Positionspapier

des Bankenverbandes zum Verständnis, der Interpretation und Chancen in der Umsetzung des RDARR Guides

Lobbyregister-No. R001458
EU-Transparenzregister-No. 0764199368-97

Berlin, 5. Mai 2026

bankenverband

Einleitung

Die Umsetzung der BCBS-239-Grundsätze im Rahmen des RDARR Guide der EZB ist in den letzten Jahren zu einem zentralen Thema der Aufsichtspraxis geworden. Insbesondere die weitere Konkretisierung der Anforderungen in Bezug auf den Anwendungsbereich, Data Lineage und den Umgang mit End-User Computing (EUC) hat die Institute dazu veranlasst, ihre bestehenden Datenmanagement- und Reporting-Strukturen zu überprüfen und, je nach Ausgangslage, weiterzuentwickeln. Jüngste Aufsichtsprüfungen sowie Rückmeldungen großer europäischer Institute deuten darauf hin, dass der RDARR Guide in Teilen einen sehr ambitionierten Zielzustand beschreibt, dessen praktische Umsetzung maßgeblich durch die Auslegung einzelner Begriffe, die Prüfungstiefe und die Erwartungen der Aufsichtsbehörden geprägt wird. Divergierende Interpretationen und operative Herangehensweisen sind daher wesentliche Treiber von Umsetzungsaufwand, Komplexität und Priorisierungskonflikten innerhalb der Institute.

Vor diesem Hintergrund halten die Privatbanken es für unerlässlich, dass die Umsetzung des RDARR Guide seine Kernziele – nämlich fundierte Managemententscheidungen auf Basis verlässlicher Datenqualität, transparente und nachvollziehbare Datenflüsse sowie eine robuste Governance – mit einem konsistenten, risikobasierten und wirtschaftlich tragfähigen Ansatz in Einklang bringt. Dieses Papier versteht sich als prinzipienbasierter Auslegungsleitfaden für RDARR, mit besonderem Fokus auf Proportionalität, Relevanz und operative Nachhaltigkeit als Kernelemente einer effektiven Umsetzung. In diesem Zusammenhang sind ein klar definierter und transparent hergeleiteter Anwendungsbereich, ein erkenntnisgeleiteter Ansatz für Data Lineage sowie ein proportionaler, risikoorientierter Umgang mit EUCs von entscheidender Bedeutung.

Für international tätige Bankengruppen, insbesondere solche mit Sitz außerhalb der EU, ergeben sich zusätzliche Herausforderungen. Dazu zählen Unterschiede in den regulatorischen Rahmenbedingungen der jeweiligen Jurisdiktionen, gruppenweite Governance-Modelle sowie die operative Zuweisung von Verantwortlichkeiten zwischen Gruppenebene und lokalen Einheiten. In solchen Umgebungen muss die RDARR-Umsetzung in bestehende Gruppenstrukturen eingebettet werden, sodass Konsistenz gewährleistet und die operative Machbarkeit erhalten bleibt.

Ziel dieses Papiers ist es, das Verständnis der Privatbanken zu wesentlichen Auslegungsfragen im Rahmen des RDARR Guide darzulegen, basierend auf praktischen Umsetzungserfahrungen, und aufsichtskonforme Ansätze zur Bewältigung identifizierter Herausforderungen aufzuzeigen. Wo illustrative Beispiele verwendet werden, dienen diese ausdrücklich der Veranschaulichung der zugrunde liegenden Prinzipien und sind nicht als verbindliche oder abschließende Anforderungen zu verstehen. Das Papier konzentriert sich auf die prinzipienbasierte Auslegung in Bezug auf den Anwendungsbereich, Data Lineage und EUC. In diesem Sinne zielt es darauf ab, den strukturierten Dialog mit den Aufsichtsbehörden zu unterstützen, den Erfahrungsaustausch zwischen den Instituten zu fördern und zu mehr Klarheit, Verhältnismäßigkeit und operativer Machbarkeit beizutragen.

Anwendungsbereich des RDARR

Grundprinzipien des RDARR-Scoping

Der RDARR Guide der EZB definiert den Anwendungsbereich von BCBS 239 bewusst über das traditionelle Risikoreporting hinaus und folgt dabei einem wirkungs- und nutzungsorientierten Ansatz. Maßgeblich ist nicht mehr allein die formale aufsichtsrechtliche Klassifizierung eines Berichts, Modells oder Datensatzes, sondern seine tatsächliche Relevanz für interne Steuerung, Entscheidungsfindung, aufsichtsrechtliche Beurteilung und externes Reporting. Der Anwendungsbereich sollte daher nicht als statische "Checkliste" verstanden werden, sondern als Ergebnis eines strukturierten Prozesses, der wesentliche Risikoauswirkungen und den praktischen Informationsnutzen in den Vordergrund stellt.Aus Sicht der Privatbanken erfordert dieser Ansatz eine strukturierte, transparente und verhältnismäßige Festlegung des Anwendungsbereichs, die aufsichtsrechtliche Ziele berücksichtigt und gleichzeitig einen undifferenzierten "alles-ist-im-Scope"-Ansatz vermeidet. Ein Einheitsansatz würde weder der wirkungsorientierten Logik des RDARR-Rahmens noch dem Verhältnismäßigkeitsprinzip gerecht werden. Er würde zudem riskieren, den Fokus von aussagekräftigen Erkenntnissen hin zu übermäßigem Umsetzungsaufwand mit begrenztem Aufsichts- oder Managementwert zu verschieben. Ein angemessenes Scoping-Konzept verfolgt daher einen doppelten Zweck: Erstens soll es den Anwendungsbereich von BCBS 239 bestimmen, indem die relevanten Berichte, Kennzahlen, Modelle und Gruppeneinheiten identifiziert werden, auf die die Grundsätze Anwendung finden. Zweitens soll es festlegen, wie dieser Anwendungsbereich im Zuge der Umsetzung entlang der Risikodatenaggregation gesteuert wird, insbesondere hinsichtlich der Tiefe und Granularität von Anforderungen wie Data Lineage.Der RDARR Guide lässt auf beiden Ebenen ausdrücklich Flexibilität zu, insbesondere hinsichtlich der Tiefe und Granularität von Anforderungen wie Data Lineage, und hält fest, dass 'Umsetzungsentscheidungen fit for purpose, gut dokumentiert sowie darauf ausgerichtet sein sollten, die notwendigen Informationen für die Steuerung des Instituts und das Management seiner Risiken bereitzustellen' (ECB RDARR Guide, 2024). Entscheidend ist eine konsistente und transparente Methodik, die institutsspezifisch angewendet, angemessen dokumentiert und gegenüber den Aufsichtsbehörden klar begründet werden kann.Proportionalität ist ein zentrales Element dieses Ansatzes. Nicht alle Datenelemente entlang der Datenaggregation erfordern das gleiche Maß an Data Lineage-Granularität, Automatisierung oder Kontrollumgebung. Stattdessen ist eine stufenweise und risikobasierte Umsetzung erforderlich, die der relativen Bedeutung der zugrunde liegenden Daten für Management- und Aufsichtszwecke Rechnung trägt.Bei der Festlegung des Ansatzes sind bestehende Governance-, Kontroll- und Prüfungsmechanismen angemessen zu berücksichtigen. Die RDARR-Umsetzung sollte auf bestehenden Strukturen aufbauen, anstatt parallele oder redundante Rahmenwerke zu etablieren. Dies gilt insbesondere für Jahresabschlüsse und das damit verbundene Finanzreporting: Aus Sicht der Privatbanken fallen solche Informationen angesichts ihrer zentralen Bedeutung für externe Stakeholder eindeutig in den RDARR-Anwendungsbereich. Gleichzeitig unterliegen Daten in Bereichen wie dem Finanzreporting bereits ausgereiften Governance- und

Sicherungsmechanismen, die durch andere regulatorische Anforderungen getrieben werden. Aus Sicht der Privatbanken sollte die RDARR-Umsetzung in diesen Bereichen daher verhältnismäßig und risiko-basiert sein, auf bestehenden Kontrollumgebungen aufbauen, soweit diese wirksam sind, anstatt parallele Dokumentationen oder Kontrollen zu verlangen, die die Datenqualität oder den aufsichtsrechtlichen Erkenntnisgewinn nicht wesentlich verbessern. Wo diese Mechanismen nachweislich wirksam und konsistent in das übergreifende Datenmanagement-Rahmenwerk integriert sind, ist die Einführung zusätzlicher RDARR-spezifischer Maßnahmen in der Regel nicht erforderlich.

Reports im Scope

Die Identifikation relevanter Berichte erfolgt anhand eines strukturierten, mehrstufigen Prozesses, der sowohl die interne Steuerungslogik des Instituts als auch die Erwartungen der Aufsichtsbehörden berücksichtigt. Ziel ist es, eine robuste und transparente Grundlage für die Definition des Anwendungsbereichs der BCBS-239-Grundsätze zu schaffen. Ausgangspunkt ist die Identifikation wesentlicher Risikoarten auf Basis des institutsinternen Risk Appetite Framework (RAF). Das RAF dient dabei als verbindender Referenzrahmen, der Geschäftsmodell, Risikoprofil und Steuerungslogik miteinander verbindet, und bildet die Grundlage für die weitere Analyse.

Die Entscheidung, ob ein Bericht in den Anwendungsbereich einbezogen oder bewusst ausgeschlossen wird, basiert auf klar definierten Kriterien, die aus drei analytischen Perspektiven beurteilt werden. Diese Perspektiven veranschaulichen, wie die zugrunde liegenden Scoping-Prinzipien in der Praxis angewendet werden können.

Die erste Perspektive betrifft die interne Steuerungsrelevanz. Berichte gelten als im Anwendungsbereich erfasst, wenn die darin enthaltenen Daten regelmäßig auf Vorstands- oder wesentlicher Managementgremienebene genutzt werden, zur Steuerung des Risikoappetits des Instituts beitragen oder Einschätzungen zu wesentlichen oder aufkommenden Risiken informieren. Entscheidend ist ihre effektive Nutzung für Entscheidungszwecke. Es ist daher unerheblich, ob ein Bericht eigenständig oder eingebettet in übergeordnetes Reporting verwendet wird, sofern er eigenständige Relevanz für Managemententscheidungen besitzt.

Die zweite Perspektive betrifft die aufsichtsrechtliche Relevanz. Berichte fallen in den Anwendungsbereich, wenn sie von Aufsichtsbehörden zur Beurteilung der finanziellen Solidität und Stabilität eines Instituts herangezogen werden, insbesondere aggregierte, nicht-statistische Aufsichtsberichte wie COREP und FINREP. Berichte oder Berichtskomponenten, die rein statistischen Zwecken dienen und hochgradig granularer oder technischer Natur sind, sollten hingegen nach Auffassung der Privatbanken vom RDARR-Anwendungsbereich ausgeschlossen werden.

Die dritte Perspektive betrifft das Finanzreporting sowie das externe Reporting. Finanzberichte, die risiko- oder leistungsrelevante Informationen enthalten und öffentlich zugänglich gemacht werden,

sollten in den Anwendungsbereich einbezogen werden, soweit sie aus Management- oder Risikosicht wesentlich sind und das Potenzial haben, Reputations- oder Kapitalmarktrisiken zu begründen. Ziel ist es sicherzustellen, dass extern veröffentlichte Informationen konsistent, vollständig und verlässlich sind.

Besonderes Gewicht sollte auf die konsistente Einbeziehung steuerungsrelevanter KRIs gelegt werden, die intern genutzt und/oder extern offengelegt werden. Diese Schnittmenge zwischen interner Steuerung und externem Reporting stellt eine Kernanwendung von RDARR dar und sollte im Anwendungsbereich klar zum Ausdruck kommen.

Modelle im Scope

Risikomodelle werden im Rahmen des Anwendungsbereichs nicht isoliert betrachtet, sondern konsistent entlang der Data Lineage beurteilt. Modelle, deren Ergebnisse in steuerungs-relevanten Berichten oder KRIs verwendet werden, sollten daher in den Anwendungsbereich einbezogen werden, wobei die Tiefe und Granularität der Anforderungen risiko-basiert und proportional anzuwenden ist. Aus Sicht der Kreditwirtschaft liefert eine separate, eigenständige Scoping-Beurteilung für Modelle keinen wesentlichen Mehrwert, da die Relevanz eines Modells bereits durch die Integration seiner Ergebnisse in wesentliche Steuerungs- und Reportingprozesse bestimmt wird.

Dementsprechend gelten aufsichtsrechtliche Modelle (z.B. IRB- oder FRTB-Modelle), wesentliche Säule-2-Modelle wie Stresstests, Modelle für ökonomisches Kapital oder Liquiditätsstress sowie zentrale Rechnungslegungs- und Risikomodelle, beispielsweise im Kontext von IFRS 9, als im Anwendungsbereich erfasst, soweit ihre Ergebnisse für Steuerungs- oder Aufsichtszwecke genutzt werden. Die Verantwortung für die Identifikation der relevanten Modellergebnisse liegt bei den jeweiligen Modellverantwortlichen, während die technische Integration in Übereinstimmung mit bestehenden Governance-Strukturen erfolgt.

Data Governance/Data Ownership

Institute sollten im Rahmen ihres Data-Governance-Rahmens Verantwortlichkeiten für Rollen wie Data Owner oder gleichwertige Positionen identifizieren und zuweisen. Ein Data Owner ist eine benannte Einzelperson oder Einheit, die für die Definition, Integrität und Governance eines definierten Datenbereichs verantwortlich ist und sicherstellt, dass angemessene Standards für Richtigkeit, Vollständigkeit und Konsistenz gemäß regulatorischen Anforderungen und internen Richtlinien etabliert und eingehalten werden. Data Owner sind für die Integrität der Daten in ihrem Verantwortungsbereich verantwortlich. Dies erfolgt in Zusammenarbeit und der Unterstützung der klar zugewiesenen Verantwortlichen für das Datenqualitätsmanagement, Kontrollen und Data Stewardship.

In global tätigen Banken ist es nicht erforderlich, dass alle Data Owner innerhalb der lokalen Einheit angesiedelt sind. Sie können strategisch in anderen Teilen der globalen Organisation positioniert werden und so unter geeigneten Governance-Strukturen ihre Verantwortlichkeiten effektiv wahrnehmen. Um eine angemessene lokale Aufsicht sicherzustellen, ist es entscheidend, geeignete Mechanismen – wie Berichtslinien oder Auslagerungsvereinbarungen – zu etablieren, um die Aufgaben der Data Owner zu überwachen.

Data Lineage

Data Lineage ist ein zentrales Element der Aufsichtserwartungen im Rahmen der BCBS 239 Grundsätze und des RDARR-Rahmens. Ihr Ziel ist es sicherzustellen, dass der Datenfluss von der Quelle über die Verarbeitung bis zum abschließenden Reporting transparent ist. Die Aufsichtsbehörden erwarten von den Instituten, dass sie den Ursprung, den Verarbeitungsweg und die Verwendung von Risikodaten nachweisen können. Ziel ist es, eine hohe Datenqualität, Konsistenz und Nachvollziehbarkeit zu erreichen, um fundierte Entscheidungen auf allen Ebenen zu ermöglichen. Die Privatbanken unterstützen dieses Ziel vollumfänglich. Gleichzeitig zeigt die Praxis, dass Data Lineage an sich kein Risiko mindert; vielmehr ist es der effektive Einsatz von Data Lineage – der zu kontrollierten Daten und einer kontrollierten Datennutzung führt – und damit den relevanten risikomindernden Faktor darstellt. Dementsprechend müssen Umfang und Tiefe der Data-Lineage-Umsetzung proportional zur Größe, Komplexität und zum Risikoprofil des Instituts sein, und die Data Lineage muss im Tagesgeschäft nutzbar und wartbar bleiben.

Ein wesentlicher Auslegungsaspekt betrifft den Ausgangspunkt für die Dokumentation der Data Lineage. Aus Sicht der Privatbanken sollte die Data Lineage an dem Punkt beginnen, an dem Daten in ein kontrolliertes, persistentes System eintreten, das Teil des reportingrelevanten Datenflusses ist. Bei global tätigen Banken ist anzuerkennen, dass die Data Lineage Systeme umfassen kann, die weltweit verteilt und nicht notwendigerweise spezifisch für die betreffende Einheit sind. Eine Ausweitung der Lineage-Dokumentation auf frühere vorbereitende oder transiente Schritte sollte durch Wesentlichkeits- und Risikoerwägungen geleitet werden, wo dies einen nachweisbaren Aufsichts- oder Managementwert bietet. Eine Ausweitung auf vorgelagerte Workflow-, Pre-Trade- oder vorbereitende Prozessschritte würde den erforderlichen Aufwand erheblich erhöhen, ohne regelmäßig verhältnismäßige zusätzliche Erkenntnisse zu liefern. Dies liegt daran, dass Risikoprofile, Managementinformationen und regulatorisches Reporting typischerweise abgeschlossene Transaktionen betreffen, die die Bilanz oder die Risikoposition des Instituts beeinflussen.

In komplexen Datenlandschaften ist eine vollständig attributbasierte, einheitsspezifische und umfassend toolgestützte Umsetzung mit erheblichen Kosten-, Wartungs- und Komplexitätsrisiken verbunden. Sie birgt zudem das Risiko, dass die durch die Data-Lineage-Dokumentation angestrebten zusätzlichen Erkenntnisse aufgrund der schieren Informationsmenge und technischen Heterogenität

ausbleiben. In der Praxis wurden die Erwartungen an vollständig automatisierte End-to-End-Tooling-Lösungen mitunter zu hoch angesetzt und können noch nicht als marktweiter Standard gelten.

Vor diesem Hintergrund erachten die Privatbanken das fit-for-purpose-Prinzip als wesentlich. Fit for purpose bedeutet, dass Datenarchitektur, Taxonomien und Data Lineage so konzipiert und dokumentiert sein müssen, dass sie die für die Steuerung des Instituts und das Management seiner Risiken innerhalb des definierten Anwendungsbereichs notwendigen Informationen bereitstellen. Die Dokumentation sollte daher zweckgerichtet und verhältnismäßig sein: Data Lineage sollte nur dort erfasst werden, wo sie einem klar identifizierbaren Aufsichts- oder Risikomanagementziel dient. Lineage, die nicht zur Steuerung, Risikoüberwachung oder zum Reporting im Anwendungsbereich beiträgt, muss nicht dokumentiert werden.

Data Lineage sollte für im Anwendungsbereich erfasste Berichte dokumentiert werden in dem Maße, das erforderlich ist, um Dateursprung, Verarbeitungsweg und Verantwortlichkeiten klar nachzuweisen, jedoch nicht notwendigerweise auf Attributebene – da dies keine zusätzlichen Erkenntnisse liefert oder die Transparenz durch Informationsüberflutung sogar verringern kann. Entscheidungen über das angemessene Granularitätsniveau sollten auf klar definierten, risiko-basierten Kriterien basieren. Institute können unterschiedliche Methoden anwenden, um zu bestimmen, wo eine erweiterte Dokumentation, Qualitätssicherung oder Governance je nach Wesentlichkeit und Nutzung gerechtfertigt ist. Mögliche Umsetzungsoptionen können beispielsweise die Identifikation von Critical Data Elements (CDEs) oder relevanter Datensätze umfassen, um die Aufmerksamkeit auf entscheidungs-relevante Datenflüsse zu lenken. Dieser Ansatz sollte als veranschaulichend und nicht als verbindliche oder präskriptive Mechanismen verstanden werden. Ebenso wichtig ist die Beurteilung, ob relevante Datenflüsse bereits durch etablierte geschäftliche oder technische Dokumentation hinreichend belegt sind und wie zusätzliche Lineage-Dokumentation in ein nachhaltiges Betriebsmodell eingebettet werden kann. Zudem sollten Wesentlichkeitserwägungen konsistent entlang des gesamten Datenflusses angewendet werden, beispielsweise indem eine weniger granulare oder vereinfachte Dokumentation von Dateneingaben zu nicht wesentlichen Portfolios oder Engagements zugelassen wird. Je nach Risikostrategie des Instituts können alternative Ansätze die Anwendung von Kontrollen auf Datensatzebene, Datenflussebene oder die Fokussierung erweiterter Governance auf ausgewählte, entscheidungsrelevante Informationen umfassen. Die Wahl des Ansatzes sollte instituts-spezifisch bleiben und Faktoren wie die Datenlandschaft, das Kontrollrahmenwerk und das Risikoprofil berücksichtigen. Um die aufsichtsrechtliche Akzeptanz eines fit-for-purpose-Ansatzes sicherzustellen, ist eine transparente Dokumentation der zugrunde liegenden Kriterien unerlässlich. Institute müssen nachweisen können, nach welchen Kriterien sie den Detailgrad festgelegt haben und wie die Lineage in Datenqualitätsprozesse, Kontrollen und Verantwortlichkeiten integriert ist. Eine Data Lineage, die lediglich formale Dokumentationsanforderungen erfüllt, aber weder in Datenqualitätsprozessen eingesetzt wird noch echte Erkenntnisse für Fachexperten liefert, erfüllt dieses Prinzip nicht. Data Lineage muss lesbar, operativ kompatibel sein und einen echten Nutzwert aufweisen.

Aus Branchenperspektive sollten bestehende Dokumentationen und etablierte Prozesse aktiv genutzt werden, um Doppelarbeit zu vermeiden und eine fortlaufend genauer Data Lineage sicherzustellen. Fachliche und methodische Konzepte, technische Spezifikationen wie Datenmodelle und Schnittstellenbeschreibungen sowie vorhandene ETL-Dokumentation können als unterstützende Belege herangezogen werden, sofern der Zusammenhang zwischen fachlichen Konzepten und technischer Umsetzung transparent und nachvollziehbar bleibt. Dieser Ansatz ermöglicht eine konsolidierte Sicht auf Datenflüsse, die Prüfungsanforderungen erfüllt und gleichzeitig die operative Belastung begrenzt, da er auf der im Tagesgeschäft bereits gepflegten Dokumentation aufbaut. Detaillierte Dokumentationen aus operativen Prozessen können ergänzend herangezogen werden, ohne dass dies automatisch zu einer formalen Anforderung führt, alle Datenpfade auf dem höchsten Granularitätsniveau nachzuweisen.

Die Privatbanken bekennen sich zu hohen Standards bei Datenqualität, Nachvollziehbarkeit und klarer Verantwortlichkeit. Gleichzeitig müssen Machbarkeit und wirtschaftliche Nachhaltigkeit angemessen gegen den Nutzen abgewogen werden. Der fit-for-purpose-Ansatz stellt sicher, dass Transparenz, Governance und Effizienz aufeinander abgestimmt sind, sodass die Umsetzung dauerhaft robust bleibt.

Umgang mit End-User-Computing-Anwendungen

End-User-Computing-Tools (EUC) sind ein integraler Bestandteil der operativen Realität vieler Institute. Sie ermöglichen es Geschäftsbereichen, Anforderungen effizient und flexibel, nah an Geschäftsprozessen umzusetzen und fördern damit Anpassungsfähigkeit und Innovation. Insbesondere im Kontext sich weiterentwickelnder regulatorischer Anforderungen, spezialisierter Analysen oder geringvolumiger Prozesse stellen EUCs häufig eine angemessene und kosteneffiziente Ergänzung zu zentralen IT-Systemen dar. Wo EUCs in steuerungsrelevanten Prozessen oder im Reporting eingesetzt werden, müssen sie angemessen dokumentiert und entlang der Data Lineage integriert werden, um Transparenz über Datenflüsse und Verarbeitungswege sicherzustellen.

Aus Sicht der Privatbanken stellt der Einsatz von EUCs keine Ausnahme von Standardprozessen dar, sondern ist Ausdruck einer effektiven Zusammenarbeit zwischen Geschäftsbereichen und IT-Funktionen. Gleichzeitig wird anerkannt, dass EUCs – wie andere Verarbeitungslösungen auch – in ein klar definiertes Governance- und Kontrollrahmenwerk eingebettet werden müssen. Ziel ist nicht die Abschaffung oder pauschale Ablösung von EUCs, sondern die Sicherstellung ihres transparenten, kontrollierten und risikoangemessenen Einsatzes im Einklang mit den Aufsichtserwartungen an Nachvollziehbarkeit, Datenqualität und Governance.

Dementsprechend sollten EUCs nicht pauschal verboten, sondern differenziert und risikobasiert gesteuert werden. Ein generelles Verbot würde weder den operativen Gegebenheiten noch dem Verhältnismäßigkeitsprinzip gerecht werden und könnte zu erheblichen Effizienzverlusten sowie einer

verminderten Anpassungsfähigkeit der Institute führen, insbesondere in Bereichen, die Flexibilität, Fachexpertise oder eine schnelle Umsetzung erfordern. Stattdessen sollten EUCs bewusst als integraler Bestandteil der Prozess- und Datenlandschaft behandelt werden, wobei Kontrollen und Automatisierung dort gestärkt werden, wo dies durch Risikoerwägungen gerechtfertigt und wirtschaftlich sinnvoll ist.

Kern einer solchen EUC-Strategie ist ein Governance-Rahmenwerk, das Transparenz über die Verfügbarkeit, den Einsatz und die Bedeutung von EUCs schafft. Dies umfasst eine zentrale Erfassung relevanter EUC-Tools, klare Rollen und Verantwortlichkeiten für deren Entwicklung, Einsatz und Pflege sowie verhältnismäßige Dokumentationsanforderungen. Ziel ist die Etablierung eines risikoorientierten Überblicks, der EUCs systematisch in Steuerungs-, Kontroll- und Prüfungsprozesse integriert. Dabei ist ein kritikalitätsbasierter Ansatz entscheidend, der auf End-to-End-Prozesse und nicht auf einzelne Tools in Isolation ausgerichtet ist. Relevante Kriterien umfassen finanzielle Auswirkungen, regulatorische Relevanz, Bedeutung für interne Steuerung und externes Reporting, Datenkritikalität und funktionale Komplexität.

Auf Basis dieser Beurteilung kann die angemessene Kontrollumgebung und der Automatisierungsgrad bestimmt werden. Eine starre Kategorisierung ist nicht zwingend erforderlich; entscheidend ist, dass das Kontrollniveau risikobasiert angehoben werden kann, wo dies notwendig ist, während alternative oder kompensierende Kontrollen dort möglich bleiben, wo eine vollständige Migration zu zentralen IT-Systemen nicht sachgerecht ist.

Manuelle oder halbmanuelle EUCs sind daher nicht nur akzeptabel, sondern in bestimmten Fällen angemessen und notwendig. Dies gilt insbesondere für EUCs mit niedrigem Risikoprofil, seltener Nutzung oder einem hohen Maß an Fachexpertise, bei denen eine vollständige Automatisierung wirtschaftlich oder funktional nicht gerechtfertigt wäre. In solchen Fällen ermöglicht ein manueller Ansatz den gezielten Einsatz von Fachexpertise und erhält die notwendige Flexibilität in den Geschäftsbereichen.

Letztlich ist nicht der Automatisierungsgrad entscheidend, sondern die Nachvollziehbarkeit, Kontrollierbarkeit und Robustheit des Prozesses. Manuelle EUCs können durch geeignete Dokumentation, definierte Arbeitsanweisungen, das Vier-Augen-Prinzip und bestehende interne Kontrollen revisionssicher gestaltet werden. Gleichzeitig ermöglicht dieser Ansatz die gezielte Allokation begrenzter IT- und Fachressourcen auf jene EUCs und Prozesse, bei denen Automatisierung tatsächlich eine signifikante Risikoreduktion und Effizienzgewinne erzielen kann.

Insgesamt folgt der Umgang mit EUCs denselben Grundprinzipien wie andere Elemente des Risikodatenmanagements: Verhältnismäßigkeit, Angemessenheit und Nachhaltigkeit. Eine differenzierte EUC-Strategie stärkt die Steuerungsfähigkeiten der Institute, erhält die notwendige Agilität in den Geschäftsbereichen und unterstützt gleichzeitig die Aufsichtserwartungen hinsichtlich Transparenz, Nachvollziehbarkeit und Datenqualität. Nach Auffassung der Privatbanken stellt ein

differenzierter und risikobasierter EUC-Ansatz eine etablierte und zukunftsweisende Praxis dar, die Aufsichtsziele unterstützt und dabei operativ machbar bleibt.

Fazit

Aus Sicht der Privatbanken ist ein klar definierter und wirkungsorientierter Anwendungsbereich zentral für die effektive und nachhaltige Umsetzung der RDARR-Anforderungen. RDARR-Ziele lassen sich nur dann erreichen, wenn Anwendungsbereich, Umsetzungstiefe und Kontrollintensität konsistent auf die tatsächliche Nutzung und Risikowirkung von Daten, Kennzahlen und Berichten ausgerichtet sind. Ein prinzipienbasierter Ansatz, der Verhältnismäßigkeit, Relevanz und operative Nachhaltigkeit priorisiert, ist daher unerlässlich, um ein undifferenziertes "alles-ist-im-Scope"-Ergebnis zu vermeiden.

In diesem Zusammenhang bieten eine strukturierte Scoping-Methodik, transparente Abgrenzung, die konsistente Integration relevanter Modelle entlang der Data Lineage und ein proportionaler, risikobasierter Ansatz für Lineage-Anforderungen eine solide Grundlage, um Aufsichtserwartungen auf eine Weise zu erfüllen, die sowohl regelkonform als auch wirtschaftlich nachhaltig ist. Die in diesem Papier beschriebenen Ansätze veranschaulichen, wie diese Prinzipien in der Praxis angewendet werden können, und sollten nicht als verbindliche oder abschließende Umsetzungsanforderungen verstanden werden. Entscheidend ist, dass Institute transparente, risikobasierte Kriterien für die Festlegung von Granularität, Automatisierungsgraden und Kontrollintensität dokumentieren und dabei bestehende, im Tagesgeschäft verankerte Dokumentations- und Kontrollmechanismen nutzen.

Für international tätige Bankengruppen sind diese Überlegungen noch ausgeprägter. Komplexe Gruppenstrukturen, heterogene IT- und Datenlandschaften sowie verteilte Governance-Modelle zwischen Headquarter und lokalen Einheiten erfordern, dass Anwendungsbereichsdefinition, Datenfluss-Nachvollziehbarkeit und Kontrollkonzepte konsistent über Jurisdiktionen hinweg konzipiert und betrieben werden. Darüber hinaus erfordern Übergabepunkte innerhalb von End-to-End-Prozessen – wie die Interaktion zwischen gruppenweiten Datenstandards und lokal gemanagter Datenbereitstellung – klare Prinzipien hinsichtlich Verantwortlichkeiten, Mindesterwartungen und Nachweisführung statt einheitlicher technischer Lösungen.

Aus Umsetzungsperspektive ist festzuhalten, dass die europäischen Aufsichtsbehörden derzeit der RDARR-Compliance eine sehr hohe Priorität einräumen, insbesondere hinsichtlich des Nachweises von Data Lineage und Governance-Arrangements. Die von vielen Instituten in diesem Bereich beobachteten Erwartungen und Prüfungsschwerpunkte gehen über jene in vergleichbaren internationalen Aufsichtsumfeldern hinaus. Für global tätige Bankengruppen, insbesondere solche mit Sitz außerhalb der EU, kann dies zu erheblichen zusätzlichen Koordinations-, Anpassungs- und Nachweisanforderungen führen, mit spürbaren Auswirkungen auf Investitionsentscheidungen und Ressourcenallokation. In einem globalen Umfeld mit weitgehend vergleichbaren Risikoprofilen können dauerhaft höhere Umsetzungsbelastungen in Europa Wettbewerbsnachteile begründen, sofern diese

nicht durch einen verhältnismäßigen, wertorientierten und konsistenten Umsetzungsansatz abgemildert werden.

Vor diesem Hintergrund tragen die in diesem Papier dargelegten prinzipienbasierten Ansätze nicht nur zur operativen Machbarkeit und aufsichtsrechtlichen Compliance bei, sondern auch zur Wettbewerbsfähigkeit des europäischen Finanzmarktes. Ein wirkungsorientierter Anwendungsbereich, ein proportionaler, risikobasierter Ansatz für Data Lineage, die gezielte Nutzung bestehender Kontrollen und ein risikobasiertes Management von EUCs ermöglichen es den Instituten, regulatorische Ziele – darunter Datenqualität, Nachvollziehbarkeit und robuste Governance – effektiv zu erfüllen, ohne unverhältnismäßige Komplexität oder Kosten zu erzeugen. Diese Ansätze tragen dazu bei, einen Rahmen zu stärken, der finanzielle Stabilität und Resilienz unterstützt und gleichzeitig die Voraussetzungen für einen leistungsstarken, innovativen und international wettbewerbsfähigen europäischen Bankensektor fördert.

Herausgeber:
Bundesverband deutscher Banken e. V.

Burgstraße 28
10178 Berlin
Deutschland

Lobbyregister-Nr. R001458
EU-Transparenzregister-Nr. 0764199368-97
USt-IdNr.: DE201591882

Kontakt:
bankenverband@bdb.de
bankenverband.de

Inhaltlich verantwortlich:
Themengruppe [Themengruppe]
[Vorname Nachname], [Position]
[Vorname Nachname], [Position]

bankenverband