Regulatory Blog

By PwC Deutschland | 12. August 2025

Next Level - Third Party Risk Management statt Outsourcing Governance

Die Erweiterung des Anwendungsbereichs der Guidelines erfolgt dahingehend, das sie nunmehr auf alle Third Party Arrangements anwendbar sein soll.

Bereits unter dem 8. Juli 2025 hat die European Banking Authority ein Konsultationspapier „**EBA Draft Guidelines on the sound management of third-party risk**“ veröffentlicht. Gegenstand des Konsultationspapiers ist eine Aktualisierung der „**EBA Guidelines on outsourcing arrangements**“ vom 25. Februar 2019. Dabei werden insbesondere folgende Ziele verfolgt:

- Erweiterung des Anwendungsbereichs der Guidelines auf andere Institutsformen
- Erweiterung des Anwendungsbereichs der Guidelines auf Third Party Arrangements und Schaffung eines umfassenden Rahmenwerks für das Third Party Risk Management
- Harmonisierung der Guidelines mit anderen Rechtsquellen, insbesondere mit der Regulation (EU) 2022/2554 (DORA)
- Verstärkung der Betrachtung des Konzentrationsrisikos auf der Anbieterseite durch die zuständigen Aufsichtsbehörden

Die **Erweiterung des Anwendungsbereichs** erfolgt zum einen hinsichtlich des Anwenderkreises dahingehend, dass zusätzlich zu den der Richtlinie 2013/36/EU (CRD) unterliegenden Kreditinstituten und Wertpapierinstituten sowie den der Richtlinie (EU) 2015/2336 (PSD) bzw. der Richtlinie 2009/110/EC (EMD) unterliegenden Zahlungsinstituten und E-Geldinstituten nunmehr auch folgende Unternehmen erfasst werden sollen:

- nicht der CRD unterfallende Wertpapierinstitute, soweit sie nicht klein und nicht verflochten im Sinne der Regulation (EU) 2019/2033 (IFR) sind,
- der Regulation (EU) 2023/1114 (MiCAR) unterfallende Emittenten von Asset Reference Tokens und
- der Richtlinie 2014/17/EU (MCD) unterfallende Kreditgeber.

Die **Erweiterung des Anwendungsbereichs** der Guidelines erfolgt zum anderen hinsichtlich des Regelungegenstands dahingehend, das sie nunmehr auf alle Third Party Arrangements anwendbar sein soll. Dies wird mit der sich immer weiter verstärkenden Inanspruchnahme von Drittparteiendienstleistern durch die Institute begründet, die eine Weiterentwicklung des traditionellen Begriffs des Outsourcings auf den breiteren Bereich der Drittparteiendienstleistern erforderlich mache. Wie aus der neu in das Konsultationspapier aufgenommenen Definition des „Third Party Arrangement“ sind davon jedoch nicht etwa alle mit Drittparteien abgeschlossenen Verträge, sondern solche Verträge umfasst, auf deren Grundlage die Drittpartei eine oder mehrere Funktionen an das Institut erbringt. Dabei wird „Funktion“ als Prozess, Dienstleistung, Tätigkeit oder Teile davon definiert und das Outsourcing als Unterfall des Third Party Arrangements angesehen. Dies führt im Ergebnis dazu, dass - ausgehend von den in den MaRisk verwendeten Begrifflichkeiten - auch der sog. sonstige Fremdbezug von Dienstleistungen künftig von den Guidelines erfasst wird. Die bisher schon ausdrücklich von der Anwendung der Guidelines befreiten Dienstleistungen wie z.B. Abschlussprüfung, globale Netzwerke und Clearing-Dienstleistungen werden jedoch auch weiterhin befreit bleiben.

Die Harmonisierung der Guidelines mit DORA bzw. ihre Abgrenzung voneinander soll durch eine zugleich erfolgende **Einschränkung des Anwendungsbereichs** der Guidelines im Hinblick auf ihren Regelungsgegenstand erfolgen. Die IKT-Drittdienstleistungen sollen künftig ausschließlich DORA unterfallen und nur noch die übrigen, d.h. die Non-IKT-Drittdienstleistungen sollen weiterhin den in der Guideline enthalten Regelungen über das Third Party Risk Management unterfallen. Technisch soll dies nicht etwa über eine entsprechende Anpassung der Definitionen des „Third Party Arrangement" oder des „Outsourcing Arrangements" erfolgen, sondern über eine Beschränkung des Anwendungsbereichs der Guideline insgesamt. Es erscheint fraglich, ob dieser Weg „gesetzgebungstechnisch" in Form einer Guideline umgesetzt werden kann. Denn Grundlage der Anforderungen an das Outsourcing sind die zu Beginn dieses Beitrags genannten Richtlinien, die eine derartige Unterscheidung nicht vorsehen. Außerdem müssen diese jeweils in nationales Recht umgesetzt wurden, was in Deutschland z.B. über § 25b KWG erfolgte, der diese Unterscheidung ebenfalls nicht vorsieht. Andererseits ist der praktische Bedarf für eine Klärung des Verhältnisses zwischen der Regulierung der IKT-Drittdienstleistungsverhältnisse durch DORA und des Outsourcings durch die anderen Regulierungen unabweisbar. Außerdem liegt die EBA mit dieser Unterscheidung auf einer Linie mit den unter dem 12. Juni 2025 veröffentlichten „**Principles on third-party risks supervision**" der ESMA und kommt damit eine Forderung des BdB in seiner Stellungnahme „**Zehn Punkte für ein modernes Drittparteien-Risikomanagement**" vom 10. Juni 2025 nach. Die EBA ihrerseits hat in ihrem Konsultationspapier zur Überarbeitung ihrer **Guidelines on Internal Governance** vom 7. August 2025 noch einmal nachgelegt und auch dort die entsprechende Abgrenzung neu eingefügt. Mithin ist davon auszugehen, dass dieser Weg auf jeden Fall weiter beschritten werden wird.

Zu einer vollständigen Harmonisierung beider Regelungskreise, die die größtmögliche Erleichterung für die Praxis bedeutet hätte, konnte man sich aber offensichtlich - wahrscheinlich vor dem Hintergrund der unterschiedlichen Rechtsquellen - doch nicht durchringen. Die betroffenen Institute werden daher auch bei der Anwendung der überarbeiteten Guidelines vor erhebliche Herausforderungen gestellt bleiben. So sieht das Konsulationspapier etwa keine ausdrückliche Regelung zur Abgrenzung zwischen IKT-Drittdienstleistungen und Non-IKT-Drittdienstleistungen vor. Diese Abgrenzung ist im digitalen Zeitalter, in dem praktisch keine Dientleistung mehr ohne Nutzung der IT erbracht werden kann, von erheblicher praktischer Bedeutung. Das Konsultationspapier beschränkt sich insoweit in einer Fußnote auf den Hinweis auf eine Q&A der ESAs zu DORA, wonach die Institute in Zweifelsfällen selbst entscheiden sollen, ob der Schwerpunkt der Leistung auf der IKT- oder der Non-IKT-Dienstleistung liegt und in Abhängigkeit davon das jeweils einschlägige Regelwerk anwenden.

Vom Umfang her legen die „**Guidelines on the sound management of third-party risk**" im Vergleich zur bisherigen Fassung nur um 3 Seiten zu. Die zahlenmäßig meisten Änderungen resultieren daraus, dass die bisher auf die „Outsourcing Arrangements" bezogenen Anforderungen nunmehr auf die „Third Party Arrangements" (TPA) erstreckt werden. Im Ergebnis wird also – um wieder in der Sprache de MaRisk zu bleiben – der sonstige Fremdbezug der Dienstleistungen den Auslagerungen gleichgestellt und es kommt unabhängig von dieser Einstufung nur noch darauf an, ob es sich bei den TPAs um critical or important TPAs handelt oder nicht, wobei die Definition des Begriffs „critical or important" an DORA angepasst wird.

Darüber hinaus erfolgt im Detail eine Vielzahl von Änderungen, von denen folgende Gruppierungen herausgehoben werden sollen

1. Änderungen betreffend das Auslagerungsregister, das zum TPA-Register wird

- In Angleichung an DORA wurden weitere Angaben zum Vertragstyp (Rahmenvertrag, Einzelvertrag), zur Inanspruchnahme des Dienstleisters auch durch andere gruppen- oder verbundangehörige Unternehmen und zur Zugehörigkeit des Dienstleisters oder Subcontractors zur Gruppe oder institutssichernden Einrichtung (die beiden letzten Angaben waren bisher jeweils nur für critical or important outsourcings vorgesehen) für alle TPAs neu aufgenommen.
- Neu ist auch das Erfordernis einer Kategorisierung der Dienstleistung anhand einer Aufstellung, die den Guidelines als Annex 1 neu beigefügt wird. Zusätzlich zum Namen sind für den Dienstleister künftig auch Kennzeichen wie LEI, EUID, Registernummer, UST ID sowie die geschätzten jährliche Kosten für das TPA in das TPA Register aufzunehmen.
- Für critical or important TPAs ist eine Aufspaltung der Angaben zur Exit Strategie in Ersetzbarkeit und Reintegration sowie der Kosten eines Scheiterns beider Alternativen, geschätzte Kosten für das letzte Jahr für das das gesamte Arrangement und eine Angabe der Bezahlwährung vorzunehmen.

2. Änderungen betreffend die Vertragsgestaltung

- Das bisher zwingend geltende Schriftformerfordernis wird durch Zulassung elektronischer Fassungen aufgegeben, die aber für alle Beteiligten dauerhaft zugänglich sein müssen. Eine Umsetzung dieses Punkts in nationales deutsches Recht wird eine Änderung des § 25b Abs. 3 Satz 3 KWG erfordern.
- Zugleich mit der Erstreckung der Anforderungen auf alle TPAs kommt es zu einer erheblichen Verschärfung der Anforderungen an die non critical or important TPAs. Denn eine Vielzahl der Anforderungen, die bisher nur für critical or important Outsourcing Agreements anwendbar waren, werden nunmehr für alle TPAs anwendbar. Nur wenige Anforderungen, wie zB die laufende Berichterstattungspflicht des Dienstleisters, die Haftpflichtversicherungspflicht, die Durchführung von Tests für den Notfallplan, das unbeschränkte Prüfungsrecht des Instituts und der Aufsichtsbehörde bleiben ausschließlich den critical or important TPAs vorbehalten.
- Für die critical or important TPAs wird im Vergleich zu bisher eine Erweiterung des Prüfungsrechts des Instituts und der zuständigen Aufsichtsbehörde (Kollisionsregel bei Beeinträchtigung der Rechte anderer Kunden, ausdrückliche Erwähnung von Onsite Inspections) gefordert. Neu ist auch die Verpflichtung zur Vereinbarung einer Transitionsphase innerhalb deren der Dienstleisterin Falle der Beendigung des TPAs weiterhin Leistungen erbringen muss.

3. Verschärfung der Änderungen an TPAs mit Dienstleitern in Drittländern und an Weiterverlagerungen/Subcontracting

- Bei TPAs mit Dienstleitern in Drittländern sind Vorkehrungen bezogen auf die lokale Rechtslage zu treffen, insbesondere bezogen auf den Datenschutz.
- Klarstellung, dass die Weiterübertragung die Verantwortung des Management Boards des Instituts nicht schmälert.
- Verpflichtung des Management Boards, die mit der Übertragung und Weiterübertragung verbundenen Risiken holistisch zu steuern und zu überwachen.
- Vor der Nutzung von pooled audits haben die Institute zu prüfen, ob diese die für sie notwendigen Informationen enthalten, was tatsächlich aber als Selbstverständlichkeit anzusehen sein sollte.

Als Folge der Überarbeitung der Guidelines erscheint eine Anpassung des AT 9 MaRisk für Banken unumgänglich. Der am 6. August 2025 BaFin zur Konsultation gestellte Entwurf **der MaRisk für Wertpapierinstitute** orientiert sich noch strikt an AT 9 der MaRisk für Banken in der aktuell geltenden Fassung und kann daher insoweit schon wieder als überholt angesehen werden, bevor er noch in Kraft getreten ist. Es bleibt abzuwarten, wie die BaFin auf die geänderten Guidelines reagieren wird und ob sie diese ggf. zum Anlass nehmen wird, die eigenen diesbezüglichen Vorgaben weiter zurückzufahren und zugleich in verstärkter Form direkt auf die EBA Guidelines zu verweisen.

Die Konsultationsfrist läuft noch bis zum 8. Oktober 2025. Zuvor erfolgt noch am 5. September 2025 eine öffentliche Anhörung der EBA in virtueller Form. Den öffentlich zugänglichen Dokumenten ist nicht zu entnehmen, bis wann mit einem Inkrafttreten der überarbeiteten Guidelines zu rechnen ist. Ein Inkrafttreten noch in diesem Jahr erscheint jedoch nicht unrealistisch. Ab Inkrafttreten der Guidelines erhalten die Institute eine Übergangsfrist von 2 Jahren, innerhalb deren sie alle TPAs an die neuen Anforderungen anpassen bzw. die nicht rechtzeitige Umsetzung an die zuständige Aufsichtsbehörde melden müssen. Soweit ein TPA aus anderen Gründen vorher angepasst wird, sind bei der Gelegenheit auch die durch die EBA Guidelines erforderlich werdenden Anpassungen vorzunehmen.

Bei den Instituten löst die Umsetzung der überarbeiteten Guidelines zu Handlungsbedarf in allen Bereichen der bisherigen Outsourcing Organisation aus, beginnend mit der Strategie über die Richtlinien bis hin zur sonstigen schriftlich fixierte Ordnung. Betroffen ist sowohl die Aufbau- als auch die Ablauforganisation. Darüber hinaus muss eine Anpassung sowohl der wesentlichen und unwesentlichen Auslagerungsverträge, als auch der Verträge über den sonstigen Fremdbezug erfolgen – soweit es sich dabei nicht um IKT-Drittdienstleistungsverträge handelt, für die stattdessen die einschlägigen DORA-Anforderungen zu beachten sind. Darüber hinaus muss das Auslagerungsregister zum TPA-Register um- bzw. aufgerüstet werden und über eine mögliche Verschmelzung mit dem DORA-IKT-Drittdienstleistungsregister nachgedacht werden. In diesem Zusammenhang sollten die Institute auch das Zusammenspiel ihrer internen Organisationseinheiten im Hinblick auf die Erfüllung der DORA-Anforderungen einerseits und des Third Party Risk Management bzw. der Outsourcing-Governance andererseits ordnen, soweit sie dies nicht bereits getan haben. Auch soweit sie dies bereits getan haben, sollten die Institute überprüfen, ob die gewählte Neuordnung auch vor dem Hintergrund der überarbeiteten Guidelines noch Bestand haben kann.

Sollten Sie Unterstützung bei der Überprüfung der Auswirkungen der EBA Guidelines auf ihr Institut, die Interpretation einzelner darin enthaltener Anforderungen oder bereits bei deren Umsetzung benötigen, stehen wir hierfür selbstverständlich sehr gerne zur Verfügung.

Laufende Updates zum Thema erhalten Sie über das regulatorische Horizon Scanning in unserer Recherche-Applikation PwC Plus. Lesen Sie **hier** mehr über die Möglichkeiten und Angebote.

Zu weiteren PwC Blogs

Schlagwörter

Bankenaufsicht (Europäische und Internationale Organisationen), Capital Requirements Regulation (CRR III), Credit Risk, Eigenmittel / Eigenkapital, Interne Modelle, Market Risk, Risk Management Banking, Third-Party Risk, crypto assets / virtual assets, prudent valuation

Kontakt

Martin Neisen
Frankfurt am Main
martin.neisen@pwc.com

Christoph Himmelmann
Frankfurt am Main
christoph.himmelmann@pwc.com