MYRA

DORA-Compliance mit Myra

Mit der DORA-Verordnung (Digital Operational Resilience Act) ist seit 17. Januar 2023 erstmals eine EU-weit einheitliche Regulierung zur Stärkung der Cybersicherheit und digitalen Resilienz des Finanz- und Versicherungsmarktes in Kraft. In sechs wesentlichen Bereichen definiert DORA hierfür konkrete Anforderungen an regulierte Unternehmen und angeschlossene IKT-Dienstleister.

Als selbst durch DORA regulierter Schutzdienstleister erfüllt Myra alle technischen, prozessualen und vertraglichen Anforderungen, die mit der neuen Verordnung einhergehen. Unsere Kunden profitieren von umfassend zertifizierten und auditierten Lösungen und Prozessen. Diese tragen maßgeblich zur Erfüllung der Compliance-Anforderungen von DORA bei.

In diesem Compliance Fact Sheet erfahren Sie, wo Myra Ihr Institut bei der DORA-Umsetzung unterstützen kann.

Disclaimer:

Bitte beachten Sie, dass die bereitgestellten Informationen nach bestem Wissen und Gewissen und mit juristischer Unterstützung erstellt wurden. Dennoch dienen Sie rein informativen Zwecken und sind nicht als rechtliche Beratung zu verstehen. Eine pauschale Beurteilung regulatorischer Vorgaben ist aufgrund der individuellen Anforderungen eines jeden Instituts nicht möglich.

Wir übernehmen keine Gewähr für Richtigkeit, Vollständigkeit oder Aktualität der folgenden Informationen. Jegliche Haftung oder Verantwortung für Handlungen, die auf der Grundlage der bereitgestellten Informationen getätigt werden, wird hiermit ausgeschlossen.

DORA-Timeline

2020
Vorbereitung und Verhandlung auf EU-Ebene

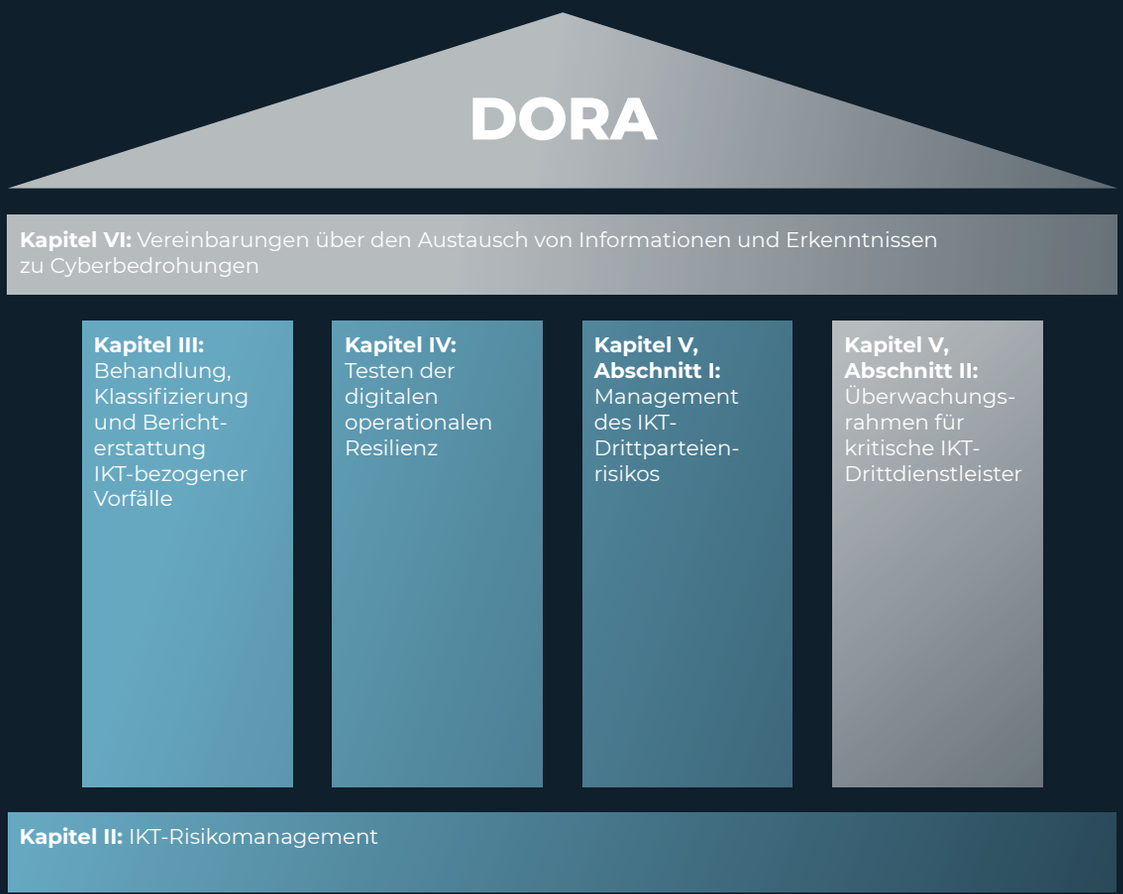
2023
Inkrafttreten der Verordnung und der Änderungsrichtlinie am 17. Januar 2023

2023/2024
Erstellung von Level-2- und Level-3-Rechtstexten, öffentliche Konsultation und nationale Umsetzungsarbeiten

2024
Finalisierung der Level-2- und Level-3-Rechtstexte und Annahme durch EU-Kommission

2025
Anwendung von DORA ab dem 17. Januar 2025

2028
Überprüfung durch die EU-Kommission



Compliance-Übersicht: DORA konzentriert sich auf sechs wesentliche Bereiche zur Stärkung der digitalen operationellen Resilienz des gesamten europäischen Finanzsektors. Myra kann mit seinen Lösungen, Prozessen und Vertragsleistungen in vier Bereichen zur Erfüllung der Compliance-Anforderungen von Finanzunternehmen beitragen.

	DORA-Anforderungen	Umsetzungsansatz durch Myra	
Kapitel II	**Artikel 6, IKT-Risikomanagementrahmen** fordert ein Regelwerk mit Strategien, Richtlinien, Verfahren und Werkzeugen, um Informationen und IT-Systeme wie Computer, Software und Infrastruktur angemessen vor Risiken wie Beschädigung und unbefugtem Zugriff zu schützen. Ziel ist die Gewährleistung der Sicherheit aller IT-Assets.	Myra bietet die geeigneten Lösungen und Dienstleistungen zum Schutz von IKT-Informationen und IKT-Assets vor Cyberangriffen auf der Infrastruktur- und Anwendungsebene. Alle Lösungen sind umfassend zertifiziert und werden regelmäßig auditiert (siehe Artikel 7).	✓
	Artikel 7, IKT-Systeme, -Protokolle und -Tools definiert Vorgaben für den Einsatz zuverlässiger und leistungsstarker IKT-Systeme, die den Geschäftsanforderungen angemessen sind und auch unter Stressbedingungen resilient bleiben. Diese Systeme ermöglichen es, Risiken effektiv zu managen.	Die Myra-Technologien und Dienstleistungen zum Schutz von IKT-Informationen und IKT-Assets vor Cyberangriffen auf der Infrastruktur- und Anwendungsebene entsprechen dem Stand der Technik gemäß ISO 27001 auf Basis von IT-Grundschutz, PCI DSS, BSI C5 Testat Typ 2, KRITIS-Nachweis gemäß § 8a Abs. 3 BSIG, IDW PS 951 n. F. Typ 2 sowie VS-NfD.	✓

	DORA-Anforderungen	Umsetzungsansatz durch Myra	
Kapitel II	**Artikel 9, Schutz und Prävention** verpflichtet zur kontinuierlichen Überwachung der Sicherheit von IT-Systemen und zum Einsatz spezieller Tools, Richtlinien und Verfahren, um Risiken zu minimieren und hohe Standards für Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten aufrechtzuerhalten. Zu diesem Zweck sind angemessene IT-Lösungen und -Prozesse einzusetzen, die die Sicherheit der Datenübertragung gewährleisten.	Myra bietet Finanzunternehmen die erforderlichen Schutzlösungen, um Verfügbarkeit, Sicherheit und Integrität von IKT-Informationen und IKT-Assets auf der Infrastruktur- und Anwendungsebene sicherzustellen. Als einer der führenden Anbieter erfüllt Myra alle 37 Kriterien des BSI für qualifizierte DDoS-Mitigation-Dienstleister.	✓
	Artikel 10, Erkennung verpflichtet zur Einführung von Mechanismen, um anomale Aktivitäten, Leistungsprobleme in IT-Netzwerken und IT-Vorfälle umgehend zu erkennen, potenzielle kritische Schwachstellen zu ermitteln, automatisch geeignete Gegenmaßnahmen einzuleiten und den Vorfall zu melden.	Das Monitoring von Myra erlaubt die Identifikation von IKT-bezogenen Vorfällen auf Traffic-Ebene. Dank frei definierbarer Schwellenwerte erkennt Myra Anomalien in Echtzeit und reagiert mit geeigneten Abwehrmaßnahmen auf Cyberangriffe. Über sämtliche Aktionen werden Kunden umgehend über die konfigurierten Kanäle und Eskalationspfade benachrichtigt.	✓
	Artikel 11, Reaktion und Wiederherstellung verpflichtet, die IKT-Geschäftsfortführungsleitlinie durch angemessene Regelungen, Pläne und Verfahren zu implementieren, um kritische Funktionen aufrechtzuerhalten, rasch und wirksam auf IT-Vorfälle zu reagieren, Schäden zu begrenzen und Wiederherstellung einzuleiten.	Die Lösungen von Myra tragen dazu bei, die Anforderungen an die IKT-Geschäftsfortführungsleitlinie von Finanzunternehmen zu erfüllen. Die Schutzlösungen von Myra greifen automatisch und sichern damit die Business Continuity.	✓
	Artikel 12, Richtlinie und Verfahren zum Backup sowie Verfahren und Methoden zur Wiedergewinnung und Wiederherstellung verpflichtet, redundante IT-Kapazitäten vorzuhalten, um den Geschäftsbetrieb abzusichern. Zentralverwahrer benötigen zudem mindestens einen sekundären Standort, der kritische Funktionen übernehmen und die Kontinuität des Geschäftsbetriebs gewährleisten kann.	Die Schutzsysteme von Myra erlauben eine Absicherung von Redundanzen über mehrere Rechenzentren und Cloud-Instanzen hinweg, um eine gleichbleibende Schutzfunktionalität und Qualität sicherzustellen.	✓
	Artikel 16, Vereinfachter IKT-Risikomanagementrahmen verpflichtet kleinere Finanzunternehmen dazu, einen soliden IT-Risikomanagementrahmen aufzubauen, die IT-Systeme zu überwachen, IT-Risiken zu minimieren, Vorfälle zu erkennen, Abhängigkeiten von Drittanbietern zu ermitteln, die Kontinuität kritischer Funktionen sicherzustellen, Notfallpläne zu testen und das Personal entsprechend zu schulen.	Unabhängig von der Unternehmensgröße sichern die Lösungen von Myra Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von IKT-Informationen und IKT-Assets auf der Infrastruktur- und Anwendungsebene. Darüber hinaus können die Lösungen zur Ermittlung und Dokumentation von Anomalien und IKT-bezogener Vorfälle eingesetzt werden.	✓
Kapitel III	**Artikel 17, Prozess für die Behandlung IKT-bezogener Vorfälle** verpflichtet, einen Prozess zur Erkennung, Behandlung und Meldung IT-bezogener Vorfälle und erheblicher Cyberbedrohungen einzurichten. Dabei werden Frühwarnindikatoren eingesetzt und Verfahren zur Ermittlung, Nachverfolgung, Protokollierung, Kategorisierung und Priorisierung der Vorfälle nach Schweregrad und Kritikalität der betroffenen Dienste implementiert.	Die Schutzlösungen von Myra dienen der Erkennung und Behandlung von IKT-bezogenen Vorfällen und Cyberangriffen auf der Infrastruktur- und Anwendungsebene. Durch die Monitoring-Funktionalitäten und anpassbare Schwellenwerte kann Myra als Frühwarnsystem für Anomalien dienen und dank Reportings zu Vorfällen auch für die Protokollierung und Meldung von Vorfällen eingesetzt werden.	✓

	DORA-Anforderungen	Umsetzungsansatz durch Myra	
Kapitel III	**Artikel 18, Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen** erfordert, IKT-Vorfälle anhand der Anzahl betroffener Kunden, der Dauer des Vorfalls, der geografischen Ausbreitung und der Datenverluste hinsichtlich Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit zu bewerten.	Durch die Monitoring- und Reporting-Funktionen der Lösungen liefert Myra detaillierte Informationen zu Dauer und Umfang von Traffic-Anomalien und Angriffen. Diese Daten können von Finanzunternehmen zur Klassifizierung von Cybervorfällen und Bedrohungen herangezogen werden.	✓
Kapitel IV	**Artikel 25, Testen von IKT-Tools und -Systemen** verpflichtet dazu, ein umfassendes Programm für Tests der digitalen operationalen Resilienz als Teil ihres IKT-Risikomanagements zu erstellen, zu pflegen und zu überprüfen. Dieses Programm beinhaltet verschiedene Testarten wie Schwachstellenanalysen, Penetrationstests und Szenario-basierte Tests, um Schwächen zu erkennen und Korrekturmaßnahmen einzuleiten.	Myra unterstützt Finanzunternehmen umfassend bei der Durchführung von Belastungs- und Penetrationstests auf der Infrastruktur- und Anwendungsebene. Wir begleiten bei der Durchführung von Tests, übernehmen das Monitoring und die Auswertung der Ergebnisse und optimieren auf Grundlage der gewonnenen Erkenntnisse das bestehende Schutz-Setup des Finanzunternehmens.	✓
	Artikel 26, Erweiterte Tests von IKT-Tools, -Systemen und -Prozessen auf Basis von TLPT verpflichtet bei Einbindung von IKT-Drittdienstleistern in Resilienz-Tests deren Mitwirkung sicherzustellen und die Einhaltung der Vorschriften zu gewährleisten. Zudem müssen die Unternehmen in Zusammenarbeit mit Dienstleistern und Testern effektive Risikomanagementkontrollen anwenden. Nach Abschluss der Tests sind die Ergebnisse, Abhilfemaßnahmen und Nachweise über die Durchführung des TLPT der zuständigen Behörde vorzulegen.	Myra sichert Finanzunternehmen die Mitwirkung bei erweiterten Tests zu, stellt die dabei aufgezeichneten Monitoring-Ergebnisse zur Analyse sowie zur Weitergabe an die zuständigen Aufsichtsbehörden bereit und optimiert das Schutz-Setup anhand der resultierenden Pläne für Abhilfemaßnahmen. Die regelmäßige Durchführung bedrohungsorientierter Penetrationstests zählt zur standardmäßigen Absicherung unserer Qualitätsstandards.	✓
Kapitel V	**Artikel 28, Allgemeine Prinzipien** verpflichtet Finanzunternehmen, bei Vertragsabschluss mit IKT-Drittdienstleistern deren Einhaltung angemessener Informationssicherheitsstandards zu überprüfen. Für kritische Funktionen müssen die Unternehmen zusätzlich sicherstellen, dass die Dienstleister die höchsten Sicherheitsstandards anwenden.	Myra wird den Anforderungen für die „aktuellsten und höchsten Qualitäts-standards für die Informationssicherheit“ gerecht. Als einer der führenden Anbieter erfüllt Myra alle 37 Kriterien des BSI für qualifizierte DDoS-Mitigation-Dienstleister. Zudem sind die Schutzlösungen von Myra umfassend zertifiziert und regelmäßig auditiert.	✓
	Artikel 30, Wesentliche Vertragsbestimmungen verpflichtet Finanzunternehmen, in Verträgen mit IKT-Drittdienstleistern die beiderseitigen Rechte und Pflichten eindeutig festzulegen, insbesondere zu Dienstleistungen, Standorten, Datenschutz, Service-Leveln, Vorfallmanagement und Aufsichtszusammenarbeit. Für kritische Funktionen sind zusätzlich quantitative Service-Level-Ziele und Notfallpläne des Dienstleisters verpflichtend.	Myra erfüllt selbstverständlich aufsichts-rechtliche Vertragsanforderungen und verfügt über das erforderliche Vertragswerk gemäß den Bestimmungen aus KWG/MaRisk/ BAIT/KAIT/ZAIT und VAIT. Auf Grundlage der noch ausstehenden technischen Regulierungsstandards zur Präzisierung der Vertragsbestimmungen werden Anpassungen erfolgen, um auch die Anforderungen der DORA-Verordnung zu erfüllen.[1]	✓

1 Die entsprechenden RTS sind aktuell in der dreimonatigen Prüfungsphase und erscheinen voraussichtlich Mitte Juni 2024.

Detailverweise in der DORA-Verordnung

IKT-Risikomanagementrahmen: Artikel 6 Absatz 2, **IKT-Systeme, -Protokolle und -Tools:** Artikel 7 a–d, **Schutz und Prävention:** Artikel 9 Absatz 1–3, **Erkennung:** Artikel 10 Absatz 1–2, **Reaktion und Wiederherstellung:** Artikel 11 Absatz 2 a–d, **Richtlinie und Verfahren zum Backup sowie Verfahren und Methoden zur Wiedergewinnung und Wiederherstellung:** Artikel 12 Absatz 4–5 b **Vereinfachter IKT-Risikomanagementrahmen:** Artikel 16 Absatz 1, a–g, **Prozess für die Behandlung IKT-bezogener Vorfälle:** Artikel 17 Absatz 1–3 a–b, **Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen:** Artikel 18 Absatz 1 a–d, **Testen von IKT-Tools und -Systemen:** Artikel 25 Absatz 1, **Erweiterte Tests von IKT-Tools, -Systemen und -Prozessen auf Basis von TLPT:** Artikel 26 Absatz 3; Absatz 5-6, **Allgemeine Prinzipien:** Artikel 28, Absatz 5, **Wesentliche Vertragsbestimmungen:** Artikel 30 Absatz 1–2 a–i; Absatz 3 a–c