MYRA

EXPERTENINTERVIEW

DORA: IT-Auslagerung und Dienstleisterwahl

MYRA
Neue digitale Sicherheit

DORA | IT-Auslagerung und Dienstleisterwahl:

Worauf Banken und Institute heute achten müssen, um die regulatorischen Herausforderungen von morgen zu bewältigen.

Die regulatorischen Neuerungen in der Finanzindustrie zeigen, dass Gesetzgeber und Aufsicht zunehmend die gesamte Wertschöpfungskette betrachten. Konzentrierte sich die BaFin lange Zeit mehrheitlich auf die Institute selbst, rücken nun vermehrt auch deren Partner und Dienstleister in den Fokus der Aufsicht.

Mit dem Gesetz zur Stärkung der Finanzmarktintegrität (FISG) erhielt die BaFin bereits Mitte 2021 neue Kompetenzen, darunter direkte Anweisungsbefugnisse gegenüber Auslagerungsunternehmen. Auch die kommende DORA-Verordnung[1] sieht eine direkte Kontrolle der Dienstleister durch die Finanzaufsicht vor. Insbesondere vor dem Hintergrund des anhaltenden Trends zur IT-Auslagerung, der neben Cloud-Computing u.a. auch Software-Entwicklung oder IT-Sicherheit umfasst, hat DORA weitreichende Folgen für die Zusammenarbeit von beaufsichtigten Unternehmen mit ihren Dienstleistern.

Nils Katzmark ist seit vielen Jahren in der Finanzindustrie als Anwalt und Experte für Aufsichtsrecht aktiv. In seiner Tätigkeit als Syndikus für verschiedene namhafte Unternehmen beschäftigt(e) er sich intensiv u.a. mit aufsichtsrechtlichen Entwicklungen und Compliance-Fragen. Im Gespräch mit Myra Security erörtert Nils Katzmark im Folgenden die zentralen Herausforderungen, die im Rahmen der DORA-Verordnung auf beaufsichtigte Unternehmen in Europa zukommen werden. Das nachfolgende Interview bezieht sich maßgeblich auf den DORA-Entwurf mit Stand September 2020.

> ***„Bereits bei der Auswahl neuer IKT-Drittanbieter sind strenge Anforderungen zu erfüllen.“***

Nils Katzmark
Rechtsanwalt und
Syndikusrechtsanwalt

Nils Katzmark ist Rechtsanwalt & Syndikus-rechtsanwalt. Nach langer Tätigkeit als Syndikus in der Finanzindustrie und Tätigkeit in einer großen deutschen Kanzlei liegt sein anwaltlicher Schwerpunkt im Bank-und Kapitalmarktrecht, insb. im Aufsichtsrecht und im Bereich der Corporate Governance. Nils Katzmark hat in Bielefeld, Bochum und Münster studiert und ist seit 2001 als Rechtsanwalt zugelassen.

Wie werden sich die neuen Anforderungen konkret auf die Prüfung auszuwählender und angeschlossener IT-Dienstleister auswirken?
Nils Katzmark: Zunächst werden IKT-Drittanbieter[2], also Unternehmen, die digitale Dienste und Datendienste erbringen, unter DORA selbst zu regulierten Unternehmen, da DORA auf diese anwendbar ist (Art. 2 Abs.1 Buchst. u)[3]. Die bereits weitgehend vorhandene Verpflichtung von Finanzunternehmen zur Vereinbarung sie selbst verpflichtender regulatorischer Standards „über vertragliche Bande“, also über Auslagerungsverträge mit u.a. ihren IKT-Drittanbietern, wird durch die unmittelbare Verpflichtung zur Einhaltung der in DORA weitgehend inhaltsgleichen Standards auf ein zweites Bein gestellt. Der Druck zur vollumfänglichen Umsetzung und Einhaltung der aufsichtsrechtlichen Standards dürfte dadurch auf Seiten der IKT-Drittanbieter steigen.

Inwiefern sind die auslagernden Institute dafür verantwortlich, eine Überprüfung beim Dienstleister zu ermöglichen (etwa Vor-Ort-Inspektionen für kritische IKT-Drittanbieter)?
Nils Katzmark: Die auslagernden Institute sind dafür weiterhin unter dem bestehenden Rechtsrahmen

[1] Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Betriebsstabilität digitaler Systeme des Finanzsektors und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014 und (EU) Nr. 909/2014
[2] u.a. Anbieter von Cloud-Computing, Software, Datenanalyse und Rechenzentren, nicht hingegen Hardwarehersteller und elektronische Kommunikationsdienste, also u.a. Internetzugangsdienste
[3] Artikelnennungen beziehen sich immer auf DORA

verantwortlich, durch Art. 33 und Art. 34 wird aber nunmehr die sog. federführende Aufsichtsinstanz u.a. auch zu Vor-Ort-Prüfungen direkt bei den IKT-Drittanbietern ermächtigt. Das Informationsregister (Art. 25 Abs. 4) verschafft Transparenz über die IKT-Drittanbieter eines Finanzunternehmens und erleichtert damit im allerersten Schritt das zielsichere Auffinden von IKT-Drittanbietern durch die Aufsichtsbehörden. Für Deutschland dürfte es insoweit dem nach MaRisk zu führenden Auslagerungsregister ähneln. Bereits bei der Auswahl neuer IKT-Drittanbieter sind strenge Anforderungen zu erfüllen, insbesondere die Erfüllung aufsichtsrechtlicher Bedingungen und die Einhaltung hoher, angemessener und aktueller Standards für Informationssicherheit.

> ***DORA-Verstöße können mit täglichen Zwangsgeldern in Höhe von 1% des durchschnittlichen globalen Tagesumsatzes geahndet werden.***

Welche Konsequenzen drohen, wenn eine Prüfung des Dienstleisters nicht möglich ist oder verzögert erfolgen sollte?
Nils Katzmark: Bei Verzögerungen können Zwangsgelder i.S.v. Art. 31 Abs. 4-7 verhängt werden. Das bedeutet die Möglichkeit, täglich ein Zwangsgeld in Höhe von 1% des durchschnittlichen globalen Tagesumsatzes auf Basis des vorangegangenen Geschäftsjahrs über einen Zeitraum von bis zu sechs Monaten verhängen zu können. Sollte die Prüfung überhaupt nicht möglich sein, kann die zuständige Aufsicht das Finanzunternehmen per Anordnung zur Kündigung des Auslagerungsvertrages zwingen. Darüber hinaus kann die Aufsicht weitere Sanktionsmaßnahmen gegen das Finanzunternehmen erwägen, wenn der Auslagerungsvertrag inhaltlich nicht den Anforderungen aus DORA entspricht.

Was können die Aufsichtsbehörden anordnen, wenn ein Auslagerungsunternehmen gegen Pflichten aus DORA verstößt?
Nils Katzmark: Die federführende Aufsichtsinstanz, d.h. EBA, ESMA oder EIOPA[4] kann gem. Art. 31 Abs. 1 i.V.m. Abs. 4 ein Zwangsgeld gegen den IKT-Drittanbieter verhängen, wenn dieser zur (i) Bereitstellung von Informationen und Unterlagen, (ii) Durchführung von allgemeinen Untersuchungen und Inspektionen und (iii) Abgabe von Berichten zur Darstellung getroffener Abhilfemaßnahmen nicht bereit war oder unzureichend mitgewirkt hat. Die mögliche Höhe des Zwangsgeldes habe ich bereits erläutert.

Bemerkenswert ist, dass die federführende Aufsichtsinstanz, also die Aufsicht über den IKT-Drittanbieter, den zuständigen Behörden derjenigen Finanzunternehmen, die diesen IKT-Drittanbieter nutzen, die Entscheidung über die Informationsanforderung zur Verfügung stellt. Diese Art „Informationskreis" schließt sich über Art. 37 Abs. 5. Demnach unterrichten zuständige Behörden die federführenden Aufsichtsinstanzen regelmäßig darüber, welche (vertraglichen) Maßnahmen sie gegenüber Finanzunternehmen getroffen haben, die mit kritischen IKT-Drittanbietern zusammenarbeiten, welche von den federführenden Aufsichtsinstanzen ausgesprochene Empfehlungen teilweise oder vollständig nicht befolgt haben.
Als Maßnahmen kommen die temporäre (bis zur Beseitigung des Risikos) teilweise oder vollständige Einstellung der IKT-Drittanbieter-Dienste oder deren dauerhafte Kündigung auf Basis der Ermächtigungsgrundlage des Art. 44 i.V.m. Art. 37 Abs. 3 in Betracht.

> ***Vorteile und Risiken von Auslagerungen in Drittländer müssen noch sorgfältiger abgewogen werden als bisher.***

Das EuGH-Urteil zu Schrems II hat EU-weit für Rechtsunsicherheit gesorgt. Werden sich die Folgen ebenso über DORA auf die europäische Finanzindustrie übertragen?
Nils Katzmark: DORA kann als Rechtsetzungsakt der EU nicht unmittelbar mit dem bahnbrechenden EuGH-Urteil Schrems II verglichen werden. Anknüpfungs- bzw. Verbindungspunkte lassen sich aber finden, beispielsweise im Art. 26 Abs. 2, der die Einhaltung des Datenschutzes (ohne weitere spezifizierende Ausführungen dazu) zur Auflage bei der Risikoanalyse zum Einsatz von IKT-Drittanbietern in Drittländern macht. Das ist nicht neu und auch nicht überraschend, denn die beiderseitige Verpflichtung der Parteien eines Auslagerungsvertrages zur Einhaltung des geltenden

[4] je nachdem, welche Institution der Gemeinsame Ausschuss auf Empfehlung des Aufsichtsforums zur Aufsicht über den jeweiligen kritischen IKT-Drittanbieter ernannt hat

(einschlägigen) Rechts ist Kernbestandteil eines jeden Auslagerungsvertrages. Die dezidierte Aufnahme dieses „Mindest-Pflichtfaktors" bei der Bewertung der Risikosituation des Finanzunternehmens bei Auslagerung in ein Drittland (neben wirksamer Rechtsdurchsetzung, anwendbarem Insolvenzrecht und Data-Recovery-Beschränkungen) zeigt aber, dass die Vorteile und Risiken bei Auslagerungen in Drittländer insbesondere im Falle der Untervergabe noch sorgfältiger abgewogen werden sollten als bisher.

Welche Kompetenzen muss ein Cloud-Dienstleister (eingestuft als kritischer IKT-Drittanbieter) voraussichtlich mitbringen, um den regulatorischen Vorgaben zu entsprechen?
Nils Katzmark: Zunächst sei gesagt, dass ein „kritischer IKT-Drittanbieter" ein nach Art. 28 Abs. 1 i.V.m. Abs. 2 benannter IKT-Drittanbieter ist, also ein Unternehmen, das digitale Dienste und Datendienste erbringt.
Ein kritischer IKT-Drittanbieter unterliegt dem Aufsichtsrahmen nach Art. 30-37. Ein als kritischer IKT-Drittanbieter klassifizierter Cloud-Dienstleister muss über umfassende, robuste und wirksame Vorschriften, Verfahren, Mechanismen und Vorkehrungen zur Steuerung derjenigen IKT-Risiken verfügen, die die Nutzung seiner digitalen Dienste für Finanzunternehmen mit sich bringt. Das bedeutet im Einzelnen, dass der Cloud-Dienstleister IKT-Anforderungen zur Gewährleistung der Sicherheit, Verfügbarkeit, Kontinuität, Skalierbarkeit und Qualität erfüllen und jederzeit hohe Standards hinsichtlich Sicherheit, Vertraulichkeit und Integrität von Daten aufrechterhalten können muss. Des Weiteren spielen die zur IKT-Sicherheit erforderliche physische Sicherheit und Risikomanagementprozesse zur Business Continuity und Recovery eine Rolle. Letztlich bedarf es zur Erreichung eines wirksamen IKT-Risikomanagements entsprechender Corporate-Governance-Regelungen, eines Ermittlungs- und Meldewesens für IKT-bezogene Vorfälle sowie regelmäßiger eigenständig erfolgender Prüfungen der IKT-Systeme und -Infrastruktur.

Welche Rolle spielen gängige Zertifizierungen und Audits bei der Überprüfung und Eignung von IT-Dienstleistern?

Nils Katzmark: Hier kommt ein weiterer Aspekt der bereits erläuterten Anforderungen an kritische IKT-Drittanbieter ins Spiel. Die Übernahme einschlägiger nationaler und internationaler Normen, die auf die Erbringung von IKT-Dienstleistungen für Finanzunternehmen anwendbar sind, spielt bei der Bewertung eine entscheidende Rolle (Art. 30 II i). Die Compliance mit solchen Normen und die Eigenzertifizierung wird daher insbesondere bei IT-Dienstleistern mit der Qualifikation eines kritischen IKT-Drittanbieters nicht nur wichtiger, sondern essenziell.

> ***Zertifizierungen werden für IT-Dienstleister essenziell.***

Die BaFin hatte bereits im vergangenen Jahr intensivere Kontrollen von Auslagerungen im Bereich IT-Dienstleistungen angekündigt. Insbesondere die operative Resilienz liegt im Fokus der Aufsicht. Wird DORA die Messlatte für Cybersicherheit regulatorisch nochmals anheben?
Nils Katzmark: Das ist aktuell schwer zu sagen.
Zum einen ist noch nicht klar, ob DORA in der heute vorliegenden Fassung kommen wird. Zum anderen wird eine Reihe von delegierten Rechtsakten und auch technischen Regulierungsstandards[5] geschaffen werden müssen. Erst nach deren Vorliegen ist ein konkreter Vergleich mit den auf nationaler Ebene schon vorhandenen Anforderungskriterien in verschiedenen Regelwerken wie etwa hierzulande BAIT, KAIT und ZAIT möglich.

Welche Dienste und Prozesse sind hinsichtlich DORA am schwierigsten auszulagern, wo sind die regulatorischen Hürden am höchsten?
Nils Katzmark: DORA verlangt in Art. 5 Abs. 9, dass Finanzunternehmen eine Strategie für ihre digitale Resilienz aufstellen, in der dargelegt wird, wie der gesamte IKT-Risikomanagementrahmen umgesetzt wird. Dazu gehört auch, dass bei Nutzung mehrerer IKT-Drittanbieter die Gründe für deren Nutzung und die wesentlichen Abhängigkeiten dargestellt werden.
Dies wird als „Politik" für die Nutzung von IKT-Diensten bezeichnet. Zudem sind Finanzunternehmen

[5] vgl. u.a. Erwägungsgrund 69 durch die europäischen Aufsichtsbehörden (EBA, ESMA und EIOPA)

verpflichtet, ein Informationsregister gem. Art. 25 Abs. 4 zu führen, welches alle vertraglichen Vereinbarungen mit IKT-Dienstleistern enthält. Für beides, d.h. Politik und Informationsregister, wird es nähere Ausführungen durch die ESA geben. Zum Informationsregister werden das technische Durchführungsstandards mit Standardvorlagen sein. Für die Politik werden es Regulierungsstandards sein, die den zu beschreibenden Inhalt der Politik festlegen und die Art von bereit-zustellender Information für das Informationsregister. Inwieweit dabei eine Differenzierung hinsichtlich der Art des ausgelagerten Dienstes stattfinden wird, die letztlich Auswirkungen auf die Komplexität einer bestimmten IKT-Auslagerung haben könnte, bleibt daher abzuwarten.

> ***„Digitalisierung und Betriebsstabilität sind zwei Seiten derselben Medaille."***

Welche Folgen könnte DORA für die globale Konkurrenzfähigkeit von Finanzunternehmen und IKT-Drittanbietern i.S.v. DORA haben?
Nils Katzmark: Zur Erinnerung sei gesagt, dass DORA zur Stärkung der operativen Resilienz geschaffen wird, nachdem die in Folge der Finanzkrise von 2008 durchgeführten Reformen primär die finanzielle Resilienz von Finanzunternehmen gestärkt haben. Stark vereinfachend könnte man sagen, dass es nach der Definition der Anforderungen an die Hardware jetzt an die Anforderungen der Security-Software geht. Positiv dürfte an DORA aus Sicht der Finanzunternehmen empfunden werden, dass die Regulierung und Beaufsichtigung von (kritischen) IKT-Drittanbietern die Anforderungen transparent(er) und die Risikoanalyse einfacher macht. Dabei spielen auch die oben angesprochenen Zertifizierungsanforderungen eine Rolle. Negativ könnte an DORA aus Sicht der Finanz-unternehmen empfunden werden, dass die Regulierung „nur" EU-weit gilt und Konkurrenz aus Drittländern (ohne Geschäftstätigkeit in der EU) gegebenenfalls geringere Anforderungen an die Betriebsstabilität zu erfüllen hat. Global agierende Finanzunternehmen könnten daher erwägen, unterschiedliche Anforderungen (soweit technisch möglich) in Drittländern anzuwenden. Andererseits ist unter dem Eindruck zunehmender Cyberkriminalität, die sich sogar als bewusst eingesetzte „Waffe" in Kriegszeiten manifestiert, digitale Resilienz ein umso wertvolleres Asset. Denn letztlich bleibt eines klar: Digitalisierung und Betriebsstabilität sind zwei Seiten derselben Medaille.

Glossar

IKT	Informations- und Kommunikations-technologie
EBA	Europäische Bankenaufsichtsbehörde
ESMA	Europäische Wertpapier- und Marktaufsichts-behörde
EIOPA	Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung
BAIT	Bankenaufsichtliche Anforderungen an die IT
KAIT	Kapitalverwaltungsaufsichtliche Anforderungen an die IT
ZAIT	Zahlungsdiensteaufsichtliche Anforderungen an die IT von Zahlungs- und E-Geld-Instituten
Ma-Risk	Mindestanforderungen an das Risikomanagement

Abkürzungen

i.V.m.	in Verbindung mit
i.S.v.	im Sinne von