DEUTSCHE BÖRSE GROUP

Per E-Mail
Konsultation-14-20@bafin.de ; B30_MaRisk@bundesbank.de

Bundesanstalt für Finanzdienstleistungsaufsicht
Graurheindorfer Straße 108
53117 Bonn

Deutsche Börse AG

MaRisk Compl. & Banking Regulation

Mergenthalerallee 61
65760 Eschborn

Postanschrift
60485 Frankfurt am Main

Telefon
+49-(0) 69-2 11-17178

Internet
deutsche-boerse.com

E-Mail
marija.kozica@
deutsche-boerse.com

04. Dezember 2020

Stellungnahme zur Konsultation 14/2020 - Mindestanforderungen an das Risikomanagement (MaRisk)

MCBR

Sehr geehrte Damen und Herren,

Die Neufassung des Rundschreibens 09/2017 (BA) - Mindestanforderungen an das Risikomanagement (MaRisk) soll vor allem der Umsetzung dezidierter Vorgaben der EBA-Leitlinien zu notleidenden und gestundeten Risikopositionen (EBA/GL/2018/06), zu Auslagerungen (EBA/GL/2019/02) sowie zu IKT- und Sicherheitsrisiken (EBA/GL/2019/04) dienen.

Wir begrüßen grundsätzlich den vorgelegten Entwurf (im Folgenden MaRisk-E) und die damit einhergehende größere Rechtssicherheit sowie die erhöhte Transparenz bezüglich aufsichtlicher Erwartungen als auch der bestehenden Aufsichts- und Verwaltungspraxis. Ungeachtet dessen möchten wir die Möglichkeit der Stellungnahme nutzen, um auf einzelne Sachverhalte mit Klarstellungsbedarf hinzuweisen sowie Anpassungen bestimmter vorgesehener Änderungen anzuregen.

Neben der Angleichung der Definition notleidender Risikopositionen an die Definition des aufsichtlichen Meldewesens, begrüßen wir insbesondere auch, dass bei der Umsetzung der EBA-Leitlinien nationale Spezifika Berücksichtigung fanden. So erachten wir die Beibehaltung möglicher Erleichterungen im Falle gruppen- und verbundinterner Auslagerungen als zweckdienlich und unterstützen diese.

Im Gegensatz dazu sehen wir vor allem im Rahmen der erweiterten vertraglichen

Mindestinhalte bei wesentlichen Auslagerungen nach AT 9 Tz. 7 MaRisk-E noch Klärungs- und Anpassungsbedarf. Unter anderem sollte das Prinzip der doppelten Proportionalität stärker bei der Ausgestaltung der vertraglichen Bestimmungen angewandt und die Zweckmäßigkeit bestimmter Vorgaben eingehender berücksichtigt werden. Dies ist insbesondere bei der Prozessierung von Daten (s. AT 9 Tz. 7 lit. d) MaRisk-E) als auch der Einforderung von Unterstützungsleistungen bei Kündigung (s. Erläuterung zu AT 9 Tz. 7 lit. l) MaRisk-E) der Fall.

Ferner sprechen wir uns für eine Anpassung der Erläuterung zur Anwendung der Risikoanalyse auf die Weiterverlagerung (AT 9 Tz. 11 MaRisk-E) aus. Während wir eine Bewertung der mit der Weiterverlagerung verbundenen Risiken im Rahmen der Risikoanalyse unterstützen, erscheint uns eine dezidierte Bewertung der Wesentlichkeit von Weiterverlagerungen im Sinne einer Klassifizierung in wesentliche und nicht wesentliche Weiterverlagerungen als nicht zweckdienlich. Ferner sollte die Bewertung von Weiterverlagerungen nur für wesentliche Primärauslagerungen verpflichtend eingeführt werden.

1. Große und komplexe Institute nach AT 1 Tz.6 MaRisk-E

Mit der Überarbeitung der MaRisk soll der Begriff der systemrelevanten Institute in AT 1 Tz. 6 MaRisk durch „große und komplexe“ Institute ersetzt werden. Als große und komplexe Institute sollen dabei in der Regel Institute gelten, „deren Bilanzsumme auf Einzelinstitutseben oder konsolidiert auf Gruppenebene 30 Milliarden Euro erreicht oder überschreitet.“

Mit Einführung des Begriffs „großes und komplexes Institut“ wird die bestehende Vielzahl an unterschiedlichen Institutsklassifizierungen zur Bestimmung der Größe oder (System-)Relevanz eines Instituts nochmals erweitert. Bereits heute zielen die Begriffe „global systemrelevantes Institut“ (§ 10f Absatz 2 KWG), „anderweitig systemrelevantes Institut“ (§10g Absatz 2 KWG), „potenziell systemgefährdendes Institut“ (§20 Absatz 1 SAG), „bedeutendes Institut“ (Artikel 6 der Verordnung (EU) 1024/2013 (SSM-VO) in Abgrenzung zum bedeutenden Institut nach § 25n KWG) sowie „großes Institut“ (Artikel 4 Absatz 1 Nummer 146 der Verordnung (EU) 575/2013 (CRR) auf eine Klassifizierung von Instituten nach ihrer Größe oder (System-) Relevanz ab.

Der Begriff des „großen Instituts“ fand dabei erst kürzlich mit der Überarbeitung der CRR durch die Verordnung (EU) 876/2019 Einzug in das Aufsichtsrecht und umfasst u.a. solche Institute, deren Gesamtwert an Vermögenswerte auf Einzelbasis oder auf Basis der konsolidierten Gesamtlage größer oder gleich 30 Milliarden Euro beträgt. Der Begriff des „großen Instituts“ beinhaltet also auch solche Institute, die nach AT 1 Tz. 6 MaRisk-E in der Regel als „groß und komplex“ gelten würden. Während mit der Klassifizierung als „großes und komplexes Institut“ nach AT 1 Tz. 6 MaRisk-E die Einhaltung verschiedener zusätzlicher Vorgaben, darunter an die Strategie, Risikodatenaggregation, Kontrollfunktionen als auch Auslagerungen, einhergehen, ist die Klassifizierung als „großes Institut“ nach Artikel 4 Absatz 1 Nummer 146 CRR lediglich mit vereinzelten erhöhten Transparenzvorgaben verbunden.

Die Einführung eines weiteren Begriffs zur Bestimmung der Größe oder (System-) Relevanz eines Instituts erscheint uns insbesondere auch vor dem Hintergrund der bestehenden Vielfalt vergleichbarer Begriffe als nicht zweckdienlich.

Darüber hinaus sind wir der Auffassung, dass ein fester Schwellenwert nicht der risikoorientierten Ausrichtung der MaRisk entspricht. Die zur risikoorientierten Anwendung der Vorgaben zugrundliegenden Kriterien Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten sollten dabei gleichwertig bei der Anwendung der MaRisk herangezogen werden. Eine angemessene Berücksichtigung weiterer Kriterien wird zwar durch die Öffnung „in der Regel“ ermöglicht, jedoch unsers Erachtens nicht ausreichend erläutert.

Wir verstehen den Vorteil eines einfachen Kriteriums zur Bestimmung von großen und komplexen Instituten. Sofern die Einstufung als global systemrelevantes oder anderweitig systemrelevantes Institut nach §§ 10f oder 10g KWG (oder als

„bedeutendes Institut“ im Sinne von Artikel 6 Abs. 4 der SSM-VO) nicht maßgeblich ist, müsste allerdings geregelt werden, nach welchem Verfahren Institute als groß und komplex bestimmt werden. Zur Bestimmung etwaiger Abweichungen von der Regel, dass Institute bei Überschreiten der 30-Milliardengrenze als groß und komplex gelten sollen, bietet sich unseres Erachtens nach die analoge Anwendung der Vorgaben der Artikel 70 bis 72 EZB-VO 468/2014 an. Dabei sollten, wie bereits hervorgehoben auch, Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten gleichermaßen herangezogen werden.

Auch vor dem Hintergrund, dass der Begriff des „großen und komplexen“ Instituts bereits in der MaRisk-Konsultation 02/2016 eingeführt wurde, jedoch nicht in die finale MaRisk überführt wurde, erachten wir eine Überprüfung der Einführung des Begriffs sowie weiterer Erläuterungen bezüglich der Klassifizierung als „großes und komplexes“ Institute für notwendig.

2. Definition notleidender Risikopositionen

Die Erläuterung zu AT 2.1 MaRisk-E wurde um eine Definition notleidender Risikopositionen erweitert. Wir begrüßen diese Erweiterung und den Verweis auf das aufsichtliche Meldewesen ausdrücklich, regen jedoch an, dies noch weiter zu konkretisieren und bezüglich der zu berücksichtigenden Risikopositionen direkt auf Annex V, Abschnitt 7 der Delegierten Verordnung (EU) 680/2014 zu verweisen, um etwaige Unklarheiten zu vermeiden.

3. Technisch-organisatorische Ausstattung

Die Anpassung des AT 7.2 MaRisk erfolgte parallel und unter Berücksichtigung der kürzlich abgeschlossen Konsultation der Bankenaufsichtlichen Anforderungen an die IT (Konsultation 13/2020). Während die BAIT durchaus auf die MaRisk verweist, erfolgt kein Verweis der MaRisk auf die spezifizierenden Vorgaben der BAIT.

Um etwaige Redundanzen und Unklarheiten zu vermeiden, regen wir an, insbesondere in AT 7.2 MaRisk-E auf die entsprechenden Vorgaben der BAIT zu verweisen.

4. Notfallmanagement

AT 7.3 Tz. 2 MaRisk soll dahingehend erweitert werden, dass im Falle der Auslagerung von zeitkritischen Aktivitäten und Prozessen das auslagernde Institut und das Auslagerungsunternehmen über aufeinander abgestimmte Notfallkonzepte verfügen sollen.

Die Formulierung „aufeinander abgestimmte Notfallkonzepte“ impliziert, dass das Auslagerungsunternehmen seine Notfallkonzepte an die Notfallkonzepte des

Instituts anzupassen hat. Dies wird in vielen Fällen jedoch nicht erforderlich sein, um den Schutzzweck der Anforderung zu erreichen. Im Falle großer Mehrmandantendienstleister, die in der Regel standardisierte Dienstleistungen an eine Vielzahl von Unternehmen anbieten, wird eine individuelle Anpassung der bestehenden Notfallkonzepte auch nicht möglich sein. Insoweit sollte unseres Erachtens erläuternd klargestellt werden, dass auch auf bestehende, nicht individualisierte Notfallkonzepte des Auslagerungsunternehmens zurückgegriffen werden darf, wenn diese im Rahmen der Risikobetrachtung des Instituts tauglich sind, das Kontinuitätsinteresse des Instituts zu wahren.

5. Auslagerungen

Wir begrüßen es grundsätzlich, dass bei der Umsetzung der EBA-Leitlinien zu Auslagerungen zum Teil nationale Spezifika berücksichtigt wurden. Insbesondere befürworten wir den klaren Bezug der Auslagerungsdefinition zu Aktivitäten und Prozessen im Zusammenhang mit der Durchführung von Bankgeschäften und Finanzdienstleistungen sowie die Berücksichtigung von begünstigenden Faktoren im Falle gruppeninterner Auslagerungen. Ungeachtet dessen erwachten wir einzelne Vorgaben bezüglich der Aufsichtserwartung als unklar oder auch als zu umfassend.

AT 9 Tz. 1 – sonstiger Fremdbezug von Leistungen

Die ausführende Erläuterung zu AT 9 Tz.1 zu sonstigem Fremdbezug von Leistungen (in Abgrenzung zu Auslagerungen) sieht eine Erweiterung der Auflistung sonstiger Fremdbezüge um weitere Beispiele vor. Wir begrüßen grundsätzlich die Auflistung weiterer Beispiele und die damit einhergehende erhöhte Transparenz bezüglich der Aufsichtspraxis, möchten jedoch anregen, die Aufzählung um weitere relevante Abgrenzungsfälle wie z.B. Hardware-Wartungsdienstleistungen (Rack-Wartung, Verkabelung, etc.) und Telekommunikationsequipment (Cisco-WebEx Geräte, etc.) zu erweitern.

Die Erläuterung zu AT 9 Tz. 1 legt zwar dar, dass einmaliger oder gelegentlicher Fremdbezug von Gütern nicht als Auslagerung im Sinne der MaRisk gilt. Diese Formulierung umfasst aber nicht den dauerhaften Bezug von Gütern. Unserem Verständnis nach können weder der einmalige oder gelegentliche noch der dauerhafte Bezug von Gütern eine Auslagerung darstellen, da Güter keine „Aktivitäten und Prozesse“ im Sinne des §25b KWG sind. Ausgehend von den vorgesehenen Änderungen der MaRisk-E ist ein grundsätzlicher Ausschluss von Gütern vom Anwendungskreis des AT 9 nicht beabsichtigt. Umso wichtiger erscheint es uns auch den dauerhaften Bezug von Gütern, insbesondere Telekommunikationsequipment, vom Begriff der Auslagerungen auszuschließen.

Weitere Abgrenzungsfälle sollten sich am Katalog der Allgemeinen Service- und Unterstützungsdienstleistungen in Ziffer 3.4.1.3 des MaRisk-

Interpretationsleitfadens Version 6.1 des Deutsche Sparkassen- und Giroverbands orientieren und insbesondere Telekommunikationsdienste sowie OTT-Kommunikationsdienste (Skype, Diligent Boardbooks, etc.) berücksichtigen.

Bei Standardsoftware (d.h. nicht speziell für das Institut entwickelter Software) ist der Abschluss von Wartungsverträgen, die den Auslagerungsanforderungen genügen, oft ausgesprochen problematisch, da die Hersteller von Standardsoftware (z.B. IBM, Microsoft, Oracle) lediglich Standardprozesse und -verträge anbieten. Es wird Instituten regelmäßig nicht möglich sein Einfluss insbesondere auch auf die Ausgestaltung der Standard-Wartungsverträge zu nehmen. Darüber hinaus wirken sich unseres Erachtens nach Standard-Wartungsverträge zu Standardsoftware, selbst wenn diese im Rahmen der Steuerung, Überwachung und Kommunikation von Risiken durch Institute verwendet werden, nicht risikoerhöhend aus. Die Wartung von Standardsoftware sollte daher nicht als Auslagerung, sondern ebenfalls als sonstiger Fremdbezug. eingestuft werden, auch wenn diese für die Durchführung von bankgeschäftlichen Aufgaben von wesentlicher Bedeutung ist.

AT 9 Tz.2 – Risikoanalyse

Mit der Anpassung der Erläuterung zu AT 9 Tz.2 MaRisk sollen die Vorgaben an die im Rahmen der Risikoanalyse zu berücksichtigenden Faktoren spezifiziert aber auch erweitert werden. U.a. sollten Institute politische Risiken sowie Risikokonzentrationen, im Sinne mehrerer Auslagerungen mit demselben Auslagerungsunternehmen im Rahmen der Risikoanalyse berücksichtigen.

Wir befürworten eine zielgerichtete und angemessene Risikoanalyse, auch unter Berücksichtigung politischer Risiken. Zum Zwecke einer klaren und zielgerichteten Umsetzung möchten wir jedoch anregen, erläuternd klarzustellen, dass sich das Institut im Rahmen der Beurteilung politischer Risiken auf verfügbare Länderrisikoanalysen von z.B. Ratingagenturen und Exportkreditversicherungen stützen darf, da eine selbständige Bewertung solcher Risiken vielen Instituten aufgrund der umfassenden Berücksichtigung verschiedener Informationen nicht möglich sein wird. Ohne eine entsprechende Klarstellung könnten insbesondere kleinere Institute von international arbeitsteiligen Prozessen ausgeschlossen werden.

Bezüglich der verpflichtenden Berücksichtigung von Risikokonzentrationen möchten wir darauf hinweisen, dass unserem Verständnis nach ausschließlich Risikokonzentrationen innerhalb des Instituts respektive der Institutsgruppe zu berücksichtigen sind. Die Einschätzung und Steuerung industrieweiter Clusterrisiken im Rahmen von gruppenexternen Auslagerungen ist Instituten regelmäßig nicht möglich, da die erforderlichen Informationen nicht zur Verfügung stehen. Ferner ist unklar, welche Konsequenzen für einzelne Institute in Falle einer industrieweiten Konzentration auf wenige Dienstleister folgen würden. Um etwaige Unklarheiten zu vermeiden, würden wir eine klarstellende Erläuterung begrüßen.

dass solche sektoralen Clusterrisiken nicht zwingend in der Risikoanalyse des Instituts zu berücksichtigen sind, sofern diese nicht von staatlichen oder internationalen Stellen zur Verfügung gestellt werden.

AT 9 Tz. 2 – Szenarioanalyse

Ferner soll, den Anpassungen der Erläuterung zu AT 9 Tz 2 MaRisk-E folgend, die Risikoanalyse (soweit sinnvoll) durch eine Szenarioanalyse ergänzt werden. Institute sind bereits heute angehalten zur Steuerung verschiedener Risiken Szenarioanalysen durchzuführen. Dies ist beispielsweise im Rahmen der Sanierungsplanung als auch des Stresstestens oder der Quantifizierung operationeller Risiken üblich. Es wäre hilfreich zu wissen, inwieweit sich die hier geforderte Szenarioanalyse an den bereits bestehenden Szenarioanalysen orientieren sollte. Wir halten folglich eine Klarstellung bezüglich Art und Umfang der durchzuführenden Szenarioanalyse für notwendig.

In Bezug auf die Ergänzung der Risikoanalyse durch eine Szenarioanalyse wäre es ferner hilfreich die aufsichtliche Erwartungshaltung bezüglich der Verwendung der Ergebnisse der Risikoanalyse besser zu verstehen. Es stellt sich insbesondere die Frage, ob die Ergebnisse der Szenarioanalyse als direkte Auswirkungen auf die Einstufung der Wesentlichkeit eines ausgelagerten Prozesses respektive einer ausgelagerten Dienstleistung zu berücksichtigen sind. Wir halten es für sinnvoll die Szenarioanalyse auf den grundlegenden Geschäftsprozess analog der vorausgehenden Ergänzung der Erläuterung zu AT 9.Tz. 2 („[…] inwiefern eine auszulagernde Aktivität oder ein auszulagernder Prozess innerhalb der Prozesslandschaft des Instituts als wesentlich einzustufen ist.“) anzuwenden und nicht auf einzelne spezifische Auslagerungen.

AT 9 Tz. 4 – „Empty Shell“

AT 9 Tz. 4 MaRisk-E folgend, sollten Auslagerungen nicht dazu führen, dass Institute nur noch leere Hüllen („empty shells“) darstellen. Wir unterstützen die Intention dieser Ergänzung der Tz.4, sind jedoch der Auffassung, dass der neu eingefügte Satz dahingehend konkretisiert werden sollte, dass über das vorstehende hinaus keine Anforderungen an den Geschäftsbetrieb des Instituts gestellt werden. Wir schlagen folglich eine Anpassung der Ergänzung wie folgt vor:

„*Auslagerungen dürfen somit nicht dazu führen, dass das Institut nur noch als leere Hülle (empty shell) existiert*“.

AT 9 Tz 4 – Befugnis der Leistungserbringung des Auslagerungsunternehmens

Nach der ergänzenden Erläuterung zu AT 9 Tz 4 MaRisk-E soll das auslagernde Institut die Befugnisse zur Erbringung der Dienstleistung durch den Dienstleiter

prüfen und Kooperations- und Collage-Vereinbarungen zwischen den relevanten Aufsichtsbehörden sicherstellen, soweit der Dienstleister seinen Sitz außerhalb des Europäischen Wirtschaftsraums (EWR) hat.

Wir erachten die Anforderung als zum Teil zu weitreichend, nicht schlüssig und zum Teil unklar formuliert.

Gefordert wird eine hypothetische Prüfung, ob die bezogene Leistung durch das Auslagerungsunternehmen innerhalb des EWR erlaubnispflichtig wäre, hätte es seinen Sitz im EWR. In diesem Fall soll das auslagernde Institut sicherstellen, dass das Auslagerungsunternehmen im Drittstaat beaufsichtigt wird.

Die Erlaubnisanforderungen in Drittstaaten weichen allerdings vielfach von denen innerhalb des EWR ab. Es bleibt somit offen, was in den Fällen gelten soll, in denen das Auslagerungsunternehmen im EWR erlaubnispflichtig wäre, in seinem Heimatstaat aufgrund der dort geltenden Gesetze aber tatsächlich keiner Erlaubnis bedarf. Ist eine Auslagerung in diesem Fall nicht möglich?

Erlaubnispflichten innerhalb des EWR bestimmen sich nach wie vor auch nach nationalen Vorschriften. Es ist unklar, welches nationale Recht für die Frage der „Erlaubnispflicht im EWR“ maßgeblich sein soll und inwiefern dabei auch gesetzliche Ausnahmen, Freistellungsmöglichkeiten, behördliche Verwaltungspraxis oder Rechtsprechung (z.B. Inlandsbezug, Teilaktstheorie) zu berücksichtigen sind.

Ferner ist unklar, welche Bedeutung die gesonderte Erwähnung der „Prozesse von Bankgeschäften“ neben dem Begriff „ausgelagerte Aktivitäten“ hat. Auch ist nicht eindeutig klar, welche Art von „Zulassung oder Registrierung durch die zuständigen Aufsichtsbehörden“ innerhalb des EWR gemeint ist. Sofern es nicht auch um z.B. rein gewerberechtliche Zulassungen und Handelsregistereintragungen etc., sondern um die Zulassung als Institut oder Wertpapierfirma gehen soll, sollte das klargestellt werden. Unseres Erachtens nach sind umfassende zusätzliche Erläuterungen notwendig, um die zusätzlichen Vorgaben bezüglich der Leistungserbringung des Auslagerungsunternehmens angemessen und zielgerichtet umzusetzen.

Darüber hinaus erscheint uns die Anforderung, dass Institute die notwendige Zulassung oder Registrierung als auch Kooperationsvereinbarungen und College-Vereinbarungen sicherstellen sollen, als zu weitreichend. Sinnvoller wäre es, die Anforderung dahingehend zu formulieren, dass das Institut sich zu vergewissern (nicht sicherzustellen) hat, dass das Auslagerungsunternehmen in dem Drittstaat zugelassen bzw. beaufsichtigt ist, sofern die in Rede stehende Leistung in diesem Drittstaat erlaubnispflichtig ist. Nur in diesem Fall ist auch die Anforderung bzgl. einer Kooperationsvereinbarung sinnvoll.

Für den Fall, dass Leistungen durch Unternehmen außerhalb des EWR erbracht werden, bitten wir um Klarstellung, wie bestehende College-Vereinbarungen oder Absichtserklärungen, deren Regelungsumfang als auch aktueller Status den

Instituten durch die Aufsicht zur Kenntnis gebracht werden und welche Vereinbarungen oder Absichtserklärungen darüber hinaus noch angestrebt werden.

AT 9 Tz. 7 Mindestinhalte von Auslagerungsverträgen

Entsprechend der EBA-Leitlinie zu Auslagerungen wurde die Liste der Mindestinhalte in Auslagerungsverträgen zu wesentlichen Auslagerungen um weitere ergänzt. Wir erachten einige der zusätzlichen Mindestinhalte als nicht durchgängig zweckdienlich und möchten auch im Rahmen der Mindestinhalte die Anwendung des Proportionalitätsprinzips zum Zwecke einer angemessenen Umsetzung anregen.

→ lit. d)

AT 9 Tz. 7 lit. d) MaRisk-E verlangt u.a. die vertragliche Festlegung von Standorten, in denen die Durchführung der Dienstleistung erfolgt und / oder kritische Daten gespeichert und verarbeitet werden.

Bei arbeitsteiligen Prozessen mit zahlreichen Unterauslagerungen, bei denen Wartung und operative Betriebssteuerung nach dem „24/7 /follow the sun" Prinzip erfolgt, wird die Festlegung der Standorte, in denen die Durchführung der Dienstleistungen erfolgt, nahezu unmöglich sein und bringt keinen Mehrwert, insbesondere, sofern von diesen Standorten kein Zugriff auf unverschlüsselte Kunden- oder Unternehmensdaten möglich ist.

Sinnvoll ist demgegenüber die Festlegung der Datenresidenz für „kritische Daten", sofern diese Regelung die vorbezeichneten international arbeitsteiligen Prozesse nicht negiert. Insoweit ist auch hier das Proportionalitätsprinzip zu wahren. Die Anforderung sollte unserer Meinung nach daher wie folgt lauten:

„*d) Standorte, in denen ~~die Durchführung der Dienstleistung erfolgt und / oder~~* kritische Daten *permanent gespeichert ~~und verarbeitet~~ werden, sowie die Regelung, dass das Institut benachrichtigt wird, wenn das Auslagerungsunternehmen den Standort wechselt.*"

Darüber hinaus sollte klarstellend - zumindest beispielhaft - erläutert werden, welche Datentypen als „kritische Daten" zu betrachten sind. Dabei sollte verdeutlicht werden, ob mit „kritischen Daten" lediglich solche, die besonderen rechtlichen Anforderungen unterfallen (personenbezogene Daten, Kundendaten) oder alle Daten, die kritisch für die Erbringung der Institutsleistungen, gemeint sind.

→ lit. e)

AT 9 Tz. 7 lit. e) MaRisk-E folgend sollen Auslagerungsverträge Angaben zur vereinbarten Dienstleistungsgüte mit eindeutigen qualitativen und quantitativen Leistungszielen enthalten.

Wir sind der Auffassung, dass ggf. nur quantitative oder nur qualitative Leistungsziele sinnvoll/möglich sind. Folglich sollte „und“ durch „und/oder" ersetzt werden.

→ lit. f)

Auslagerungsverträge wesentlicher Auslagerungen sollen nach AT 9 Tz. 7 lit. f) MaRisk-E zukünftig (soweit zutreffend) Angaben, dass das Auslagerungsunternehmen für bestimmte Risiken eine Versicherung abzuschließen hat, enthalten.

Hier ist eine Klarstellung wünschenswert, dass ein Versicherungsabschluss nicht zwingend erforderlich ist und vertragliche Angaben bei Abstandnahme von einer Versicherung entbehrlich sind. Des Weiteren sollte klargestellt werden, dass bei gruppeninternen Auslagerungen eine Versicherung durch das Auslagerungsunternehmen stets entbehrlich ist.

→ lit. k)

Die bestehenden Vorgaben bezüglich der vertraglichen Vereinbarung datenschutzrechtlicher Bestimmungen und sonstiger Sicherheitsanforderungen werden über die Neufassung der Erläuterung zu AT 9 Tz. 7 MaRisk-E weiter spezifiziert. So wird klargestellt, dass zu den sonstigen Sicherheitsanforderungen vor allem Zugangsbestimmungen zu Räumen und Gebäuden (z. B. Rechenzentren) sowie Zugriffsberechtigungen auf Softwarelösungen zum Schutz wesentlicher Daten und Informationen zählen. Es wird ferner klargestellt, dass die Einhaltung dieser Anforderungen fortlaufend zu überwachen ist.

Die Anforderung der "fortlaufenden Überwachung" scheint über eine regelmäßige Beurteilung hinauszugehen. Dies ergibt sich aus dem Umkehrschluss aus AT 9 Tz. 9 MaRisk-E, wo die Formulierung "regelmäßige Beurteilung" durch "laufende Überwachung" ersetzt wurde. Die Erwartungshaltung der Aufsicht sollte an dieser Stelle weiter spezifiziert werden. Hier ist eine Klarstellung wünschenswert, welches Kontrollniveau gefordert wird.

Die Anforderungen an die vertraglich vereinbarten datenschutzrechtlichen Bestimmungen werden überdies dahingehend spezifiziert, dass Institute sicherstellen sollen, dass sie auf ihre Daten im Fall einer Insolvenz, Abwicklung oder der Einstellung der Geschäftstätigkeit des Auslagerungsunternehmens weiterhin zugreifen können.

Wir erachten vertragliche Vereinbarungen zur Sicherstellung der Daten als ausreichend um der Spezifizierung des AT 9 Tz. 7 lit. k) MaRisk-E zu entsprechen. Wir regen folglich an dies klarstellend ebenfalls in die Erläuterungen zu AT 9 Tz. 7 lit. k) MaRisk-E aufzunehmen.

→ lit. l)

Mit der Erweiterung der Erläuterungen zu AT 9 Tz. 7 MaRisk-E soll die Aufsichtspraxis entsprechend der bestehenden als auch erweiterten

Mindestinhalte weiter spezifiziert werden.

U.a. wird die bereits bestehenden Anforderungen an Kündigungsrechte (AT 9 Tz. 7 lit. l) MaRisk-E) durch eine neue Erläuterung dahingehend ergänzt, dass das Auslagerungsunternehmen im Falle einer Kündigung dazu verpflichtet ist, das Institut bei der Übertragung der ausgelagerten Aktivität bzw. des ausgelagerten Prozesses an ein anderes Auslagerungsunternehmen oder dessen Reintegration in das Institut zu unterstützen.

Wir erachten eine zusätzliche klarstellende Ergänzung der Erläuterung dahingehend für erforderlich, dass diese Unterstützungsleistungen nur zu vereinbaren sind, wenn dies für die Migration erforderlich oder zweckmäßig ist. So wäre beispielsweise die verpflichtende Vereinbarung zur Migrationsunterstützung im Falle eines bezogenen Rechenzentrums nicht zielführend, da der Rechenzentrumsbetreiber in der Regel keine sinnvolle Migrationsunterstützung erbringen kann.

→ lit. o)

AT 9 Tz. 7 lit. o) MaRisk-E verlangt, dass Regelungen, die sicherstellen, dass das Auslagerungsunternehmen in einer mit den Werten und dem Verhaltenskodex des auslagernden Instituts im Einklang stehenden Weise handelt, ebenfalls im Auslagerungsvertrag enthalten sind.

Obgleich wir ein verantwortungsvolles Verhalten von Unternehmen grundsätzlich befürworten und unterstützen, ist insbesondere für Mehrmandantendienstleister problematisch, sich zahlreichen unterschiedlichen Verhaltenskodizes zu unterwerfen. Des Weiteren erscheint uns der hier verwendete Begriff „sicherstellen“ als zu weitreichend. Etwas sicherzustellen beinhaltet die Verantwortung eine Garantiezusage einzufordern, die nach deutschem Recht mit unbegrenzter und verschuldensunabhängiger Haftung einhergeht.

Die Regelung sollte deswegen dahingehend geändert werden, dass sich das Institut vergewissern muss, dass das Auslagerungsunternehmen über verbindliche Richtlinien verfügt, die mit den Werten und dem Verhaltenskodex des Instituts oder aber international anerkannter Standards und Kodizes kompatibel sind.

AT 9 Tz. 9 – Steuerung und Überwachung von Auslagerungen

Im Rahmen der Neufassung der Vorgaben des AT 9 Tz. 9 MaRisk-E wurde die bisher geforderte „regelmäßige Beurteilung“ der Leistung des Auslagerungsunternehmens durch eine „laufende Überwachung“ ersetzt.

Aus dem geänderten Wortlaut der Anforderung geht unseres Erachtens nach nicht hervor, welche geänderten aufsichtlichen Erwartungen mit der Anpassung einhergehen. Zum Zwecke einer konsistenten als auch zielgerichteten Umsetzung der angepassten Vorgaben, würden wir eine Erläuterung dazu begrüßen. Insbesondere sollte (unter Berücksichtigung des Proportionalitätsprinzips)

spezifiziert werden wie groß die Zeitintervalle und wie hoch die Kontrolldichte der Überwachungshandlungen einer „laufenden“ Überwachung in Abgrenzung zu einer „regelmäßigen“ Beurteilung sind.

AT 9 Tz. 11 – Weiterverlagerung

Wie bisher auch, sind die Vorgaben zum Auslagerungsmanagement nach AT 9 Tz. 11 MaRisk auch bei der Weiterverlagerung von Auslagerungen zu beachten. Mit der nun neu hinzugefügten Erläuterung zu AT 9 Tz. 11 MaRisk-E, ergibt sich insbesondere bezüglich der Bestimmung der Wesentlichkeit von Weiterverlagerungen zusätzlicher Klärungsbedarf.

Während wir eine Bewertung der mit der Weiterverlagerung verbundenen Risiken im Rahmen der Risikoanalyse unterstützen, sprechen wir uns gegen eine dezidierte Bewertung der Wesentlichkeit von Weiterverlagerungen im Sinne einer Klassifizierung in wesentliche und nicht wesentliche Weiterverlagerungen aus. Ferner erachten wir einige der Aspekte, die im Rahmen der Risikoanalyse nach AT 9 Tz. 2 MaRisk-E zu berücksichtigen sind als nicht angemessen für die Bewertung einer Weiterverlagerung.

Auslagerungen werden bereits heute unter Berücksichtigung aller Weiterverlagerungsrisiken bewertet, jedoch erfolgt keine dezidierte Bewertung der Wesentlichkeit im Sinne einer Klassifizierung in wesentliche und nicht wesentliche Weiterverlagerungen. Mit der Bewertung der mit der Weiterverlagerung verbundenen Risiken im Rahmen der Risikoanalyse wird bereits eine angemessene Berücksichtigung dieser Risiken sichergestellt. Eine zusätzliche Bewertung der Wesentlichkeit im Sinne einer Klassifizierung in wesentliche und nicht wesentliche Weiterverlagerungen würde unseres Erachtens keinen zusätzlichen Nutzen stiften, jedoch den Arbeitsaufwand massiv erhöhen. Die Bewertung einer Weiterverlagerung sollte primär darauf abzielen mögliche Risiken bezüglich der Einhaltung regulatorischer Anforderungen durch das auslagernde Institut zu identifizieren. Die „Bewertung der Wesentlichkeit von Weiterverlagerungen“, wie im zweiten Satz der Erläuterung zu AT 9 Tz.11 MaRisk-E gefordert, sollte sich folglich nur auf die Bewertung der Weiterverlagerung als Auslagerung in Abgrenzung zu sonstigem Fremdbezug im Sinne von AT 9 Tz.1 beziehen.

Um etwaige Missverständnisse sowie Interpretationsspielräume zu vermeiden, möchten wir anregen den zweiten Satz der Erläuterung zu AT 9 Tz.11 MaRisk-E zu streichen. Alternativ schlagen wir vor, den Satz sinngemäß wie folgt anzupassen:

„*Hierzu zählt auch die Bewertung ~~der Wesentlichkeit~~ von Weiterverlagerungen gemäß AT 9 Tz 1*.“

In diesem Zusammenhang möchten wir darüber hinaus anregen, die Bewertung der Weiterverlagerung aus Sicht des Auslagerungsunternehmen durch das Institut klarstellend auszuschließen.

Die Erläuterung zu AT 9 Tz. 2 MaRisk-E wurde um weitere Aspekte, die bei der Risikoanalyse zu berücksichtigen sind, erweitert. Durch die Ergänzung der Erläuterung zu AT 9 Tz.11 MaRisk-E wären diese auch bei der Bewertung von Weiterverlagerungen anzuwenden. Einige der Aspekte erachten wir jedoch für die Bewertung der Risiken einer Weiterverlagerung als nicht angemessen. Insbesondere erscheint uns die Berücksichtigung des Schutzbedarfs der weiterverlagerten Daten als zu weitreichend und nicht zweckdienlich, da der Schutzbedarf der ausgelagerten Daten sich mit einer Weiterverlagerung nicht erhöhen kann. Wir bitten diesen Aspekt klarstellend von der Bewertung der Risiken weiterverlagerte Aktivitäten und Prozesse auszunehmen.

Darüber hinaus möchten wir anmerken, dass wir davon ausgehen, dass aufgrund der hohen Granularität der Arbeitsteilung bei Auslagerungsunternehmen (z.B. im Bereich Cloud Computing) die Umsetzung dieser Anforderung mit sehr hohen Aufwänden verbunden ist. Dies mag im Bereich wesentlicher Primärauslagerungen angemessen sein; im Bereich nicht wesentlicher Auslagerungen kann diese Regelung jedoch zu unangemessenen Aufwänden des auslagernden Instituts führen. Wir sprechen uns daher klar dafür aus, das Prinzip der Proportionalität auch auf diese Vorgabe anzuwenden. Im Falle nicht-wesentlicher Auslagerungen sollte es Instituten frei stehen auf eine Bewertung der Weiterverlagerung (im Sinne des AT 9 Tz 1) zu verzichten.

6. Inkrafttreten und Übergangsfristen

Mit der Veröffentlichung der Konsultation 14/2020 wurden keine Angaben hinsichtlich des Umsetzungszeitraums gemacht. Obgleich die EBA-Leitlinie zu Auslagerungen ab dem 30. September 2019 gilt, sprechen wir uns für einen angemessenen Umsetzungszeitraum aus. Die Neufassung der MaRisk stellt nicht nur eine Erläuterung der bestehenden Aufsichtspraxis dar, sondern erfordert eine dezidierte Implementierung zusätzlicher und geänderter Vorgaben. Insbesondere sollten angemessene Umsetzungs- und Übergangsfristen für die Umsetzung der zusätzlichen Mindestinhalte von Auslagerungsverträgen sowie der Sicherstellung etwaiger Kooperationsvereinbarungen oder Collage-Vereinbarungen im Falle von Auslagerungen zu Unternehmen in Drittstaaten, gesetzt werden. Auch vor dem Hintergrund der dezidierten Behandlung von Wertpapierfirmen unter der Verordnung (EU) 2019/2033 (IFR) ab dem 28. Juni 2021 sowie der Änderungen durch das anstehenden Wertpapierfirmengesetzes, sollten die Vorgaben der MaRisk-E zum Zwecke einer konsistenten Umsetzung nicht vor dem 28. Juni 2021 Anwendung finden.

Es ist notwendig, den Zeitpunkt des Inkrafttretens der MaRisk klar zu definieren und darüber hinaus festzulegen, welche Übergangsfristen den Instituten bis zur

vollständigen Einhaltung der neuen Vorgaben gewährt werden. Dabei könnte ein gestaffeltes Inkrafttreten abhängig vom erwarteten Umsetzungsaufwand ebenfalls in Betracht gezogen werden.

***

Wir würden uns über die Berücksichtigung unserer Anmerkungen im weiteren Verlauf der Ausgestaltung der MaRisk freuen. Für etwaige Rückfragen stehen wir Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen

Rainer Gallei
Regulatory Legal

Marija Kožica
MaRisk Compliance & Banking Regulation