GVB Genossenschaftsverband Bayern

DORA

Digital Operational Resilience Act

Erfahrungen aus der bankwirtschaftlichen Praxis

Genossenschaftsverband Bayern

DORA (Digital Operational Resilience Act)

Erfahrungen aus der bankwirtschaftlichen Praxis

1 Allgemeine Anmerkungen

Mit DORA (Digital Operational Resilience Act) wurde innerhalb der EU erstmals eine einheitliche Regulierung über den gesamten Finanzsektor hinweg zum Thema Cybersicherheit, IKT-Risiken und digitale operationelle Resilienz geschaffen. Die Verordnung trat im Januar 2023 in Kraft und war bis Januar 2025 von den betroffenen Unternehmen umzusetzen. Zusätzlich wurden seitdem zahlreiche Level 2-Rechtsakte (RTS/ITS) erlassen, welche den Level 1-Text konkretisieren.

Hinsichtlich der immer stärkeren Abhängigkeit des Finanzsektors von digitalen Systemen sowie deren zunehmender Vernetzung ist es sinnvoll, Themen wie Cybersicherheit und IKT-Risiken in den Blick zu nehmen. Hinsichtlich der kleinteiligen Ausgestaltung des Regelwerks ist der Gesetzgeber jedoch an einigen Stellen über das Ziel hinausgeschossen:

- Beispielsweise führt der entsprechende delegierte Rechtsakt dazu, dass zu viele Vorfälle dokumentiert und bewertet werden müssen. Zudem sind auch kleine Banken theoretisch dazu verpflichtet, beim Auftreten von IKT-Vorfällen ununterbrochen meldebereit zu sein.
- Die Dokumentations- und Meldevorgaben für das IKT-Risikomanagement sind zu kleinteilig und führen zu großem bürokratischem Aufwand bei den Banken.

Insbesondere das Management des IKT-Drittparteienrisikos verursacht enormen administrativen Aufwand. Sowohl der Inhalt und die Regelungstiefe als auch die Sinnhaftigkeit des Umfangs des Informationsregisters sind zu hinterfragen. So sind die verpflichtenden Angaben zu den ausgelagerten IKT-Dienstleistungen deutlich zu umfangreich. Vor allem die Bestimmungen zur Überwachung der Unterauftragsvergabe gehen dabei über die eigentliche Intention des Gesetzgebers im Zusammenhang mit DORA hinaus. Zudem sind die Anforderungen an die Verträge mit IKT-Drittdienstleistern so hoch, dass auch die Anforderungen an wesentliche Auslagerungen gemäß MaRisk von den Banken nicht vollumfänglich übernommen werden konnten.

Besonders Doppelarbeiten bezüglich des Managements des IKT-Drittparteienrisikos und des Auslagerungsrechts (z.B. Informationsregister und Auslagerungsregister, Pflicht zur Erstellung von Risikoanalysen und Anzeigepflichten in beiden Regimen, unabgestimmte Mindestvertragsinhalte) müssen zeitnah aufgelöst werden.

Zusätzlicher Druck auf die Banken entsteht durch die sehr kurzen Umsetzungsfristen aufgrund der späten Finalisierung der technischen Standards (Level 2). In manchen Fällen werden dabei die Vorgaben aus dem Level 1-Text durch die von den Europäischen Aufsichtsbehörden (ESAs) entwickelten technischen Standards noch einmal verschärft (siehe Beispiel zur Definition von IKT-Vorfällen unter Punkt 2.3). Ob dies dann jeweils dem politischen Willen des Gesetzgebers entspricht, ist fraglich.

Gerade die kleinsten Banken stellt die Umsetzung von DORA vor große Herausforderungen. Obwohl es in den allermeisten Fällen unmöglich erscheint, dass von einer einzelnen Volksbank bzw. Raiffeisenbank eine Bedrohung für die europäische Cybersicherheit ausgeht, wird das Prinzip der Proportionalität kaum berücksichtigt. Hier muss sich sowohl der Gesetzgeber als auch die Aufsicht in ihrer täglichen Aufsichtspraxis grundsätzlich die Frage stellen, ob sie den Fortbestand der kleinsten – oftmals wirtschaftlich kerngesunden – Banken gewährleisten möchte.

Vor dem Hintergrund der zahlreichen Belastungen dieser wichtigen Verordnung ist zu kritisieren, dass erst für das Jahr 2028 eine Überprüfung der DORA-Verordnung durch die EU-Kommission durchgeführt werden soll. Denn Probleme insbesondere in Zusammenhang mit der überproportionalen Belastung kleiner Institute sind schon heute deutlich erkennbar.

2 Konkrete Verbesserungsvorschläge am bestehenden Regelwerk

2.1 Banken genügend Zeit zur Umsetzung geben

Ausgangslage

Die DORA-Verordnung (EU) 2022/2554 wurde Anfang 2023 veröffentlicht und ist seit Januar 2025 anzuwenden. Daher wurde in der öffentlichen Kommunikation von einer zweijährigen Umsetzungsfrist gesprochen. Die Details der Umsetzung hingen jedoch maßgeblich von der Ausgestaltung weiterer Durchführungsverordnungen ab, deren Ausarbeitung an die Behörden delegiert wurde. Diese RTS und ITS wurden teilweise mit großen Verzögerungen beschlossen, sodass zwischen finaler Veröffentlichung und Inkrafttreten nur wenige Wochen lagen. Beispielsweise wurde der ITS zum Informationsregister (EU) 2024/2956 erst am 29. November 2024 beschlossen. Einzelne Regulierungsstandards, wie der technische Regulierungsstandard 2025/532 zur Unterauftragsvergabe vom 02.07.2025, lagen sogar erst deutlich nach Geltung von DORA final vor.

Problem

Kurze Umsetzungsfristen führen zu unnötigen Doppelarbeiten im Voraus und binden erhebliche Personalkapazitäten, was gerade bei kleineren Banken (mit einer Mitarbeiterzahl teilweise im zweistelligen Bereich) zu unnötigen Belastungen führt.

Lösung

Der Gesetzgeber muss den Banken ausreichend Zeit geben, die beschlossenen Rechtsakte umzusetzen.

2.2 Umfang der Dokumentationsanforderungen reduzieren

Ausgangslage

Finanzunternehmen haben (i.d.R. ohne Berücksichtigung von Proportionalität in Bezug auf Größe und Risikorelevanz) mit DORA eine sehr große Menge umfangreicher Dokumentationsanforderungen zu erfüllen: Dazu gehören 3 (neue) Strategiedokumente, 5 (überwiegend neue) Leitliniendokumente, 16 (neue) Richtliniendokumente sowie 37 sonstige (meist neue bzw. on-top) Dokumente, Verfahren, Tools- und Protokolle.

Problem

In Summe hat eine mittelgroße Volksbank bzw. Raiffeisenbank mit DORA allein 350-400 DIN A4-Seiten Strategie-, Leitlinien-, Richtlinien und Verfahrensanweisungen in ihrem

Organisationshandbuch. Der vom Gesetzgeber verlangte "Governance-Dreiklang" aus den Verfahrensanweisungen vorgelagerten Strategie-, Leit- und Richtliniendokumenten kann bei großen, multinationalen Finanzinstituten angebracht sein. Bei kleinen und mittleren Häusern mit kurzen Wegen führt dies lediglich zu bürokratischem Mehraufwand ohne Verbesserung der operationellen digitalen Resilienz.

Lösung

Die Dokumentationsanforderungen für kleine und mittlere Institute müssen reduziert werden. Konkret wäre eine einfachere Governance-Struktur im Anweisungs- und Strategiewesen, wie z.B. ein größenabhängiger Verzicht auf separate Leit- und Richtlinien hilfreich, wenn die Verfahrensanweisungen, Protokolle und Tools schon hinreichend konkret sind und ein entsprechendes Niveau bieten.

Auch der Verzicht auf die Führung eines Zertifikateregisters, wenn die Verantwortlichkeit für Kryptographische Schlüssel und Zertifikate im Wesentlichen bei zentralen Rechenzentren/Verbundinternen Dienstleistern liegt, wäre eine sinnvolle Alternative.

2.3 Definition sowie Wesentlichkeitsschwellen für „schwerwiegende IKT-Vorfälle“ in Level 2 – Text anpassen

Ausgangslage

Laut Art. 3 der DORA-Verordnung (EU) 2022/2554 (**Level 1-Text**) sind IKT-Vorfälle folgendermaßen definiert:

- *„IKT-bezogener Vorfall“: [Ein] von dem Finanzunternehmen nicht geplantes Ereignis bzw. eine entsprechende Reihe verbundener Ereignisse, das bzw. die die Sicherheit der Netzwerk- und Informationssysteme beeinträchtigt und nachteilige Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder auf die vom Finanzunternehmen erbrachten Dienstleistungen hat;*
- *„zahlungsbezogener Betriebs- oder Sicherheitsvorfall“: [Ein] von den in Artikel 2 Absatz 1 Buchstaben a bis d aufgeführten Finanzunternehmen nicht geplantes Ereignis bzw. eine entsprechende Reihe verbundener Ereignisse, unabhängig davon, ob es sich um IKT-bezogene Vorfälle handelt oder nicht, das bzw. die nachteilige Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit zahlungsbezogener Daten oder auf die vom Finanzunternehmen bereitgestellten zahlungsbezogenen Dienste hat;*
- *„schwerwiegender IKT-bezogener Vorfall“: [Ein] IKT-Vorfall, der umfassende nachteilige Auswirkungen auf die Netzwerk- und Informationssysteme hat, die kritische oder wichtige Funktionen des Finanzunternehmens unterstützen;*

- *„schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfall“: [Ein] zahlungsbezogene[r] Betriebs- oder Sicherheitsvorfall, der umfassende nachteilige Auswirkungen auf die bereitgestellten zahlungsbezogenen Dienste hat;*

Somit setzt die Legaldefinition eines „IKT-bezogenen Vorfalls“ auf Level 1 eine „Beeinträchtigung der Sicherheit“ der entsprechenden Systeme voraus. „**Schwerwiegende IKT-Vorfälle**” müssen “**umfassende nachteilige Auswirkungen**” auf Systeme haben, die kritische oder wichtige Funktionen unterstützen.

Problem

In Art. 6 des Level 2-Textes zur Einstufung von IKT-Vorfällen (EU) 2024/1772 weicht der Gesetzgeber von seiner Legaldefinition ab bzw. instrumentalisiert die im Level 1-Text, Art. 18 Abs. 1e genannte Klassifizierung der IKT-Vorfälle (als schwerwiegend) nach "Kritikalität der betroffenen Dienste". Damit ist das laut Level 1-Text auf kritische und wichtige Funktionen beschränkte Ausmaß auf praktisch alles anzuwenden, was Kreditinstitute machen:

„Art. 6 Kritikalität der betroffenen Dienste
Um die in Artikel 18 Absatz 1 Buchstabe e der Verordnung (EU) 2022/2554 genannte Kritikalität der betroffenen Dienste zu bestimmen, bewerten die Finanzunternehmen, ob der Vorfall

a. *IKT-Dienste oder Netzwerk- und Informationssysteme zur Unterstützung kritischer oder wichtiger Funktionen des Finanzunternehmens beeinträchtigt oder beeinträchtigt hat;*
b. *von dem Finanzunternehmen erbrachte Finanzdienstleistungen beeinträchtigt oder beeinträchtigt hat, die einer Zulassung oder Registrierung bedürfen oder von den zuständigen Behörden beaufsichtigt werden;*
c. *einen erfolgreichen, böswilligen und unbefugten Zugriff auf die Netzwerk- und Informationssysteme des Finanzunternehmens darstellt oder dargestellt hat.*“

Insbesondere lit. b. führt dazu, dass in Verbindung mit Art. 8 des Level 2-Textes Vorfälle als **schwerwiegend** eingestuft werden müssen, die weder eine kritische oder wichtige Funktion betreffen noch die Sicherheit der Systeme beeinträchtigen.

Das bedeutet konkret eine sehr hohe Anzahl an Vorfällen, die theoretisch in die Betrachtung einbezogen werden müssen. Um diese für Dritte nachvollziehbar zu dokumentieren, entsteht den Banken ein erheblicher Verwaltungs- und Dokumentationsaufwand.[1]

[1] Praktisch hat eine mittelgroße Volksbank Raiffeisenbank in Bayern in den ersten viereinhalb Monaten des Jahres 2025 bereits 51 Vorfälle nach den Wesentlichkeitsschwellen (Art. 8 i.V.m. Art. 9 (EU) 2024/1772) dokumentiert und bewertet, um sich nicht der strafbewährten Ordnungswidrigkeit (bis zu 5 Millionen Euro laut KWG §56 (5e) Abs. 2) bei nicht, zu spät oder falsch abgegebenen

Lösung

Der europäische Gesetzgeber ist an dieser Stelle über das Ziel hinausgeschossen, den zuständigen Behörden einen Überblick über die Sicherheitslage zu verschaffen bzw. eine Gefährdung für das Europäische Finanzsystem rechtzeitig zu erkennen. Sowohl die Definition eines „schwerwiegenden Vorfalls“ als auch die Wesentlichkeitsschwellen im Level 2-Text müssen angepasst werden. Ansonsten werden perspektivisch zu viele für das Finanzsystem und die IKT-Sicherheit des Finanzsystems vollkommen irrelevante Meldungen abgegeben.

2.4 Kleinere Banken von 24/7-Meldeverpflichtung befreien

Ausgangslage[2]

"Grundsätzlich gilt gem. Artikel 5 Abs. 1 lit. a Delegierte Verordnung (EU) 2025/301 eine Meldefrist von 4 Stunden nach Klassifizierung des Vorfalls als schwerwiegend, wobei die Meldung innerhalb von 24 Stunden nach Erkennung zu erfolgen hat. Dabei ist die Meldung so schnell wie möglich abzugeben. Eine Erleichterung für Wochenenden und Feiertage gem. Artikel 5 Abs. 4 Delegierte Verordnung (EU) 2025/301, wonach eine Vorfallsmeldung (Erst-, Zwischen- oder Abschlussmeldung) bis 12 Uhr am nächsten Werktag abgegeben werden darf, gilt gem. Artikel 5 Abs. 5 Delegierte Verordnung (EU) 2025/301 nur für Finanzunternehmen, die

a. kein Kreditinstitut,

b. keine zentrale Gegenpartei,

c. kein Betreiber von Handelsplätzen und

d. kein weiteres Finanzunternehmen, das gemäß den nationalen Vorschriften zur Umsetzung von Artikel 3 NIS-2 als wesentliches oder bedeutendes Unternehmen wichtige Einrichtung eingestuft wurde.

sind."

Vorfallsmeldungen) auszusetzen. Kein einziger Vorfall hat nach Einschätzung der Bank die Sicherheit der Netzwerk- und Informationssysteme beeinträchtigt. In einigen Fällen wäre die Bank aufgrund der extrem niedrigen Meldeschwellen fast tatsächlich meldepflichtig geworden. Auch an dieser Stelle ist der bürokratische Aufwand enorm: Das pdf einer vollständigen Erst-/Folge und Abschlussmeldung umfasst gut 14 Din-A4-Seiten.

[2] Vgl. Fragen und Antworten der BaFin zur Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle: https://www.bafin.de/DE/Aufsicht/DORA/Meldewesen_IKT_Vorfaelle/FAQ/FAQ_artikel.html;jsessionid=09993474338A7D73FA1A2E2CB2F9C512.internet962?nn=19669324

Problem

Alle Volksbanken und Raiffeisenbanken bräuchten eine 24/7 Bereitschaft für die Erkennung und Meldung schwerwiegender IKT-Vorfälle. Denn zum einen ist die Bank für bankeigene Systeme sowie IKT-Dienstleister außerhalb des Verbundes selbst in der Pflicht.
Zum anderen muss die Bank auch im Fall einer Störung bei einem verbundinternen Dienstleister noch einmal eine separate Meldung abgeben. Diese 24/7 Bereitschaft ist für kleine und mittlere Institute (mit Mitarbeiterkapazitäten teilweise im zweistelligen Bereich) unzumutbar.

Lösung

Bankeigene Systeme kleinerer und mittlerer Banken haben in der Regel keine Relevanz für die Cyber-Lage des Europäischen Finanzsystems. Alle Systeme, die essenziell für kritische und wichtige Funktionen sind, werden meist ausschließlich von verbundinternen Dienstleistern betrieben. Diese sind bei Vorfällen ohnehin 24/7 meldepflichtig.

Der Gesetzgeber oder die BaFin in Ihrer nationalen Auslegungspraxis sollten bei kleinen und mittleren Instituten von einer 24/7 Meldeverpflichtung absehen, wenn die Meldung nicht kritisch für die Cyber-Sicherheit des Finanzsystems ist (d.h. vor allem bei bankeigenen Systemen kleinerer Banken sowie kleinen IKT-Dienstleistern), sowie wenn die Meldung über die zentralen IKT-Dienstleister für kritische und wichtige Funktionen gewährleistet ist.

2.5 Detailliertheit der Dokumentations- und Meldevorgaben für das IKT-Risikomanagement reduzieren

Ausgangslage

Die Vorgaben des Level-2 Textes zur Konkretisierung des IKT-Risikomanagements (EU) 2024/1774 sind kleinteilig und führen zu großem Aufwand bei den Banken bzw. überbordender Bürokratie. Im Folgenden einige Beispiele:

- Die in Art. 6 Abs. 3 und 4 vorgegebene Pflicht, "führende Praktiken und Normen" bzw. die Verschlüsselungs-"Technologie aufgrund von Entwicklungen im Bereich der Kryptoanalyse" entsprechend aktuell zu halten, ist für kleine und mittlere Institute nicht machbar. Hier müssen sie sich voll auf einen zentralen IKT-Dienstleister verlassen. Falls hier „führende Praktiken und Normen“ bzw. Technologieentwicklungen nicht erfüllt werden können, müssen laut Abs. 5 Abhilfe- und Überwachungsmaßnahmen aufgezeichnet werden. Dies führt wiederum zu erheblichem bürokratischem Aufwand bei den Banken.
- Die in Art. 6 Abs. 2b implizite Vorgabe, die "Verschlüsselung von Daten, die gerade verwendet werden, soweit erforderlich" zu regeln, ist in der IT bei Weitem noch nicht "State-of-the-Art" und kann, je nachdem wie „Erforderlichkeit“ künftig in der

Verwaltungspraxis interpretiert wird, die Systemanforderungen und Komplexität exponentiell erhöhen.

- Die Trennung und Segmentierung von Netzwerken (vgl. Art. 13 a) sollte nicht durch einen Rechtstext vorgegeben werden.
- Die geforderte Nutzung eines gesonderten und speziellen Netzwerks für die Verwaltung von IKT-Assets (vgl. Art. 13 c) ergibt praktisch keinen Sinn.
- Die Ausweitung des Changemanagements auf "alle Änderungen an Software, Hardware, Firmware-Komponenten, Systemen oder Sicherheitsparametern" und "alle" in Artikel 17 (1) a bis h aufgezählte (Dokumentations- bzw. Aufzeichnungs-) Anforderungen ist in der Praxis so nicht einmal für die zentralen IKT-Dienstleister oder Hyperscaler umsetzbar, da sich die IT schneller ändert als dies dokumentiert werden kann. Für die IKT-Systeme im Verantwortungsbereich kleiner und mittlerer Banken führt der Wegfall der in den BAIT enthaltenen Wesentlichkeitsgrenze für Änderungen in den IT-Systemen zu erheblichen Mehraufwänden bei Dokumentation von Änderungen in IT-Systemen.

Problem

Die Granularität sowie der generell hohe Detaillierungsgrad und der weitgehende Entfall von Wesentlichkeitsgrenzen und Proportionalität innerhalb der kompletten Delegierten Verordnung (EU) 2024/1774 passt nicht zu einem Wirtschaftsraum, der sich marktwirtschaftlichen und freiheitlichen Prinzipien verpflichtet fühlt. Zudem werden kleine und mittlere Institute in gleichem Umfang belastet wie Großbanken. Denn der von der EU-Kommission unter Proportionalitätsgesichtspunkten erarbeitete vereinfachte IKT-Risikomanagementrahmen greift nicht für kleine und mittlere Kreditinstitute, sondern lediglich für kleine Finanzunternehmen wie z.B. kleine Versicherungs- und Finanzvermittler.

Lösung

Die Anwendung des "Vereinfachten IKT-Risikomanagementrahmens" sollte auch für kleine und mittlere Institute mit zentralem gruppeninternem Rechenzentrum ermöglicht werden – und damit lediglich Anwendung des vollumfänglichen IKT-Risikomanagementrahmens auf das zentrale Rechenzentrum bzw. weitere gruppeninterne zentrale IKT-Dienstleister haben. Alternativ wäre auch die Schaffung einer Wesentlichkeitsgrenze bzw. eine stärkere Anwendung des Proportionalitätsprinzips analog dem bisherigen BAIT-Regulierungsregime in DORA eine Möglichkeit, die Belastungen für kleine und mittlere Institute zu senken. Entsprechende Anforderungen sind in Erwägungsgrund 53 von DORA formuliert, aber im weiteren Verfahren nicht adäquat umgesetzt.

2.6 Regelungen im Einklang mit internationalen Standards ausgestalten

Ausgangslage

Die BAIT versuchte, Regelungen möglichst im Einklang mit internationalen Standards zu treffen. Mit DORA vermischt der Gesetzgeber jedoch die Verpflichtung zu gängigen Standards, die sich meist dynamisch und mit Fachexpertise zum Beispiel im ISO 27001/2 oder dem BSI-Grundschutz weiterentwickeln, mit dem Setzen rechtlich verpflichtender, statischer und bürokratisch aufgeblähter Vorgaben.

Problem

Für die bayerischen Volksbanken und Raiffeisenbanken führt das zu doppeltem Dokumentationsaufwand: Ob und in welchem Umfang die Banken jeweils die Vorgaben/Maßnahmen/Empfehlungen aus gängigen Standards erfüllen, sowie parallel die Detailvorgaben der DORA, ist fraglich. So gibt der internationale Standard ISO 27001 lediglich 140 Sollmaßnahmen vor. Im Sollmaßnahmenkatalog des verbundinternen Verfahrenslieferanten, der die internationalen ISO-Standards mit den detaillierten Vorgaben aus der DORA zusammenführen soll, stehen aktuell hingegen bis zu 384 Sollmaßnahmen.

In Summe ist eine mittelgroße Volksbank bzw. Raiffeisenbank aktuell bei rund 100.000 einzelnen Sollmaßnahmen, die es für ihr IKT-Portfolio mit IKT-Drittdienstleistern zu vereinbaren gilt, deren Umsetzung nachgehalten werden muss bzw. die sie selbst umzusetzen hat.[3]

Lösung

Sicherlich sind hier auch noch Effizienzgewinne beim verbundinternen Verfahrenslieferanten möglich. Trotzdem könnte der europäische Gesetzgeber an dieser Stelle für deutliche bürokratische Entlastungen sorgen, indem er sich bei der Formulierung technischer Vorgaben zurückhält und dies analog dem bisherigen BAIT-Regulierungsregime den Entwicklern gängiger Standards überlässt. Die Kreditinstitute sollten dann die Wahlfreiheit haben, welchen gängigen Standards sie sich verpflichten wollen.

Außerdem sollte der EU-Gesetzgeber die Definition und Einstufung relevanter IKT-Dienstleistungen weniger weit fassen. Als gutes Beispiel hat die BaFin bereits mehrmals die

[3] Eine mittelgroße Volksbank Raiffeisenbank müsste z.B. nach den Vorgaben von DORA mit ihrem regionalen Dienstleister für die Aufstellung und Wartung ihrer Alarmanlagen über 110 Sollmaßnahmen vereinbaren und deren Umsetzung beim Dienstleister überwachen. Die Liste mit den Sollmaßnahmen „Anhang zur Anlage Informationssicherheit“ umfasst ausgedruckt fast 20 Din-A4-Seiten. Im Ergebnis besteht die Gefahr, dass sich langfristig mittelständische, regionale Dienstleister aus dem Geschäft mit den Primärbanken zurückziehen. Die Banken werden verstärkt auf die großen überregionalen Anbieter (mit entsprechend großen Rechts- und Compliance-Abteilungen) ausweichen müssen, was die Abhängigkeits- und Klumpenrisiken im IKT-Portfolio eher vergrößern wird.

Auslegung eingegrenzt, wann es sich bei einer Dienstleistung um eine IKT-Dienstleistung im Sinne von DORA handelt, obwohl in den DORA-Erwägungsgründen ursprünglich eine weite Auslegung als Maßgabe gesetzt ist.

2.7 Keine Doppelarbeiten bezüglich IKT-Drittparteienmanagement und Auslagerungsrecht

Ausgangslage

Bereits vor Geltung von DORA stellten zahlreiche IKT-Drittdienstleistungen (wesentliche) Auslagerungen bei den Banken dar. Wesentliche Auslagerungen sind seit vielen Jahren über § 25b KWG i.V.m. AT 9 MaRisk umfassend und detailliert reguliert. So müssen beispielsweise für wesentliche Auslagerungen Risikoanalysen erstellt, umfangreiche Auslagerungsregister erstellt und gepflegt werden, wesentliche Auslagerungen oder wesentliche Änderungen dieser bei der Aufsicht angezeigt werden und vertragliche Mindestinhalte mit den Dienstleistern vereinbart werden.

Problem

DORA sieht mit einer eigenen Risikoanalyse, dem Informationsregister, eigenen Anzeigenpflichten und eigenen Mindestvertragsinhalten eigene, oftmals aber redundante Pflichten vor. Sofern eine IKT-Dienstleistung auch eine wesentliche Auslagerung darstellt, müssen die Pflichten aus dem Auslagerungsrecht und nach DORA grundsätzlich nebeneinander erfüllt werden. Dies verursacht einen erheblichen, nicht sachgerechten Aufwand bei den Banken.

Entgegen dem Proportionalitätsgrundsatz werden kleine Institute wie Volksbanken und Raiffeisenbanken hier im Verhältnis zu von der EZB regulierten Instituten (SIs) stärker belastet, da große, von der EZB beaufsichtige Institute seit Anfang des Jahres von der Meldung von Auslagerungsregistern befreit sind. Eine solche Erleichterung zur Vermeidung von Doppelarbeiten ist für kleine Banken derzeit nicht vorgesehen.

Lösung

Bis zu einer Harmonisierung der beiden Regelungskreise DORA und Auslagerung und damit einer Reduzierung von Doppelarbeiten sollten aufsichtliche Regelungen in AT 9 MaRisk für IKT-Dienstleistungen, die auch wesentliche Auslagerungen darstellen, ausgesetzt werden soweit sie zu Doppelarbeiten führen.

Künftig wäre überdies bei Einführung eines neuen Regimes wie DORA vorab eine Harmonisierung mit bereits bestehenden Regelungskreisen dringend erforderlich.

2.8 Rechtssicherheit durch Überführung der Q&A der EU-Kommission ESA 2999-DORA030 in den Gesetzestext von DORA

Ausgangslage

Die Definition von „IKT-Dienstleistungen“ in Art. 3 Nr. 21 DORA wurde vom europäischen Gesetzgeber weit gefasst. Zudem folgt aus Erwägungsgrund 63 zu DORA, dass auch Finanzunternehmen, die IKT-Dienstleistungen für andere Finanzunternehmen erbringen, im Rahmen von DORA zu betrachten sind.

Mit Q&A ESA 2999-DORA030 hat die EU-Kommission am 22.01.2025, also nach Geltungsbeginn von DORA, klargestellt, dass IKT-Dienstleistungen, die von einem regulierten Finanzunternehmen für andere Finanzunternehmen erbracht werden und mit einer regulierten Finanzdienstleistung verbunden sind oder von dieser abhängig sind, keine IKT-Dienstleistungen in Bezug auf das IKT-Drittparteienrisikomanagement darstellen. In einem Finanzverbund wie dem der Genossenschaftlichen FinanzGruppe werden zahlreiche IKT-Dienstleistungen insbesondere zwischen Primärbanken und dem Zentralinstitut, also zwischen zwei regulierten Finanzunternehmen, von diesem Tatbestand umfasst.

Problem

Die Vorbereitungen auf DORA waren planmäßig bis zum 17.01.2025 vorzunehmen und somit in Unkenntnis der erst später veröffentlichten Q&A vom 22.01.2025. Die weite Definition der IKT-Dienstleistungen in DORA hat einen umfangreichen Arbeitsaufwand (z.B. Erstellen von Risikobewertungen, Anpassung vertraglicher Vereinbarungen, Vorbereitung des Informationsregisters) ausgelöst, der bei Kenntnis der Q&A nicht entstanden wäre. Zudem erscheint die Einschränkung gesetzlicher Vorgaben mit erheblichen Auswirkungen per Q&A unangemessen und mit Rechtsrisiken behaftet.

Lösung

Künftig müssen zentrale gesetzliche Anforderungen mit erheblichen Auswirkungen vor Geltungsbeginn neuer Gesetze ganzheitlich durchdacht und entsprechend geregelt werden. Hierdurch könnten Unsicherheiten und vor allem unnötiger Ressourceneinsatz vermieden werden.
Nachträglich sollte im konkreten Falle zumindest der Inhalt der Q&A kurzfristig in die DORA als Level 1-Verordnung übernommen werden, um Rechtssicherheit für die betroffenen Finanzunternehmen herzustellen.