DORA-Readiness für Provider-Verträge

Was bestehende IT-Outsourcing-Verträge jetzt leisten müssen

Ausgangslage

Mit dem Digital Operational Resilience Act (DORA) hat die EU ein Regulierungswerk geschaffen, das die digitale Betriebsstabilität des Finanzsektors durchgängig festlegt. Die Verordnung ist seit dem 17. Januar 2025 unmittelbar anwendbar und gilt für nahezu alle beaufsichtigten Finanzunternehmen — von Banken und Versicherern über Kapitalverwaltungsgesellschaften bis hin zu Zahlungsdienstleistern. Für die IT bedeutet das eine grundlegende Neubewertung von Drittparteien-Risiken und bestehenden Provider-Verträgen.

Die Herausforderung liegt weniger in der technischen Umsetzung als in der Breite des Eingriffs in gewachsene Vertragslandschaften. Nahezu jeder strategische IT-Vertrag muss überprüft, in Teilen nachverhandelt und dokumentiert werden — parallel zu Service Due Diligence, Exit-Strategien und einem laufenden Informationsregister gegenüber der Aufsicht.

Was Artikel 30 DORA konkret fordert

Artikel 30 DORA listet die Mindestvertragsinhalte für Vereinbarungen mit IKT-Drittdienstleistern auf. Gegenüber klassischen Outsourcing-Regelwerken ist der Katalog deutlich konkreter und strenger — er umfasst rund 40 Pflichtpunkte, die in der Summe nur wenige Bestandsverträge heute vollständig erfüllen.

Kernbereiche im Überblick

- **Leistungsbeschreibung und Service Levels:** vollständige, überprüfbare Beschreibung der Dienste inklusive quantitativer SLAs und Standorte der Leistungserbringung.
- **Datenverarbeitung und -schutz:** Ort der Verarbeitung, Speicherung und Verfügbarkeit von Daten, Vertraulichkeits- und Integritätsanforderungen.
- **Sicherheit und Resilienz:** Anforderungen an Sicherheitsniveaus, Incident Response, Business Continuity und Disaster Recovery.
- **Audit-Rechte und Aufsicht:** uneingeschränkte Prüfungsrechte für das Finanzunternehmen und die zuständigen Behörden, einschließlich Vor-Ort-Prüfungen.
- **Unterauftragsverhältnisse:** Transparenz, Zustimmungsvorbehalte und Durchgriffspflichten entlang der Subcontracting-Kette.
- **Exit und Kündigung:** belastbare Exit-Klauseln, Mitwirkungspflichten des Providers, Datenrückgabe und geordnete Übergabe an Nachfolger.
- **Meldung und Zusammenarbeit:** Information bei Störungen, Cyber-Vorfällen und aufsichtlichen Anfragen in engen Fristen.

Typische Gaps in bestehenden Verträgen

In der Praxis zeigen sich wiederkehrende Muster, an denen Bestandsverträge am DORA-Maßstab scheitern:

- Exit-Regelungen existieren formal, bleiben aber operativ unverbindlich — kein Exit-Plan, keine Mitwirkungspflicht in der Transition, keine Kostenregelung.

• Audit-Rechte sind auf jährliche, angekündigte Prüfungen beschränkt und umfassen weder Vor-Ort- noch anlassbezogene Audits durch die Aufsicht.

• Subcontracting ist nur generisch geregelt; eine durchgängige Transparenz über die Kette gibt es nicht.

• Daten-Lokation und -Verarbeitung sind nicht abschließend definiert, insbesondere bei Cloud- und SaaS-Komponenten.

• Meldefristen bei Störungen liegen hinter den DORA-Vorgaben zurück oder sind nicht eindeutig vereinbart.

Vorgehen: Von der Bestandsaufnahme zur Nachverhandlung

Eine DORA-Readiness ist kein einmaliges Dokumentations-Projekt, sondern ein strukturiertes Programm, das Vertrags-, Service- und Compliance-Logik miteinander verbindet. Bewährt hat sich ein Vorgehen in vier Schritten:

1. Service Due Diligence

Für jeden IKT-Drittdienstleister wird zunächst der tatsächliche Service umfassend erfasst: Leistungsinhalt, Kritikalität, Standorte, Datenkategorien, Unterauftragnehmer, operative Abhängigkeiten. Diese Inventarisierung ist nicht nur Grundlage für den regulatorisch geforderten Informationsregister-Eintrag, sondern auch für die spätere Vertrags-Gap-Analyse.

2. Gap-Analyse gegen den DORA-Katalog

Bestehende Verträge werden systematisch gegen die rund 40 Pflichtinhalte des Artikel 30 DORA abgeglichen. Das Ergebnis ist eine vertrags- und themenbezogene Gap-Liste, die eine belastbare Priorisierung erlaubt — unterschieden nach rechtlicher, operativer und aufsichtlicher Dringlichkeit.

3. Priorisierte Nachverhandlung

Statt in einer Einzelvertragssicht zu verhandeln, hat sich der Cluster-Ansatz bewährt: inhaltlich ähnliche Provider (z.B. Hyperscaler, Netzwerk-Integratoren, Fach-SaaS) werden parallel bearbeitet. Pro Cluster werden Standard-Klauseln definiert, die dann mandantenspezifisch angepasst werden. Das reduziert Verhandlungsaufwand und sichert gleichzeitig Konsistenz über das Portfolio.

4. Vertrags-Repository und Governance

Die Ergebnisse fließen in ein zentrales Vertrags-Repository, das den regulatorischen Dokumentationspflichten gerecht wird und die laufende Pflege (Änderungen, Re-Assessments, Exit-Tests) unterstützt. Ohne dauerhafte Governance ist die erreichte Readiness nach sechs Monaten wieder Makulatur.

Pull-Quote

> *DORA ist keine Compliance-Übung, die man auslagern kann. Die Pflichten treffen das Finanzunternehmen — nicht den Provider. Wer Verträge nur vom Juristen ergänzen lässt, ohne die Services und das Betriebsmodell mitzudenken, baut Risiken auf statt sie abzubauen.*

Praxis-Empfehlungen

• **Früh starten.** Die Verhandlungsbereitschaft der großen Provider ist endlich; Standard-Addenda sind begehrt.

- **Service und Vertrag gemeinsam betrachten.** Ein DORA-konformer Vertragstext ohne belastbares Service Management bleibt Papier.
- **Priorisieren.** Nicht alle Provider sind kritisch. Die Klassifizierung nach Kritikalität entscheidet über Tiefe und Reihenfolge.
- **Exit testen, nicht nur schreiben.** Ein Exit-Plan, der nicht mindestens einmal simuliert wurde, ist keiner.
- **Register pflegen.** Das Informationsregister ist kein Snapshot, sondern ein laufendes Artefakt.

Fazit

DORA zwingt Finanzunternehmen dazu, ihre Provider-Landschaft nicht nur vertraglich, sondern operativ durchgängig zu beherrschen. Das ist unbequem — aber es bringt Transparenz, klare Rollen und belastbare Steuerung zurück in ein Feld, das in vielen Häusern über Jahre gewachsen und nur noch schwer steuerbar war. Wer die Umsetzung strukturiert angeht, gewinnt nicht nur aufsichtliche Sicherheit, sondern auch Verhandlungsmacht für die nächsten Vertragsrunden.

Über 3rd opinion

Die 3rd opinion GmbH berät Unternehmen im IT Sourcing, Contract & Provider Management sowie im Service Management. Wir begleiten DORA-Readiness-Programme von der Bestandsaufnahme bis zur laufenden Governance — unabhängig, produktneutral und mit Fokus auf belastbare Entscheidungsgrundlagen.