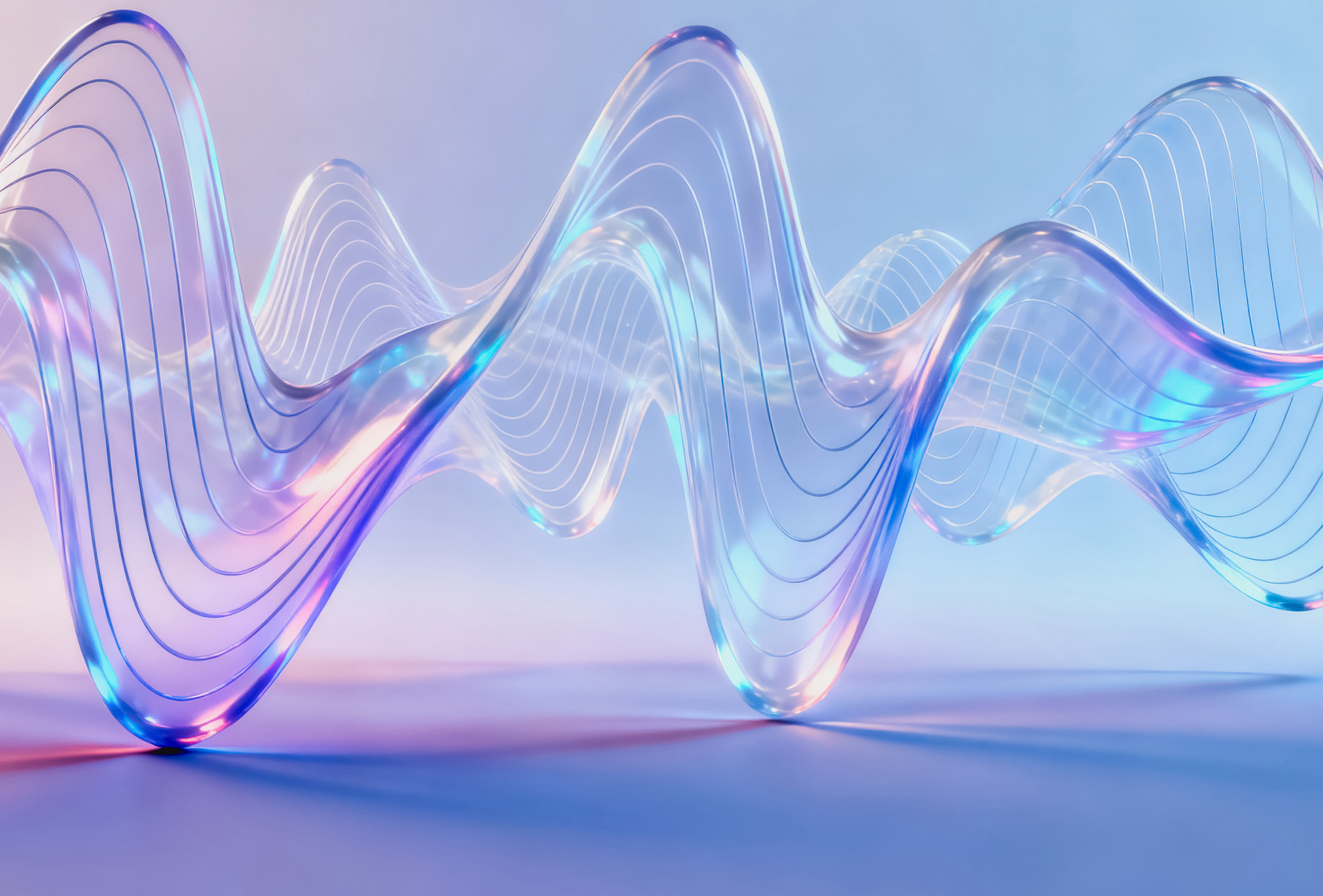
KPMG spotixx

Gemeinsam stärker: Kooperation als Schlüssel im Kampf gegen moderne Finanzkriminalität

November 2026



Sicher, digital, gemeinsam: Datenaustausch auf Basis von Artikel 75 AML und Artikel 83 PSR

Warum überleben manche Gemeinschaften und andere nicht? Die Antwort ist seit Jahrtausenden die gleiche: Zusammenarbeit. In der Gruppe wurde gejagt, Karawanen ermöglichten die sichere Erschließung von Handelswegen und Wissen wurde von Generation zu Generation weitergegeben. Nicht aus Idealismus, sondern weil es funktionierte. Gruppen, die kooperierten, waren stärker, schneller, widerstandsfähiger. Was für Einzelne unsichtbar blieb, wurde im Kollektiv erkennbar.

Dieses Prinzip hat sich nicht verändert. Auch heute gilt: Wer Informationen austauscht und zusammenarbeitet, erkennt Muster früher, handelt präziser und schützt sich besser. Doch gerade in der Bekämpfung von Betrug und Geldwäsche, wo nicht nur Privatpersonen, sondern auch Unternehmen und der Staat durch ausfallende Steuern oder Reputationsverluste geschädigt werden, arbeiten Institutionen noch weitgehend isoliert.

Kriminelle hingegen arbeiten längst zusammen. In gut organisierten Netzwerken agieren sie in vielen Instituten, verschieben Gelder über Landesgrenzen und nutzen die Datensilos der Banken gezielt aus. Wer dem wirksam begegnen will, muss dasselbe tun: zusammenarbeiten. Aber sicher: datenschutzwahrend und abgesichert gegen Datendiebstahl.

Dieses Whitepaper knüpft an die Tradition der Kooperation an und beleuchtet, wie moderne Lösungen durch Kooperation im Bankensektor neue Sicherheits- und Qualitätsstandards ermöglichen können.

Kernpunkte des Artikel 75 AML-VO

Informationsaustausch im Rahmen von Partnerschaften für den Informationsaustausch

1. Mitglieder dieser Partnerschaften dürfen Informationen austauschen, sofern dies zur Erfüllung der Pflichten aus Kapitel III und Artikel 69 zwingend erforderlich ist, wobei Grundrechte und Verfahrensgarantien gewahrt bleiben.
2. Verpflichtete müssen ihre Aufsichtsbehörden über die Teilnahme informieren, welche die Einhaltung der Verordnung prüfen und Auflagen erteilen können.
3. Der Austausch bezieht sich auf Verdachtsfälle im Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung.
4. Der Austausch muss vertraulich erfolgen und den Datenschutz wahren; eine zweckfremde Nutzung ist untersagt.

Kernpunkte des Artikels 83a PSR

1. Teilnahmepflicht: PSPs müssen sich an Informationsaustauschsystemen beteiligen.
2. Datenaustausch: Erlaubt zur Verhinderung/ Aufdeckung von Betrug bei objektivem Verdacht.
3. Umsetzung: Details zu IT-Plattformen werden durch Vereinbarungen geregelt.

In jüngster Vergangenheit sind besonders zwei gesetzliche Vorgaben wichtig. Mit Artikel 75 der AML-VO wird erstmals ein klarer europäischer Rahmen geschaffen, der es Banken erlaubt, Anti-Geldwäsche (AML)-relevante Informationen und sogar ausdrücklich operative Transaktionsdaten untereinander auszutauschen (vgl. Art. 75 Abs. 1 und 3), um Geldwäsche- und Terrorismusfinanzierungsrisiken sektorübergreifend schneller zu erkennen. Gleichzeitig adressiert die Regulierung die Voraussetzungen für diesen Austausch, etwa durch klare Anforderungen an Zweckbindung, Dokumentation und kontrollierte Zusammenarbeit zwischen den beteiligten Instituten.

Dies ist eine Chance, bestehendes Silodenken in der AML-Praxis zu überwinden. Denn noch agieren Institute isoliert, was das Ausnutzen von Schwachstellen für Personen mit krimineller Energie erheblich erleichtert. Skalierbare, verknüpfte Kollaborationsmodelle ermöglichen wesentlich bessere Ergebnisse bei der Früherkennung komplexer, institutsübergreifender Geldwäschenetzwerke und bieten eine reelle Chance, der kriminellen Energie wirksame Mittel entgegenzusetzen.

© 2026 KPMG AG Wirtschaftsprüfungsgesellschaft, eine Aktiengesellschaft nach deutschem Recht und ein Mitglied der globalen KPMG-Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer Private English Company Limited by Guarantee, angeschlossen sind. Alle Rechte vorbehalten.

Was ermöglicht Artikel 75 noch? Der Kern des Artikels zielt explizit auf den Aufbau strukturierter Partnerschaften ab, die eine Verbesserung des Informationsaustauschs ermöglichen. Wenn die Regelungen umgesetzt werden, entsteht eine engere Zusammenarbeit zwischen Banken, Aufsichtsbehörden und Financial Intelligence Units (FIUs).

Gemäß Artikel 83a der Payment Services Regulation (PSR) müssen Zahlungsdienstleister über Transaktionsüberwachungsmechanismen für die Aufdeckung und Verhinderung von betrügerischen Zahlungsvorgängen verfügen. In diesem Zusammenhang ist es sinnvoll, dass Zahlungsdienstleister folgende betrugsrelevante Informationen untereinander austauschen:

- Informationen über den Zahlungsdienstnutzenden (Standort der Nutzenden, Zeitpunkt der Transaktion, verwendete Geräte und Geräte-IP, Ausgabegewohnheiten, Onlinegeschäft)
- Informationen über das Zahlungskonto und Zahlungsvorgangshistorie
- Informationen über den Vorgang (Zahlungsbetrag und IBAN)
- Informationen über die Sitzungsdaten (IP-Adresse)

Grundsätzlich zielt der multilaterale Austausch von Betrugsdaten darauf ab, atypische Nutzung von Zahlungsdiensten zu erkennen, um im Vorfeld Zahlungsbetrug zu verhindern. Damit schafft er die Grundlage für überprüfbare, vertrauenswürdige Prozesse und macht kooperative Modelle überhaupt erst praktikabel. Zusammen entsteht ein klares Zielbild: ein integriertes, vernetztes Ökosystem, welches Zusammenarbeit ermöglicht und gleichzeitig höchste Anforderungen an Datenschutz und Compliance erfüllt. Für kriminelle Netzwerke wird dieses Zusammenspiel deutliche Konsequenzen haben. Es steigert nicht nur die Effizienz des Transaktionsmonitorings, sondern verbessert auch die Fähigkeit, europaweit kohärente Risikobilder zu erstellen.



© 2026 KPMG AG Wirtschaftsprüfungsgesellschaft, eine Aktiengesellschaft nach deutschem Recht und ein Mitglied der globalen KPMG-Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer Private English Company Limited by Guarantee, angeschlossen sind. Alle Rechte vorbehalten.

Das Problem: Isolation in einer vernetzten Welt

Wenn heute ein Verdacht auf Betrug oder Geldwäsche entsteht, passiert in den meisten Fällen Folgendes: ein Griff zum Telefon, das Schreiben einer E-Mail. Dann wird gewartet – manchmal wochenlang. Eine Antwort, wenn sie kommt, ist unvollständig, schwer zu dokumentieren und kaum nachvollziehbar.

Denn jede Bank sieht nur ihren eigenen Ausschnitt. Betrügerinnen oder Betrüger, die bei einem Institut auffallen, eröffnen am nächsten Tag andernorts ein neues Konto. Verdächtige Netzwerke, die sich über mehrere Banken erstrecken, bleiben unsichtbar. Die Verschleierung illegaler Erträge aus Delikten wie Menschen-, Waffen- oder Drogenhandel funktioniert gerade deshalb so gut, weil jede Institution nur ein Fragment des Gesamtbildes sieht.

Das Ergebnis: langsame Aufklärung, hohe Fehleranfälligkeit, erheblicher manueller Aufwand und Täterinnen oder Täter, die dem System immer einen Schritt voraus sind.



© 2026 KPMG AG Wirtschaftsprüfungsgesellschaft, eine Aktiengesellschaft nach deutschem Recht und ein Mitglied der globalen KPMG-Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer Private English Company Limited by Guarantee, angeschlossen sind. Alle Rechte vorbehalten.

Die Lösung: die spotixx Information Sharing Plattform

Die spotixx Information Sharing Plattform ermöglicht Banken und Finanzinstitutionen, im Verdachtsfall schnell, sicher und digital zusammenzuarbeiten. Statt Telefon und E-Mail bietet die Plattform eine strukturierte Onlineumgebung für den Informationsaustausch zwischen Instituten: mit Dashboard, Graphenanalyse und Chatfunktion. Dabei unterstützt KPMG Unternehmen, diese leistungsfähige Datenaustauschplattform zu implementieren, die technische, organisatorische und regulatorische Anforderungen erfüllt. Durch tiefes Fachwissen in AML, Prozessdesign und moderner Datenarchitektur begleitet KPMG den gesamten Implementierungsprozess der spotixx Information Sharing Plattform – von der Strategie bis zur technischen Umsetzung. So entsteht eine robuste, skalierbare Lösung, die effizienten Datenaustausch und bessere Risikoerkennung ermöglicht.

Funktionsweise

Sicherheit steht bei der spotixx Information Sharing Plattform an erster Stelle. Die Plattform nutzt die quantensichere Multi-Party-Computation-Technologie (MPC) von Roseman Labs: sensible Daten werden bereits beim sendenden Institut verschlüsselt und bleiben während der gemeinsamen Analyse geschützt. So werden zu keinem Zeitpunkt Rohdaten geteilt. Anschließend werden die verschlüsselten Informationen auf mehreren unabhängigen Servern bei verschiedenen EU-Cloud-Anbietern verarbeitet. Kein einzelner Server hat dabei jemals Zugang zu den vollständigen Daten. Jedes Institut sieht ausschließlich die Ergebnisse, die für den eigenen Verdachtsfall relevant sind. Im Unterschied zu einem klassischen Datentreuhänder gibt es keine zentrale Stelle, die jemals Zugriff auf Klardaten hat: Die Daten bleiben unter der Kontrolle der jeweiligen Institution. Jede Abfrage wird lückenlos protokolliert und im erhärteten Verdachtsfall kann die gesamte Fallakte direkt an die FIU übermittelt werden.

Multi-Party Computation (MPC)

Multi-Party Computation ist ein kryptographisches Verfahren, das es ermöglicht, gemeinsam Berechnungen über vertrauliche Daten durchzuführen, ohne dass eine beteiligte Partei jemals die Eingabedaten der anderen sieht. Die Berechnung wird auf mehrere, unabhängige Server verteilt, die jeweils nur verschlüsselte Fragmente verarbeiten. Erst das Zusammenspiel aller Server erzeugt ein verwertbares Ergebnis, ohne die zugrundeliegenden Daten preiszugeben.

Vorteile:

- Keine zentrale Instanz sieht oder speichert jemals Klardaten
- Quantensicher: auch gegen zukünftige Angriffe durch Quantencomputer geschützt
- Kein Vertrauen in eine zentrale dritte Instanz erforderlich
- Datensouveränität bleibt vollständig bei den teilnehmenden Instituten

Sicherheit und Compliance

Die spotixx Information Sharing Plattform wurde von Grund auf für die Anforderungen der Finanzbranche konzipiert. Personenbezogene Daten verlassen zu keinem Zeitpunkt die Institution: Abfragen erfolgen ausschließlich verschlüsselt, als Ergebnis wird lediglich zurückgemeldet, ob eine Übereinstimmung vorliegt. Rohdaten werden weder übertragen noch zentral gespeichert. Die gesamte Verarbeitung erfolgt auf unabhängigen Servern bei drei verschiedenen europäischen Cloud-Anbietern innerhalb der EU.

Die Plattform ist vollständig DSGVO-konform und erfüllt die Prinzipien von Privacy by Design und Datenminimierung. Jede Abfrage, jedes Ergebnis und jede Interaktion wird dokumentiert: eine lückenlose Auditierbarkeit, die den Anforderungen der Finanzregulierung entspricht.

Gleichzeitig greifen hier die Anforderungen aus Artikel 83a der PSR, die einen verstärkten Fokus auf sichere, nachvollziehbare und standardisierte Datenverarbeitung im Zahlungsverkehr legt. Insbesondere die Themen Zugriffskontrolle, Datenintegrität und vollständige Nachvollziehbarkeit von Verarbeitungsschritten werden durch die Architektur der Plattform gezielt adressiert.

Technologien wie Multi-Party-Computation ermöglichen dabei genau das, was regulatorisch gefordert ist: einen sicheren Datenaustausch, ohne dass sensible Rohdaten offengelegt werden. So wird regulatorische Compliance nicht nur erfüllt, sondern technisch unterstützt und skalierbar gemacht.

© 2026 KPMG AG Wirtschaftsprüfungsgesellschaft, eine Aktiengesellschaft nach deutschem Recht und ein Mitglied der globalen KPMG-Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer Private English Company Limited by Guarantee, angeschlossen sind. Alle Rechte vorbehalten.

Was sich konkret verändert

Heute stehen verdächtige Personen nur auf institutsinternen Listen. Betrügerinnen und Betrüger können von Bank zu Bank wechseln, ohne erkannt zu werden. Kriminelle Netzwerke bleiben verborgen, weil niemand das Gesamtbild sieht. Und im Verdachtsfall läuft die Kommunikation über Telefon und E-Mail: langsam, fehleranfällig und schwer zu dokumentieren.

Mit der spotixx Information Sharing Plattform ändert sich das grundlegend. Warnungen und Watchlists werden bankübergreifend geführt, ohne dass Rohdaten preisgegeben werden. Betrügerinnen und Betrüger werden auch dann erkannt, wenn sie zwischen Instituten wechseln. Verdeckte Netzwerke werden durch Graphenanalyse sichtbar, über Institutsgrenzen hinweg. Die Zusammenarbeit findet digital und in Echtzeit statt: über Dashboard, Chat und strukturierte Fallbearbeitung. Weniger manuelle Arbeit, schnellere Ergebnisse, weniger Fehler.

Auf einen Blick

Ohne spotixx	Mit spotixx
• Institutsinterne Blocklists • Kriminelle Netzwerke bleiben unsichtbar • Betrügerinnen und Betrüger eröffnen unter falscher Identität Konten bei mehreren Banken und bleiben lange unentdeckt • Einzelne Transaktionen wirken unauffällig, da jede Bank nur einen Ausschnitt sieht • Kommunikation per Telefon und E-Mail • Langsame, fehleranfällige Aufklärung • Manuelle Dokumentation für die FIU	• Gemeinsame Watchlists zwischen Instituten • Graphenanalyse deckt verdeckte Strukturen auf • Auffällige Muster werden institutsübergreifend erkannt, sodass Betrug frühzeitig gestoppt wird • Zusammengeführte Hinweise zeigen ein auffälliges Transaktionsmuster über mehrere Institute hinweg • Digitale Zusammenarbeit in Echtzeit • Schnellere Ergebnisse, weniger Fehler • Komplette Fallakte per Klick an die FIU

KPMG begleitet seit vielen Jahren erfolgreich Banken und Finanzinstitute, wenn es um die Neu- und Weiterentwicklung der technischen und organisatorischen Maßnahmen geht. Neu hinzu kommt, dass KPMG durch vielfältige Projekte bei fast allen Finanzinstituten Kontakte pflegt und belastbare Netzwerke nutzen kann.

Artikel 75 führt zu zusätzlichen Anforderungen, darunter beispielsweise:

- Moderne Daten- und Austauschmechanismen zwischen Banken
- Risikoadaptierte und effizienzbasierte Datenverarbeitungskonzepte und Privacy-Enhancing-Technologien
- Prüfungssicherer Informationsfluss zwischen Banken mit Blick auf Datenschutzvorgaben
- Erfahrung in der Implementierung von gemeinsamen Plattformen sowie der Entwicklung von kollaborativen Monitoring-Modellen
- Harmonisierung von technischen Standards in Banken

Diese Punkte einzeln anzugehen ist das Geschäftsmodell von vielen spezialisierten Beratungsunternehmen. Eine gemeinsame integrierte Lösung innerhalb eines Ökosystems auszurollen, verlangt interdisziplinäre Zusammenarbeit die vielfach in Projekten erprobt wurde. Genau hier sind der Beratungsansatz und die multidisziplinäre Aufstellung von KPMG der Weg zum Erfolg für Projekte im Bereich der Neuaufstellung und Kollaboration in AFC-Abteilungen. Denn auch hier können durch Kollaborationen erhebliche Effizienzgewinne erzielt werden, immer mit Blick auf den Nutzen der Kund*innen.

Zusätzlich werden die Anforderungen durch Entwicklungen und Vorgaben im Artikel 83a PSR weiter präzisiert, insbesondere im Hinblick auf technische Sicherheitsstandards, Datenverarbeitungskontrollen und die revisionssichere Ausgestaltung von Austauschprozessen.

© 2026 KPMG AG Wirtschaftsprüfungsgesellschaft, eine Aktiengesellschaft nach deutschem Recht und ein Mitglied der globalen KPMG-Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer Private English Company Limited by Guarantee, angeschlossen sind. Alle Rechte vorbehalten.

Fazit: Zusammenarbeit war und bleibt ein Vorteil

Von den ersten Siedlungen bis zur modernen Finanzwelt zeigt sich ein durchgängiges Muster: Gemeinschaften, die bereit waren, Wissen auszutauschen und gemeinsam zu handeln, waren widerstandsfähiger, sicherer und erfolgreicher. An diesem Prinzip hat sich nichts geändert.

Mit Artikel 75 schafft der Gesetzgeber nun einen klaren regulatorischen Rahmen für den institutionsübergreifenden Informationsaustausch und die Zusammenarbeit zwischen Unternehmen. Ergänzend dazu konkretisieren regulatorische Entwicklungen wie Artikel 83a PSR die Anforderung an eine sichere, nachvollziehbare und kontrollierte Verarbeitung sensibler Zahlungs- und Transaktionsdaten.

Die Botschaft ist eindeutig: Kollaboration ist nicht nur erlaubt, sie wird erwartet. Finanzinstitute, die sich frühzeitig mit den technischen und organisatorischen Voraussetzungen befassen, verschaffen sich einen entscheidenden Vorsprung. Denn wenn die Anforderungen greifen, wird es nicht reichen, erst dann mit der Umsetzung zu beginnen.

Die Technologie existiert. Der regulatorische Rahmen steht. Was es jetzt braucht, ist die Bereitschaft, den nächsten Schritt zu gehen: Nicht irgendwann, sondern jetzt.

Denn eins hat sich seit den Anfängen der Menschheit nicht geändert: Zusammenarbeit ist kein Risiko, sondern die Grundlage für Resilienz, bessere Entscheidungen und langfristigen Wettbewerbsvorteil in einer zunehmend vernetzten Welt.



Über spotixx

spotixx ist ein wachsendes Fintech mit Sitz in Frankfurt und Wilhelmshaven. Als eigenfinanziertes Unternehmen entwickelt spotixx sichere, skalierbare Lösungen, die es Finanzinstitutionen ermöglichen, bei der Erkennung und Prävention von Finanzkriminalität zusammenzuarbeiten. Die spotixx Information Sharing Plattform verbindet Privacy-Enhancing-Technologien mit moderner Cloud-Infrastruktur und arbeitet unter strengen EU-Datenschutz- und Regulierungsanforderungen.

© 2026 KPMG AG Wirtschaftsprüfungsgesellschaft, eine Aktiengesellschaft nach deutschem Recht und ein Mitglied der globalen KPMG-Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer Private English Company Limited by Guarantee, angeschlossen sind. Alle Rechte vorbehalten.

Kontakt

KPMG AG
Wirtschaftsprüfungsgesellschaft



Volker Smielick
Director,
FS Regulatory & Compliance
M +49 151 55382357
vsmielick@kpmg.com



Kim Binder
Manager,
FS Regulatory & Compliance
M +49 160 94420583
kimbinder@kpmg.com

www.kpmg.de

www.kpmg.de/socialmedia

Die enthaltenen Informationen sind allgemeiner Natur und nicht auf die spezielle Situation einer Einzelperson oder einer juristischen Person ausgerichtet. Obwohl wir uns bemühen, zuverlässige und aktuelle Informationen zu liefern, können wir nicht garantieren, dass diese Informationen so zutreffend sind wie zum Zeitpunkt ihres Eingangs oder dass sie auch in Zukunft so zutreffend sein werden. Niemand sollte aufgrund dieser Informationen handeln ohne geeigneten fachlichen Rat und ohne gründliche Analyse der betreffenden Situation.

© 2026 KPMG AG Wirtschaftsprüfungsgesellschaft, eine Aktiengesellschaft nach deutschem Recht und ein Mitglied der globalen KPMG-Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer Private English Company Limited by Guarantee, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind Marken, die die unabhängigen Mitgliedsfirmen der globalen KPMG-Organisation unter Lizenz verwenden.