MYRA

WHITEPAPER

DORA: Digitale Widerstandsfähigkeit für Versicherer

Executive Summary

Versicherer sind in hohem Maß auf Informations- und Kommunikationstechnologie (IKT) angewiesen – nicht zuletzt aufgrund der stetig steigenden Nachfrage nach digitalen Angeboten. Das macht Versicherer besonders anfällig für Cybervorfälle, die als größter Risikofaktor für die Finanz- und Versicherungsindustrie gelten. Digitale Betriebsstabilität ist daher essenziell.

Um die Cyberresilienz zu stärken, setzen Aufsichtsbehörden auf eine zunehmend straffere Regulatorik. So auch die EU – der Digital Operational Resilience Act (DORA) soll zum einen sicherstellen, dass alle Beteiligten des Sektors die erforderlichen Sicherheitsvorkehrungen getroffen haben, um IKT-bezogene Cybervorfälle abzuwehren oder abzumildern. Zum anderen soll DORA die dafür notwendigen Anforderungen EU-weit harmonisieren.

Compliance-Herausforderungen durch DORA

DORA enthält neue bzw. konkretisierte Vorschriften in Bezug auf Governance, IKT-Risikomanagement, Klassifizierung und Meldung IKT-bezogener Vorfälle, Prüfung der digitalen Betriebsstabilität (Belastbarkeitstests), Steuerung des Risikos durch IKT-Drittanbieter sowie Vereinbarungen zum Informationsaustausch. Daraus ergeben sich neue Herausforderungen und zahlreiche Mehrbelastungen für Versicherungsunternehmen, weil sie ihre Prozesse überprüfen und an die gegenüber nationalen Regelungen wie den MaGo oder VAIT erweiterten Anforderungen anpassen müssen. Das betrifft insbesondere die Zusammenarbeit mit IKT-Drittanbietern.

Drittanbieter auf dem Prüfstand

DORA führt einen Aufsichtsrahmen zur direkten Überwachung von kritischen ITK-Dienstleistern ein, die im Versicherungssektor tätig sind. Um mögliche Strafen zu vermeiden, müssen Versicherer sicherstellen, dass alle Vorgaben – etwa hinsichtlich Risikobewertung, Berichtspflichten und Prüfungsrechten – korrekt umgesetzt sind. Deshalb empfiehlt sich eine erneute Evaluierung, einschließlich Risikoanalyse, der bestehenden Outsourcing-Partner.

Wahl des Dienstleisters ist entscheidend

Mit der Unterstützung hochspezialisierter und zertifizierter Dienstleister können Versicherer die Compliance-Herausforderungen rund um DORA effizient und schnell bewältigen. DSGVO-konforme Rechtssicherheit bei Datenschutz und Auftragsdatenverarbeitung lassen sich mit europäischen Anbietern am einfachsten realisieren. Zwar besteht seit Juli 2023 mit dem EU-US Data Privacy Framework ein neuer Angemessenheitsbeschluss, der den rechtssicheren Datentransfer zwischen der EU und den USA ermöglicht. In der Vergangenheit wurden die Vorgängerabkommen aber jeweils vom Europäischen Gerichtshof kassiert, was jedes Mal Rechtsunsicherheit für die Zusammenarbeit mit US-Dienstleistern zur Folge hatte.

Ausgangslage: Straffere Regulatorik stellt Versicherer vor neue Hürden

Die Finanz- und Versicherungsindustrie steht seit jeher im Fokus von Kriminellen. Früher stürmten maskierte Verbrecher mit vorgehaltener Waffe in Institute, um Gold und Bargeld zu stehlen. Heute haben es Cyberkriminelle auf wertvolle digitale Assets abgesehen.

Versicherungsunternehmen verwalten kritische Datensätze, wie etwa Gesundheitsakten im Fall von Krankenversicherungen. Auch die mathematisch komplexen Berechnungen zur Preisgestaltung von Versicherungspolicen sind als Geschäftsgeheimnis eine attraktive Beute für Cyberkriminelle.

Vor diesem Hintergrund müssen Versicherungen ihre Cyberresilienz und IT-Sicherheit fortlaufend verbessern, Aufsichtsbehörden reagieren auf die digitale Transformation mit einer strafferen Regulatorik, die Versicherungen mehr Engagement bei IT-Sicherheit, Datenschutz und Compliance abverlangt.

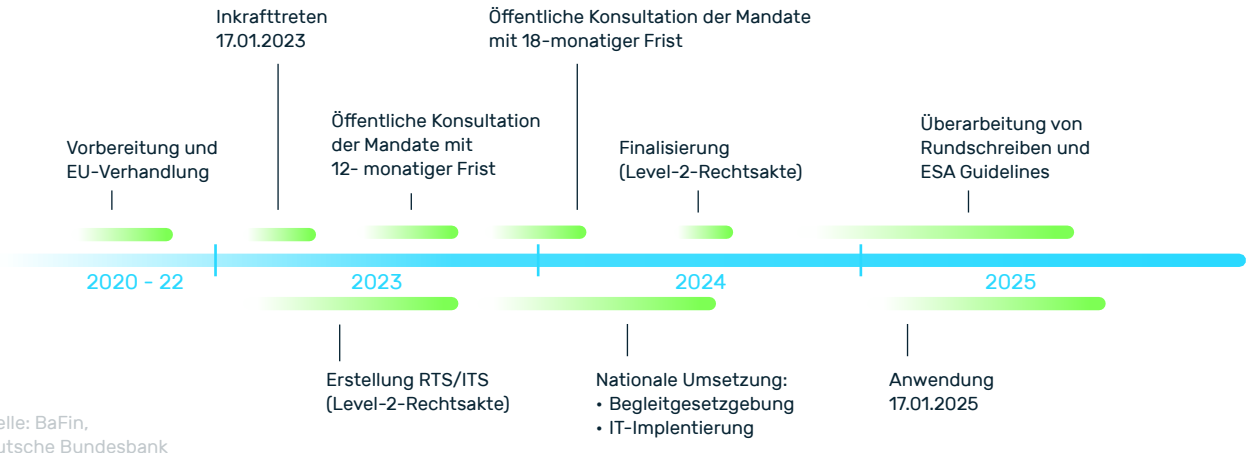
> *Versicherer sind ein beliebtes Ziel von Cyberattacken.*
>
> *Dr. Frank Grund, Exekutivdirektor für die Versicherungsaufsicht bei der BaFin*

DORA führt einen umfassenden Rechtsrahmen auf EU-Ebene ein, der neue beziehungsweise konkretisierte Vorschriften zur digitalen Betriebsstabilität für alle beaufsichtigten Versicherungen, Banken und Finanzdienstleister enthält.

Der Rechtsakt ist Teil eines Maßnahmenpakets zur Digitalisierung des Finanz- und Versicherungssektors, mit dem die Kommission Europas Wettbewerbsfähigkeit und Innovation fördern will. Außer mehr Cybersicherheit verspricht DORA gleiche Wettbewerbsbedingungen für alle Anbieter im europäischen Binnenmarkt – gemäß dem Grundsatz „Gleiche Tätigkeit, gleiche Risiken, gleiche Regeln". So sollen künftig in ganz Europa dieselben regulatorischen Vorgaben für Unternehmen aus der Branche gelten.

Konkret strebt DORA eine EU-weite Harmonisierung der Regeln für das IKT-Risikomanagement sowie der Klassifizierung und Meldung von IKT-Vorfällen an. Zudem sollen EU-weite Standards für digitale operative Belastbarkeitstests definiert werden, um noch unbekannte Anfälligkeiten und Risiken besser zu erkennen. Darüber hinaus geht DORA mit einem Aufsichtsrahmen für kritische ITK-Drittanbieter neue Wege bei der Überwachung von Dienstleistern.

DORA Timeline



Quelle: BaFin, Deutsche Bundesbank

Versicherer müssen bei IT-Sicherheit und Compliance nachjustieren

Aus deutscher Perspektive erweitert bzw. verschärft DORA die Anforderungen an die IT für Versicherungen aus bestehenden Regularien wie den MaGo oder VAIT. Für viele Unternehmen bedeuten die Neuerungen daher erheblichen Mehraufwand. Sie müssen ihre Prozesse bezüglich Governance, IKT-Risikomanagement, Berichterstattung, Belastbarkeitstests, IKT-Risiken Dritter sowie Informationsaustausch überprüfen und gegebenenfalls anpassen oder neu aufsetzen.

Neue EU-Meldevorschriften fordern etwa die Bereitstellung von Berichten zur Ursachenanalyse spätestens einen Monat nach Auftreten eines größeren IKT-Vorfalls. Die Entwicklung von Reaktions- und Wiederherstellungsplänen ist verpflichtend. Die DORA-Vorschriften haben auch direkte Auswirkungen auf die Zusammenarbeit mit IKT-Dienstleistern wie Cloud-Computing-Providern.

Technische Normen als Richtlinien für Compliance

DORA sieht zwar keine Standardisierung spezifischer IKT-Systeme, -Instrumente oder -Technologien vor, setzt aber die angemessene Anwendung europäischer und international anerkannter technischer Normen (z.B. ISO) oder bewährter Branchenverfahren voraus. Dazu zählen etwa die ISO-27000-Familie oder die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte ISO 27001 auf Basis von IT-Grundschutz. Beide befassen sich mit der Ausgestaltung eines Informationssicherheits-Managementsystems (ISMS) und der Einführung aller notwendigen Sicherheitsmaßnahmen.

Ein nach diesen Standards betriebenes ISMS ermöglicht es, potenzielle Risiken frühzeitig zu erkennen und mittels darauf zugeschnittener Gegenmaßnahmen zu minimieren. Auf diese Weise können Unternehmen die Vertraulichkeit, Verfügbarkeit und Integrität sämtlicher Informationen sicherstellen. Allerdings ist eine Zertifizierung nach ISO 27001 allein kein Freifahrtschein für DORA-Konformität.

Zusammenarbeit mit Drittanbietern prüfen

Die Europäischen Aufsichtsbehörden (ESAs) werden unter anderem für die Überwachung des Risikos durch IKT-Drittanbieter technische Regulierungsstandards (Technical Regulatory Standards, RTS) sowie technische Durchführungsstandards (Implementing Technical Standard, ITST) ausarbeiten – diese sollen die ESAs der Kommission bis zum 17. Januar 2024 übermitteln. Das wird manche Versicherer zwingen, sich nach neuen Ausgliederungspartnern umzusehen, denn es ist absehbar, dass nur hochspezialisierte und zertifizierte Anbieter diese Standards erfüllen können. Die Deutsche Kreditwirtschaft erwartet in diesem Zusammenhang eine noch größere Regulierungsdichte und -tiefe.[1]

1 https://die-dk.de/media/files/20201214_DK-Positionen_DORA.pdf

Kernziele von DORA: Erhöhte Cyberresilienz und EU-weite Harmonisierung der dafür nötigen Anforderungen

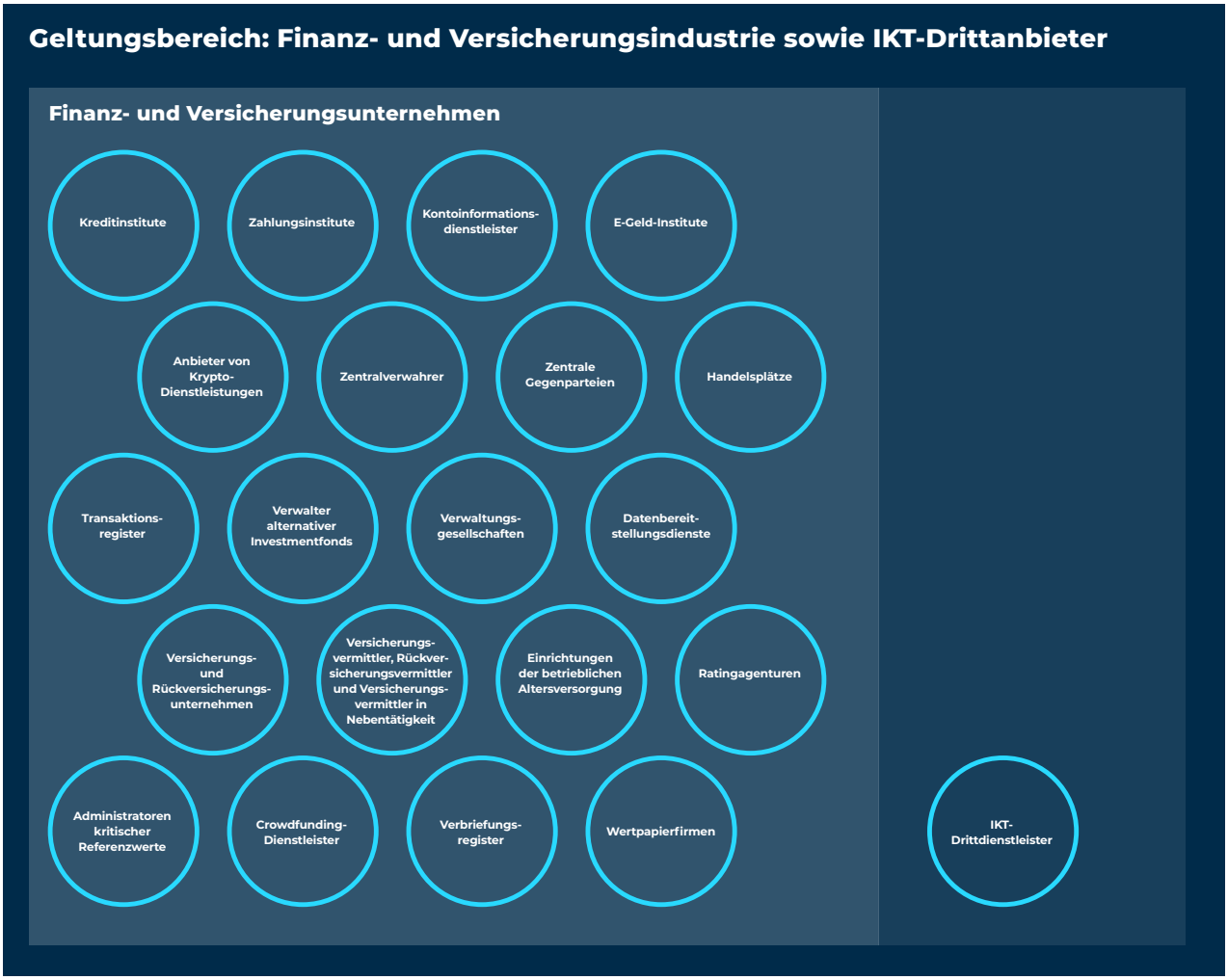
Die Folgen eines Cyberangriffs oder einer Störung bei einem wichtigen, grenzüberschreitend agierenden Finanz- oder Versicherungsunternehmens können weitreichende Auswirkungen auf andere Unternehmen, Teilsektoren oder gar die gesamte übrige Wirtschaft haben. Deshalb ist die digitale Betriebsstabilität im Finanz- und Versicherungssektor von entscheidender Bedeutung. Die EU-Kommission sieht hier noch Nachbesserungsbedarf und hat einige Probleme identifiziert, die DORA lösen soll:

Problem aus EU-Sicht	Angestrebte Lösung
Hohe IKT-Abhängigkeit macht Versicherer und Banken anfällig für Cyberangriffe	Cyberresilienz durch neue bzw. konkretisierte Anforderungen stärken
Fragmentierte und inkonsistente nationale Compliance-Regeln	Fragmentierung und nationale Sonderwege durch EU-weite Harmonisierung abbauen
Hoher regulatorischer Aufwand für europaweit tätige Unternehmen durch fehlende Rechtsklarheit	Rechtliche Klarheit zu Vorschriften für digitale Resilienz schaffen
Fehlen einheitlicher Meldepflichten erschwert Arbeit der Aufsichtsbehörden	Klassifizierung und Meldung von IKT-bezogenen Vorfällen vereinheitlichen
Ausgelagerte Dienstleistungen können nicht direkt durch Aufsichtsbehörden überwacht werden	Aufsichtsrahmen zur direkten Überwachung kritischer IKT-Dienstleister einführen

> *Wir erwarten von den Unternehmen auch strukturelle Anpassungen. IT-Vorfälle müssen erkannt, behoben und – idealerweise – verhindert werden. Mit unseren Prüfungen wollen wir herausfinden, wo die Dinge im Argen liegen.*
>
> *Dr. Frank Grund, Exekutivdirektor Versicherungs- und Pensionsfondsaufsicht, BaFin*

Eine Regulierung für alle

DORA gilt für alle auf EU-Ebene regulierten Finanzunternehmen, von Kredit-, Zahlungs- und E-Geld-Instituten über Versicherungsunternehmen bis hin zu Ratingagenturen. Zusätzlich betrifft die neue Regulierung auch IKT-Drittanbieter, die Dienstleistungen im Finanzsektor erbringen.



Wann treten die DORA-Regelungen in Kraft?

Die finale Fassung von DORA ist am 16. Januar 2023 in Kraft getreten. Die darin formulierten Anforderungen für alle betroffenen Finanzunternehmen greifen unmittelbar, sind aber erst 24 Monate nach Inkrafttreten durchsetzbar. Unternehmen und Institute haben also zwei Jahre Zeit, die neuen Vorgaben umzusetzen. Parallel erarbeiten die ESAs noch die technischen Regulierungs- und Durchführungsstandards (RTS, ITS), welche die Anwendung der neuen Regeln konkretisieren. Die Anwendung von DORA erfolgt dann ab dem 17.01.2025.

Als EU-Verordnung ist DORA unmittelbar wirksam und damit nicht auf eine Überführung in die nationale Gesetzgebung der Mitgliedstaaten angewiesen – wie das etwa bei Richtlinien wie NIS-2 der Fall ist.

Im Fokus: Auswirkungen von DORA auf das Outsourcing von IKT-Dienstleistungen

DORA wird unter anderem zu Anpassungen bei bestehenden nationalen Regelungen zu Ausgliederungen wie z.B. der MaGo und VAIT führen. Gemäß DORA müssen in der EU tätige Versicherer vorab das Risiko einer Ausgliederung bewerten und eine Due-Diligence-Prüfung durchführen, um geeignete Drittanbieter zu identifizieren. Ergänzend dazu heißt es in Artikel 28 Absatz 5: „Finanzunternehmen dürfen vertragliche Vereinbarungen nur mit IKT-Drittdienstleistern schließen, die angemessene Standards für Informationssicherheit einhalten. Betreffen diese vertraglichen Vereinbarungen kritische oder wichtige Funktionen, so berücksichtigen die Finanzunternehmen vor Abschluss der Vereinbarungen angemessen, ob die IKT-Drittdienstleister die aktuellsten und höchsten Qualitätsstandards für die Informationssicherheit anwenden." Zudem sind Verträge mit Drittanbietern durch Analysen von Weiterverlagerungen gründlich zu prüfen, um Konzentrationsrisiken zu vermeiden.

Vertragliche Vereinbarungen mit Dienstleistern aus Drittländern müssen Datenschutz, effektive Durchsetzung des Rechts, insolvenzrechtliche Bestimmungen im Fall des Konkurses des Drittanbieters sowie Einschränkungen, die in Bezug auf die dringende Wiederherstellung der Unternehmensdaten entstehen können, berücksichtigen.

Oversight Framework: Neuer Ansatz zur Beaufsichtigung kritischer IKT-Drittanbieter

Eine wesentliche Neuerung ist das Oversight Framework für kritische IKT-Drittanbieter. Es sieht vor, dass diese direkt von einer der ESAs kontrolliert werden. Die jeweils federführende ESA kann dann auch Informationen anfordern, externe und Vor-Ort-Inspektionen bei den Dienstleistern durchführen, Empfehlungen und Anweisungen aussprechen und bei Nichteinhaltung von Vorgaben Geldstrafen verhängen (bis zu 1 % des durchschnittlichen weltweiten Tagesumsatzes) oder sogar Vertragskündigungen anordnen. Ob ein IKT-Drittanbieter als kritisch eingestuft wird, entscheidet der gemeinsame Ausschuss der ESAs anhand einer in DORA festgelegten Kriterienliste.

Drittanbieter werden sich also auf strengere Regulierung einstellen müssen. Die neuen Aufsichtsmöglichkeiten der ESAs entbinden Versicherer jedoch nicht von ihrer regulatorischen Verantwortung für genutzte IKT-Dienstleister. Wer Dienstleistungen ausgliedert, muss nach wie vor sicherstellen, dass alle in DORA definierten Anforderungen zum Risikomanagement und zur Überwachung der mit kritischen IKT-Drittanbietern geschlossenen vertraglichen Vereinbarungen erfüllt sind.

Wichtige Vertragsbestimmungen

Artikel 30 von DORA schreibt für die vertraglichen Vereinbarungen über die Nutzung von IKT-Diensten eine Reihe von Bestimmungen vor. Unter anderem müssen Verträge diese Themenfelder abdecken:

- Art & Umfang der ITK-Dienstleistung
- Ort(e) der Leistungserbringung
- Datenschutzvorgaben
- Notfallsupport-Vorgaben
- Kooperationsverpflichtung mit zuständigen Behörden
- Notfallpläne
- TLPT (Threat-Led-Penetration-Test)
- Prüfungsrechte
- Kündigungsrechte
- Verpflichtung zur Teilnahme an Awareness-Schulungen
- Ausstiegsstrategien

DORA-Vorgaben erfordern Umdenken bei der Dienstleisterwahl

Nur wenige Drittanbieter können die hohen Anforderungen von DORA vollständig erfüllen. Ob ihr aktueller Dienstleister dazu gehört, sollten Versicherer auf jeden Fall genau überprüfen.

Vor allem beim Thema Datenschutz und Auftragsdatenverarbeitung schauen die Aufsichtsbehörden inzwischen viel genauer hin. Dienstleister müssen – wie die Versicherer selbst – alle Vorschriften der europäischen Datenschutz-Grundverordnung (EU-DSGVO) korrekt umsetzen. Das können letztlich nur europäische Partner in Gänze leisten. In der Praxis werden sich die strengen Anforderungen durch die Wahl eines zertifizierten Drittanbieters aus der EU deutlich einfacher umsetzen lassen.

Von Vornherein als Outsourcing-Partner ausgeschlossen sind IKT-Drittdienstleister ohne Geschäftspräsenz in der EU, deren Betriebsausfall systemische Auswirkungen auf die Erbringung von Finanzdienstleistungen hätte. Vor diesem Hintergrund empfiehlt es sich für Versicherer, ihre Outsourcing-Partner neu zu evaluieren – inklusive Risikoanalyse der Vertragspartner – und sich frühzeitig auf einen eventuell erforderlichen Dienstleisterwechsel vorzubereiten.

Strittige Rechtslage bei außereuropäischen Partnern

Mit dem Wegfall des Privacy-Shield-Abkommens für den transatlantischen Datentransfer zwischen Europa und den USA standen Kooperationen mit US-Anbietern lange Zeit auf wackeligen Füßen. Seit Juli 2023 können auf Grundlage des EU-US Data Privacy Frameworks wieder Datentransfers zwischen europäischen und US-amerikanischen Unternehmen getätigt werden. Die neue „Rechtssicherheit“ ist allerdings mit Vorsicht zu genießen. In Fachkreisen wird der Nachfolger von Privacy Shield kontrovers diskutiert. Der Datenschützer Max Schrems hat bereits angekündigt, juristisch gegen das EU-US Data Privacy Framework vorzugehen, da es „keine substanzielle Änderung des US-Überwachungsrechts“ biete.

Übersicht: die zentralen Anforderungen von DORA an Versicherer

Viele der in DORA[2] formulierten Anforderungen sind grundsätzlich schon aus bestehenden Regularien für den Finanzsektor wie den EBA-Leitlinien, MaGo oder VAIT bekannt und werden in der Praxis bereits umgesetzt. Das gilt zum Beispiel für die Einbeziehung der Geschäftsleitung, die Ernennung von Ausgliederungsbeauftragten, das Erarbeiten von Krisenkommunikationsplänen sowie das Management und die Klassifizierung von Vorfällen. Hier entsteht für die meisten Versicherer keine Mehrbelastung.

Teilweise gehen die DORA-Anforderungen aber auch über die Vorgaben von MaGo, VAIT und Co hinaus oder schärfen diese. Das betrifft beispielsweise den Bereich IKT-Risikomanagement (einschließlich Risikomanagementrahmen, Identifizierung, Schutz und Prävention, Erkennung anomaler Aktivitäten sowie Gegenmaßnahmen und Wiederherstellung), die Beaufsichtigung von IKT-Drittanbietern und die Prüfung von IKT-Systemen.

Zudem verfolgt DORA statt eines prinzipienorientierten einen regelbasierten Ansatz mit konkreten Vorgaben zur Zielerreichung. Die von den ESAs noch auszuarbeitenden Standards werden detaillierte Umsetzungsmethoden festlegen, was Versicherer und Finanzdienstleistern im Vergleich zu den bisherigen Regelungen weniger Handlungsspielraum lässt.

Angesichts der geplanten direkten Kontrollen von IKT-Drittanbietern durch die ESAs werden Versicherer auch überprüfen müssen, ob ihre Dienstleister die strengen Vorgaben umsetzen können (siehe Fokus-Thema Seite 7). Die folgenden Seiten geben einen kompakten Überblick über die zentralen Anforderungen von DORA.

2 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R2554

Governance und Organisation

- **Starke Einbeziehung der Geschäftsleitung:** Die Geschäftsleitung definiert, genehmigt und überwacht alle Vorkehrungen im Zusammenhang mit dem IKT-Risikomanagementrahmen und ist für die Umsetzung rechenschaftspflichtig. Dazu zählen das Festlegen der Risikotoleranz, das Zuweisen klarer Rollen und Zuständigkeiten, die Vergabe angemessener Budgets, die Freigabe von Audit-, Business-Continuity- und Wiederherstellungsplänen sowie das Überprüfen der Zusammenarbeit mit IKT-Drittanbietern.
- **Ernennung eines Ausgliederungsbeauftragten:** Finanzunternehmen müssen eine Funktion einrichten oder ein Mitglied der höheren Führungsebene benennen, das die mit IKT-Drittanbietern geschlossene Vereinbarungen überwacht und dokumentiert.
- **Fortbildungspflichten:** Um IKT-Risiken und deren Auswirkungen auf die Geschäftstätigkeit nachvollziehen und bewerten zu können, sind Mitglieder der Geschäftsleitung verpflichtet, regelmäßig Fachschulungen zu absolvieren.

IKT-Risikomanagement

- **IKT-Risikomanagementrahmen:** Finanzunternehmen müssen über einen IKT-Risikomanagement-rahmen verfügen, der es ihnen ermöglicht, IKT-Risiken schnell, effizient und umfassend zu adressieren. Die dadurch sichergestellte Betriebsstabilität soll den geschäftlichen Bedürfnissen, der Größe und der Komplexität des Finanzinstituts entsprechen. DORA ergänzt bzw. konkretisiert hier die Anforderungen von MaGo und Co.
- **Identifizierung:** Unternehmen müssen Geschäftsfunktionen und diese unterstützende Informations-ressourcen, die potenzielle Quellen eines IKT-Risikos darstellen, identifizieren, klassifizieren und dokumentieren. Das gilt insbesondere für Systembereiche, die mit internen und externen IKT-Systemen vernetzt sind. Wer nicht als Kleinstunternehmen gilt, muss für alle Altsysteme regelmäßig, mindestens jedoch einmal jährlich, eine spezifische IKT-Risikobewertung durchführen.
- **Schutz und Prävention:** Die Funktionsweise der IKT-Systeme muss kontinuierlich überwacht und kontrolliert werden, um einen angemessenen Schutz zu gewährleisten. Dafür sind vorbeugend geeignete Sicherheitsstrategien, -richtlinien, -verfahren und -tools zu implementieren.
- **Erkennung:** Unternehmen müssen über Mechanismen verfügen, um anomale Aktivitäten umgehend zu erkennen und alle potenziellen Schwachstellen zu ermitteln. Dies wird im Vergleich zu MaGo zu Mehrbelastungen führen.
- **Reaktion und Wiederherstellung:** Unternehmen sind verpflichtet, Reaktions- und Wiederherstellungs-maßnahmen zu ergreifen sowie entsprechende Notfallstrategien und -pläne zur Fortführung des Geschäftsbetriebs zu entwickeln. Selbst Firmen, die sonst bereits viele der IKT-Risikomanagement-Anforderungen von DORA erfüllen, sollten daher prüfen, ob auch ihre Reaktions- und Wiederher-stellungsstrategien und -pläne den erweiterten Regeln in diesen Bereichen entsprechen.
- **Kommunikation:** Firmen müssen einen Krisenkommunikationsplan erarbeiten, der „eine verantwortungsbewusste Offenlegung IKT-bezogener Vorfälle oder erheblicher Anfälligkeiten“ gegenüber Kunden, anderen Finanzunternehmen und der Öffentlichkeit ermöglicht.

Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle

- **Prozess für die Behandlung IKT-bezogener Vorfälle:** Finanzunternehmen müssen einen spezifischen Incident-Management-Prozess zur Identifizierung, Verfolgung, Protokollierung, Kategorisierung und Klassifizierung von IKT-bezogenen Vorfällen einrichten und anwenden.
- **Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen:** Die Klassifizierung IKT-bezogener Vorfälle muss anhand von Anzahl, Kunden-Relevanz, Dauer, Ausfallzeit, betroffene Gebiete, Verluste von Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit, Kritikalität der betroffenen Dienste sowie die wirtschaftlichen Auswirkungen.
- **Meldung schwerwiegender IKT-bezogener Vorfälle und freiwillige Meldung erheblicher Cyber-bedrohungen:** Unternehmen sind verpflichtet, schwerwiegende IKT-Vorfälle innerhalb vorgeschriebener Fristen und unter Verwendung harmonisierter Berichtsvorlagen der zuständigen Behörde zu melden.

Testen der digitalen operationalen Resilienz

- **Allgemeine Anforderungen für das Testen der digitalen operationalen Resilienz:** Als integralen Bestandteil des IKT-Risikomanagementrahmens fordert DORA von Unternehmen die Einführung eines soliden und umfassenden Programms zur Prüfung der digitalen Betriebsstabilität, das IKT-Instrumente, -systeme und -prozesse abdeckt. Das Programm muss die gesamte Bandbreite geeigneter Testmethoden umfassen, darunter Analysen von Open-Source-Software, Bewertungen der Netzsicherheit, Lückenanalysen, Analysen und Überprüfungen der physischen Sicherheit, Scansoftwarelösungen, Kompatibilitätstests, Leistungstests, End-to-End-Tests oder Penetrationstests. Alle kritischen IKT-Systeme und -Anwendungen sind mindestens einmal jährlich zu prüfen.
- **Erweiterte Tests von IKT-Tools, -Systemen und -Prozessen auf Basis von TLPT:** Bestimmte Finanzinstitute müssen mindestens alle drei Jahre erweiterte Prüfungen ihrer IKT-Instrumente, -systeme und -prozesse anhand bedrohungsorientierter Penetrationstests (Threat Led Penetration Testing, TLPT) auf Basis von TIBER-EU[3] durchführen. Diese Tests ermöglichen eine realitätsnahe Überprüfung der Cyberwiderstandsfähigkeit eines Unternehmens unter kontrollierten Bedingungen. Ziel ist es, Schwachstellen in kritischen Systemen, organisatorischen Strukturen und Prozessen zu identifizieren und anschließend zu beseitigen. Dazu führen Red-Teaming-Dienstleister auf Grundlage einer spezifischen Bedrohungsanalyse Attacken auf die Produktivsysteme durch, wobei sie aktuelle Vorgehensweisen realer Angreifer imitieren. Die angegriffenen operativen Stellen sind nicht über die Tests informiert und versuchen, die Attacken mit allen verfügbaren Mitteln abzuwehren. Die erweiterten Prüfungen gehen über das hinaus, was MaGo, VAIT und Co fordern. Betroffene Firmen sollten daher genau verfolgen, wie die ESAs die Durchführungskriterien ausarbeiten.

Management des IKT-Drittparteienrisikos

- **Allgemeine Prinzipien:** Finanzunternehmen müssen das Risiko durch IKT-Drittanbieter innerhalb ihres IKT-Risikomanagementrahmens in Einklang mit bestimmten Grundsätzen steuern. Diese umfassen Verantwortung und Haftung, Verhältnismäßigkeit, eine Strategie für das Risiko durch IKT-Drittanbieter, Dokumentation und Aufzeichnung, Analyse vor Vertragsabschluss, Informationssicherheit, Prüfungen und Inspektionen, Kündigungsrechte sowie Ausstiegsstrategien. Das Oversight Framework ersetzt nicht die Steuerung des Risikos, das die Nutzung von IKT-Drittanbietern mit sich bringt, durch Finanzunternehmen und tritt weder in irgendeiner Form noch für irgendeinen Aspekt an deren Stelle.
- **Vorläufige Bewertung des IKT-Konzentrationsrisikos auf Unternehmensebene:** Die verpflichtende vorläufige Bewertung durch die Finanzunternehmen zielt darauf ab, festzustellen, ob der Abschluss einer vertraglichen Vereinbarung in Bezug auf IKT-Dienste zu einem Vertrag führen würde, der nicht ohne Weiteres ersetzbar ist. Ebenso soll sie zeigen, ob mehrere vertragliche Vereinbarungen über die Erbringung von IKT-Diensten mit demselben oder einem eng verbundenen Dienstleister getroffen wurden. Dadurch sollen Konzentrations- und Lock-in-Risiken vermieden werden.
- **Wesentliche Vertragsbestimmungen:** Die Rechte und Pflichten des Finanzunternehmens und des IKT-Drittanbieters müssen eindeutig zugewiesen und in einer vertraglichen Vereinbarung festgelegt werden, deren detaillierter Umfang in den Rechtsvorschriften definiert wird.

Vereinbarungen über den Austausch von Informationen

- **Vereinbarungen über den Austausch von Informationen und Erkenntnissen zu Cyberbedrohungen:** DORA soll einen europäischen Standard etablieren, der es Finanzunternehmen ermöglicht, auf freiwilliger Basis Informationen und Erkenntnisse zu Cyberbedrohungen untereinander auszutauschen, um die digitale Betriebsstabilität zu stärken. Das umfasst Indikatoren für Beeinträchtigungen, Taktiken, Techniken, Verfahren, Cybersicherheitswarnungen und Konfigurationstools.

3 https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

Roundup: DORA-Konformität steht und fällt mit dem Dienstleister

Die mit DORA angestrebte Umsetzung EU-weiter Sicherheitsstandards, harmonisierter Tests und einheitlicher Berichtsstrukturen ist ein notwendiger Schritt zur Stärkung der Cyberwiderstandsfähigkeit im europäischen Finanz- und Versicherungssektor. Denn je mehr sich das Tagesgeschäft von Versicherern, Banken und Finanzdienstleistern in digitale Umgebungen verlagert, desto wichtiger wird die Absicherung gegen Cyberbedrohungen. Das haben auch die Aufsichtsbehörden erkannt.

> *Ein Phänomen, das gleichermaßen für Chancen und Risiken steht, ist die Digitalisierung. Sie hilft Banken und Versicherern, Prozesse zu beschleunigen, und bietet neue Vertriebs- und Ertragsmöglichkeiten. Sie macht die Unternehmen aber auch verletzlich. Operationelle Resilienz ist daher für uns Aufseher genauso wichtig wie finanzielle Resilienz geworden.*
>
> *Mark Branson, Präsident der BaFin*

Daraus resultiert eine striktere und umfangreichere Regulatorik, die für immer höhere Compliance-Herausforderungen sorgt. Für Versicherer bedeutet DORA in Summe eine deutliche Mehrbelastung: Sie werden sich intensiver denn je mit ihrer IT-Architektur sowie Compliance-Themen befassen und im Detail die Maßnahmen, die unter MaGo und VAIT bereits getroffen wurden, überprüfen und anpassen müssen.

Eine wesentliche Neuerung bringt DORA im Bereich der Zusammenarbeit mit Drittanbietern. Hier müssen Versicherer ihre IKT-Dienstleister auf jeden Fall genau prüfen und neu bewerten, um sicherzustellen, dass alle DORA-Vorgaben erfüllt sind. Auf Cybersicherheit spezialisierte Dienstleister mit technologischem Know-how, den relevanten Zertifizierungen und Expertise in Sachen Ausgliederung und sektorspezifischer Compliance können hier effektiv unterstützen. Mit ihrer Hilfe sind Versicherer in der Lage, alle regulatorischen Vorgaben ohne großen Inhouse-Aufwand zu erfüllen und gleichzeitig ihre technisch-prozessualen Anforderungen effektiv abzudecken.

Disclaimer:

Bitte beachten Sie, dass noch nicht alle Informationen zu den konkreten Vorgaben von DORA final vorliegen. Es besteht daher die Möglichkeit, dass sich rechtliche Rahmenbedingungen und Bestimmungen möglicherweise ändern können. Eine Überarbeitung des Whitepapers erfolgt, sobald die finalen Informationen kommuniziert wurden.

Wir übernehmen keine Gewähr für die Richtigkeit, Vollständigkeit oder Aktualität der Informationen in diesem Whitepaper. Die Inhalte dienen lediglich zu Informationszwecken und stellen keine rechtliche Beratung dar. Jegliche Haftung oder Verantwortung für Handlungen, die auf der Grundlage der in diesem Whitepaper bereitgestellten Informationen getätigt werden, wird hiermit ausgeschlossen.

Security, Performance und Compliance aus einer Hand

- **DORA-ready:** Myra erfüllt alle zentralen Anforderungen von DORA hinsichtlich Risikomanagement, Reporting, Testing und Ausgliederung
- **Revisionssicher:** Myra erfüllt alle Anforderung an Ausgliederungen gemäß MaGo, VAIT und DORA
- **Investitionssichere Technologie:** vollautomatische Angriffsmitigation, hochperformante Auslieferung, maximale Skalierbarkeit
- **Rechtssicherer Datenschutz:** DSGVO-konformer Spezialanbieter mit Branchenexpertise
- **Hochzertifizierte Qualität:** ISO 27001 auf Basis von IT-Grundschutz, PCI-DSS-zertifiziert, BSI-KRITIS-qualifiziert, BSI-C5-Testat Typ 2, IDW PS 951 Typ 2, DIN-EN-50600-zertifizierte Rechenzentren, Trusted Cloud
- **Green IT:** Zertifizierte Umwelt- und Energiemanagementsysteme der Rechenzentren nach ISO 14001 und ISO 50001

Erstklassige Service-Qualität dank BSI-zertifizierter Sicherheit

Die Myra-Technologie ist vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach dem Standard ISO 27001 auf Basis von IT-Grundschutz zertifiziert. Zudem erfüllen wir als einer der führenden Anbieter weltweit alle 37 Kriterien des BSI für qualifizierte KRITIS-Sicherheitsdienstleister. Damit setzen wir den Maßstab in der IT-Sicherheit.

ISO 27001 BSI zertifiziert auf der Basis von IT-Grundschutz Zertifikat Nr.: BSI-IGZ-0479-2021 | PCI DSS Certified | BSIG KRITIS-qualifiziert | EU-DSGVO konform | BSI C5 Testat Typ 2 | Trusted Cloud Service 10043 | ISAE 3402 IDW PS 951 Type 2 | DIN EN 50600 zertifiziert Betriebssicheres Rechenzentrum

Zertifiziert vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach ISO 27001 auf Basis von IT-Grundschutz | Zertifiziert nach Payment Card Industry Data Security Standard | KRITIS-qualifiziert nach §3 BSI-Gesetz | Konform mit der (EU) 2016/679 Datenschutz-Grundverordnung | BSI-C5-Testat Typ 2 | Geprüfter Trusted Cloud Service | IDW PS 951 Typ 2 (ISAE 3402) geprüfter Dienstleister | Zertifizierung von Rechenzentren nach DIN EN 50600

Wir schützen, was zählt. In der digitalen Welt.

Die Myra-Technologie überwacht, analysiert und filtert schädlichen Internet-Traffic bevor virtuelle Angriffe einen realen Schaden anrichten. Unsere zertifizierte Security-as-a-Service-Plattform schützt Ihre digitalen Geschäftsprozesse vor vielfältigen Risiken wie DDoS-Angriffen, Bot-Netzwerken und Angriffen auf Datenbanken.

Die Bundesregierung | 1822direkt Ein Unternehmen der Frankfurter Sparkasse | Finoa | Liechtensteinische Landesbank 1861 | Finanzportal | datatrans. | flatex DEGIRO | inous