
Anlage 7: DORA-Addendum

DORA-Addendum

zu den Nutzungsbedingungen OeKB Fondsdaten Portal in der Version 6.0 / Jänner 2025

Präambel

Am 14.12.2022 wurde die EU-Verordnung 2022/2554 über die digitale operationale Resilienz im Finanzsektor (in der Folge „**DORA VO**“) erlassen. Diese muss ab dem 17.1.2025 von den betroffenen Unternehmen angewandt werden.

Bei gegenständlicher Dienstleistung handelt es sich um eine dauerhaft bereitgestellte IKT-Dienstleistung, die von Oesterreichische Kontrollbank Aktiengesellschaft als IKT-Drittdienstleister gemäß Definition der DORA VO (kurz „**OeKB**“ oder „**IKT-Drittdienstleister**“) erbracht wird.

Ergänzend zu den Nutzungsbedingungen OeKB Fondsdaten Portal in der Version 6.0 / Dezember 2024 (kurz „**Nutzungsbedingungen**“), gelten die vorliegenden Bestimmungen zum Management des IKT-Drittparteienrisikos gemäß der DORA VO (in der Folge „**Addendum**“) im Verhältnis zu Datenmeldern und Datenbeziehern, die als Finanzunternehmen vom Geltungsbereich des Art 2 Abs 2 der DORA VO erfasst sind. Das Addendum geht bei allfälligen inhaltlichen Widersprüchen von einzelnen Klauseln zwischen den Nutzungsbedingungen diesen vor.

I.

Begriffsbestimmungen

- (1) „**IKT-Drittdienstleister**“ ist gem. Art 3 Z 19 DORA VO ein Unternehmen, das IKT-Dienstleistungen bereitstellt.
- (2) „**Sub-Dienstleister**“ sind jene Dienstleister, an die der IKT-Drittdienstleister Unteraufträge für IKT-Dienstleistungen vergibt.
- (3) „**IKT-Dienstleistungen**“ sind gem. Art 3 Z 21 DORA VO digitale Dienste und Datendienste, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern dauerhaft bereitgestellt werden, einschließlich Hardware als Dienstleistung und Hardwaredienstleistungen, wozu auch technische Unterstützung durch den Hardwareanbieter mittels Software- oder Firmware- Aktualisierungen gehört, mit Ausnahme herkömmlicher analoger Telefondienste.
- (4) „**IKT-bezogener Vorfall**“ ist gem. Art 3 Z 8 DORA VO ein vom Auftraggeber 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 Auftraggeber erbrachten Dienstleistungen hat.
- (5) „**Finanzunternehmen**“ ist ein Unternehmen gem. Art 2 Abs. 1 Buchstabe a bis t DORA VO, für das die DORA VO zur Anwendung kommt.

II.

Vertragsbestimmungen

- (6) **Vertragsinhalt:** Die OeKB verweist auf die zum Zwecke des Austauschs und Abrufs von Fondsdaten im FundsXML Schnittstellenformat gemäß den Nutzungsbedingungen erfolgende Bereitstellung des OeKB Fondsdaten Portals (IKT-Dienstleistung). Die IKT-Dienstleistung wird unter Berücksichtigung des Schnittstellenformats, wie es von der Arbeitsgruppe FundsXML und der Vereinigung Österreichischer Investmentgesellschaften spezifiziert und von der OeKB technisch umgesetzt wurde, erbracht. Die technische Umsetzung wird von den Vertragsparteien auf Anpassungserfordernisse, insbesondere im Hinblick auf aktualisierte Spezifikationen des Schnittstellenformates tourlich geprüft und bei Bedarf einvernehmlich angepasst. Entsprechende Anpassungen und Ergänzungen der Service Levels kann das

Finanzunternehmen jedenfalls dann verlangen, wenn die vereinbarte Dienstleistungsgüte nicht erreicht wird.

- (7) **Eignung:** OeKB bestätigt hiermit, dass sie über die Eignung, Kapazität, sowie alle gesetzlich vorgeschriebenen Zulassungen verfügt, um die vereinbarte IKT-Dienstleistung in Übereinstimmung mit den für sie relevanten Gesetzes- und Verwaltungsvorschriften zuverlässig und professionell auszuführen. Insbesondere bestätigt die OeKB, dass sie über die zur ordnungsgemäßen Leistungserbringung erforderliche technische, personelle und finanzielle Ausstattung verfügt.
- (8) **Vergabe von Sub-Aufträgen für IKT-Drittdienstleistungen:** Sub-Beauftragungen sind ohne Zustimmung durch das Finanzunternehmen zulässig, sofern dadurch die Kontinuität der vertragsgegenständlichen Leistungserbringung und Informationssicherheit nicht beeinträchtigt werden. Die OeKB hat in jedem Fall ihre Sub-Dienstleister sorgfältig auszuwählen und darauf zu achten, dass diese über die erforderliche fachliche Qualifikation verfügen. OeKB verpflichtet sich, ihre Verpflichtungen an ihre Sub-Dienstleister zu überbinden und sich die Rechte, die das Finanzunternehmen gegenüber der OeKB hat, auch im Verhältnis der OeKB zu ihren Sub-Dienstleistern zu sichern. Gegenüber dem Finanzunternehmen haftet die OeKB weiterhin vollständig für die Leistungserbringung gemäß Vertrag und die Erfüllung der Pflichten gemäß diesem Addendum für die von einem Sub-Dienstleister zu erbringenden IKT-Dienstleistungen.
- (9) **Standort der Leistungserbringung und Datenverarbeitung:** Die vertraglich vereinbarte Dienstleistung sowie die Verarbeitung und Speicherung von diesen Daten im Rahmen der Leistungserbringung erfolgt durch OeKB derzeit ausschließlich in Österreich. Eine Datenverarbeitung in einem Mitgliedsstaat der Europäischen Union (EU) oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) ist zulässig. Die OeKB verpflichtet sich, die Finanzunternehmen zu benachrichtigen, wenn sie eine Änderung des bisher vereinbarten Standortes in ein anderes Land, an dem die vertraglich vereinbarte IKT-Dienstleistung bereitgestellt und an denen Daten verarbeitet werden sollen, einschließlich des Speicherorts, beabsichtigt. Das Finanzunternehmen hat kein Zustimmungsrecht zur Änderung des Standortes, ist aber berechtigt außerordentlich zu kündigen, wenn der neue Standort aus seiner Sicht eine Gefahr insbesondere für die Datenverarbeitung darstellt.
- (10) **Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit:** Hinsichtlich der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit in Bezug auf den Datenschutz, einschließlich des Schutzes personenbezogener Daten verpflichtet sich die OeKB diese zu gewährleisten und wird

diesbezüglich auf die bereits bestehenden Vereinbarungen gemäß Punkt 5 der Nutzungsbedingungen verwiesen. Die OeKB ergreift alle erforderlichen Maßnahmen, um ein dem Risiko der Verarbeitung angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen schließen insbesondere die Fähigkeit ein, die Vertraulichkeit, die Integrität, die Verfügbarkeit sowie der Belastbarkeit der Systeme auf Dauer sicherzustellen und die Verfügbarkeit der Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. Die OeKB informiert das Finanzunternehmen über die implementierten IKT-Sicherheitsmaßnahmen auf Anfrage an fondsdaten@oekb.at.

- (11) **Insolvenz, Abwicklung, Einstellung der Geschäftstätigkeit des IKT-Drittdienstleisters oder eine (Teil)Beendigung der IKT-Dienstleistung:** In diesem Fall werden die Vertragsparteien zusammenwirken, um eine ordnungsgemäße Überleitung auf einen anderen IKT-Drittdienstleister oder auf das Finanzunternehmen zu ermöglichen. Die Vertragsparteien werden in diesem Falle die Pflichten im Rahmen der Überleitung gemeinsam, möglichst unter Einbeziehung der VÖIG, erarbeiten und festlegen. Die OeKB wird – soweit rechtlich möglich - ihre Leistungen nach dem Vertrag so lange entgeltlich gemäß der bisherigen Regelung im Vertrag erbringen, bis die Überleitung abgeschlossen ist. Eine solche Überleitung hat in einem angemessenen Zeitrahmen zu erfolgen und darf nicht ohne triftigen Grund aufgehoben oder verschoben werden. Die OeKB hat insbesondere die von ihr bis dahin verarbeiteten Daten wiederherzustellen und in einem der Stand der Technik entsprechenden leicht zugänglichen Format dem Finanzunternehmen zur Verfügung zu stellen sowie nach Rückgabe an das Finanzunternehmen eventuell angefertigte Kopien unverzüglich zu löschen oder zu vernichten; Unterlagen und Daten, die die OeKB aufgrund zwingender gesetzlicher Vorgaben auch nach der Vertragsauflösung aufbewahren muss, müssen mit Ablauf dieser gesetzlichen Aufbewahrungsfristen auf eigene Kosten der OeKB umgehend vernichtet oder gelöscht werden. Der OeKB wird dem Finanzunternehmen die Löschung/Vernichtung von Finanzunternehmen-Daten bei sich und Dritten auf Wunsch des Finanzunternehmens schriftlich bestätigen bzw. mitteilen, aus welchen Gründen eine Löschung/Vernichtung unterblieb und konkretisieren, wann eine solche in der Zukunft stattfinden wird.
- (12) **Meldung von und Unterstützung bei IKT-bezogenen Vorfällen:** OeKB informiert das Finanzunternehmen über jeden IKT-bezogenen Vorfall gemäß Punkt (4), der mit dem Vertragsgegenstand in Verbindung steht und sich in der Sphäre der OeKB oder einer ihrer Sub-Dienstleister ereignet, umgehend nach Kenntnis schriftlich, was auch über die Website der OeKB (www.oekb.at) erfolgen kann. OeKB leistet darüber hinaus bei jeder Art von IKT-

bezogenen Vorfall gemäß Punkt (4), der mit der für OeKB bereitgestellten IKT-Dienstleistung in Verbindung steht, ohne zusätzliche Kosten Unterstützung.

- (13) **Einholung von Informationen:** Das Finanzunternehmen ist berechtigt, von OeKB alle Informationen, soweit noch nicht beim Finanzunternehmen vorhanden oder auf der Website der OeKB abrufbar, anzufordern, die das Finanzunternehmen zur Ermittlung, Steuerung und Überwachung der mit der IKT-Dienstleistung verbundenen Risiken, aber auch insbesondere für die tourliche Berichterstattung im Zusammenhang mit dem Informationsregister oder sonstige Meldungen an die für das Finanzunternehmen zuständigen Behörden und Abwicklungsbehörden benötigt werden. OeKB hat die angeforderten Informationen innerhalb einer angemessenen Frist an das Finanzunternehmen zu übermitteln. Auf Verlangen der für das Finanzunternehmen zuständigen Behörden und Abwicklungsbehörden ist das Finanzunternehmen daher auch berechtigt, diese Informationen und Berichte an diese herauszugeben.
- (14) **Zusammenarbeit mit den für Finanzunternehmen zuständigen Behörden:** Die OeKB verpflichtet sich, vollumfänglich mit den für das Finanzunternehmen zuständigen Behörden und Abwicklungsbehörden zusammenzuarbeiten, einschließlich der von diesen benannten Personen.
- (15) **Einhaltung von angemessenen Standards für Informationssicherheit:** Die OeKB hält bei der Leistungserbringung angemessene Standards für Informationssicherheit ein.
- (16) **Vereinbarung von weiteren außerordentlichen Kündigungsgründen:** Die Artikel 28 Absatz 7 lit. a) bis d) DORA VO berechtigen das Finanzunternehmen zur außerordentlichen Kündigung (sofortige Deregistrierung gemäß Nutzungsbedingungen) aufgrund eines durch OeKB nicht behobenen wesentlichen Verstoßes gemäß den vereinbarten Vertragsbedingungen.
- (17) **Teilnahme an Schulungen:** Die OeKB entwickelt eigene Programme zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz, die im Rahmen der internen Mitarbeiterschulung obligatorisch sind. Eine Teilnahme an Schulungen des Finanzunternehmens ist daher für diese Dienstleistung grundsätzlich nicht vorgesehen. Wenn es vom Finanzunternehmen ausdrücklich von OeKB verlangt werden sollte, wird OeKB jedoch an solchen Programmen sowie Schulungen des Finanzunternehmens gegen Vergütung durch das Finanzunternehmen teilnehmen.