MYRA

WHITEPAPER

DORA: Harmonisierte Regulatorik für mehr Cybersicherheit im EU-Finanzsektor erhöht Compliance-Hürden

Executive Summary

Der Finanzsektor ist in hohem Maß auf Informations- und Kommunikationstechnologie (IKT) angewiesen – nicht zuletzt aufgrund der stetig steigenden Nachfrage nach digitalen Angeboten. Das macht Banken und Finanzdienstleister besonders anfällig für Cybervorfälle, die als größter Risikofaktor für die Finanzindustrie 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 Finanzsektors die erforderlichen Sicherheitsvorkehrungen getroffen haben, um IKT-bezogene Cybervorfälle abzuwehren oder abzumildern. Zum anderen soll DORA die dafür notwendigen Anforderungen EU-weit harmonisieren.

Höhere Compliance-Hürden 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 Finanzunternehmen, weil sie ihre Prozesse überprüfen und an die gegenüber nationalen Regelungen wie MaRisk und BAIT 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 Finanzsektor tätig sind. Um mögliche Strafen zu vermeiden, müssen Finanzunternehmen 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.

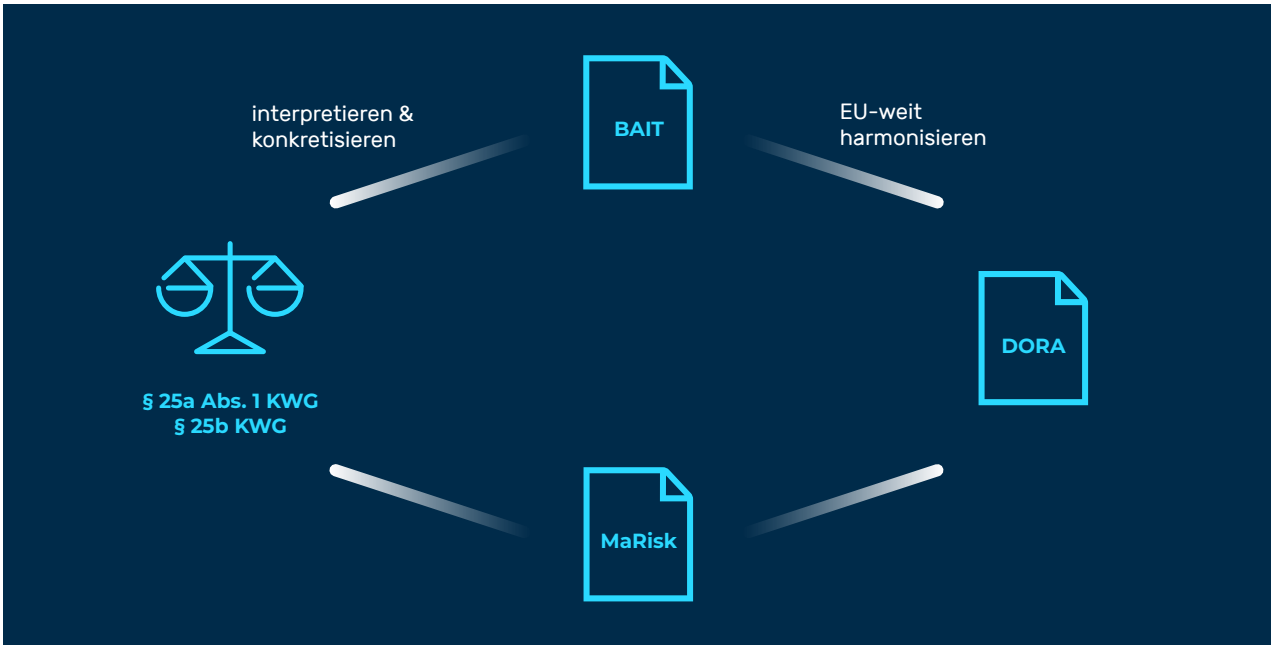
Wahl des Dienstleisters ist entscheidend

Mit der Unterstützung hochspezialisierter und zertifizierter Dienstleister können Finanzunternehmen die mit DORA einhergehenden Compliance-Hürden ohne großen Mehraufwand meistern. Wer nach dem Wegfall des Privacy-Shield-Abkommens absolute Rechtssicherheit bei Datenschutz und Auftragsdatenverarbeitung will, sollte zudem einen Anbieter aus der EU wählen. Damit ist sichergestellt, dass alle regulatorischen Anforderungen an IT-Sicherheit, Datenschutz und Compliance vollumfänglich erfüllt sind.

Ausgangslage: Straffere Regulatorik stellt Finanzindustrie vor neue Herausforderungen

Die Finanzindustrie steht seit jeher im Fokus von Kriminellen. Früher stürmten maskierte Verbrecher mit vorgehaltener Waffe in die Bank, um Gold und Bargeld zu stehlen. Heute haben es Cyberkriminelle auf wertvolle digitale Assets abgesehen. Laut Boston Consulting Group[1] sind Banken und Finanzdienstleister 300-mal häufiger das Ziel von Cyberangriffen als andere Unternehmen. Die Allianz listet Cybervorfälle in ihrem Risk Barometer 2023 sogar als größten Risikofaktor für die Finanzbranche.[2]

Vor diesem Hintergrund müssen Banken ihre Cyberresilienz und IT-Sicherheit fortlaufend verbessern, so wie sie sich mit gepanzerten Transportern, Tresorräumen und Wachpersonal vor Raubüberfällen schützen. Aufsichtsbehörden reagieren auf die digitale Transformation mit einer strafferen Regulatorik, die Instituten mehr Engagement bei IT-Sicherheit, Datenschutz und Compliance abverlangt.



MaRisk und BAIT interpretieren und konkretisieren gleichermaßen die gesetzlichen Anforderungen aus dem KWG (§ 25a Abs. 1/ § 25b). Zielsetzung von DORA ist wiederum, übergeordnet einheitliche Vorgaben für die Finanzindustrie zu definieren. Die existierende Regulierung soll dabei unter Wahrung der Verhältnismäßigkeit auf europäischer Ebene harmonisiert werden.

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

Der Rechtsakt ist Teil eines Maßnahmenpakets zur Digitalisierung des Finanzsektors, mit dem die Kommission Europas Wettbewerbsfähigkeit und Innovation im Finanzsektor fördern will. Außer mehr Cybersicherheit verspricht DORA gleiche Wettbewerbsbedingungen für alle Anbieter von Finanzdienstleistungen 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 Finanzbranche 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.

1 Boston Consulting Group - Global Wealth 2019 - Reigniting Radical Growth
2 Allianz Global Corporate & Specialty - Allianz Risk Barometer 2023

Finanzunternehmen müssen bei IT-Sicherheit und Compliance nachjustieren

Aus deutscher Perspektive erweitert bzw. verschärft DORA die Anforderungen an die IT für Finanzunternehmen aus bestehenden Regularien wie den MaRisk. Für viele Banken und Finanzdienstleister 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) ausarbeiten – diese sollen die ESAs der Kommission bis zum 17. Januar 2024 übermitteln. Das wird manche Institute zwingen, sich nach neuen Auslagerungspartnern umzusehen, denn es ist absehbar, dass nur hochspezialisierte und zertifizierte Anbieter diese RTS erfüllen können. Die Deutsche Kreditwirtschaft erwartet in diesem Zusammenhang eine noch größere Regulierungsdichte und -tiefe.[3]

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

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

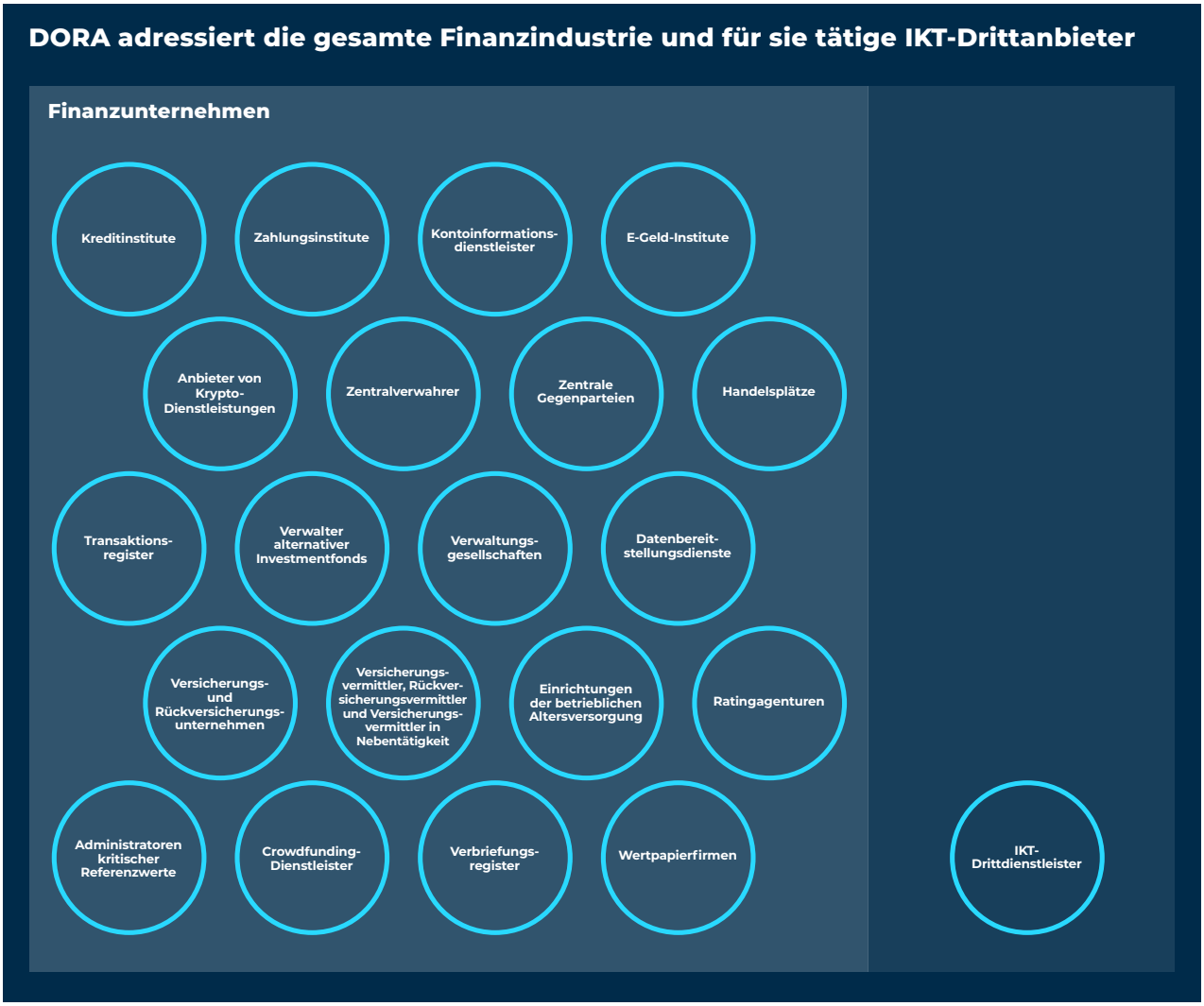
Die Folgen eines Cyberangriffs oder einer Störung bei einem wichtigen, grenzüberschreitend agierenden Finanzdienst können weitreichende Auswirkungen auf andere Unternehmen, Teilsektoren oder gar die gesamte übrige Wirtschaft haben. Deshalb ist die digitale Betriebsstabilität im Finanzsektor von entscheidender 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 Finanzunternehmen 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 Finanzunternehmen 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

> *Die Harmonisierung der verschiedenen europäischen Regulierungsansätze zur Sicherheit der Finanz-IT, die der DORA-Entwurf anstrebt, ist ein notwendiger Schritt zur Verbesserung der Cyberwiderstandsfähigkeit im Finanzsektor.*
>
> *Bundesverband deutscher Banken e.V.*

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 werden die ESAs noch technische Standards ausarbeiten, welche die Anwendung der neuen Regeln konkretisieren.

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

DORA wird unter anderem zu Anpassungen bei bestehenden nationalen Regelungen zu Auslagerungen wie z.B. der MaRisk und BAIT führen. Gemäß dem aktuellen DORA-Entwurf müssen in der EU tätige Finanzunternehmen vorab das Risiko einer Auslagerung 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 geplante Oversight Framework für kritische IKT-Drittanbieter. Es sieht vor, dass diese künftig 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 einem Prozent des 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 Finanzunternehmen jedoch nicht von ihrer regulatorischen Verantwortung für genutzte IKT-Dienstleister. Wer Dienstleistungen auslagert, 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 hochspezialisierte und zertifizierte Drittanbieter können die hohen Anforderungen von DORA vollständig erfüllen. Ob ihr aktueller Dienstleister dazu gehört, sollten Finanzunternehmen auf jeden Fall genau überprüfen.

Vor allem beim Thema Datenschutz und Auftragsdatenverarbeitung schauen die Aufsichtsbehörden inzwischen viel genauer hin. Dienstleister müssen – wie die Finanzunternehmen selbst – alle Vorschriften der europäischen Datenschutz-Grundverordnung (EU-DSGVO) korrekt umsetzen. Das können letztlich nur europäische Partner leisten. In der Praxis werden sich die strengen Anforderungen durch die Wahl eines zertifizierten Drittanbieters aus der EU deutlich einfacher umsetzen lassen. Hier können sich Finanzunternehmen sicher sein, dass alle Vorgaben hinsichtlich Sicherheit, Datenschutz und Compliance erfüllt sind.

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 Finanzunternehmen, ihre Outsourcing-Partner neu zu evaluieren – inklusive Risikoanalyse der Vertragspartner – und sich frühzeitig auf einen eventuell erforderlichen Dienstleisterwechsel vorzubereiten.

Rechtsunsicherheit bei außereuropäischen Partnern

Mit dem Wegfall des Privacy-Shield-Abkommens für den transatlantischen Datentransfer zwischen Europa und den USA stehen Kooperationen mit US-Anbietern auf wackeligen Füßen. Rechtssichere Datentransfers sind aufgrund der konträren Positionierung von europäischer DSGVO und US-Recht nur schwer umzusetzen. Daran ändern auch die Anfang Juni von der EU-Kommission verabschiedeten neuen Standardvertragsklauseln nichts, weil sie etwaige Konflikte mit nationalem Recht von Drittstaaten in letzter Konsequenz nicht abschließend lösen. Ein besonderes Hemmnis stellt in diesem Zusammenhang der US CLOUD Act dar, der international operierende US-Unternehmen zur Herausgabe von Daten verpflichtet, wenn diese von US-Behörden angefragt werden. Durch die Wahl lokaler Anbieter, die der europäischen Rechtsprechung unterliegen, lassen sich solche Hürden umgehen.

Übersicht: die zentralen Anforderungen von DORA an Banken und Finanzdienstleister

Viele der in DORA[4] formulierten Anforderungen sind grundsätzlich schon aus bestehenden Regularien für den Finanzsektor wie den EBA-Leitlinien, MaRisk oder BAIT bekannt und werden in der Praxis bereits umgesetzt. Das gilt zum Beispiel für die Einbeziehung der Geschäftsleitung, die Ernennung von Auslagerungsbeauftragten, das Erarbeiten von Krisenkommunikationsplänen sowie das Management und die Klassifizierung von Vorfällen. Hier entsteht für die meisten Finanzunternehmen keine Mehrbelastung.

Teilweise gehen die DORA-Anforderungen aber auch über die Vorgaben von MaRisk 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 technischen Regulierungsstandards werden detaillierte Umsetzungsmethoden festlegen, was Banken und Finanzdienstleistern im Vergleich zu den bisherigen Regelungen weniger Handlungsspielraum lässt.

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

4 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 Auslagerungsbeauftragten:** 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 MaRisk 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 MaRisk 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 einer Reihe von Kriterien erfolgen, die vom Gemeinsamen Ausschuss der ESAs weiterentwickelt werden sollen.
- **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[5] 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 MaRisk 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 geplante 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 mit einem marktbeherrschenden IKT-Drittanbieter 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.

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

Fazit: Dienstleister nehmen eine zentrale Rolle bei der Bewältigung der Mehrbelastung durch die DORA-Regulatorik ein

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

> *[…] IT-Governance und Informationssicherheit [haben] für die Aufsicht inzwischen den gleichen Stellenwert wie die Ausstattung der Institute mit Kapital und Liquidität.*
>
> *Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)*

Daraus resultiert eine striktere und umfangreichere Regulatorik, die für immer höhere Compliance-Hürden sorgt. Für Banken und Finanzdienstleiser 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 MaRisk und BAIT bereits getroffen wurden, überprüfen und anpassen müssen.

Eine wesentliche Neuerung bringt DORA im Bereich der Zusammenarbeit mit Drittanbietern. Hier müssen Institute 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 Auslagerung / Compliance für den Finanzsektor können hier effektiv unterstützen. Mit ihrer Hilfe sind Finanzunternehmen in der Lage, alle regulatorischen Anforderungen ohne großen Inhouse-Aufwand zu erfüllen und ihre Bedürfnisse nach Cybersicherheit, Performance und Compliance gleichermaßen abzudecken.

Das macht Myra zum richtigen Partner für die Finanzindustrie

- Myra erfüllt alle zentralen Anforderungen von DORA hinsichtlich Risikomanagement, Reporting, Testing und Auslagerung
- Revisionssicher: Myra erfüllt alle Anforderung an die wesentliche Auslagerung nach KWG § 25, MaRisk AT9 und BAIT
- Investitionssichere Technologie: vollautomatische Angriffsmitigation, hochperformante Auslieferung, maximale Skalierbarkeit
- 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, Trusted Cloud, IDW PS 951 Typ 2

Erstklassige Service-Qualität dank zertifizierter Sicherheit

Als Spezialanbieter im Finanzsektor und in anderen sensiblen Bereichen ist es für Myra selbstverständlich, dieselben strengen Anforderungen zu erfüllen wie unsere Kunden. Die umfassenden Zertifizierungen von Myra sorgen dafür, dass unsere Kunden bei Sicherheit und Compliance das Maximum erreichen. Myra ist hochzertifiziert und erfüllt als einer der führenden Anbieter alle 37 Kriterien des BSI für qualifizierte KRITIS-Sicherheitsdienstleister. Damit setzen wir den Maßstab in der IT-Sicherheit.

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

Myra Security ist der neue Maßstab für globale IT-Sicherheit

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.