Kunze | Schimm

Drittparteienmanagement nach DORA und MaRisk

Fassung: Mai 2025

1. Auflage 2025

Redaktionsstand: Mai 2025

Herausgeber: Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V. · BVR,
Berlin

Autoren: Dr. Christoph Kunze und Berit Schimm

Satz und Gestaltung: DG Nexolution eG, Wiesbaden

Herstellung: WirmachenDruck.de, Backnang

Titelbild: © AdobeStock, ThamDesign

Bestell-Nr. 963 600 **DG nexolution**

ISBN 978-3-87151-343-5

© DG Nexolution eG, Leipziger Straße 35, 65191 Wiesbaden (2025),
fachinformationen@dg-nexolution.de

Urheberrechts-Bestimmungen

Dieses Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Nutzung der Inhalte dieses Werkes für Text- und Data-Mining im Sinne des § 44b UrhG ist ausdrücklich vorbehalten (§ 44b Abs. 3 UrhG) und daher verboten. Die Inhalte dieses Werkes dürfen auch nicht zur Entwicklung, zum Training und/oder zur Anreicherung von KI-Systemen, insbesondere von generativen KI-Systemen, verwendet werden.

Haftungsausschluss

Der Text gibt die Rechtsauffassung der Autoren wieder. Weder sie noch der Verlag oder der Herausgeber des Werks haften für die Richtigkeit der Interpretation.

Die Hinweise, Ratschläge und Wertungen sind von den Autoren, dem Herausgeber und dem Verlag sorgfältig erwogen und geprüft, dennoch kann eine Garantie nicht übernommen werden. Eine Haftung der Autoren, des Herausgebers oder des Verlages und seiner Beauftragten für Personen-, Sach- und Vermögensschäden ist ausgeschlossen.

Wertfreie Ansprache

Hinweis: Aus Gründen der besseren Lesbarkeit verwenden wir die männliche Form (generisches Maskulinum). Wir meinen immer alle Geschlechter im Sinne der Gleichbehandlung. Die verkürzte Sprachform hat redaktionelle Gründe und ist wertfrei.

Inhaltsverzeichnis

Vorwort	7
Abkürzungsverzeichnis	9
1 Auslagerungen, IKT-Dienstleistungen und Abgrenzung der Einordnung	13
1.1 Begriff der „Auslagerung“	14
1.2 Definition der „IKT-Dienstleistungen“	17
1.2.1 Kriterien zur Einordnung als IKT-Dienstleistung	18
1.2.2 IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen	22
2 Auslagerungs- und Dienstleisterstrategie	27
2.1 Auslagerungsstrategie	27
2.2 Strategie zum IKT-Drittparteienrisiko und Leitlinie zum IKT-Drittparteienrisikomanagement	29
2.2.1 Strategie zum IKT-Drittparteienrisiko	30
2.2.2 Leitlinie für die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen	32
3 Beauftragtenwesen	35
3.1 Zentraler Auslagerungsbeauftragter / zentrales Auslagerungsmanagement	35
3.2 Funktion zur Überwachung der IKT-Dienstleistungen	37
4 Risikoanalyse	39
4.1 Auslagerungsrisikoanalyse (MaRisk)	39
4.2 Risikoanalyse unter DORA	42

5	Auslagerungs-/IKT-Dienstleistersteuerung	45
5.1	Steuerung und Überwachung von Auslagerungen	45
5.2	Überwachung des IKT-Dienstleisters unter DORA	46
6	Exit-Strategien und Ausstiegspläne	51
6.1	Ausstiegsprozesse und Handlungsoptionen bei Auslagerung	51
6.2	Ausstiegsstrategie zu IKT-Dienstleistungen	52
7	Vertragsgestaltung	55
7.1	Anforderungen an Verträge gemäß KWG und MaRisk	55
7.2	Anforderungen an Verträge gemäß DORA	61
7.2.1	Zusammenspiel von DORA- mit den MaRisk-Klauseln	63
7.2.2	Gegenüberstellung der inhaltlichen Ausgestaltung der Verträge im Zusammenspiel von MaRisk und DORA	64
7.2.3	Zu den vertraglichen Regelungen im Einzelnen	71
7.2.3.1	Klare und vollständige Beschreibung und Leistungsniveau .	71
7.2.3.2	Bedingungen für die Weiterverlagerung bzw. die Unterauftragsvergabe	71
7.2.3.3	Standort	73
7.2.3.4	Informationssicherheit	73
7.2.3.5	Geschäftsfortführungsmanagement	74
7.2.3.6	Berichtspflichten	76
7.2.3.7	Überwachung	77
7.2.3.8	Prüfrechte und Zusammenarbeit mit der Bankaufsicht	78
7.2.3.9	Kündigung	80
7.2.3.10	Beendigung – Zugang zu Daten und Unterstützung	81
8	Meldewesen	83
8.1	Anzeigeverordnung und Auslagerungsregister	83
8.2	Informationsregister	88
8.2.1	Angaben zum Informationsregister	88
8.2.2	Hinweise zur Erstellung des Informationsregisters	90
8.2.3	Übersicht der zu befüllenden Templates mit Erläuterungen	93
8.2.4	Einreichung des Informationsregisters über das Meldeportal der BaFin	96
8.2.5	Klassifizierung und Meldung schwerwiegender IKT- bezogener Vorfälle	98

Anhang	101
Anhang 1 Arbeitshilfen und Musterdokumente	101
1.1 Mustervertragsklauseln	101
1.2 Beispiel für Klauseln bei IKT-Dienstleistungen, die keine kritischen oder wichtigen Funktionen unterstützen	144
1.3 Musteranschreiben	148
1.4 Auszüge aus der Musterrisikoanalyse	150
Anhang 2 Auszüge aus rechtlichen Regelungen	237
2.1 VERORDNUNG (EU) 2022/2554 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor (DORA) .	237
2.2 DELEGIERTE VERORDNUNG (EU) 2024/1773 DER KOMMISSION vom 13. März 2024 zur Ergänzung der Verordnung (EU) 2022/2554: Technische Regulierungsstandards zur Spezifizierung des detaillierten Inhalts der Leitlinie für vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden	248
2.3 DELEGIERTE VERORDNUNG (EU) 2025/532 DER KOMMISSION vom 24. März 2025 zur Ergänzung der Verordnung (EU) 2022/2554: Technische Regulierungsstandards zur Präzisierung der Aspekte, die ein Finanzunternehmen bei der Untervergabe von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen bestimmen und bewerten muss	258
2.4 DURCHFÜHRUNGSVERORDNUNG (EU) 2024/2956 DER KOMMISSION vom 29. November 2024 zur Ergänzung der Verordnung (EU) 2022/2554: Festlegung technischer Durchführungsstandards im Hinblick auf Standardvorlagen für das Informationsregister	266

Vorwort

Das Management der Informations- und Kommunikationstechnologie (IKT) und der damit verbundenen Risiken durch Finanzunternehmen unterliegt mit der Verordnung zur „Digitalen operationalen Resilienz im Finanzsektor“ (DORA) seit dem 17. Januar 2025 einheitlichen gesetzlichen Anforderungen in der EU.

Finanzunternehmen sollen über einen soliden, umfassenden und gut dokumentierten IKT-Risikomanagementrahmen als Teil ihres Gesamtrisikomanagementsystems verfügen, um ein hohes Niveau digitaler operationaler Resilienz zu gewährleisten. DORA umfasst ausgehend von den IKT-Risiken detaillierte Anforderungen an die Informationssicherheit, einschließlich des Managements IKT-bezogener Vorfälle und einschlägiger Tests. Im Einklang mit den Anforderungen an die Geschäftsfortführung von Funktionen der Bank sind Pläne zur Reaktion auf Störungen und Ausfälle der IKT zu erstellen, die diese Funktionen unterstützt.

Da Finanzunternehmen Teile ihrer IKT-Leistungen durch Drittdienstleister erbringen lassen, resultieren IKT-Risiken häufig aus den damit verbundenen IKT-Dienstleistungen. Diese Risiken sind im IKT-Risikomanagementrahmen zu berücksichtigen und unterliegen unter DORA einer Vielzahl von Anforderungen. Dies trifft insbesondere auf deutsche Genossenschaftsbanken zu, die große Teile ihrer IKT an den zentralen Dienstleister Atruvia ausgelagert haben, daneben IKT-Dienstleistungen weiterer Dienstleister aus der GFG und darüber hinaus beziehen und IKT nur zu einem marginalen Teil selbst entwickeln.

Die Ausführungen in dieser Broschüre konzentrieren sich auf das IKT-Drittparteienerisikomanagement nach DORA im Vergleich und in Abgrenzung zum Auslagerungsmanagement. Derzeit sind die Auslagerungsanforderungen zusätzlich zu beachten, sofern es sich bei der IKT-Dienstleistung zugleich um eine Ausla-

gerung gemäß KWG/MaRisk handelt. Die gesetzlichen Anforderungen nach DORA und die Vorgaben aus den MaRisk bestehen parallel und komplementär. Perspektivisch ist mit einer Harmonisierung der Regelungen zu rechnen.

Berlin im Mai 2025

Dr. Christoph Kunze

Berit Schimm