsourcing-Lösungen können die Effizienz steigern und operative Belastungen reduzieren, was zu Kosteneinsparungen führt. Externe Anbieter bringen spezialisiertes Fachwissen und Ressourcen mit, die auf Marktpraktiken und breite regulatorische Anforderungen ausgerichtet sind. Dies ermöglicht eine schnellere Anpassung an sich ändernde Compliance-Standards und den Einsatz branchenführender Praktiken. Zudem bieten externe Lösungen oft eine bessere Skalierbarkeit, was bei wachsenden Anforderungen Kostenvorteile bringen kann (siehe Kasten).

Herausforderungen der Compliance-Auslagerung

Die Auslagerung der PSD2-Compliance an externe Dienstleister bringt für Banken verschiedene Herausforderungen mit sich. Denn trotz der Delegation bleibt die Gesamtverantwortung für die Einhaltung der Vorschriften bei den Banken selbst, was eine sorgfältige und kontinuierliche Überwachung des Dienstleisters erforderlich macht.

Ein zentrales Risiko stellt der Datenschutz dar, da sensible Kundeninformationen an Dritte weitergegeben werden müssen. Dies erfordert die Implementierung robuster Sicherheitsmaßnahmen, um potenzielle Datenschutzverletzungen zu verhindern. Zudem besteht die Gefahr einer zu starken Abhängigkeit vom Outsourcing-Partner, was problematisch werden kann, wenn dieser seine Leistungen nicht wie vereinbart erbringt oder sein Geschäft aufgibt. Nicht zuletzt führt die Zusammenarbeit mit externen Dienstleistern zu einem erhöhten Kommunikationsaufwand, der die Effizienz der Bankprozesse beeinträchtigen kann. Diese Faktoren müssen Banken sorgfältig abwägen und managen, um eine erfolgreiche Auslagerung der PSD2-Compliance zu gewährleisten.

Allen Herausforderungen zum Trotz: Der Kostenfaktor bleibt ein starkes Argument für die Auslagerung der PSD2-Compliance an einen im Markt gut eingeführten externen Partner. Ein von Qwist entwickelter ROI-Kalkulator liefert die Zahlen zu dieser Aussage: Bei einer angenommenen Teamgröße von 21,5 Mitarbeitern und unter Be-

Argumente für Compliance-Outsourcing

Kosteneinsparungen von bis zu 70 Prozent: Durch die Auslagerung können Personalkosten für interne Compliance-Mitarbeiter sowie Investitionen in spezielle Software und IT-Infrastruktur reduziert werden.

Skalierbarkeit: Externe Lösungen bieten mehr Flexibilität bei schwankenden Compliance-Anforderungen. So können Unternehmen besser auf regulatorische Änderungen reagieren.

Produktivitätssteigerung: Studien zeigen, dass durch externe Compliance-Lösungen die Produktivität deutlich gesteigert werden kann, in einem Fall um bis zu 75 Prozent bei der Einhaltung von Exportvorschriften.

Zugang zu Fachwissen: Externe Dienstleister verfügen oft über spezialisiertes Compliance-Knowhow und aktuelle Kenntnisse zu regulatorischen Anforderungen. Dies kann die Qualität der Compliance-Arbeit verbessern.

Schnellere Anpassung: Outsourcing-Partner können sich in der Regel schneller an sich ändernde Compliance-Standards und neue Regulierungen anpassen.

Risikominimierung: Professionelle Dienstleister können durch ihre Expertise und etablierte Prozesse das Risiko von Compliance-Verstößen reduzieren.

Fokussierung auf Kerngeschäft: Durch die Auslagerung können sich Unternehmen besser auf ihr Kerngeschäft konzentrieren.

Unabhängigkeit: Eine ausgelagerte Compliance-Funktion kann eine größere Unabhängigkeit und Objektivität gewährleisten. Dies ist besonders wichtig für eine effektive Risikokontrolle.

Technologischer Vorsprung: Outsourcing-Anbieter setzen häufig fortschrittliche Technologien für das Compliance-Management ein, die für einzelne Unternehmen zu teuer wären. Dies ermöglicht eine bessere Vorhersage und Bewältigung von Compliance-Risiken.

rücksichtigung der branchenüblichen Betriebskosten im Hinblick auf Infrastruktur und Entwickler-Tools ergab sich ein beeindruckendes Einsparpotenzial von über 73 Prozent der Kosten nach nur drei Jahren.

Kostenimplikationen von PSD3, PSR und FIDA

Die PSD3 zielt darauf ab, den Rahmen der PSD2 zu erweitern, insbesondere in den Bereichen Betrugsprävention, Open Banking und Verbraucherschutz. Eine wesentliche Änderung betrifft die Verbesserung des Open Banking durch erweiterte Datenzugriffsrechte und strengere Anforderungen an API-Qualität und -Verfügbarkeit. Dies könnte für Banken erhebliche Investitionen in ihre IT-Infrastruktur erforderlich machen. Zudem werden voraussichtlich umfassendere Vorschriften zur starken Kundenauthentifizierung (SCA) eingeführt, was Anpassungen bestehender Authentifizierungssysteme nach sich ziehen dürfte. Neue Regeln zum Datenaustausch und zur Betrugsprävention könnten ebenfalls technische Upgrades und zusätzliche Sicherheitsmaßnahmen erfordern. Banken und Finanzinstitute müssen sich darauf einstellen, ihre Prozesse und Geschäftsmodelle entsprechend anzupassen, was wiederum mit Implementierungs- und Schulungskosten verbunden sein wird.

Die PSD3 wird von zwei weiteren Regelungen begleitet: Die Umsetzung von FIDA und PSR bringt erhebliche finanzielle Herausforderungen für Finanzinstitute mit sich. FIDA erweitert das Konzept von Open Banking zu Open Finance, indem es den Datenzugang auf weitere Finanzdienstleistungen wie Sparkonten, Depots, Hypotheken und Versicherungen ausdehnt. Im Gegensatz zur kostenlosen Bereitstellung unter PSD2 ermöglicht FIDA kostenbasierte Entgelte für den Datenzugriff. Die PSR überführt Teile der PSD2 in eine direkt anwendbare EU-Verordnung und erweitert den Satz an vorgeschriebenen Geschäftsvorfällen, zum Beispiel auf Lastschriften und Daueraufträge. Zudem führt die PSR neue Sicherheitsanforderungen ein, wie den verpflichtenden Abgleich des Namens des Begünstigten mit der IBAN.

Insbesondere die Implementierung erweiterter API-Funktionalitäten und die Anpassung bestehender IT-Infrastrukturen erfordern signifikante Investitionen. Banken müssen nicht nur ihre Systeme für den Zugriff auf zusätzliche Datenquellen wie Sparkonten, Depots und Versicherungen aufrüsten, sondern auch neue Sicherheitsmaßnahmen implementieren. Die Erweiterung des Datenzugriffs auf weitere Finanzdienstleister wie Versicherungen und Fondsgesellschaften erhöht zudem den Komplexitätsgrad und damit die Kosten. Gleichzeitig bietet sich durch die neuen Regelungen die Möglichkeit, kostenbasierte Entgelte für den Datenzugriff zu erheben, was zumindest teilweise zur Refinanzierung beitragen kann. Dennoch stellt die Balance zwischen Compliance-Anforderungen und Innovationsinvestitionen eine zentrale Herausforderung dar - insbesondere für kleinere Institute mit begrenzten Ressourcen.

Kostenkontrolle bei sich ändernden Regularien

Die Einbindung eines externen Partners kann bei der Bewältigung sich ändernder Regularien wie PSD2, PSD3, FIDA und PSR entscheidende Vorteile bieten. Externe Spezialisten verfügen über umfassende Erfahrung und aktuelles Fachwissen zu regulatorischen Entwicklungen, was interne Teams oft nicht in gleichem Maße vorhalten können. Dies ermöglicht eine schnellere und präzisere Anpassung an neue Anforderungen. Zudem können externe Partner durch ihre Skaleneffekte oft kostengünstigere Lösungen anbieten als eine interne Implementierung. Sie bringen darüber hinaus oft innovative Technologien und Best Practices mit, die die Effizienz steigern und langfristig Kosten senken.

Ein weiterer wichtiger Aspekt ist die Flexibilität: Externe Dienstleister können je nach Bedarf skaliert werden, was besonders bei schwankenden regulatorischen Anforderungen von Vorteil ist. Darüber hinaus entlastet die Auslagerung von Compliance-Aufga-

ben die internen Ressourcen, sodass sich das Unternehmen stärker auf sein Kerngeschäft und strategische Initiativen konzentrieren kann. Die Zusammenarbeit mit einem externen Partner kann auch das Risikomanagement verbessern, da spezialisierte Anbieter oft über fortschrittlichere Überwachungs- und Reporting-Tools verfügen. Insgesamt kann die strategische Partnerschaft mit einem externen Compliance-Experten nicht nur die Kostenkontrolle verbessern, sondern auch die Qualität und Zuverlässigkeit der Compliance-Aktivitäten erhöhen.

Die Analyse der PSD2-Compliance-Strategien im Bankensektor offenbart einen klaren Trend: Mittlere und kleinere Banken haben bereits den richtigen Weg eingeschlagen, indem sie verstärkt auf externe Partner für die Umsetzung der komplexen regulatorischen Anforderungen setzen. Diese Herangehensweise ermöglicht es ihnen, von spezialisiertem Fachwissen zu profitieren und gleichzeitig ihre Kosten zu optimieren. Große Banken hingegen, die derzeit noch über die notwendigen personellen und finanziellen Ressourcen für eigene Compliance-Abteilungen verfügen, lassen ein enormes Einsparpotenzial ungenutzt.

Flexibilität und Anpassungsfähigkeit im Fokus

PSD3, PSR und FIDA werfen ihre Schatten voraus. Bei der Entscheidung für eine kosteneffiziente Compliance-Strategie spielt die Flexibilität und Anpassungsfähigkeit an zukünftige Regulierungen eine entscheidende Rolle. Ein zukunftssicheres Compliance-System muss in der Lage sein, sich schnell an neue regulatorische Anforderungen anzupassen, ohne dabei übermäßige Kosten zu verursachen. Dies erfordert eine modulare und skalierbare Architektur, die es ermöglicht, neue Compliance-Module nahtlos zu integrieren oder bestehende anzupassen.

In Anbetracht der steigenden Komplexität und der kontinuierlichen Weiterentwicklung regulatorischer Anforderungen wird die Zusammenarbeit mit spezialisierten externen Partnern zunehmend zu einem entscheidenden Wettbewerbsvorteil. Dies ermöglicht es Banken aller Größenordnungen, sich auf ihr Kerngeschäft zu konzentrieren, während sie gleichzeitig von effizienten, kostenoptimierten und zukunftssicheren Compliance-Lösungen profitieren - denn eins ist sicher: Die PSD3 ist in Regulierungsfragen mit Sicherheit noch nicht das letzte Wort! ■