# Microsoft Kundenvertrag
## DORA-Finanzdienstleistungen-Addendum

Der Kunde unterliegt zusätzlichen Compliance- und Regulierungsanforderungen der DORA (wie unten definiert). Dementsprechend ergänzen die Bedingungen dieses DORA-Addendums für Finanzdienstleistungen („**DORA-Addendum**") die Bedingungen der Änderung für Finanzdienstleistungen („**FSA**") zum Vertrag des Kunden, und zwar ausschließlich in dem Umfang, in dem: (a) DORA für den Kunden gilt, und (b) DORA es erfordert. Die in diesem DORA-Addendum niedergelegten Rechte und Pflichten gelten für die Parteien nach dem in der DORA, Art. 4, genannten Grundsatz der Verhältnismäßigkeit.

Alle Begriffe, die in diesem DORA-Addendum verwendet, aber nicht definiert werden, haben dieselbe Bedeutung wie in der FSA oder an anderer Stelle des Vertrags. Soweit dieses DORA-Addendum im Widerspruch zum FSA (in seiner jeweils gültigen Fassung) steht, gelten die Bedingungen dieses DORA-Addendums.

## *1. Begriffsbestimmungen*

**1.1 Ergänzend zu den Definitionen im FSA gelten folgende Begriffsbestimmungen:**

„**Kritische oder wichtige Onlinedienste**" bezeichnet nach DORA, Art. 28 (3), die Onlinedienste von Microsoft, wie in der geltenden Produktdokumentation beschrieben, die vom Kunden so konfiguriert werden, dass sie die kritischen oder wichtigen Funktionen des Kunden unterstützen können.

„**DORA**" bezeichnet die EU-Verordnung Nr. 2022/2554 über die digitale operationale Resilienz im Finanzsektor.

„**Informations- und Kommunikationstechnologie (IKT)-Vorfall**" bezeichnet ein einzelnes Ereignis oder eine Reihe verknüpfter Ereignisse, die die Nutzung eines kritischen oder wichtigen Onlinedienstes durch den Kunden beeinträchtigen und vom Kunden nicht geplant sind, die Sicherheit des Netzwerks und der Informationssysteme des Kunden gefährden und sich nachteilig auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder auf die vom Kunden bereitgestellten Dienste auswirken.

„**Wichtiger Anbieter**" bezeichnet einen wesentlichen Unterauftragnehmer (einschließlich eines Unterverarbeiters) von Microsoft, der kritische oder wichtige Onlinedienste unterstützt. Microsoft stellt eine aktuelle Liste der wichtigen Anbieter zur Verfügung, die auf Anfrage des Kunden erhältlich ist.

## *2. Ermöglichung der Kunden-Compliance*

**2.1 Kunden-Penetrationstests; Teilnahme an Kundenschulungen.** Ausschließlich in dem vom Kunden und von Microsoft im Rahmen von DORA geforderten Umfang wird Microsoft an bedrohungsgesteuerten Penetrationstests des Kunden (TLPT) in Bezug auf kritische oder wichtige Onlinedienste nach den unter DORA, Art. 26 (11), erlassenen technischen Regulierungsstandards, wie in der FSA und der veröffentlichten Dokumentation von Microsoft dargelegt, teilnehmen und uneingeschränkt kooperieren. Auf Wunsch des Kunden kann Microsoft Personal bereitstellen, das im Rahmen eines separaten Professional Services-Auftrags an den IKT-Sicherheitssensibilisierungsprogrammen des Kunden und an der Schulung zur digitalen operativen Belastbarkeit teilnimmt.

## *3. Uneingeschränkte Prüfungsrechte des Kunden*

**3.1 Kopien und alternative Zusicherungen.** Bei einer Prüfung durch den Kunden oder eine Aufsichtsbehörde kann dem Kunden oder der Aufsichtsbehörde gestattet werden, Kopien der relevanten Dokumentation von Microsoft vor Ort anzufertigen, wenn diese Dokumentation für den Betrieb von Microsoft entscheidend ist. Für den Fall, dass eine im Rahmen von DORA durchgeführte Kundenprüfung die Rechte anderer Microsoft-Kunden stören oder beeinträchtigen würde, wird Microsoft wirtschaftlich vertretbare Anstrengungen unternehmen, um einen alternativen, einvernehmlich vereinbarten Weg zu finden, um ein ähnliches Maß an Sicherheit in Bezug auf das Thema der Prüfungsanforderung zu bieten.

## *4. Zusätzliche Kündigungsrechte des Kunden*

**4.1 Kündigungsmitteilung.** Der Begriff „Angemessene schriftliche Mitteilung" im Sinne von Abschnitt 6 der FSA wird nach den Leitlinien und Erwartungen der Aufsichtsbehörden ausgelegt.

**4.2 Zusätzliche Kündigungsrechte des Kunden.** Der Kunde ist ferner berechtigt, einen kritischen oder wichtigen Onlinedienst nach den (und vorbehaltlich der) in Abschnitt 6 des FSA dargelegten Bedingungen und Verfahren zu kündigen („Zusätzliche Kündigungsrechte des Kunden"), wenn Microsoft nachweislich Schwächen in Bezug auf sein gesamtes IKT-Risikomanagement aufweist, und zwar in Bezug auf die Art und Weise, wie Microsoft die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Kundendaten sicherstellt..

## *5. IKT-Vorfall*

**5.1 Hilfe bei IKT-Störungen.** Microsoft stellt dem Kunden im Hinblick auf einen IKT-Vorfall angemessene Unterstützung zu Kosten bereit, die sich nach den zum Zeitpunkt des IKT-Vorfalls aktuellen, veröffentlichten Support-Angeboten von Microsoft richten. Zusätzlich zu den Verpflichtungen von Microsoft hinsichtlich der Meldung von Sicherheitsvorfällen wird Microsoft den Kunden benachrichtigen, wenn Microsoft Kenntnis von einer Entwicklung erlangt, die nach Einschätzung von Microsoft wesentliche Auswirkungen auf die Fähigkeit von Microsoft haben könnte, die kritischen oder wichtigen Onlinedienste in Übereinstimmung mit den geltenden Vereinbarungen zum Servicelevel (SLA) bereitzustellen.

## *6. Wichtige Anbieter*

**6.1 Zustimmung zur Nutzung wichtiger Anbieter.** Die Parteien erkennen an und vereinbaren, dass Microsoft mit wichtigen Anbietern zusammenarbeiten kann, um dem Kunden kritische oder wichtige Onlinedienste bereitzustellen. Microsoft bleibt dafür verantwortlich, dass wichtige Anbieter ihre Verpflichtungen aus dem Vertrag einhalten.

**6.2 Audit wichtiger Anbieter.** Der Kunde (in seiner Eigenschaft als FS-Vertreter), die FS-Einrichtungen oder die Aufsichtsbehörden haben das uneingeschränkte Recht, wichtige Anbieter in Übereinstimmung mit dem Umfang, den Richtlinien und den Verfahren, die in der FSA des Kunden vorgesehen sind, zu untersuchen oder zu prüfen.

**6.3 Richtlinie für Daten wichtiger Anbieter, Standort und Ausfall wichtiger Anbieter.** Die Verpflichtungen von Microsoft in Abschnitt 2.e der FSA gelten für wichtige Anbieter, soweit Microsoft diese wichtigen Anbieter mit der Verarbeitung, Übertragung oder Speicherung von Kundendaten beauftragt, die DORA unterliegen. Wichtige Anbieter stellen ausgelagerte kritische oder wichtige Onlinedienste von Standorten aus bereit, die mit der jeweiligen Standortzusage von Microsoft für jeden solchen kritischen oder wichtigen Onlinedienst übereinstimmen. Microsoft stellt sicher, dass seine Verträge mit wichtigen Anbietern Bedingungen enthalten, die die wichtigen Anbieter zur Einhaltung aller geltenden Gesetze und behördlichen Anforderungen verpflichten.

**6.4 Geschäftskontinuität des wichtigen Anbieters.** Microsoft verlangt von wichtigen Anbietern, dass sie Geschäftskontinuitätspläne implementieren und testen.

**6.5 Risikobewertung für wichtige Anbieter.** Vor Beauftragung eines neuen wichtigen Anbieters führt Microsoft eine Risikobewertung durch: (a) Standort des wichtigen Anbieters, (b) Standort der Muttergesellschaft des wichtigen Anbieters und (c) Standort, von dem aus der wichtige Anbieter Dienste im Namen von Microsoft erbringen wird.

**6.6 Wesentliche Änderungen an Untervertragsvereinbarungen.** In Übereinstimmung mit dem DPA wird Microsoft den Kunden mindestens 6 Monate im Voraus benachrichtigen, wenn ein neuer wichtiger Anbieter Zugriff auf Kundendaten erhält, und den Kunden mindestens 30 Tage im Voraus benachrichtigen, wenn ein neuer wichtiger Anbieter Zugriff auf personenbezogene Daten erhält. Microsoft wird den Kunden über Änderungen an Untervertragsvereinbarungen informieren, soweit diese Änderungen die Fähigkeit von Microsoft, kritische oder wichtige Onlinedienste in Übereinstimmung mit den geltenden Dienstgütevereinbarungen zu erbringen, wesentlich beeinträchtigen könnten. Wenn der Kunde mit diesen

Änderungen nicht einverstanden ist, kann er – parallel zu seinen DPA-Rechten – jedes Abonnement für den betroffenen kritischen oder wichtigen Onlinedienst ohne Vertragsstrafe oder Kündigungsgebühr kündigen, indem er vor Ablauf der geltenden Kündigungsfrist eine schriftliche Kündigung einreicht. Nach der Kündigung entfernt Microsoft Zahlungsverpflichtungen für Abonnements oder andere anwendbare unbezahlte Arbeiten für die beendeten Abonnements aus diesbezüglichen Folgerechnungen.

**6.7 Beaufsichtigung wichtiger Anbieter.** Durch die Bereitstellung der Onlinedienste erklärt sich Microsoft damit einverstanden, alle ausgelagerten kritischen oder wichtigen Onlinedienste, die von wichtigen Anbietern ausgeführt werden, in dem Umfang zu beaufsichtigen und zu überwachen, der erforderlich ist, um den Verpflichtungen von Microsoft im DPA und diesem DORA-Addendum nachzukommen. Microsoft stellt sicher, dass die schriftlichen Verträge mit wichtigen Anbietern folgende Bedingungen enthalten: (a) Festlegung der Überwachungs- und Berichtspflichten der wichtigen Anbieter gegenüber Microsoft und, sofern vereinbart, gegenüber dem Kunden; und (b) Verpflichtung der wichtigen Anbieter, mindestens das von Microsoft im DPA geforderte Datenschutzniveau zu gewährleisten, einschließlich der Beschränkungen für die Offenlegung verarbeiteter Daten (wie im DPA definiert). Microsoft ist für die Handlungen und Unterlassungen der wichtigen Anbieter rechenschaftspflichtig und haftbar, als wären es seine eigenen Handlungen und Unterlassungen.

Diese Zusatzvereinbarung tritt mit der Annahme ihrer Bestimmungen in Kraft und läuft entweder (i) am letzten Tag des 36. Kalendermonats nach der Annahme oder (ii) am Tag der Beendigung des Vertrags aus, je nachdem, was zuerst eintritt.