Auslagerungen (Outsourcing): Eine Einführung für IT-Dienstleister mit Präzisierungen für Finanzinstitute

22.08.2024

Key takeaways

- **Die Auslagerung betrieblicher Funktionen an externe IT-Dienstleister bietet Finanzinstituten betriebswirtschaftliche Vorteile, birgt jedoch auch relevante Risiken, die von den beteiligten Parteien mitigiert werden müssen.**
- **Neue Technologien sind oft komplex und daher anfälliger für Cyber-Attacken oder technische Störungen. Weitere Risiken können durch eine etwaige Weiterdelegation von IT-Dienstleistungen an Subdienstleister entstehen, da Probleme bei einem Subdienstleister die gesamte Wertschöpfungskette beeinträchtigen können. Diese Abhängigkeiten und Risiken sind oft schwer abzuschätzen und zu kontrollieren.**
- **Eine effektive interne Governance, fundierte IT-Kenntnisse und ein umfassendes Verständnis der aufsichtsrechtlichen Anforderungen sind entscheidend, um die mit der Auslagerung verbundenen Risiken zu minimieren. Alle diese Kenntnisse und Überlegungen müssen bei der Vertragsgestaltung und -verhandlung in die entsprechenden Dienstleistungsverträge einfliessen.**

Einleitung

Auslagerungen (engl. Outsourcing), d.h. die Ausgliederung einzelner betrieblicher Funktionen oder gar ganzer Unternehmensbereiche an Dritte, sind seit den 1960er-Jahren ein bedeutendes Instrument der effizienten Unternehmensführung. Auslagerungen gestatten es den Unternehmen, sich auf ihre Stärken und Kernkompetenzen zu fokussieren und "Hilfsfunktionen" externen Dienstleistern zu übertragen, die diese besser bzw. kosteneffizienter erledigen können. Die Unternehmen des Finanzsektors machen hier keine Ausnahme, sondern übergeben immer häufiger Dienstleistungen an spezialisierte Anbieter.

Beispielsweise kann sich ein Vermögensverwalter auf den Anlageprozess konzentrieren und die Fondsadministration, Wertschriftenverwahrung oder den Vertrieb an Dritte vergeben. Dies erlaubt eine schlanke Organisation und bindet weniger Kapital, was die Gründung neuer Marktteilnehmer erleichtert. Ein weiteres Beispiel ist eine Lebensversicherungsgesellschaft, die ihre IT-Infrastruktur an externe IT-Dienstleister auslagert. Dadurch kann die Lebensversicherungsgesellschaft ihre internen Ressourcen auf die Entwicklung neuer Versicherungsprodukte und die Risikobewertung konzentrieren, während die externen Dienstleister für einen effizienten Betrieb sorgen.

Die zunehmende Bedeutung der Informationstechnologie (Stichworte: Digitalisierung, Cloud) verstärkt dieses Muster noch weiter. Auslagerungen ermöglichen es Unternehmen im Finanzsektor, technologisch auf dem neuesten Stand zu bleiben, ohne selbst umfassende IT-Investitionen tätigen zu müssen. Gleichzeitig macht es den Finanzmarkt aber auch anfälliger für Risiken, insbesondere für Cyber-Attacken und Datenschutzverletzungen.

In diesem Legal Update erörtern wir die rechtlichen Rahmenbedingungen und Herausforderungen, die mit der Auslagerung von Tätigkeiten im Finanzsektor verbunden sind. Wir beleuchten insbesondere die Risiken und Chancen, die mit der Auslagerung von IT-Dienstleistungen einhergehen, und geben einen Überblick über die regulatorischen Grundsätze, sowie Anforderungen und bewährten Praktiken, die Unternehmen beachten müssen, um ihre Strategien erfolgreich und sicher umzusetzen.

Auslagerungen im Finanzsektor

Grundsätze der Regulierung in der Schweiz

Bereits im Jahre 1999 erliess die Eidgenössische Bankenkommission (EBK), eine Vorgängerorganisation der Eidgenössischen Finanzmarktaufsicht (FINMA), ein erstes Rundschreiben zum Thema Auslagerungen bei Banken (EBK Rs. 99/2). Die FINMA hat sodann dieses Rundschreiben (FINMA Rs. 2008/7, später ersetzt durch Rs. 2018/3) im Jahre 2009 übernommen.

Die FINMA übt ihre Aufsicht über Finanzinstitute durch einen dualen Ansatz aus, der sowohl auf gesetzlichen Vorschriften als auch auf sogenannten "Rundschreiben" basiert. Dieser duale Ansatz findet sich in Art. 7 Abs. 1 des Finanzmarktaufsichtsgesetzes (FINMAG). Die gesetzlichen Vorschriften wie bspw. das Bankengesetz bilden die Grundlage für die Aufsichtspflichten der FINMA. Nebst den bestehenden Gesetzen und den entsprechende Ausführungsverordnungen erlässt die FINMA Rundschreiben, um detaillierte Leitlinien und Klarstellungen zu den regulatorischen Anforderungen zu schaffen. Die Rundschreiben dienen der Bereitstellung interpretativer Richtlinien, der Festlegung detaillierter Regeln und der Förderung der Konsistenz in der regulatorischen Durchsetzung. Auch wenn Rundschreiben keine formellen Gesetze sind, üben sie einen bestimmenden Einfluss auf die Umsetzung der gesetzlichen Pflichten durch die Finanzinstitute aus.

Neben dem Outsourcing Rundschreiben hat die FINMA seitdem weitere Aspekte wie operationale Risiken insgesamt oder Cybervorfälle in zusätzlichen Rundschreiben und Aufsichtsmitteilungen angesprochen und punktuell aktualisiert. Aufsichtsmitteilungen sind dabei spezifische Mitteilungen, die die FINMA herausgibt, um besondere oder dringende

regulatorische Themen zu behandeln und zusätzliche Klarstellungen zu bieten.

Im FINMA Rs. 2018/3 wird Outsourcing (Auslagerung) definiert als die Situation, bei der ein Unternehmen einen Dienstleister beauftragt, selbständig und dauernd eine für die Geschäftstätigkeit des Unternehmens wesentliche Funktion ganz oder teilweise zu erfüllen. Dabei sind jene Funktionen wesentlich, von denen die Einhaltung der Ziele und Vorschriften der Finanzmarktaufsichtsgesetzgebung signifikant abhängt. Die nachstehende Tabelle gibt eine Idee davon, welche Situationen die FINMA in ihrer Verwaltungspraxis als Outsourcing betrachtet und welche nicht:

Outsourcing bejaht	Outsourcing verneint
Gesamte Wertschriftenverwaltung / Zahlungsabwicklung bei einem einzigen Dienstleister	Teilnahme an Effektenabwicklungssystem oder an Zahlungssystemen
	Korrespondenzbankensysteme
	Physische Geldlieferungen und Transporte
	Geldautomatenversorgung
Datenaufbewahrung / Betrieb und Unterhalt von Datenbanken / Betrieb von IT-Systemen	Software-Entwicklung / Software-Lizenzierung / Wartung von Software
Compliance-Funktionen / interne Geldwäschereifachstelle	
	Rechts- und Steuerberatung

Quelle: Anhang aus FINMA Rundschreiben (Rs) 2008/7 (aufgehoben)

Die Tabelle gibt nur die Stossrichtung wieder. Selbstverständlich müssen immer die Umstände im konkreten Fall geprüft werden. Tendenziell dürfte eine Auslagerung von Funktionen, bei denen mit einer Vielzahl von Kunden direkt kommuniziert wird (unabhängig vom Kommunikationsmittel) als Outsourcing qualifizieren. Untergeordnete Hilfsdienstleistungen für den Anlageprozess wie z.B. das Erstellen und Darstellen von Modellstrategien und Modellportfolios ohne Einbezug von Kundendaten können demgegenüber noch unterhalb der Schwelle zur Wesentlichkeit liegen. Ob Software-Entwicklung oder Wartung von Software heute immer noch eher nicht als Outsourcing qualifiziert, erscheint angesichts neuerer Erscheinungen wie Software-as-a-Service Lösungen und Cloud-Computing als diskutabel.

Im Kern stützen sich die FINMA Rundschreiben und Mitteilungen auf die in den einzelnen Finanzmarktgesetzen enthaltenen allgemein gefassten Anforderungen an eine angemessene Organisation der Banken, Finanzinstitute und Versicherungsunternehmen.

Spezielle Vorschriften für Finanzinstitute

Für die seit dem 1. Januar 2020 im Finanzinstitutsgesetz (FINIG) geregelten Finanzinstitute, d.h. für Vermögensverwalter und Trustees, Verwalter von Kollektivvermögen, Wertpapierhäuser und Fondsleitungen, bestehen konkrete Anforderungen an Auslagerungen bereits auf Gesetzesstufe. Allerdings verwendet weder das Gesetz noch seine Ausführungsverordnung (FINIV) den Begriff des Outsourcings oder der Auslagerung. Stattdessen wird im Gesetz von einer Übertragung von Aufgaben gesprochen (Art. 14 FINIG, Art. 15 FINIV): Eine Übertragung von Aufgaben nach Art. 14 Abs. 1 FINIG liegt vor, wenn Finanzinstitute einen Dienstleistungserbringer beauftragen, selbstständig und dauernd eine wesentliche Aufgabe ganz oder teilweise wahrzunehmen, und sich dadurch die der Bewilligung zugrunde liegenden Umstände ändern. Zweckmässiger wäre es für alle beaufsichtigten Institute, d.h. gleichermassen für Banken, Versicherungen und Finanzinstitute, von einer wesentlichen Auslagerung zu sprechen, für die zusätzliche aufsichtsrechtliche Bestimmungen gelten, während andere Auslagerungen nach den allgemeinen obligationenrechtlichen Regeln gestaltet werden dürfen. (So wird im deutschen Recht unterschieden, wie in § 25b des Kreditwesengesetzes (KWG) ersichtlich.)

Das Gesetz und die Verordnung legen pro Art des Finanzinstituts fest, welche Aufgaben als aufsichtsrechtlich wesentlich gelten und die somit unter die Vorschriften zur Übertragung von Aufgaben fallen:

Vermögensverwalter und Trustees	Verwalter von Kollektivvermögen	Fondsleitungen	Wertpapierhäuser
▪ Portfolioverwaltung ▪ Anlageberatung ▪ Portfolioanalyse ▪ Anbieten von Finanzinstrumenten	▪ Portfolioverwaltung ▪ Risikomanagement	▪ Fondsgeschäft ▪ Aufbewahrung ▪ Administration	▪ Effektenhandel ▪ Ausgabe v. Derivaten

Der Adressatenkreis des ursprünglich nur für Banken und Versicherungen erlassenen FINMA Rundschreibens 2018/3 zum Outsourcing schliesst seit 2020 die Verwalter von Kollektivvermögen, die Fondsleitungen sowie die Wertpapierhäuser ausdrücklich mit ein. Für Versicherungsunternehmen ist eine Meldung und vorgängige Genehmigung durch die FINMA erforderlich (Art. 4 Abs. 2 Bst. j Versicherungsaufsichtsgesetz). Eine vergleichbare Situation besteht für die erfassten Finanzinstitute. Abhängig von den spezifischen Umständen des Einzelfalls müssen sie die geplante Auslagerung entweder der FINMA zumindest melden oder gar ebenfalls eine vorherige Bewilligung einholen (Art. 8 und 10 FINIG).

Entgegen dem Wortlaut von Art. 14 Abs. 1 FINIG müssen der FINMA anlässlich des Bewilligungsgesuchs alle ausgelagerten Tätigkeiten gemeldet werden, d.h. auch die sogenannt "unwesentlichen" Tätigkeiten. Die FINMA entscheidet einzelfallweise, ob eine wesentliche oder eine unwesentliche Auslagerung vorliegt. So gilt bei Vermögensverwaltern und Trustees

gemäss der aktuellen FINMA-Praxis beispielsweise die Auslagerung von Risk Management und Compliance als relevante Auslagerung, weitere Beispiele sind Vermögensverwaltung von Trustvermögen, IT oder auch Trust-Buchhaltungen. In der Tendenz lässt sich sagen, dass FINMA bei ausgelagerten Tätigkeiten mehrheitlich von wesentlichen Tätigkeiten ausgeht.

Es empfiehlt sich daher, das FINMA-Rundschreiben 2018/3 zum Outsourcing analog auch auf Vermögensverwalter und Trustees anzuwenden, obschon diese vom Anwendungsbereich des Rundschreibens ausgenommen sind. Insbesondere müssen Vermögensverwalter und Trustees Grundprinzipen bei Delegationen festlegen wie die Voraussetzungen, unter welchen eine Delegation möglich ist, wie die Instruktionen im Rahmen der Delegation erfolgen sowie Festlegung von Zuständigkeiten und Kontrollen. Delegationsverträge haben immer schriftlich zu erfolgen. Für FINMA, Aufsichtsorganisation und Revisionsstelle ist vertraglich ein jederzeitiges, vollumfängliches und ungehindertes Einsichts- und Prüfrecht in Bezug auf die ausgelagerte Funktion einzuräumen.

Neue Erkenntnisse aus der Aufsichtspraxis

Vernetzung bedeutet hier Risiko

Auslagerungen von Finanzdienstleistungen haben in den vergangenen Jahren stark zugenommen. Laut dem FINMA-Risikomonitor 2023 lagern mehr als 60 % der beaufsichtigten Unternehmen wesentliche Bereiche, vor allem IT-Dienstleistungen, aus. Besonders betroffen sind Bereiche wie Cloud-Computing, Datenverarbeitung und Cybersecurity. In einigen Bereichen des Finanzsektors ist ein Grossteil der beaufsichtigten Unternehmen dabei von wenigen spezialisierten IT-Dienstleistern abhängig, was gewissermassen eine Art "digitale Monokultur" darstellt. Der Einsatz von Systemen der künstlichen Intelligenz (KI) spielt dabei bereits jetzt eine bedeutende Rolle und wird diesen Trend weiter verstärken. Diese Entwicklung bringt neben den bereits erläuterten Vorteilen auch erhebliche Herausforderungen für den Finanzmarkt mit sich. Ein zentralisiertes Modell kann zu weitreichenden Problemen führen: Der Ausfall eines wichtigen Dienstleisters könnte gravierende Folgen haben, da die Technologien zunehmend komplexer und anfälliger für Cyber-Angriffe oder technische Störungen werden. Besonders besorgniserregend sind sog. "Zero-Day-Angriffe", bei denen Angreifer bislang unbekannte Sicherheitslücken ausnutzen, bevor Schutzmassnahmen aktiviert werden können. Diese Art von Angriff stellt eine erhebliche Herausforderung für beaufsichtigte Unternehmen dar, da solche Schwachstellen oft nur schwer mit herkömmlichen Sicherheitsmassnahmen identifiziert werden können. Ein Beispiel für die Auswirkungen solcher Angriffe ist der MOVEit-Vorfall, der zeigt, wie der Ausfall eines Mehrmandanten-Dienstleisters erhebliche Störungen bei vielen Unternehmen gleichzeitig verursachen kann – die Finanzbranche bildete hierbei keine Ausnahme. MOVEit war Ziel eines Angriffs, bei dem Sicherheitslücken ausgenutzt wurden, was zu erheblichen Störungen und Datenverlusten führte. Ein weiteres Beispiel ist der kürzlich aufgetretene Vorfall bei CrowdStrike. Derartige Ausfälle können einen Kaskadeneffekt auslösen, der entweder einen einzelnen Finanzsektor oder gar den gesamten Finanzmarkt nachteilig beeinflussen, da diese Technologien oft komplexer und anfälliger für Cyber-Attacken oder technische Störungen sind. Weitere Risiken können durch eine etwaige Weiterverlagerung von IT-Dienstleistungen an Subdienstleister entstehen, da Probleme bei einem Subdienstleister die gesamte Wertschöpfungskette beeinträchtigen können. Diese Abhängigkeiten und Risiken sind für auslagernde Unternehmen im Finanzsektor oft schwer abzuschätzen und zu kontrollieren.

Dieser allgemeine Trend wird noch durch neueste Entwicklungen wie "Modular Finance" oder "Open Banking" verstärkt. Die Schweizerische Bankiervereinigung (SBV) definiert Open Banking als Geschäftsmodell, das auf dem standardisierten und gesicherten Austausch von Daten zwischen der Bank und vertrauenswürdigen Drittanbietern basiert. Drittanbieter können auch andere Finanzdienstleister sein. Dabei wird die Wertschöpfungskette von Bank- und Finanzdienstleistungen weiter aufgebrochen, auf verschiedene hochspezialisierte Anbieter verteilt und für die Kunden mittels digitaler Tools wieder zu einer einheitlichen Client Experience verbunden.

	Outsourcing	Open Banking
Kontrolle über Leistung	Bank	Drittpartei
Zustimmung der Kunden nötig?	Nein	Ja
Einfluss auf Wertschöpfungskette	Integriert	Abhängig von der Geschäftsstrategie
Drittpartei handelt...	...im Auftrag und im Interesse der Bank	...vorab im Interesse des Kunden

Quelle: Schweizerische Bankiervereinigung

Einige Statistiken aus Deutschland

Wie eingangs dargestellt betreffen Auslagerungen die interne Organisation eines Unternehmens. In der Regel wird über Auslagerungen nicht berichtet, so dass es für Aussenstehende nicht leicht ist, sich ein Bild zur quantitativen Bedeutung dieses Themas und zu den dabei fast zwangsläufig entstehenden Verflechtungen zu machen. Für Deutschland hat die Bundesanstalt für Finanzdienstleistungsaufsicht BaFin kürzlich in einem Fachartikel anhand von Datenanalysen illustriert, wie eng bestimmte Unternehmen miteinander verflochten sind. Seit der Verallgemeinerung der Meldepflicht für wesentliche Auslagerungen in den Jahren 2021/2022 haben ca. 1'900 beaufsichtigte Unternehmen ca. 20'800 wesentliche Auslagerungen neu gemeldet. Im Durchschnitt resultieren daraus pro Unternehmen rund 11 wesentliche Auslagerungen. Dabei zeigen sich einige Unterschiede je nach Geschäftsmodell: Kreditinstitute (Banken) schlagen durchschnittlich mit ca. 9, Zahlungs- und E-Geldinstitute mit ca. 13 und Kapitalverwaltungsgesellschaften (Fondsleitungen) mit ca. 42 Auslagerungen zu Buche.

Vorher bereits bestehende und nicht veränderte Auslagerungen sind in diesen Zahlen zwar nicht enthalten. Die so aufgebaute Datenbasis erlaubt es der BaFin jedoch bereits, Verflechtungen zwischen den beteiligten Unternehmen sichtbar zu machen. Grafische Darstellungen (Netzwerkgraphen) erlauben es der Behörde, Konzentrationen auf bestimmte Dienstleister zu erkennen, die als Mehrmandanten-Dienstleister tätig sind. Ebenso können Auslagerungsstrukturen innerhalb einzelner Vertragsbeziehungen sichtbar gemacht werden, vor allem mit Blick auf Weiterverlagerungen auf Subdienstleister (Dienstleisterketten). Solche Dienstleisterketten sind – offensichtlich – nicht unüblich. Wie bereits oben angerissen, können sie dann problematisch werden, wenn sich bspw. Störungen bei einem Subdienstleister kaskadenartig auf andere Parteien ausweiten und dadurch eine ganze Gruppe von

Finanzinstituten beeinträchtigen.

Hier widerspiegelt sich die Feststellung, dass der Finanzsektor bei der Erbringung von Finanzdienstleistungen zunehmend von Technologie und Technologieunternehmen abhängig ist. Wie die letzten Jahre aufzeigten, macht dies Finanzinstitute anfällig für Cyberangriffe oder andere Zwischenfälle. Hier knüpft DORA, der europäische Digital Operational Resilience Act (Regulation (EU) 2022/2554) an, der ab dem 17. Januar 2025 wirksam werden wird. DORA umfasst Bestimmungen zu IKT-Risk Management, IKT-Partner Management, Stresstests, Vorfallmeldungen, Informationsaustausch zwischen Aufsichtsbehörden sowie zu einer "Aufsicht-light" für kritische Dienstleister.

Artikel 17 DORA verpflichtet sowohl die Finanzinstitute selbst als auch bestimmte kritische Dienstleister dazu, Prozesse für die Behandlung IKT-bezogener Vorfälle zu bestimmen, einzurichten und zu betreiben, um IKT-bezogene Vorfälle zu erkennen, zu behandeln und zu melden. Die Regulierung stützt sich auf die Erkenntnis, dass Vorfallmeldungen nicht nur für das betroffene Unternehmen von Bedeutung sind, sondern dem gesamten Finanzmarkt dienen.

Neue Schweizer Meldepflichten zu Cyber-Vorfällen

Mit der FINMA-Aufsichtsmitteilung 05/2020 "Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG" wurde die auf die allgemeine Meldepflicht abgestützte Pflicht, Cyber-Attacken der FINMA anzuzeigen, näher umschrieben. Gemäss FINMA zeigen die seither eingegangenen Meldungen unterschiedliche Entwicklungen in der Bedrohungslage, den Angriffsmethoden und den Zielen der Angriffe.

Die FINMA-Aufsichtsmitteilung 03/2024 baut auf diesen Erkenntnissen auf und betont die Notwendigkeit eines proaktiven Umgangs mit Cyber-Risiken, insbesondere durch die Überwachung der Dienstleister. Es wurde festgestellt, dass nur "sehr wenige Institute nach der Identifikation von schwerwiegenden Sicherheitslücken proaktiv" ihre wichtigsten Dienstleister kontaktierten, um Schwachstellen zu identifizieren und zu schliessen. Diese Lücke im Risikomanagement könnte auf das Fehlen eines vollständigen und aktuellen Inventars ihrer Dienstleister zurückzuführen sein. Obwohl das FINMA-Rundschreiben "Rundschreiben 2018/3 – Outsourcing" bereits heute vorschreibt, dass Finanzinstitute ein detailliertes und aktuelles Inventar ihrer Dienstleister führen müssen, um eine umfassende Übersicht über alle externen Dienstleister sowie deren Bedeutung für die operative Sicherheit und Stabilität des Unternehmens zu erhalten, wird diese Anforderung häufig nicht ausreichend, nicht konsequent genug und/oder nicht auf kontinuierlicher Basis umgesetzt. Es ist leicht ersichtlich, dass ohne ein solches Inventar nur schwer festgestellt werden kann, ob beim Dienstleister kritische Daten gespeichert sind oder dieser mit der Erbringung einer kritischen Funktion beauftragt ist.

Die FINMA-Aufsichtsmitteilung 03/2024 fordert daher verstärkte Massnahmen, wie die regelmässige Überprüfung der Cyber-Sicherheit von Dienstleistern und die Durchführung von Szenario-basierten Cyber-Risiko-Übungen, um das Risiko von kaskadierenden Auswirkungen von Cyber-Vorfällen auf Finanzinstitute und deren Dienstleister zu minimieren.

Nächste Schritte

Zwei Dinge müssen Banken und andere Finanzdienstleister heutzutage besonders gut beherrschen, die mit der gerne auf Tradition verweisenden Finanzwelt früherer Zeiten wenig zu tun haben: Neben einer guten internen Governance müssen sie erstens fit in Sachen IT sein. Sie müssen sich zweitens in aufsichtsrechtlichen Themen aller Art bestens auskennen, um mit den Aufsichtsbehörden konstruktiv kommunizieren zu können.

Heute werden sich die wenigsten Institute in Sachen IKT ganz auf eigene Kapazitäten verlassen (es gibt natürlich sehr bekannte Ausnahmen). Institute, die sich auf externe Dienstleister stützen, sind gut beraten, ein umfassendes Inventar aller dieser Verhältnisse zu erstellen, seien sie nun wie die grösseren Banken dazu verpflichtet oder nicht. Sie sollten dabei klar definieren, was für sie kritische Daten sind und wo diese gespeichert sind. Sie sollten eine angemessene Klassifizierung ihrer Dienstleister vornehmen und die erforderlichen Kontrollmassnahmen zur Reduktion der identifizierten Risiken mit ihren Dienstleistern zusammen definieren und vertraglich vereinbaren. Eine so umgesetzte interne Governance und ein diszipliniertes Stakeholdermanagement für wesentliche Dienstleister ist ein unverzichtbares Erfordernis für ein wirksames Schutzdispositiv gegen Cyber-Vorfälle und andere IT-Risiken.

Die IT-Dienstleister selbst sind der Schweizer Regulierung nicht unterworfen. Da die Institute jedoch verpflichtet sind, die an sie ausgelagerten Prozesse in ihr Schutzdispositiv aufzunehmen, haben die IT-Dienstleister ein grosses Interesse daran, das Risikomanagement ihrer Kunden so gut wie möglich zu unterstützen. IT-Dienstleister im Finanzbereich müssen sich somit mit dem Finanzmarktrecht auskennen.

In diesem Kontext kann der Einsatz von Künstlicher Intelligenz (KI) nicht nur "Teil des Problems", sondern auch Teil der Lösung sein. KI kann nämlich helfen, die Überwachung und Analyse der Aktivitäten von IT-Dienstleistern zu automatisieren, um potenzielle Sicherheitsrisiken frühzeitig zu erkennen und darauf zu reagieren. KI-Systeme können auch dabei unterstützen, die Einhaltung von Leistungskennzahlen (KPIs) und Service-Level-Agreements (SLAs) zu überwachen und sicherzustellen. Zudem ermöglicht KI eine kontinuierliche Anpassung der Schutzmassnahmen an neue Bedrohungen und regulatorische Anforderungen.

Das Zusammenwirken von Finanzinstituten und IT-Dienstleistern muss in den Dienstleistungsverträgen geregelt und dokumentiert werden. Diese Verträge sollten von Juristen erstellt werden, um rechtliche Anforderungen abzudecken, während Fachspezialisten sicherstellen müssen, dass technische und operationale Details präzise festgelegt werden. Der Vertrag sollte Leistungskennzahlen (KPIs), Service-Level-Agreements (SLAs) sowie Sicherheits- und Notfallregelungen enthalten.

Es ist wichtig, dass die Businessvertreter sich im fertigen Vertrag wiederfinden, um ihre geschäftlichen Anforderungen zu reflektieren, ebenso wie regelmässige Überprüfungen und Anpassungen des Vertrags, um aktuellen Anforderungen und Entwicklungen gerecht zu werden. So wird gewährleistet, dass die Zusammenarbeit effizient, rechtskonform und risikominimiert erfolgt. Der Einsatz von KI kann dabei eine entscheidende Rolle spielen, um diese Ziele zu erreichen und die Sicherheitsarchitektur der Finanzinstitute weiter zu stärken.

Autoren: Markus Winkler (Counsel), Xenia Pisarewski (Associate), Armina Burkic (IT Analyst)

Keine Rechts- oder Steuerberatung

Dieses Legal Update gibt einen allgemeinen Überblick über die Rechtslage in der Schweiz und erhebt keinen Anspruch auf Vollständigkeit. Es stellt keine Rechts- oder Steuerberatung dar. Falls Sie Fragen zu diesem Legal Update haben oder Rechtsberatung hinsichtlich Ihrer Situation benötigen, wenden Sie sich bitte an Ihren Ansprechpartner bei Pestalozzi Rechtsanwälte AG oder an eine der in diesem Legal Update erwähnten Kontaktpersonen.

Andrea Huber

Partner
Attorney at law, LL.M.

Pestalozzi Attorneys at Law Ltd
Feldeggstrasse 4
8008 Zürich
Switzerland
T +41 44 217 92 41
andrea.huber@pestalozzilaw.com

Markus Winkler

Counsel
Attorney at law, Dr. iur.

Pestalozzi Attorneys at Law Ltd
Feldeggstrasse 4
8008 Zürich
Switzerland
T +41 44 217 92 59
markus.winkler@pestalozzilaw.com