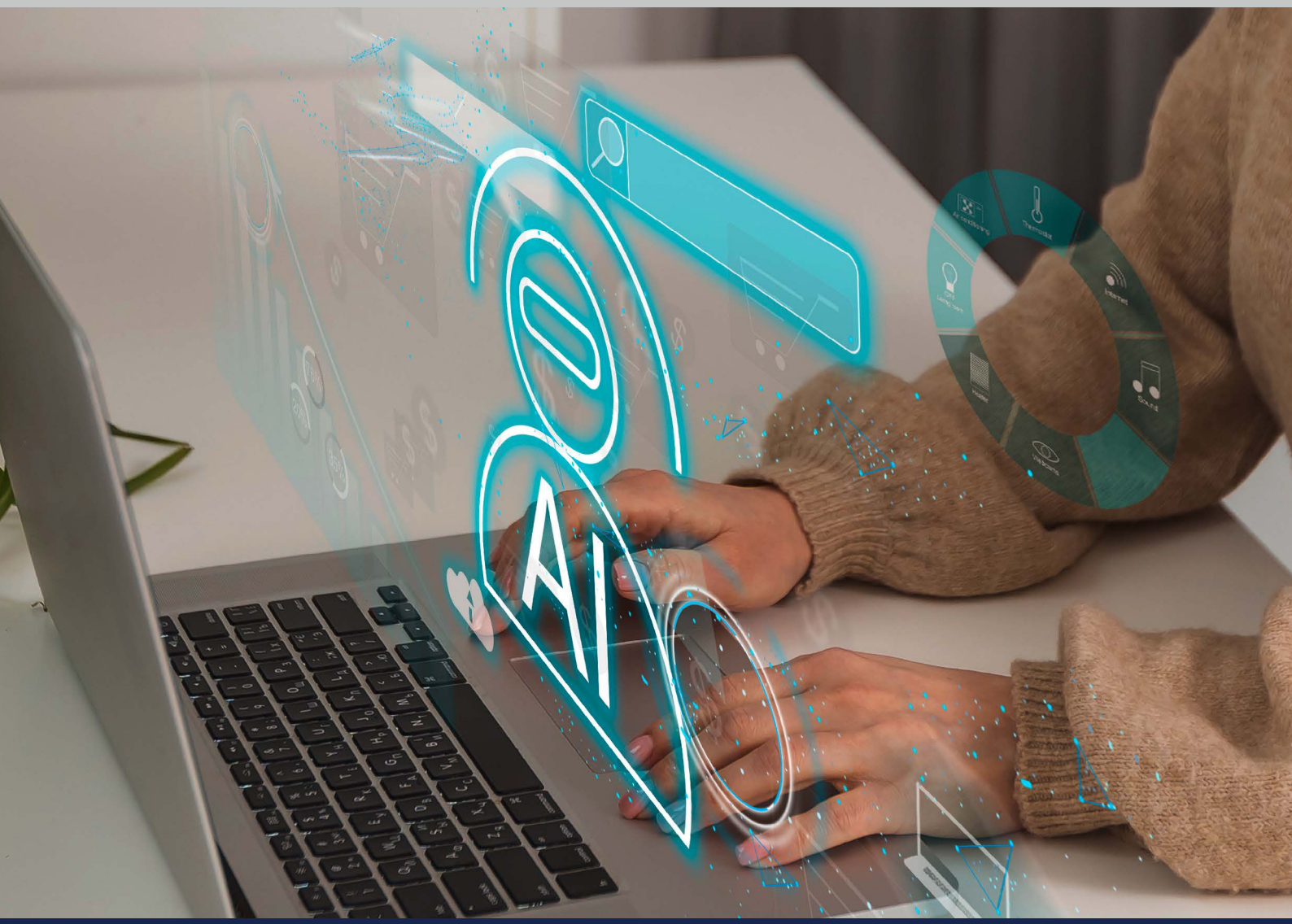
FORUM



Von Onboarding bis Offboarding: DORA-Lifecycle für IKT-Drittanbieter

So steuern Finanzunternehmen Drittparteienbeziehungen entlang des DORA-Lebenszyklus

Josefine Spengler

Sehr geehrte Leser*innen,

mit DORA (Verordnung (EU) 2022/2554) gelten neue Anforderungen an das Lifecycle-Management von IKT-Drittparteienbeziehungen. Finanzunternehmen müssen IT- und Cloud-Dienstleister strukturiert von Onboarding bis Offboarding steuern – von Planung und Vertragsgestaltung über Monitoring bis zur Beendigung und zum Exit. Dieses Whitepaper gibt einen kompakten Überblick über regulatorische Anforderungen, zentrale Phasen und praktische Herausforderungen und zeigt, wie Sie Ihre DORA-Compliance und operative Resilienz stärken.

Über die Autorin

Josefine Spengler ist Fachanwältin für IT-Recht und Expertin für Zahlungsdiensteaufsichtsrecht, IT- und Datenschutzrecht sowie Geldwäsche-Compliance. Sie berät insbesondere zu regulatorischen IT-Anforderungen im Finanzsektor und entwickelt praxisnahe Datenschutz- und Compliance-Konzepte. Als Spezialistin für das FinTech-Umfeld verbindet sie juristische Expertise mit technischem Verständnis und ist zudem Autorin des Blogs PAYMENT.TECHNOLOGY.LAW.

Rechtsgrundlagen und interne Dokumente zum IKT-Drittparteienmanagement

Die Kernvorgaben zum Management der IKT-Drittparteienbeziehungen finden sich in Art. 28 DORA. Sie decken den gesamten Lebenszyklus eines IKT-Bezugs ab und werden durch einen Level-2-Rechtsakt zu DORA, den RTS „Leitlinie zur Nutzung von IKT-Dienstleistungen“ (RTS Third Party Policy – RTS TPPol[1]) konkretisiert.

Gemäß Art. 28 Abs. 2 DORA müssen Finanzunternehmen, die nicht lediglich den vereinfachten Risikomanagementrahmen nach Art. 16 DORA anwenden müssen, im Rahmen ihres IKT-Risikomanagements eine Strategie für das IKT-Drittparteienrisiko beschließen und diese regelmäßig überprüfen. Die Strategie berücksichtigt ggfs. auch die Strategie zur Nutzung mehrerer IKT-Anbieter auf Gruppen- oder Unternehmensebene (vgl. Art. 6 Abs. 9 DORA) und umfasst insbesondere eine Leitlinie für den Einsatz von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen. Sie gilt auf individueller sowie – soweit relevant – auf konsolidierter Gruppenebene. Das Leitungsorgan trägt die Verantwortung, das Gesamtrisikoprofil des Unternehmens sowie Umfang und Komplexität der Geschäftsaktivitäten einzubeziehen und die aus IKT-Drittparteienverträgen resultierenden Risiken fortlaufend zu bewerten.

Die entsprechenden Finanzunternehmen sind nach Art. 28 Abs. 2 DORA, Art. 4 RTS TPPol auch verpflichtet, eine Leitlinie für die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen zu erstellen, die sämtliche Anforderungen an das Management der IKT-Drittparteienbeziehung dokumentiert und operationalisiert, sofern kritische oder wichtige Funktionen durch den IKT-Provider unterstützt werden.

Diese Leitlinie ist keine reine Formalität. Sie stellt vielmehr den Maßstab für Auswahl, Vertragsgestaltung, Überwachung und Exit dar und schafft einen verbindlichen Rahmen, an dem sowohl interne Stakeholder (Management, Compliance, IT, Einkauf) als auch die Aufsicht jederzeit messen können, ob das Finanzunternehmen seine Pflichten nach DORA ordnungsgemäß erfüllt. Die Leitlinie muss gemäß Art. 1 RTS TPPol alle relevanten Risikofaktoren bei der Nutzung von IKT-Drittparteien für kritische oder wichtige Funktionen systematisch abbilden – von der Art der Dienstleistung über Standort, Daten- und Zulassungs- / Beaufsichtungsfragen bis hin zu Konzentrationsrisiken, Übertragbarkeitsthemen und möglichen Auswirkungen auf die Geschäftskontinuität.

Die Leitlinie ist jährlich zu überprüfen und bei Bedarf zu aktualisieren. Sie muss eine Methode zur Einstufung kritischer oder wichtiger IKT-Dienstleistungen enthalten, klare Zuständigkeiten und ausreichende Expertise im Unternehmen sicherstellen sowie gewährleisten, dass Drittdienstleister über ausreichende Ressourcen verfügen. Zudem ist ein verantwortliches Leitungsmitglied mit Berichtspflichten zu benennen. Die Leitlinie muss mit den DORA-Rahmenwerken für Risikomanagement, Informationssicherheit, Business Continuity und Incident-Reporting im Einklang stehen, unabhängige Prüfungen vorsehen und sicherstellen, dass Verträge Aufsichtspflichten, Prüfungs- und Zugangsrechte sowie die Zusammenarbeit mit Behörden gewährleisten (vgl. Art. 3 RTS TPPol).

Phasen des Lifecycle-Management eines IKT-Drittparteienbezugs

Mit DORA wurde erkannt, dass Risiken aus der Nutzung externer IKT-Dienstleister nicht punktuell, sondern über den gesamten Lebenszyklus einer IKT-Drittparteienbeziehung hinweg entstehen – von der ersten Planung über die Vertragsgestaltung und laufende Überwachung bis hin zur Beendigung und geordneten Exit-Strategie.

Ziel der regulatorischen Vorgaben ist es daher, dass Finanzunternehmen ihre Abhängigkeiten zu externen IKT-Anbietern strukturiert, nachvollziehbar und risikoorientiert steuern. Jede Phase des Zyklus bringt eigene Pflichten mit sich, die eng miteinander verzahnt sind und sicherstellen sollen, dass operationelle Resilienz, Informationssicherheit und Aufsichtsinteressen jederzeit gewahrt bleiben.

Im Folgenden werden die vier Phasen des Lifecycle-Managements dargestellt. Jede Phase enthält spezifische Anforderungen, die Finanzunternehmen in ihre Prozesse und Governance-Strukturen implementieren müssen:

Phase 1 – Planung

Rechtsgrundlagen: Art. 28 Abs. 4 DORA; Art. 5–7 RTS TPPol; Art. 29 DORA; Art. 6–8 RTS TPPol

Bevor eine Vereinbarung mit einem IKT-Drittdienstleister abgeschlossen wird, müssen die Finanzunternehmen eine umfassende Vorbereitungs- und Planungsphase durchlaufen. Diese enthält folgende Schritte:

- Kategorisierung: Zunächst ist zu prüfen, ob es sich bei der geplanten Dienstleistung um eine IKT-Dienstleistung im Sinne von DORA handelt. Nur dann greifen die besonderen DORA-Pflichten.
- Kritikalitätsbeurteilung: Es folgt die Beurteilung, ob die Dienstleistung eine kritische oder wichtige Funktion unterstützt. Diese Einstufung bestimmt das Maß der aufsichtsrechtlichen Anforderungen.
- Interne Strategie-Compliance: Die geplante IKT-Dienstleistung muss mit der internen Strategie und den Governance-Vorgaben des Unternehmens vereinbar sein.
- Regulatorische Compliance: Es ist zu beurteilen, ob die aufsichtsrechtlichen Bedingungen für die Auftragsvergabe erfüllt sind.
- Ex-ante-Risikobewertung: Es ist eine Risikoanalyse des geplanten IKT-Bezugs vorzunehmen, um mögliche operationelle, rechtliche und sicherheitsrelevante Risiken zu identifizieren (vgl. Art. 5 RTS TPPol). Zusätzlich und explizit muss bewertet werden, ob die geplante IKT-Dienstleistung zu Konzentrationsrisiken führt. Hierzu eine Bewertung nach den Vorgaben von Art. 29 DORA vorzunehmen.
- Due Diligence Verfahren: Das in der Leitlinie festgelegte Verfahren für die Auswahl und Bewertung der künftigen IKT-Drittdienstleister ist zu durchlaufen. Der Anbieter selbst ist dabei einer Eignungsprüfung zu unterziehen (Art. 28 Abs. 4 lit. d), Art. 6 RTS TPPol). Es ist zu beurteilen, ob der Anbieter über Reputation, Ressourcen, Sicherheit, Risikomanagement, Zulassungen und ethische Standards verfügt, technologische Entwicklungen beherrscht, Subunternehmer einsetzt, im Drittstaat tätig ist und Audit- sowie Zugangsrechte gewährt. Zudem ist sicherzustellen, dass er über wirksame Maßnahmen zur Risikominderung und Geschäftsfortführung verfügt. Die Sorgfaltsprüfung stützt sich auf Audits, Zertifizierungen, Berichte oder sonstige relevante Informationen, wobei mehrere

Elemente kombiniert werden können, um ein angemessenes Sicherheitsniveau der Leistungsfähigkeit zu gewährleisten.

- Entscheidung zu Subunternehmer-Einsatz: Werden kritische oder wichtige Funktionen durch den geplanten IKT-Drittdienstleister unterstützt, muss das Finanzunternehmen entscheiden, ob der IKT-Drittdienstleister hierzu Unterauftragnehmer einsetzen darf. Die Eignung des IKT-Drittdienstleisters zum Management der Unterauftragnehmer ist dann ebenfalls zu bewerten (vgl. Art. 3 RTS SUB[2]).
- Interessenkonflikte: Es sind mögliche Interessenkonflikte zu identifizieren und zu adressieren.
- Mindestvertragsinhalte: Vor Abschluss der Vertragsverhandlungen müssen abschließend die Anforderungen an Mindestvertragsinhalte aus Art. 30 DORA und Art. 8 RTS TPPol erfüllt sein.
- Einhaltung von Standards für die Informationssicherheit: Finanzunternehmen dürfen gemäß Art. 28 Abs. 5 DORA vertragliche Vereinbarungen nur mit IKT-Drittdienstleistern schließen, die angemessene Standards für Informationssicherheit einhalten. Betreffen diese vertraglichen Vereinbarungen kritische oder wichtige Funktionen, müssen die IKT-Drittdienstleister die aktuellsten und höchsten Qualitätsstandards für die Informationssicherheit anwenden. Vor Vertragsabschluss ist daher zu prüfen und zu dokumentieren, ob der IKT-Drittdienstleister diese Voraussetzungen erfüllt.

Phase 2 – Anzeige- und Registerpflichten

Rechtsgrundlage: Art. 28 Abs. 3 DORA

Nach Abschluss der Planungsphase greifen die besonderen Anzeige- und Registerpflichten. Diese dienen der Transparenz gegenüber der Aufsicht und der systematischen Erfassung sämtlicher IKT-Drittparteienbeziehungen im Unternehmen.

- Anzeigepflichten gegenüber der BaFin: Finanzunternehmen müssen die Absicht einer wesentlichen Auslagerung unverzüglich anzeigen. Darüber hinaus besteht eine nachträgliche Mitteilungspflicht, sobald eine zunächst nicht-kritische Auslagerung eine kritische oder wichtige Funktion betrifft. Die Aufsicht wird damit in die Lage versetzt, frühzeitig Risiken aus neuen oder sich verändernden Drittparteienbeziehungen zu erkennen.
- Informationsregister: Alle vertraglichen Vereinbarungen mit IKT-Drittdienstleistern (auch solche, die keine kritischen oder wichtigen Funktionen beim Finanzunternehmen unterstützen) sind gemäß Art. 28 Abs. 3 DORA in einem Informationsregister zu erfassen. Dieses Register muss sämtliche relevanten Angaben enthalten (Art, Umfang und Gegenstand der Dienstleistung, kritische Bedeutung, Standort des Anbieters etc.). Es stellt das zentrale Instrument zur Risikotransparenz und Übersicht über alle Auslagerungen dar.

Finanzunternehmen müssen der Aufsicht mindestens jährlich oder auf Verlangen das aktuelle Informationsregister vorlegen. Zudem besteht eine unverzügliche Mitteilungspflicht gegenüber der Aufsicht bei jeder neuen Vereinbarung mit IKT-Dienstleistern, die kritische oder wichtige Funktionen unterstützen oder wenn eine Funktion nachträglich als kritisch oder wichtig eingestuft wird.

Phase 3 – Überwachung während der Laufzeit

Rechtsgrundlagen: Art. 9 RTS TPPol, Art. 28 Abs. 6 DORA

Die Pflichten eines Finanzunternehmens enden nicht mit dem Abschluss der Auslagerungsvereinbarung. Vielmehr verlangt DORA ein laufendes, systematisches Monitoring sämtlicher IKT-Drittparteienbeziehungen auch während der Vertragsdauer. Ziel ist es, Risiken frühzeitig zu erkennen, die Vertragstreue der Anbieter sicherzustellen und jederzeit die Kontrolle über Unterstützungsleistungen für kritische oder wichtige Funktionen zu behalten.

Finanzunternehmen müssen deshalb ein kontinuierliches Monitoring etablieren. Hierzu gehören folgende Elemente:

- Kontinuierliche Leistungsüberwachung: Die Leistungserbringung muss anhand der im Vertrag definierten Kennzahlen (KPIs / KRIs) und Qualitätsstandards überprüft werden – etwa in Bezug auf die Einhaltung von Service Level Agreements (SLAs), die Informationssicherheit oder die Verfügbarkeit der Systeme.
- Nutzung von Provider-Reports: Regelmäßig bereitgestellte Berichte des Anbieters (z. B. Tätigkeitsberichte, Incident-Reports, Business-Continuity-Management-Reports) sind aktiv auszuwerten und in das interne Risikomanagement einzubeziehen.
- Eigene Audits und Prüfungen: Neben den Berichten der Anbieter müssen Finanzunternehmen eigene Audits durchführen, um die Einhaltung der vertraglichen und regulatorischen Vorgaben unabhängig zu überprüfen. Art, Umfang und Häufigkeit dieser Audits ist gemäß Art. 28 Abs. 6 DORA auf Grundlage eines risikobasierten Ansatzes vorab festzulegen. Bei technisch komplexen Auslagerungsverträgen muss das Finanzunternehmen sicherstellen, dass die eingesetzten internen oder externen Revisoren – oder ein Revisorenpool – über die notwendigen Fachkenntnisse und Fähigkeiten verfügen, um wirksame Audits und Bewertungen durchführen zu können.
- Abhilfemaßnahmen und Eskalationen: Stellt das Monitoring Defizite fest, sind geeignete Maßnahmen zu ergreifen – von Vertragsstrafen und Eskalationsverfahren bis hin zu Nachbesserungen oder Anpassungen im Vertragsmanagement.
- Überwachung der Subunternehmerkette: Finanzunternehmen müssen Transparenz über die eingesetzten Unterauftragnehmer sicherstellen und das Risiko im Zusammenhang mit dem Einsatz von Unterauftragnehmern fortlaufend bewerten.
- Interne Berichterstattung: Die Ergebnisse des Monitorings sind regelmäßig an die Geschäftsleitung zu berichten, sodass diese ihre Verantwortung für die Drittparteiensteuerung wahrnehmen kann.
- Aufsichtsrechtliche Berichtspflichten: Zusätzlich ist jährlich gegenüber der BaFin über die Anzahl und Kategorien der Anbieter sowie die Arten der bezogenen IKT-Dienstleistungen Bericht zu erstatten (mittels Informationsregister).

Phase 4 – Beendigung und Exit

Rechtsgrundlagen: Art. 28 Abs. 7–8 DORA; Art. 10 RTS TPPol

Die letzte Phase im Lifecycle-Management betrifft die Beendigung von Drittparteienbeziehungen. Auch dieser Abschnitt ist in DORA umfassend reguliert, um sicherzustellen, dass Finanzunternehmen jederzeit handlungsfähig bleiben und Abhängigkeiten von IKT-Drittdienstleistern beherrschbar bleiben. Er umfasst folgende Punkte:

- Mindestkündigungsrechte: Verträge mit IKT-Drittdienstleistern müssen zwingend einen Katalog an Kündigungsrechten enthalten. Diese greifen insbesondere bei wesentlichen Rechts- oder Vertragsverletzungen, erheblichen Mängeln im IKT-Risikomanagement oder der Informationssicherheit sowie Einschränkungen der Aufsichtsrechte durch den Anbieter.
- Exit-Strategien und -Pläne: Zentral ist die Pflicht, vorab klare Exit-Strategien zu entwickeln. Dazu gehören die Definition von Übergangs- und Ausstiegspfaden, die Sicherstellung der Datenrückführung und Datenportabilität sowie Vorkehrungen zur Vermeidung von Vendor-Lock-in, also einer faktischen Abhängigkeit von einem einzigen Anbieter.

Exit-Strategien sind nicht bloße Theorie, sondern müssen realistisch umsetzbar und in die Geschäftsfortführungsplanung integriert sein.

- Geordneter Wind Down: Treten die im Vertrag oder in der Regulierung definierten Kündigungs-Trigger ein, muss das Finanzunternehmen das Kündigungsrecht ausüben und den Ausstiegsplan konsequent umsetzen. Dies umfasst sowohl technische Maßnahmen (z. B. Datenmigration, Systemumstellung) als auch organisatorische und rechtliche Schritte, um den Geschäftsbetrieb ohne Unterbrechung fortzuführen. Die entsprechenden Schritte sind sorgfältig zu dokumentieren und – je nach Komplexität und Größe der IKT-Drittdienstleisterbeziehung – in einem geordneten Abwicklungsprojekt zu steuern.

Mit den vier Phasen – Planung, Anzeige- und Registerpflichten, Überwachung während der Laufzeit sowie Beendigung und Exit – schafft DORA einen klar strukturierten Lifecycle-Ansatz für IKT-Drittparteienbeziehungen. Finanzunternehmen sind verpflichtet, Risiken nicht punktuell, sondern über den gesamten Lebenszyklus hinweg zu identifizieren, zu steuern und transparent zu dokumentieren.

Damit stellt DORA sicher, dass Abhängigkeiten von IKT-Drittdienstleistern beherrschbar bleiben, die operationelle Resilienz des Finanzsektors gestärkt wird und die aufsichtsrechtliche Kontrolle jederzeit gewährleistet ist. Der Lifecycle ist somit kein formales Compliance-Konstrukt, sondern ein zentrales Instrument für eine sichere, nachhaltige und regulatorisch konforme Nutzung von IKT-Dienstleistungen.

Praktische Herausforderungen

In der Praxis stellen sich jedoch eine Reihe konkreter Herausforderungen, die den Umgang mit IKT-Drittparteien erheblich prägen:

Abhängigkeit von Hyperscalern

Gerade die großen Cloud-Anbieter (z. B. AWS, Microsoft Azure und Google Cloud) dominieren den Markt und sind in vielen Fällen alternativlos, wenn es um Skalierbarkeit, Sicherheit und Innovationsgeschwindigkeit geht. Damit geht aber auch ein erhebliches Problem einher: Die Finanzunternehmen haben nur begrenzte Verhandlungsmacht bei der Vertragsgestaltung. Standardisierte Service Level, Haftungsbegrenzungen und Einschränkungen bei Audit- oder Sub-Outsourcing-Klauseln sind kaum verhandelbar. DORA verlangt jedoch gerade bei kritischen oder wichtigen Funktionen individualisierte und aufsichtsrechtlich belastbare Vertragsklauseln. Die Finanzunternehmen müssen daher Strategien entwickeln, wie sie mit dieser Asymmetrie umgehen – etwa durch interne Risikomitiganten, Multi-Cloud-Ansätze und die enge Dokumentation von Abweichungen.

Ressourcenlimitierte Compliance-Teams

Kleinere Institute und FinTechs verfügen oft nicht über große Compliance- oder Vendor-Management-Abteilungen. Die Anforderungen aus DORA bedeuten jedoch einen erheblichen Mehraufwand im Zusammenhang mit dem Management von IKT-Drittparteienbeziehungen. Der Aufbau von skalierbaren Prozessen wird daher entscheidend sein: Automatisierung in der Registerpflege, Nutzung externer Audit-Reports (z. B. ISAE 3402, SOC 2) sowie Outsourcing bestimmter Prüfprozesse an spezialisierte Dienstleister könnten helfen, die regulatorischen Pflichten auch mit knappen Ressourcen zu erfüllen.

Non-EU Anbieter

Viele IKT-Services werden außerhalb der EU erbracht – sei es durch Rechenzentren in Drittländern oder durch globale Sub-Outsourcing-Ketten. Dies erhöht nicht nur die operativen Risiken, sondern birgt auch aufsichtsrechtliche und geopolitische Implikationen: Datenzugriffsrechte von Drittstaaten, Fragen der Durchsetzbarkeit von Audit-Klauseln oder die Abhängigkeit von geopolitisch sensiblen Regionen (z. B. USA, Asien) müssen bei der Risikobewertung berücksichtigt werden. DORA verlangt hier explizite und sehr granulare Ex-ante-Risikobewertungen und ausreichend tiefgehende Exit-Strategien, damit solche Szenarien abgefedert werden können.

Technische Integration

Schließlich ist auch die technische Umsetzung eine Herausforderung: Das von DORA geforderte Informationsregister lässt sich nicht isoliert in Excel-Tabellen führen. Es erfordert eine enge Integration mit bestehenden IKT-Asset-Management- und Vertragsmanagementsystemen. Nur so können Daten zu Verträgen, Services, Verantwortlichkeiten, Sub-Outsourcing und Risikoanalysen konsistent gepflegt und für das jährliche Reporting an die Aufsicht aufbereitet werden. Für viele Institute bedeutet dies eine IKT- und Prozessmodernisierung, die viele Ressourcen binden wird.

Insgesamt zeigt sich: Während DORA einen klaren regulatorischen Rahmen vorgibt, liegt die eigentliche Herausforderung in der praktischen Operationalisierung.

Fazit und Ausblick

Der durch DORA vorgegebene Lifecycle-Ansatz für IKT-Drittparteienbeziehungen verdeutlicht, dass Finanzunternehmen ihre Abhängigkeiten von externen IKT-Dienstleistern nicht nur im Moment des Vertragsschlusses, sondern ganzheitlich und fortlaufend steuern müssen. Von der sorgfältigen Planung über die Anzeige- und Registerpflichten, das kontinuierliche Monitoring bis hin zum geordneten Exit spannt DORA ein enges Regelungsnetz, das Transparenz, Resilienz und Aufsichtskonformität gewährleisten soll. IKT-Drittparteienbeziehungen sind damit nicht mehr nur „Procurement“, sondern werden zu einem zentralen Baustein der digitalen Resilienzstrategie.

Während viele Häuser bislang nur punktuell Outsourcing-Leitlinien oder Cloud-Guidelines kannten, entsteht nun ein europaweit einheitlicher Rahmen für den gesamten Lebenszyklus von IKT-Drittparteienbeziehungen. Das bedeutet:

- Mehr Governance, weniger Ad-hoc – Institute brauchen ein klar dokumentiertes, von der Geschäftsleitung getragenes Modell.
- Mehr Transparenz – durch Informationsregister, Reporting an die Aufsicht und eine laufende Dokumentation.
- Mehr Prüfung – durch verstärkte Audit- und Monitoringpflichten auch während der Vertragslaufzeit.
- Mehr Resilienz – durch strukturierte Exit-Strategien, systematische Due Diligence und eine enge Steuerung auch von Sub-Outsourcing-Ketten.

Für die Praxis stellt sich die Frage, wie schnell Institute diese Vorgaben umsetzen können. Gerade FinTechs, die bislang pragmatisch und flexibel einkauften, müssen nun Compliance-Prozesse etablieren, die zuvor oft nur Großbanken kannten. Die Praxis zeigt auch, dass die Umsetzung der Vorgaben alles andere als trivial ist. Marktkräfte (Hyperscaler-Dominanz), Ressourcenengpässe, internationale Abhängigkeiten und die technische Komplexität fordern Institute weit über ein reines „Abhaken von Compliance-Pflichten“ hinaus. Viele Häuser stehen vor der Aufgabe, ihre IKT- und Governance-Strukturen vollständig neu zu denken und gleichzeitig wirtschaftlich effizient zu bleiben.

Die regulatorischen Anforderungen werden zudem nicht beim Lifecycle-Management stehenbleiben. Mit Blick auf die zunehmende Konzentration der IKT-Dienstleistungen im Markt, die fortschreitende technologische Entwicklung (Cloud, KI, Automatisierung) und die wachsende Abhängigkeit von globalen Anbietern wird das Thema Drittparteienresilienz weiter an Bedeutung gewinnen. Künftig dürften verstärkt auch Fragen nach europäischer Souveränität, technologischer Unabhängigkeit und einer noch stärkeren aufsichtlichen Kontrolle von „Critical Third-Party“-Anbietern in den Fokus rücken.

---

[1] Delegierte VO 2024/1773 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Spezifizierung des detaillierten Inhalts der Leitlinie für vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden

[2] Delegierte VO 2025/532 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Präzisierung der Aspekte, die ein Finanzunternehmen bei der Untervergabe von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen bestimmen und bewerten muss.

Praxiswissen für Ihren Erfolg im Job

Veranstaltungen für IT, Digitalisierung und Künstliche Intelligenz

Erhalten Sie in unseren Weiterbildungen fundiertes und praxisnahes Know-how zur digitalen Transformation und IT-Compliance im Bankensektor unter Berücksichtigung der aufsichtsrechtlichen Anforderungen aus DORA, MaRisk, DSGVO, IT-Sicherheitsgesetz und den EBA-ICT-Guidelines.
Jetzt informieren.

e-Learning – Klicken und Lernen

Das FORUM Institut bietet mit hochwertigen e-Learning-Programmen eine flexible Weiterbildungsform. Entscheiden Sie selbst, wann und wo Sie lernen.
Jetzt testen.

Inhouse-Seminare – Maßgeschneiderte Lösungen

Alle unsere Seminare eignen sich auch hervorragend als Inhouse-Training.
Jetzt individuelles Angebot anfordern.

FORUM · Institut für Management GmbH • Postfach 10 50 60 • 69040 Heidelberg • Germany
Telefon: +49 6221 500-500 • Fax: +49 6221 500-555 • www.forum-institut.de