Unlock Tomorrow:
Souverän durch Compliance

#UnlockTomorrow
www.keylane.com

Keylane Axon

Die Kontrolle über regulatorische Anforderungen gewinnen

Vertrauen ist die Grundlage zwischen Versicherungsunternehmen und Versicherungsnehmern. Wenn sich ein Versicherungsnehmer nicht auf seinen Anbieter, Makler oder Servicestelle verlassen kann, sucht er nach einer vertrauenswürdigeren Alternative.

Aus Sicht der Versicherungsnehmer haben Versicherungsunternehmen keinerlei Raum für Fehler, müssen alle vertraglichen Verpflichtungen erfüllen und Ansprüche fair und konsequent auszahlen - ohne Wenn und Aber.

Um Vertrauen zu schaffen, müssen Versicherungsunternehmen strenge Compliance-Vorschriften einhalten. Diese Regeln bieten Versicherungsnehmern Schutz und fördern eine nachhaltige sowie langfristige Versicherungsbranche. Erfolg und Vertrauen in die Branche werden durch solide Risikomanagementpraktiken und Marktintegrität definiert.

Aufsichtsbehörden in der Versicherungsbranche sind heute strenger denn je, wenn es darum geht, die Einhaltung der Vorschriften durchzusetzen. Nicht selten werden Verstöße in Form von Geldbußen, rechtlichen Schritten und Sanktionen geahndet. Es liegt daher auf der Hand, dass Maßnahmen zur Einhaltung der Compliance-Vorgaben für den Erfolg und die **Geschäftskontinuität** von entscheidender Bedeutung sind und zu Recht höchste Priorität genießen.

In diesem Whitepaper werden die zentralen Herausforderungen im Zusammenhang mit der Einhaltung von Vorschriften diskutiert. Es wird erläutert, wie Keylane mit Versicherern zusammenarbeitet, um ihre vollständige Compliance sicherzustellen und ihren anhaltenden Erfolg als führender Anbieter in der Versicherungsbranche zu gewährleisten.

Die Themen, die behandelt werden, sind:

- Verständnis der kritischen Rolle des Compliance-Beauftragten und seiner Beziehung zur Geschäftskontinuität.
- Investitionen, Wartung und Prüfung von Ausfallsicherheits- und Failover-Systemen.
- Sinnvolle Berichterstattung über Vorfälle und effektives Risikomanagement.
- Einhaltung des Datenschutzes und der Privatsphäre und die sich entwickelnden Anforderungen der Outsourcing-Aufsicht.

Heutzutage hat die Versicherungsaufsicht die Durchsetzung von Vorschriften verschärft und ahndet Verstöße strenger.

Die Rolle der Compliance-Beauftragten

Die Rolle eines Compliance-Beauftragten in der Versicherungsbranche hat sich im Laufe der Jahre deutlich weiterentwickelt und ist heute eine wichtige Funktion, die die Kontinuität des Geschäftsbetriebs direkt beeinflusst und unterstützt.

Während früher die Rolle des Compliance-Beauftragten darin bestand, Anweisungen und Richtlinien zu verwalten und einzuhalten, hat sich die Rolle heute erheblich erweitert und umfasst nun die strikte Einhaltung der gesetzlich verankerten Compliance- und Regulierungsgesetze. Compliance-Beauftragte sind heute **wichtige Berater** für den Vorstand von Versicherungsunternehmen. Sie setzen sich für eine verantwortungsvolle Geschäftstätigkeit ein, die in vollem Einklang mit den geltenden Gesetzen und Vorschriften steht.

Compliance-Beauftragte müssen sich auch mit **komplexen Themen** befassen, z. B. mit sich überschneidenden Vorschriften und länderspezifischen bzw. regionalen Anforderungen und überwachen Gesetzesänderungen und Branchenstandards. Weiter beraten sie das Management und entwickeln Richtlinien, Verfahren und Systeme, um sicherzustellen, dass das Unternehmen die **gesetzlichen Anforderungen erfüllt**.

Die Komplexität des Compliance- und Regulierungsmanagements führt dazu, dass mehrere gemeinsame strategische Themen und Problembereiche auftreten. Keylane verfügt über fast drei Jahrzehnte Erfahrung und ist daher einzigartig positioniert, um allen modernen Versicherungsanbietern die vollständige Einhaltung der Compliance-Vorgaben zu gewährleisten und ihnen ein sicheres Gefühl zu geben.

Stärkung der Widerstandsfähigkeit

Vorschriften wie EU/DORA und BAFin/VAIT zielen darauf ab, die **Widerstandsfähigkeit** sowohl von Finanzmarktteilnehmern als auch von Infrastrukturanbietern gegen IT-Ausfälle und Cyber-Bedrohungen zu verbessern. In der Praxis bedeutet dies, dass die Versicherer eine Reihe von Prozessen und Systemen implementieren müssen, um die operationellen Risiken zu mindern. Dazu gehört die Implementierung von Failover-Systemen und Datensicherungslösungen, und, was ebenso wichtig ist, die Sicherstellung, dass diese Systeme **ordnungsgemäß getestet werden**. Der Zweck eines Disaster-Recovery-Plans besteht nicht nur darin, die Kontinuität des Geschäftsbetriebs im Falle einer schwerwiegenden Systemstörung zu gewährleisten, sondern auch darin, den Beteiligten die Gewissheit zu geben, dass der Geschäftsbetrieb eines Versicherers reibungslos funktioniert.

Darüber hinaus haben viele Versicherer ihre Investitionen in den Schutz vor Cyberangriffen erhöht. Um diesen Bedrohungen einen Schritt voraus zu sein, ist es wichtig, kontinuierlich und langfristig in die Cybersicherheit zu investieren. Dabei müssen Bedrohungen und Schwachstellen ständig überwacht werden, und bei Bedarf sollten präventive Maßnahmen ergriffen werden.

VAIT/ BaFin

Die VAIT (Versicherungsaufsichtliche Anforderungen an die IT) ist ein von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) in Deutschland formulierter Leitfaden. Diese Anforderungen zielen darauf ab, die Erwartungen der BaFin in Bezug auf die Governance-Anforderungen in Bezug auf Informationssicherheit und Informationstechnologie im Versicherungs- und Betriebsrentenbereich zu klären. Sie bieten eine Anleitung zu angemessenen technischen und organisatorischen Ressourcen für IT-Systeme, wobei der Schwerpunkt auf Informationssicherheit und Risikomanagement liegt. Im Wesentlichen wird in den VAIT dargelegt, wie Versicherungsunternehmen ihre IT-Infrastruktur verwalten und organisieren sollten, um regulatorische Standards zu erfüllen und robuste Sicherheitspraktiken zu gewährleisten.

Redundanz und der Backup-Systeme

Bei kritischen Systemausfällen müssen Versicherer redundante Systeme in Bereitschaft halten, um sicherzustellen, dass kritische Geschäftsprozesse und Daten jederzeit verfügbar und voll funktionsfähig sind. Eine solche Failover-Umgebung mit eigener, unabhängiger Hardware, Netzwerkverbindungen, Stromversorgungen und Datenspeichern muss sofort einsatzbereit sein, um eine vollständige Geschäftskontinuität zu gewährleisten.

Diese Anforderungen gelten für die gesamte Anwendungslandschaft, nicht nur für neue Kernsysteme. Die Anwendungslandschaft muss geclustert und segmentiert werden, was den Aufbau von Firewalls und die Neugestaltung von Zugriffsrechten und Privilegien erfordert. Das ist keine einfache Aufgabe, insbesondere für Versicherer, deren Kerngeschäft auf älteren Systemen und Plattformen basiert. Ältere Softwarearchitekturen sind oft nur begrenzt leistungsfähig, und die Wartung doppelter Standby-Mainframes kann teuer sein.

Angesichts dieser Herausforderungen möchten Versicherungsanbieter heute in Kernplattformen investieren, die vollständig in einer Cloud-Umgebung gehostet und betrieben werden können. Indem Versicherer die Verantwortung für die vollständige Compliance an einen Partner auslagern, erhalten sie auch eine umfassende Backup- und Failover-Funktionalität.

Keylane hostet seine Axon-Plattform unabhängig für jeden Kunden in einer vollständig geclusterten, geografisch getrennten und hochverfügbaren Umgebung und erfüllt so sämtliche an den Markt gestellte Anforderungen. Zusätzlich erhält jeder Kunde umfassende Unterstützung von einem engagierten Team von Keylane-Experten.

Disaster-Recovery-Planung und -Tests

Die aktuellsten Vorschriften verlangen, dass Versicherer jetzt über umfassende Disaster-Recovery-Pläne verfügen müssen. Diese Pläne müssen nachweisen, dass die vorhandene Systemredundanz angemessen, funktionsfähig und zweckdienlich ist. Ein umfassender Disaster-Recovery-Plan sollte alle notwendigen **Wiederherstellungsschritte** für den Fall eines IT-Systemausfalls oder einer Datenpanne aufzeigen.

Im Klartext: Die Aufsichtsbehörden zwingen die Versicherer, ihre Notfallpläne zu testen, um deren Wirksamkeit zu gewährleisten oder um Schwachstellen aufzudecken. Es ist daher unerlässlich, dass die Versicherer Tests und Simulationen unter realen Bedingungen durchführen, um ihre gut durchdachten Pläne in der Praxis zu testen.

Tischsimulationen bieten eine gute Möglichkeit, Disaster-Recovery-Verfahren zu testen. Um jedoch genau zu verstehen, ob die Anwendung, die Datenbank und die Infrastruktur so funktionieren, wie in der Disaster-Recovery-Dokumentation angegeben, sind praktische technische Tests erforderlich. Das Testen von Notfallwiederherstellungsplänen in einem realen Szenario ist jedoch kein triviales Unterfangen, und gut konzipierte Tests und Simulationen sind zeitaufwändig und binden wichtige Ressourcen.

Die Kosten für Notfallwiederherstellungstests sind oft hoch, da sie komplex sind und unterschiedliche Kompetenzbereiche erfordern. Zudem können Tests direkte Auswirkungen auf die Geschäftsabläufe haben. Unternehmen genehmigen möglicherweise seltener Tests aufgrund wahrgenommener Nachteile, was zu blinden Flecken und potenziellen Schwachstellen führen kann. Dies erhöht die Wahrscheinlichkeit einer fehlgeschlagenen Wiederherstellung im Ernstfall – ein Teufelskreis.

Keylane: Kompromissloser Ansatz bei der Notfallwiederherstellung und technische Tests sind Standard.

Keylane verfolgt bei der Notfallwiederherstellung einen kompromisslosen Ansatz und hat vollständige technische Notfallwiederherstellungstests zu einem Standardbestandteil seines IT-Betriebs gemacht (was die Wiederherstellung von Daten und Berichten einschließt).

Keylane führt bis zu zehn vollständige Wiederherstellungstests pro Jahr durch und gibt die Ergebnisse sofort an seine Kunden weiter. Als Teil dieser umfangreichen Tests läuft Keylane sieben Tage lang im Failover-Modus, **um sicherzustellen**, dass der Geschäftsbetrieb nicht unterbrochen wird.

Ausgefeilte Cybersicherheitsmaßnahmen

Da der Abfluss von Daten durch Cyberangriffe wie Malware, Ransomware und Phishing-Betrug immer ausgefeilter und häufiger wird (und die zusätzliche Bedrohung durch KI-gestützte Angriffe das Risiko erheblich erhöht), kann der potenzielle Schaden für die Gesellschaft nicht hoch genug eingeschätzt werden. Als Reaktion auf diese zunehmenden Bedenken schreibt der Gesetzgeber den Versicherern vor, robuste und zukunftssichere **Cybersicherheitsmaßnahmen** einzuführen und aufrechtzuerhalten.

Die meisten Versicherungsunternehmen verfügen bereits über eine erste Verteidigungsschicht, wie beispielsweise Firewall, Antiviren-Software und Intrusion-Detection-Systeme. Hinzu kommen regelmäßige Sicherheitsupdates, Mitarbeiterschulungen zu bewährten Verfahren im Bereich der Cybersicherheit und in einigen Fällen auch „Red Team vs. Blue Team"-Übungen.

Um diesen sich schnell entwickelnden Bedrohungen einen Schritt voraus zu sein, werden engagierte Experten benötigt, die jedoch sehr gefragt und schwer zu halten sind. Es gibt keine hundertprozentig sicheren Maßnahmen, um digitale Unternehmen vollständig vor gegenwärtigen und zukünftigen Cyberangriffen zu schützen. Dennoch muss ein Gleichgewicht gefunden werden, das ein solides Schutzniveau bietet, ohne die Fähigkeit eines Versicherers einzuschränken, effektiv mit Kunden und Geschäftspartnern zusammenzuarbeiten.

Keylane betrachtet Cybersicherheit als eine **integrierte strategische Dienstleistung**. Zusätzlich zu den grundlegenden Maßnahmen implementiert Keylane ausgefeilte Gegenmaßnahmen, zu denen mikrosegmentierte Netzwerke, Endpoint-Detection, Response/Extended-Detection, Response-(EDR/XDR) und ein undurchdringlicher Datentresor (IDV) gehören, der Daten vor unbefugten Zugriffsversuchen schützt.

Altsysteme werden nicht mehr so gründlich gesichert und aktualisiert wie moderne Systeme.

Wartung und System-Updates

Keylane betreibt seine Software-Suite auf einer bewährten und sicheren Infrastruktur, und die Anwendung von Sicherheits-Patches und die Durchführung kritischer Updates werden als kritische Aktivitäten behandelt. Durch das Verfolgen und Verarbeiten von Updates auf der Grundlage des neuesten **Common Vulnerability Security System** (CVSS) integriert Keylane Systemaktualisierungen und Wartungsaufgaben als einen Standardbestandteil seiner täglichen Arbeit.

Für Versicherer, die für ihre Kernprozesse auf Altsysteme angewiesen sind, ist die Realität jedoch nicht ganz so einfach. Altsysteme werden nicht mehr nach demselben Standard gesichert und auf dem neuesten Stand gehalten wie ihre modernen Gegenstücke. Updates werden seltener bereitgestellt, und ihre Installation erfordert in der Regel einen erheblichen Aufwand und spezielle Kenntnisse. Erschwerend kommt hinzu, dass viele Anbieter keinen Support mehr anbieten oder keine Haftung für ihre Plattformen oder einzelne Legacy-Komponenten übernehmen. Diese wachsende Diskrepanz zwingt Versicherer, die von **Legacy-Komponenten** abhängig sind, auf einen unhaltbaren Weg: Sie müssen immer höhere Prämien für erweiterten Support zahlen.

Diese Komplexität führt zu weiteren negativen regulatorischen Auswirkungen, mit denen umgegangen werden muss. Um die Fehlerbehebung und Wiederherstellung zu unterstützen, muss die Dokumentation und Konfiguration aller IT-Systeme auf dem neuesten Stand sein, wie es die Vorschriften und Standards verlangen. Dies kann ein gewaltiges Unterfangen sein und ist oft zeitaufwändig, vielschichtig und ressourcenintensiv, insbesondere wenn ein Versicherer auf externe Parteien angewiesen ist.

Für seine Kunden löst Keylane diese Probleme durch "Infrastructure as Code". Das bedeutet, dass alle Infrastrukturkonfigurationen und Systemdokumentationen mit einem Versionskontrollsystem versehen sind und alle Aktualisierungen der Umgebung vollständig automatisiert werden, um 100 % Transparenz und Konsistenz zu gewährleisten.

Vorfall-Berichterstattung

Aus organisatorischer Sicht ist es wichtig, dass alle Mitarbeiter die Bedeutung des Incidentreportings und die korrekten Verfahren, wie z. B. Eskalationspfade und Schwellenwerte, verstehen.

Neben den umfangreichen Schulungsprogrammen hat Keylane gut dokumentierte Prozesse für die Meldung von Vorfällen implementiert, einschließlich des Umgangs mit Mängeln. Diese Prozesse schreiben vor, wann und wie ein Manager, ein Kunde oder ein Partner zu informieren ist, und beschreiben detailliert, wie Updates zum Lösungsstatus zu übermitteln sind.

Mehrere Vorschriften erzwingen, dass **bedeutende IT-bezogene Vorfälle**, die zu erheblichem Schaden hätten führen können, unverzüglich an die Aufsichtsbehörden gemeldet werden müssen. Das gilt sowohl für tatsächliche als auch Beinahe-Vorfälle. Versicherer müssen also über eine klare und umfassende Richtlinie verfügen, in der festgelegt ist, was ein Vorfall ist, wie Vorfälle zu melden sind, wer für die Meldung verantwortlich ist und welcher Zeitrahmen für die Meldung gilt.

Digital Operational Resilience Act (DORA)

Der Digital Operational Resilience Act (DORA) ist eine EU-Verordnung, die am 16. Januar 2023 in Kraft trat und ab dem 17. Januar 2025 gelten wird. Sie zielt darauf ab, die IT-Sicherheit von Finanzunternehmen wie Banken, Versicherungen und Wertpapierfirmen zu stärken und sicherzustellen, dass der Finanzsektor in Europa in der Lage ist, im Falle einer schweren Betriebsstörung widerstandsfähig zu bleiben. DORA führt zu einer Harmonisierung der Vorschriften für die betriebliche Widerstandsfähigkeit des Finanzsektors, die für 20 verschiedene Arten von Finanzunternehmen und IKT-Drittdienstleistern gelten.

Eine zentrale Herausforderung besteht jedoch darin, **die Auswirkungen** eines Vorfalls **richtig zu verstehen**. EU/DORA zum Beispiel hat eine sehr klare und spezifische Definition, wie ein Vorfall gemeldet werden muss - wie viele Kunden betroffen waren, wie viel Geld verloren ging usw.

Keylane unterstützt seine Kunden bei der Einhaltung der Vorschriften und bietet Standards für die Berichterstattung an die Aufsichtsbehörden.

Wirksames IKT-Risikomanagement

Eine weitere wichtige Forderung im Zusammenhang mit der Einhaltung von Compliance-Vorgaben ist die Einführung eines wirksamen IKT-Risikomanagements. Dabei handelt es sich um einen **fortlaufenden Prozess** zur Erkennung von und Reaktion auf neue Bedrohungen und Schwachstellen, der eine kontinuierliche Überwachung der IKT-Systeme und -Umgebungen erfordert.

Alle Versicherer müssen über ein dokumentiertes und gut umgesetztes **Informationssicherheitsmanagementsystem** (ISMS) verfügen. Ein ISMS legt dar, wie potenzielle Risiken und Bedrohungen für IKT-Komponenten identifiziert und priorisiert werden, und unterstützt Versicherungsunternehmen bei der effektiven Zuweisung von Ressourcen auf der Grundlage der Schwere einer Bedrohung.

Ein häufiger Fallstrick ist es, ein ISMS nur auf dem Papier zu haben, ohne dass es in der Praxis funktioniert.

Um das zu vermeiden, benötigt man sowohl Kenntnisse über Geschäftsprozesse als auch technisches Verständnis. Mitarbeiter mit diesen kombinierten Fähigkeiten sind jedoch selten, und ein Team mit unterschiedlichen Fähigkeiten hat oft Schwierigkeiten, die tatsächlichen **geschäftlichen Auswirkungen** eines technischen Problems zu verstehen.

Das ISMS von Keylane basiert auf den Anforderungen von ISO27001, für die Keylane vollständig zertifiziert ist. Der Risikobeauftragte bei Keylane ist für den ERM-Prozess (Enterprise Risk Management) verantwortlich. Vierteljährlich legt er Geschäftsanforderungen und sich entwickelnde Risikolandschaften vor, die die Risikotoleranzen überschreiten, und diskutiert diese.

Sobald Risiken identifiziert wurden, ergreifen wir Maßnahmen, um diese zu mindern und die Auswirkungen zu reduzieren. Bei Keylane ist dieser Prozess Teil unserer Standardgeschäftsvorgänge und im Risikominderungsplan festgehalten.

Einhaltung von Datenschutz und Privatsphäre

Compliance-Arbeit im Zusammenhang mit Datenschutz und Privatsphäre bedeutet, dass Organisationen die relevanten Gesetze, Vorschriften und Standards einhalten, die die Erfassung, Verarbeitung, Speicherung und Weitergabe von personenbezogenen Daten regeln.

Vor allem die **Datenschutz-Grundverordnung** (DSGVO) ist ein rechtlicher Rahmen, der den Umgang von Unternehmen mit personenbezogenen Daten in der EU verändert hat.

Axon, die einheitliche Versicherungsplattform von Keylane, bietet **End-to-End-Unterstützung** für die Einholung der Zustimmung zur Verwendung personenbezogener Kundendaten, sei es bei der Beantragung von Policen, bei der Schadensregistrierung oder bei der strikten Data Governance im Hinblick auf die Verwaltung aller datenschutzrelevanten Daten im Laufe der Zeit.

Wenn es um die Einhaltung der DSGVO geht, ist der für die Datenverarbeitung Verantwortliche eine wichtige Instanz. Der für die Datenverarbeitung Verantwortliche legt die Zwecke, Bedingungen und Mittel der Verarbeitung personenbezogener Daten fest. Im Wesentlichen entscheidet er, wie und warum personenbezogene Daten verarbeitet werden.

Der Kunde ist zu jeder Zeit der für die Datenverarbeitung Verantwortliche und trägt die volle Verantwortung für die Maßnahmen zum Schutz personenbezogener Daten vor unbefugtem Zugriff, Offenlegung, Änderung und Zerstörung. Der für die Datenverarbeitung Verantwortliche ist auch für die Einhaltung der DSGVO-Anforderungen rechenschaftspflichtig und kann bei Nichteinhaltung mit Strafen belegt werden.

Die ISO 27001-zertifizierten Dienste von Keylane garantieren die Datensicherheit für ihre Kunden durch ein ausgereiftes Informationssicherheitsmanagementsystem mit einem bewährten Risikomanagementprozess für Unternehmen. Dies wird in einer Datenverarbeitungsvereinbarung zwischen dem für die Datenverarbeitung Verantwortlichen (Kunde) und Keylane näher erläutert.

DSGVO (Datenschutz-Grundverordnung)

Die Datenschutz-Grundverordnung (DSGVO) ist eine EU-weite Regelung zum Schutz personenbezogener Daten. Seit ihrem Inkrafttreten am 25. Mai 2018 ist sie verbindlich für alle Unternehmen, die Daten von Bürgern der Europäischen Union verarbeiten. Die Verordnung definiert grundlegende Datenschutzprinzipien und -pflichten, um die Rechte und Freiheiten natürlicher Personen zu gewährleisten. Ihr Hauptziel besteht darin, den Datenschutz zu vereinheitlichen und zu stärken, indem sie klare Vorgaben für die Datenverarbeitung festlegt.

Die Versicherungsplattform von Axon gewährleistet ein umfassendes Einwilligungsmanagement und Data Governance für persönliche Kundendaten bei der Beantragung von Policen, im Schadensfall und im langfristigen Datenschutz.

Strengere Outsourcing-Aufsicht

Das EU/DORA-Gesetz, das ab Januar 2025 in der Europäischen Union in Kraft tritt, ist für viele CIOs ein wichtiges Thema.

Ein Grund dafür ist die sich verändernde Beziehung zwischen einem Versicherungsunternehmen und seinen relevanten Outsourcing-Partnern. EU/DORA stellt **strengere Anforderungen** an Outsourcing-Vereinbarungen, indem es von den Versicherern verlangt, ein System zur Überwachung der Einhaltung der Compliance und der vertraglichen Verpflichtungen von Drittanbietern einzuführen.

Viele Versicherungsunternehmen stehen unter Zeitdruck, um Wissenslücken vor dem Inkrafttreten

des EU/DORA-Gesetzes zu schließen. Diese Aufgabe erfordert ein tiefes Verständnis der Vertragsdetails, kritischer **Outsourcing-Anforderungen**, Vorschriften und ihrer Auswirkungen auf die Leistungserbringung über die gesamte Outsourcing-Partnerkette hinweg.

Die Serviceverträge von Keylane decken die notwendigen regulatorischen Anforderungen ab. Darüber hinaus legt Keylane großen Wert auf fachübergreifende Sitzungen, in denen alle Aspekte der Service Level Agreements gründlich überprüft werden. Zusätzlich zu allen rechtlichen Verpflichtungen legt Keylane klare Überwachungs- und Berichterstattungsverfahren fest und führt regelmäßige Audits, Bewertungen, Sicherheitskontrollen und Leistungsüberprüfungen durch.

Keylane stellt außerdem Service Level Reports, ISO 27001-Zertifizierungs- und ISAE3402-Assurance-Berichte zur Verfügung. Diese Berichte und Überprüfungen sind wesentliche Säulen in der Kommunikation zwischen Versicherer und prüfenden Parteien.

Keylane bietet Service Level Reports, ISO 27001-Zertifizierung und ISAE3402-Assurance-Berichte, die für eine effektive Kommunikation zwischen Versicherern und Prüfern entscheidend sind.

Compliance mit Vertrauen

Es ist offensichtlich, dass Regulierung und Compliance in der Versicherungsbranche entscheidend sind, um Vertrauen und Engagement bei den Versicherungsnehmern zu fördern und eine stabile, berechenbare Branche zu gewährleisten.

Angesichts der zahlreichen Compliance- und Regulierungsprobleme, die es jederzeit zu beachten gilt, müssen Versicherer die **Geschäftskontinuität** stets im Auge behalten. Das ist jedoch keine einfache Aufgabe. Die Verantwortung für die Einhaltung von Vorschriften ist enorm, und ohne den richtigen Partner an der Spitze, der bei der Verwaltung und Aufrechterhaltung dieses Geschäftsbereichs hilft, können ernsthafte Probleme auftreten. Diese können die geschäftliche Flexibilität eines Versicherers einschränken, die Kosten erhöhen und den Ruf gefährden. Die Versicherungsplattform (Software und Infrastruktur) ist das zentrale Element. Sie bildet das Herzstück sowohl des Geschäfts- als auch des IT-Betriebs und ist entscheidend für die Einhaltung der Compliance.

Wenn ein Unternehmen jedoch eine Versicherungsplattform nutzt, die auf veralteten oder nicht mehr aktuellen Komponenten basiert und kritische funktionale Abhängigkeiten sowie veraltete Dokumentation aufweist, wird die vorausschauende Compliance-Arbeit zu einer anspruchsvollen Aufgabe. Versicherungsunternehmen müssen sicherstellen, dass die von ihnen beauftragte Plattform für ein neues Kernversicherungssystem alle **aktuellen und zukünftigen** gesetzlichen Anforderungen erfüllen kann.

Wenn Sie nach einem **vertrauenswürdigen Partner** suchen, der Sie bei der Einhaltung von Compliance unterstützt, sollten Sie darauf achten, dass er mit Ihrem Unternehmen und den gesetzlichen Anforderungen übereinstimmt. Außerdem sollte er risikobewusst und proaktiv gegenüber Cyberangriffen sein und eine transparente Unternehmenskultur sowie eine nachweisliche Erfolgsbilanz bei der Unterstützung von Anbietern in der Versicherungsbranche aufweisen.

Eine Partnerschaft mit Keylane

Unsere Experten bei Keylane haben eine beeindruckende, nachweisliche Erfolgsbilanz bei der Implementierung von Technologien. Gemeinsam mit kompetenten Partnern schaffen sie ein Ökosystem, das es Keylane-Kunden ermöglicht, innovative Dienstleistungen und Produkte anzubieten. Gleichzeitig fördert es den Gewinn, das Kundenwachstum und echte Marktinnovationen.

Keylane hat seinen Hauptsitz in Utrecht in den Niederlanden, beschäftigt über 700 Mitarbeiter und bietet Dienstleistungen für über 225 Versicherungsunternehmen in den Niederlanden, Belgien, Deutschland, Dänemark, Norwegen und der Schweiz an.

T **+49 895 41 96 375**
E **info.dach@keylane.com**
w **keylane.com/de**

#UnlockTomorrow
www.keylane.com

Keylane Axon