Microsoft-Kundenvertrag

Zusatzvereinbarung zu Finanzdiensten

Die Geschäftsbestimmungen dieser Zusatzvereinbarung zu den Finanzdienstleistungen („**Zusatz**“) ergänzen die Geschäftsbestimmungen des Microsoft-Kundenvertrags (der „**Vertrag**”), der für die Nutzung der Onlinedienste durch den Kunden gilt. Der Kunde unterliegt der Aufsicht einer Finanzdienstleistungsaufsichtsbehörde sowie bestimmten Konformitäts- und regulatorischen Anforderungen. Diese Zusatzvereinbarung umfasst bestimmte zusätzliche Leistungen für den Kunden zur Erfüllung dieser regulatorischen Anforderungen. Die in dieser Zusatzvereinbarung gewährten Rechte dürfen nicht in einer Weise ausgeübt werden, die den Datenschutz oder die Sicherheit der Daten anderer Microsoft-Kunden gefährden oder die Stabilität oder Leistung eines Onlinedienstes bedrohen oder beeinträchtigen würde.

1. Begriffsbestimmungen

In Großbuchstaben geschriebene Begriffe (im Quelltext), die in dieser Zusatzvereinbarung verwendet, aber nicht definiert werden, haben die im Vertrag angegebene Bedeutung (gegebenenfalls einschließlich der Produktbestimmungen, einschließlich des Glossars zu den Produktbestimmungen und der Datenschutz- und Sicherheitsbestimmungen für Onlinedienste, oder des Datenschutznachtrags zu den Produkten und Services von Microsoft [„**DPA**“]). Die folgenden Definitionen werden in dieser Zusatzvereinbarung verwendet:

„**Kunde**“ bedeutet für Zwecke dieser Zusatzvereinbarung die juristische Person, die den Vertrag geschlossen hat, und/oder alle verbundenen Unternehmen, die Finanzdienstleistungen anbieten, unter der Aufsicht einer Aufsichtsbehörde stehen und Onlinedienste im Rahmen des Vertrags in Anspruch nehmen.

„**Kundenprüfer**“bezeichnet für Zwecke dieser Zusatzvereinbarung sowohl die internen als auch die externen Prüfer des Kunden.

„**Finanzdienstleistungen**“ bedeutet ohne Einschränkung Bank-, Kredit-, Versicherungs- und Zahlungsdienstleistungen, Wertpapierhandel, Terminhandel, Wertpapierbörsen, Ausgabe von E-Geld und andere Dienstleistungen, die mit der Anlage, der Kreditvergabe, dem Handel und der Verwaltung von Geld und Vermögenswerten verbunden sind.

„**Onlinedienste**“ bezeichnet für die Zwecke dieser Zusatzvereinbarung die Onlinedienste, die in den Datenschutz- und Sicherheitsbestimmungen für Onlinedienste als „Kern-Onlinedienste“ definiert werden und Prüfungen nach SSAE 18 SOC 1 Typ II und SSAE 18 SOC 2 Typ II unterliegen.

„**Aufsichtsbehörde**“ bezeichnet eine Aufsichts- oder Verhaltensregulierungsbehörde mit Aufsichts- oder Abwicklungsrechten, wie sie nach anwendbarem Recht oder anwendbaren Vorschriften über den Kunden oder Microsoft als Anbieter von Onlinediensten für den Kunden vorgesehen sind.

„**Unterauftragsverarbeiter**“ hat die gleiche Bedeutung wie im DPA definiert.

2. Ermöglichung von Kunden-Compliance

a. Allgemeines Zugriffsrecht. Gemäß den Bestimmungen des Vertrags hat der Kunde jederzeit das Recht, über die Standardfunktionen der Onlinedienste auf Kundendaten zuzugreifen, auch im Falle einer Insolvenz, Abwicklung oder Einstellung des Geschäftsbetriebs von Microsoft, unter Berücksichtigung des anwendbaren Rechts.

b. Penetrationstests durch den Kunden und Microsoft. Der Kunde hat die Möglichkeit, Schwachstellen- und Penetrationstests der Aufstellung des Kunden in den Onlinediensten oder andere ähnliche Tests durchzuführen, die für einen bestimmten Onlinedienst gelten, den der Kunde nutzt. Der Kunde muss alle Tests nach den aktuellen Richtlinien und Verfahren von Microsoft, die solche Tests regeln, durchführen, was unter anderem bedeuten kann, dass der Kunde Microsoft im

Voraus über alle Tests benachrichtigen muss und den Kunden daran hindert, sich an andere Microsoft-Kunden zu wenden. Mindestens einmal jährlich wird Microsoft Penetrationstests durch Dritte für die im Vertrauensstellungsportal aufgeführten Onlinedienste in Auftrag geben. Zu diesen Tests gehört der Nachweis der Datenisolation zwischen Mandanten in den getesteten mandantenfähigen Onlinediensten. Diese Informationen stehen den Kunden über das Dienstvertrauensstellungsportal (https://servicetrust.microsoft.com/viewpage/PenTest oder eine von Microsoft festgelegte Nachfolgeseite) zur Verfügung.

c. **Prüfungen von Onlinediensten durch Microsoft.** Im Namen der Kunden, einschließlich des Kunden und der Prüfer des Kunden, veranlasst Microsoft die Durchführung von Prüfungen der Sicherheit der Computer, der Computerumgebung und der physischen Datenzentren, die es bei der Verarbeitung von Kundendaten (einschließlich personenbezogener Daten) für jeden Onlinedienst nutzt. Für jede Prüfung wird abschließend ein Microsoft-Prüfbericht („Prüfbericht“) erstellt, wie in den DPA ausgeführt.

d. **Logische Trennung.** Microsoft verwendet eine logische Trennung für die Speicherung und Verarbeitung von Kundendaten, um eine Vermischung dieser Daten mit den Daten anderer Microsoft-Kunden zu verhindern.

e. **Datenresidenz- und Datenübertragungsrichtlinien.** Kundendaten, die Microsoft im Auftrag des Kunden verarbeitet, werden wie im DPA angegeben verarbeitet, übertragen und gespeichert. Der Kunde kann unter https://www.microsoft.com/de-de/trust-center/privacy/data-location oder einer von Microsoft festgelegten Nachfolgewebsite auf zusätzliche Details zu den Richtlinien für den Onlinedienst in Bezug auf Datenresidenz und Datenübertragung zugreifen.

3. Uneingeschränkte Prüfungs- oder Überwachungsrechte für die Aufsichtsbehörde

a. Für den Fall, dass die Aufsichtsbehörde eine Untersuchung oder Prüfung der Abläufe und Kontrollen der Onlinedienste verlangt, um die Aufsichtspflichten der Aufsichtsbehörde, unter anderem die Prüfung oder Untersuchung von Microsoft als direktem Dienstanbieter des Kunden, zu erfüllen, gewährt Microsoft der Aufsichtsbehörde ein uneingeschränktes Recht zur Untersuchung oder Prüfung der Onlinedienste. Dies umfasst die Gewährung des uneingeschränkten Zugangs zu allen relevanten Geschäftsräumen (z. B. Firmensitze und Betriebszentren), einschließlich der gesamten Palette der relevanten Geräte, Systeme, Netzwerke, Informationen und Daten, die für die Bereitstellung der ausgelagerten Funktion verwendet werden, einschließlich der damit verbundenen Finanzinformationen, des Personals und der externen Prüfer von Microsoft. Der Zutritt zu den Räumlichkeiten unterliegt der Gewährleistung der Gesundheit und Sicherheit aller an einer Untersuchung beteiligten Personen sowie der Sicherheit aller mit einer Untersuchung verbundenen Daten, Geräte und Einrichtungen. Soweit auf solche Informationen virtuell zugegriffen werden kann, werden die Parteien daran arbeiten, solche Anfragen durch virtuelle Online-Kommunikation und gemeinsame Nutzung von Dokumentation über gesicherte Protokolle zu bearbeiten. Dies kann bei Bedarf eine Prüfung von Unterauftragsverarbeitern umfassen, die im Abschnitt des DPA festgelegt sind, der sich auf Unterauftragsverarbeiter bezieht und derzeit den Titel „Mitteilungen und Kontrollen bei der Nutzung von Unterauftragsverarbeitern“ trägt. Solche Aktivitäten werden unter der Koordination und Aufsicht von Microsoft und vorbehaltlich aller Bestimmungen dieser Zusatzvereinbarung durchgeführt.

b. Die Aufsichtsbehörde kann beim Kunden einen direkten Zugriff auf die Kundendaten anfordern. Der Kunde kann diese Anforderung erfüllen, indem er direkt (i) Personen, die von der Regulierungsbehörde benannt werden, administrative Rechte gewährt oder (ii) einen Drittanbieter von Diensten benennt, der auf eine solche Anfrage der Regulierungsbehörde direkt antworten kann. Wenn Microsoft eine solche Anfrage von der Aufsichtsbehörde erhält, wird Microsoft diese an den Kunden weiterleiten. Der Kunde oder der benannte Drittanbieter ist für die Beantwortung der Anfrage verantwortlich und wird sie nicht durch Weiterleitung solcher Angelegenheiten an Microsoft umgehen. Die Aufsichtsbehörde erhält keinen Zugriff auf Daten, die anderen Microsoft-Kunden gehören.

c. Der Kunde und Microsoft kommen für ihre Kosten im Zusammenhang mit den in diesem Abschnitt 3 beschriebenen Aktivitäten selbst auf.

d. Microsoft stimmt zu, mit Aufsichtsbehörden zusammenzuarbeiten, soweit dies für die Zwecke der Aufsichtstätigkeit der Aufsichtsbehörde angemessen und notwendig ist, auch wenn der Kunde die Onlinedienste direkt von Microsoft lizenziert oder wenn der Kunde eine Drittanbieterlösung lizenziert, die Onlinedienste nutzt.

e. Die finanziellen Verpflichtungen der Parteien sind im Vertrag zwischen den Parteien festgelegt.

f. Der Kunde kann seinen Zugriff auf Kundendaten an Vertreter der Aufsichtsbehörde delegieren.

g. Microsoft erklärt sich bereit, mit den Aufsichtsbehörden des Kunden zusammenzuarbeiten, einschließlich der Möglichkeit, dass die Aufsichtsbehörden Fragen direkt an Microsoft richten können, soweit dies für die Zwecke der Aufsicht angemessen und erforderlich ist. Microsoft wird die besagte Zusammenarbeit gemäß den Bestimmungen dieser Zusatzvereinbarung leisten.

4. Uneingeschränkte Prüfungsrechte des Kunden

a. Allgemeine Prüfungsrechte. Wie in dieser Zusatzvereinbarung dargelegt, gewährt Microsoft dem Kunden und den Kundenprüfern uneingeschränkte Inspektions- und Prüfungsrechte in Bezug auf die Outsourcing-Vereinbarung(en), wie in Abschnitt 4(b) angegeben, damit der Kunde die Outsourcing-Vereinbarungen überwachen und die Einhaltung aller geltenden behördlichen und vertraglichen Anforderungen (einschließlich wenn der Kunde die Onlinedienste direkt von Microsoft lizenziert oder wenn der Kunde eine Drittanbieterlösung lizenziert, die Onlinedienste nutzt) sicherstellen kann (die „**Kundenprüfungen**"). Dies umfasst die Gewährung des uneingeschränkten Zugangs zu allen relevanten Geschäftsräumen (z. B. Firmensitze und Betriebszentren), einschließlich der gesamten Palette der relevanten Geräte, Systeme, Netzwerke, Informationen und Daten, die für die Bereitstellung der ausgelagerten Funktion verwendet werden, einschließlich der damit verbundenen Finanzinformationen, des Personals und der externen Prüfer von Microsoft. Die Ausübung dieser Rechte unterliegt dem Grundsatz der Verhältnismäßigkeit in Bezug auf die Kritikalität dieser Onlinedienste bei der Ausübung wesentlicher Funktionen des Kunden. Der Zutritt zu den Räumlichkeiten unterliegt der Gewährleistung der Gesundheit und Sicherheit aller an einer Untersuchung und Prüfung beteiligten Personen sowie der Sicherheit aller mit einer Untersuchung und Prüfung verbundenen Daten, Geräte und Einrichtungen. Soweit auf solche Informationen virtuell zugegriffen werden kann, werden die Parteien daran arbeiten, solche Anfragen durch virtuelle Online-Kommunikation und gemeinsame Nutzung von Dokumentation über gesicherte Protokolle zu bearbeiten.

b. Umfang des Kundenaudits. Der Kunde hat das Recht, bei sich selbst, seinen regulierten Partnern, den Kundenprüfern oder der Aufsichtsbehörde auf alle Informationen zuzugreifen, die erforderlich sind, um seine Einhaltung der einschlägigen rechtlichen Verpflichtungen zu gewährleisten und sicherzustellen, dass:

1. Die Onlinedienste mit den Produktbestimmungen, dem DPA und dieser Zusatzvereinbarung übereinstimmen;

2. die Vereinbarungen zum Servicelevel eingehalten werden;

3. die Integrität und Vertraulichkeit der Kundendaten in Übereinstimmung mit den Geschäftsbestimmungen des DPA und dieses Zusatzes geschützt werden und

4. Die dem Kunden zur Verfügung gestellten Onlinedienste sicher sind.

c. Kundenprüfverfahren. Microsoft gestattet dem Kunden die Durchführung von Kundenprüfungen, einschließlich von Prüfungen vor Ort (bei Bedarf), wie im Folgenden beschrieben:

1. Nach angemessener schriftlicher Vorankündigung gestattet Microsoft dem Kunden die Durchführung einer Kundenprüfung der Geschäftsräume von Microsoft und der vom Kunden genutzten Onlinedienste. Datum, Uhrzeit und Ort der Kundenprüfung werden einvernehmlich zwischen dem Kunden und Microsoft vereinbart. Dies kann bei Bedarf eine Prüfung von Unterauftragsverarbeitern umfassen, die im Abschnitt des DPA festgelegt sind, der sich auf Unterauftragsverarbeiter bezieht und derzeit den Titel „Mitteilungen und Kontrollen bei der Nutzung von Unterauftragsverarbeitern" trägt. Solche Aktivitäten

werden unter der Koordination und Aufsicht von Microsoft und vorbehaltlich aller Bestimmungen dieser Zusatzvereinbarung durchgeführt. Aus Gründen der Klarheit: In diesem Absatz soll nicht das Recht des Kunden auf Prüfung eingeschränkt werden, und Microsoft bestätigt, dass ein Vertrag über Datum, Uhrzeit und Ort der Prüfung unter Berücksichtigung des Umfangs und der Gründe für die Anforderung der Prüfung nicht unangemessen zurückgehalten oder verzögert wird, dass in einer Not- oder Krisensituation eine begrenzte vorherige angemessene Benachrichtigung möglich ist und dass eine solche Terminplanung nicht dazu verwendet wird, das Ziel der Prüfung zu gefährden.

2. Der Kunde erklärt sich damit einverstanden, dass er die Kosten trägt, die Microsoft im Zusammenhang mit der Kundenprüfung entstehen (4.000 US-Dollar pro Tag für jeden Microsoft-Mitarbeiter, zuzüglich angemessener Reisekosten). Diese Kosten werden in einer Leistungsbeschreibung ausgewiesen. Eine Microsoft-Engineering-Quelle, die nur für einen Teil eines einzigen Tags benötigt wird, wird dem Kunden anteilig in Rechnung gestellt. Microsoft berechnet nur Gebühren für Leistungen, die nach Zeitsätzen erbracht werden. Außerdem berechnet Microsoft keine Gebühren für administrative Tätigkeiten, die von Microsoft-Mitarbeitern ausgeübt werden, wie die Organisation von Meetings, die Begleitung von Besuchern oder das Kopieren von Unterlagen. Falls es Streitigkeiten über Kosten im Zusammenhang mit einer Kundenprüfung gibt, werden die Parteien die Angelegenheit an ihre zuständigen Führungskräfte zwecks Schlichtung weiterleiten.

3. Die folgenden Richtlinien gelten für jede Kundenprüfung:

- **A.** Microsoft wird eine angemessene Zahl von entsprechend qualifizierten und sachkundigen Microsoft-Mitarbeitern benennen und dem Kunden zur Verfügung stellen, um die Kundenprüfung zu erleichtern.
- **B.** Der Kunde kann einen unabhängigen Prüfer damit beauftragen, die Kundenprüfung in seinem Namen durchzuführen, vorausgesetzt, der Kunde bestätigt mit vorheriger schriftlicher Mitteilung in angemessener Frist, dass dieser Kundenprüfer befugt ist, im Namen des Kunden zu handeln.
- **C.** Der Kunde kann die Kundenprüfungen direkt oder mit seinem Prüfer durchführen. Der Kunde bleibt für die Überwachung und Anleitung des Kundenprüfers im Zusammenhang mit der Durchführung einer solchen Kundenprüfung verantwortlich und muss die Leistungsbeschreibung für jede durchzuführende Kundenprüfung genehmigen.
- **D.** Die Kundenprüfung wird im Einklang mit den sicherheitsbezogenen Richtlinien und Verfahren von Microsoft durchgeführt, um die Gesundheit und Sicherheit der beteiligten Personen zu gewährleisten und die Verfügbarkeit, Sicherung und Vertraulichkeit der Kundendaten sowie der Geräte und Einrichtungen von Microsoft zu schützen.
- **E.** Die Kundenprüfung wird in einer Weise durchgeführt, die jede unangemessene oder unnötige Unterbrechung des Betriebs von Microsoft vermeidet.
- **F.** Alle von Microsoft oder ihren Prüfern im Zusammenhang mit einer Kundenprüfung zur Verfügung gestellten Informationen und Unterlagen werden vom Kunden, seinen Partnern, den Kundenprüfern und der Aufsichtsbehörde als vertrauliche Informationen von Microsoft behandelt oder Microsoft verlangt, diese als solche zu behandeln.

4. Die Ausübung dieser Rechte unterliegt dem Grundsatz der Verhältnismäßigkeit in Bezug auf die Frage, ob diese Onlinedienste für kritische oder wichtige Funktionen der Tätigkeiten des Kunden genutzt werden.

5. Zusätzliche Kundenvorteile

Microsoft erkennt die Bedürfnisse der Finanzdienstleistungsbranche und bietet eine Reihe von Funktionen an, um Kunden bei regulatorischen Angelegenheiten zu unterstützen.

a. Für den Fall, dass die Aufsichtsbehörde neue oder aktualisierte Anleitungen veröffentlicht, die sich auf die Onlinedienste beziehen, wird Microsoft auf schriftliche Anfrage eines Kunden an Microsoft eine schriftliche Antwort auf diese Anleitungen vorbereiten, einschließlich der Art und Weise (und des Umfangs), wie (und in welchem Umfang) die Onlinedienste die Anleitungen entweder durch vorhandene Funktionen oder geplante Änderungen an der Roadmap für die Onlinedienste berücksichtigen.

b. Wenn der Kunde, der entweder im eigenen Namen oder auf Anweisung seiner Regulierungsbehörde handelt, die Änderung einer neuen oder vorhandenen Dienstefunktion oder -steuerung benötigt, kann der Kunde eine solche Funktion oder Steuerung von Microsoft anfordern, und Microsoft wird innerhalb einer angemessenen Frist antworten, sodass die Parteien erörtern können, ob eine Berücksichtigung einer solchen Anforderung durchführbar ist und, falls ja, wie diesen Anforderungen des Kunden entsprochen werden kann.

c. Für den Fall, dass Microsoft und der Kunde keine für beide Seiten zufriedenstellende Lösung finden können, um Bedenken hinsichtlich regulatorischer Änderungen oder Änderungen der Onlinedienste auszuräumen, teilt Microsoft dem Kunden den Grund bzw. die Gründe mit, warum Microsoft nicht in der Lage oder nicht willens ist, diese Änderung(en) umzusetzen. In Übereinstimmung mit Abschnitt 6 kann sich der Kunde dann dafür entscheiden, den jeweiligen Onlinedienst ohne Vertragsstrafe zu kündigen, indem er eine angemessene schriftliche Kündigungsmitteilung vorlegt.

d. Wie im DPA beschrieben, stellt Microsoft sicher, dass seine Verträge mit Unterauftragsverarbeitern Bestimmungen enthalten, die die Unterauftragsverarbeiter zur Einhaltung aller Gesetze und regulatorischen Anforderungen verpflichten, die für die ausgelagerten Onlinedienste relevant sind und von Microsoft im DPA verlangt werden. Bei der Bereitstellung der Onlinedienste verpflichtet sich Microsoft, die Unterauftragsverarbeiter in dem Umfang zu beaufsichtigen, der zur Erfüllung der im Rahmen des DPA und dieser Zusatzvereinbarung für Microsoft geltenden Verpflichtungen erforderlich ist. Microsoft ist für die Handlungen und Unterlassungen dieser Unterauftragsverarbeiter verantwortlich und haftet so als wären es die eigenen Handlungen und Unterlassungen.

6. Zusätzliche Kündigungsrechte des Kunden

Der Kunde kann ohne Vertragsstrafe einen Onlinedienst in den folgenden Fällen kündigen, indem er Microsoft eine angemessene schriftliche Mitteilung zusendet, die das anwendbare Szenario und angemessene Angaben zu den Gründen umfasst, auf denen die Kündigungsmitteilung beruht:

a. Auf ausdrückliche Anweisung einer Regulierungsbehörde;

b. Nach dem in Abschnitt 5(c) und Abschnitt 6 beschriebenen Kündigungsrecht;

c. Bei einem Verstoß von Microsoft gegen geltendes Recht, Vorschriften oder ihre Verpflichtungen aus diesem Zusatz;

d. Bei festgestellten Hindernissen, die die Leistung der ausgelagerten Funktion beeinträchtigen können;

e. Wenn der Kunde hinreichend nachweisen kann, dass es Schwächen hinsichtlich der Verwaltung und Sicherheit von Kundendaten oder -informationen gibt;

f. Wenn der Kunde hinreichend nachweisen kann, dass es wesentliche Änderungen gibt, die sich auf die Bereitstellung der Onlinedienste durch Microsoft auswirken; oder

g. Wenn Microsoft gegen eine seiner Verpflichtungen gemäß Abschnitt 5(d) verstößt, die über einen Zeitraum von 30 Tagen (sofern heilbar) nicht behoben werden kann, hat der Kunde das Recht, alle betroffenen Onlinedienste gemäß den Bestimmungen dieses Abschnitts 6 zu kündigen.

Für den Fall, dass der Kunde einige oder alle Onlinedienste gemäß diesem Abschnitt 6 kündigt, ist der Kunde verpflichtet, alle vor der Kündigung genutzten, aber noch nicht in Rechnung gestellten Onlinedienste zu bezahlen, und alle fälligen Beträge aus unbezahlten Rechnungen werden sofort fällig und zahlbar. Zur Klarstellung: Microsoft erstattet dem Kunden keine Zahlungen oder Kosten für professionelle Dienstleistungen, die mit einem gekündigten Onlinedienst zusammenhängen oder sich aus dieser Kündigung ergeben. Wenn der Kunde eine vertragliche Verpflichtung zur Nutzung von Onlinediensten eingegangen ist, wird auf diese Verpflichtungen, einschließlich der bereits für noch nicht in Anspruch genommene Onlinedienste in Rechnung gestellten Beträge, nicht verzichtet und die Parteien erklären sich damit einverstanden, diese Verpflichtungen anderen Onlinediensten neu zuzuweisen.

7. Sicherheitsvorfälle

a. Wichtige Ereignisse. Wenn Microsoft von einem Sicherheitsvorfall (wie im DPA definiert) Kenntnis erlangt, wird Microsoft den Kunden zusätzlich zu den im DPA beschriebenen Verpflichtungen über die Art, die häufigen Ursachen und die vernünftigerweise zu erwartende Lösung dieses Sicherheitsvorfalls informieren eine wesentliche Auswirkung auf den Dienst oder eine nachteilige Auswirkung auf die Nutzung der Onlinedienste durch den Kunden und wird Mitteilungen über die Risiko-Bedrohungsbewertungen von Microsoft oder andere Umstände bereitstellen, die schwerwiegende Auswirkungen haben können.

b. Beschränkte Erstattung bestimmter Kosten. Soweit ein Sicherheitsvorfall ausschließlich dadurch verursacht wird, dass Microsoft seine Verpflichtungen aus dem Vertrag nicht erfüllt, und vorbehaltlich der auf die jeweiligen Onlinedienste anwendbaren Haftungsbeschränkungen, erstattet Microsoft dem Kunden alle angemessenen Behebungskosten, die dem Kunden im Zusammenhang mit dem Sicherheitsvorfall entstehen. „Angemessene Sanierungskosten" bestehen aus (a) tatsächlichen Kosten für Zahlungen, Bußgelder, Vertragsstrafen, Sanktionen, angemessene Anwaltskosten, Gerichtskosten oder -gebühren oder andere Rechtsmittel oder Schulden und etwaige Zinsen darauf, die von einem Gericht, Tribunal, Schiedsgericht, einer Regierungsstelle oder Aufsichtsbehörde für einen von Microsoft verursachten Sicherheitsvorfall auferlegt werden; (b) zusätzlichen wirtschaftlich vertretbaren Auslagen, die dem Kunden entstehen, um den von Microsoft verursachten Sicherheitsvorfall zu verwalten oder zu beheben, einschließlich, aber nicht beschränkt auf Kosten, die mit der Wiederherstellung, Korrektur oder Reparatur des betroffenen Onlinedienstes verbunden sind; (c) kommerziell vertretbaren Auslagen für gesetzlich vorgeschriebene Benachrichtigungen der Endnutzer des Kunden über den von Microsoft verursachten Sicherheitsvorfall (jedoch nicht die Kosten für professionelle Dienstleistungen von Drittanbietern, einschließlich solcher, die sich auf Krisenmanagement, Öffentlichkeitsarbeit oder Medienarbeit beziehen, bei denen es sich um indirekte Schäden und Folgeschäden gemäß Vertrag handelt). Der Kunde muss alle diese Ausgaben dokumentieren, und auf Anfrage von Microsoft müssen diese Ausgaben von einem unabhängigen, international anerkannten Experten der Finanzdienstleistungsbranche, der von beiden Parteien ausgewählt wird, überprüft werden. Um Zweifel auszuschließen, werden die von Microsoft gemäß diesem Absatz erstatteten Kosten als direkte Schäden gekennzeichnet, die der Haftungsbeschränkung im Vertrag unterliegen, und nicht als indirekte, Folge-, Sonder- oder beiläufige Schäden, die im Vertrag ausgeschlossen sind.

c. Meldung von computerbezogenen Sicherheitsvorfällen. Für den Fall, dass Microsoft feststellt, dass ein computerbezogener Sicherheitsvorfall aufgetreten ist, der die Informationssysteme oder die in solchen Systemen enthaltenen Informationen im Zusammenhang mit den dem Kunden bereitgestellten Onlinediensten erheblich stört oder beeinträchtigt oder diese mit hinreichender Wahrscheinlichkeit erheblich beeinträchtigen oder beeinträchtigen wird, und wenn ein solcher computerbezogener Sicherheitsvorfall vier oder mehr Stunden lang auftritt, benachrichtigt Microsoft schnellstmöglich einen vom Kunden benannten Ansprechpartner, der von dem computerbezogenen Sicherheitsvorfall betroffen ist. Der Kunde ist für die Pflege korrekter Kontaktdaten für alle mit dem Vertrag verbundenen Onlinedienste verantwortlich. Die Mitteilung an den Kunden kann auf von Microsoft ausgewählten Wegen erfolgen, z. B. per E-Mail oder Telefon. Für die Zwecke dieser Zusatzvereinbarung bedeutet „Computerbezogener Sicherheitsvorfall" ein Vorkommnis, das zu einem tatsächlichen Schaden an einem Informationssystem oder den darin enthaltenen Informationen führt (wie vom Office of the Comptroller of the Currency in den

Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 FR 66424 (23. November 2021)) definiert.

8. Geschäftskontinuität von Onlinediensten

Microsoft erkennt an, dass der Kunde von seiner Regulierungs- oder nationalen Abwicklungsbehörde aufgefordert werden kann sicherzustellen, dass er in der Lage ist, seine Geschäfte im Falle (1) regulatorischer oder anderer rechtlicher Maßnahmen, die den Kunden oder einen seiner Partner betreffen, (2) der Beendigung oder des Ablaufs des Vertrags oder (3) einer Naturkatastrophe oder eines ähnlichen Notfalls, die Microsoft betreffen, weiterzuführen. Microsoft und der Kunde kommen wie folgt überein:

a. Kontinuität nach Intervention der Regulierungsbehörde. Im Fall einer Intervention beim Kunden durch eine Aufsichtsbehörde oder nationale Abwicklungsbehörde gemäß anwendbarem Recht oder anwendbaren Vorschriften erfüllt Microsoft die Anforderungen der Aufsichtsbehörde oder nationalen Abwicklungsbehörde und unterstützt die Aufsichtsbehörde oder nationale Abwicklungsbehörde bei der Aufrechterhaltung der Geschäftskontinuität des Kunden, wie zutreffend, indem sichergestellt wird, dass die Aufsichtsbehörde oder nationale Abwicklungsbehörde eine vollständige administrative Kontrolle über die Onlinedienste erhält.

b. Kontinuität nach der Übertragung von Rechten durch den Kunden.

1. Im Falle einer Insolvenz, Umstrukturierung, Liquidation oder einer anderen Handlung, die sich auf den Kunden auswirkt, wie durch geltendes Recht oder Vorschriften für die Finanzdienstleistungen vorgesehen (z. B, „too big to fail", „Sanierungs- und Abwicklungsprozess", „Sonderverwaltung" und ähnliche Regelungen und Maßnahmen), und in dem Umfang, der erforderlich ist, um die Kontinuität der Bereitstellung der vom Kunden gemäß Vertrag erworbenen Onlinedienste durch Microsoft aufrechtzuerhalten, und falls erforderlich, wird Microsoft dem Kunden zugestehen, seine Rechte gemäß Vertrag abzutreten, unterzulizenzieren oder zu übertragen an (A) mindestens einen seiner Partner oder (B) eine Drittpartei, die das entsprechende Geschäft oder Vermögenswerte oder Gesellschaftskapital des Kunden ganz oder teilweise erwirbt oder anderweitig nachfolgt. In jedem Fall ist die juristische Person, auf die Rechte übertragen werden, der „**Übertragungsempfänger**" und hat über die Standardprozesse und -tools von Microsoft Zugriff auf Kundendaten.

2. Vorbehaltlich des vorstehenden Abschnittes 8(b)(1) wird Microsoft weder den Vertrag kündigen noch die Erfüllung seiner Pflichten aus dem Vertrag aussetzen oder verzögern, sofern die folgenden Bedingungen erfüllt sind:

A. Der Übernehmer (oder Kunde) muss alle Gebühren und Entgelte zahlen, die der Kunde nach den Bedingungen des Vertrags an Microsoft für Dienstleistungen zu zahlen hat, die vor der Übertragung und durch die Erneuerung oder den Ersatz des Vertrags erbracht wurden.

B. Der Übertragungsempfänger und Microsoft bemühen sich in gutem Glauben, diesen Vertrag zu verlängern oder ihn gegebenenfalls durch geeignete Bedingungen zu ersetzen, damit Microsoft die Onlinedienste für den Übertragungsempfänger bereitstellen kann.

C. Wenn sich Microsoft und der Übertragungsempfänger nicht innerhalb von zwölf Monaten nach der Übertragung der Rechte auf den Übertragungsempfänger über die Bestimmungen wie in diesem Abschnitt 8(b) beschrieben einig werden, kann Microsoft diesen Vertrag durch Mitteilung an den Übertragungsempfänger kündigen.

D. Die Gesamthaftung von Microsoft und ihren Partnern gegenüber dem Kunden, den Partnern des Kunden, dem Übernehmer und dessen Partnern wird die Gesamthaftung von Microsoft und ihren Partnern gemäß Vertrag nicht übersteigen.

3. Falls der Übertragungsempfänger einen neuen Vertrag abschließen möchte, bemühen sich die Parteien angemessen darum, Bestimmungen festzulegen, die im Hinblick auf die Übertragung gemäß diesem Abschnitt 8(b) angemessen sind.

c. Kontinuität nach Beendigung oder Ablauf des Vertrags.

1. Kündigt der Kunde den Vertrag aus irgendeinem Grund oder läuft die Vertrag aus oder endet er aus einem anderen als dem in Abschnitt 8(c)(2) weiter unten genannten Grund, so kann der Kunde die Onlinedienste auf monatlicher Basis für bis zu zwölf Monate oder länger verlängern, wenn eine Regulierungsbehörde ausdrücklich schriftlich verlangt, dass Microsoft die Onlinedienste weiterhin zur Verfügung stellt, und zwar ab dem Datum der Kündigung durch eine entsprechende Mitteilung an Microsoft. Während dieses Zeitraums stellt Microsoft weiterhin die Onlinedienste gemäß den Bestimmungen des Vertrags bereit und der Kunde nutzt und bezahlt diese Onlinedienste weiterhin. Darüber hinaus kann der Kunde während dieses Zeitraums seine Kundendaten über die Standardprozesse und -tools von Microsoft abrufen. Der Abruf von Kundendaten aus den Onlinediensten in das ausgewählte System oder den ausgewählten Onlinedienst des Kunden erfolgt auf Kosten des Kunden und auf vom Kunden gewählten Wegen. Der Kunde kann sich für die Unterstützung bei der Übertragung von Kundendaten und der entsprechenden Funktion, sofern zutreffend, an die Professional Services-Organisation von Microsoft oder einen anderen Anbieter wenden. Der Kunde kann den erweiterten Dienst durch eine Kündigung an Microsoft beenden. Die Kündigung wird zum Ende des Monats wirksam, der auf die dreißig Tage folgt, nachdem die Kündigungsmitteilung bei Microsoft eingegangen ist. Nach dem Datum des Inkrafttretens der Dienststornierung unterliegt die Entfernung von Kundendaten aus den Onlinediensten den Regelungen des Abschnitts „Datenspeicherung und -löschung" des DPA.
2. Kündigt Microsoft den Vertrag aufgrund eines ungeheilten Vertragsbruchs durch den Kunden, wird Microsoft die Onlinedienste auf monatlicher Basis bis zu zwölf Monate lang oder länger ab dem Datum der Kündigung weiter zur Verfügung stellen, falls eine Regulierungsbehörde ausdrücklich schriftlich verlangt, dass Microsoft die Onlinedienste weiterhin erbringt. Während dieses Zeitraums stellt Microsoft weiterhin die Onlinedienste gemäß den Bestimmungen des Vertrags bereit und der Kunde nutzt und bezahlt diese Onlinedienste weiterhin. Darüber hinaus kann der Kunde während dieses Zeitraums seine Kundendaten über die Standardprozesse und -tools von Microsoft abrufen. Der Abruf von Kundendaten aus den Onlinediensten in das ausgewählte System oder den ausgewählten Onlinedienst des Kunden erfolgt auf Kosten des Kunden und auf vom Kunden gewählten Wegen. Der Kunde kann sich für die Unterstützung bei der Übertragung von Kundendaten und der entsprechenden Funktion, sofern zutreffend, an die Professional Services-Organisation von Microsoft oder einen anderen Anbieter wenden. Der Kunde kann den erweiterten Dienst durch eine Kündigung an Microsoft beenden. Die Kündigung wird zum Ende des Monats wirksam, der auf die dreißig Tage folgt, nachdem die Kündigungsmitteilung bei Microsoft eingegangen ist. Nach dem Datum des Inkrafttretens der Dienststornierung unterliegt die Entfernung von Kundendaten aus den Onlinediensten den Regelungen des Abschnitts „Datenspeicherung und -löschung" des DPA.

d. Umkehrbarkeit.

1. Falls der Vertrag wie in diesem Abschnitt 8 beschrieben gekündigt wird oder abläuft und der Kunde seine Kundendaten auf einen anderen Onlinedienst migrieren möchte, kann der Kunde seitens der Professional Services Organization von Microsoft zu den dann geltenden Tarifen für solche Dienste Unterstützung bei diesem Übergang anfordern.
2. Der Kunde kann jederzeit während der in Abschnitt 8(c) beschriebenen, verlängerten Servicelaufzeit Unterstützung bei der Migration oder dem Übergang sowie Unterstützung beim Abrufen seiner Kundendaten seitens der Professional Services-Organisation von Microsoft anfordern.

e. **Geschäftsfortführungs- und Notfallwiederherstellungspläne von Microsoft.** Microsoft sichert zu und gewährleistet, dass es über angemessene Pläne für Geschäftsfortführung und Notfallwiederherstellung verfügt und diese während der Dauer des Vertrags aufrechterhalten und testen wird, um den normalen Betrieb und die ordnungsgemäße Bereitstellung der Onlinedienste im Notfall und in Übereinstimmung mit den anwendbaren Gesetzen und Vorschriften wiederherzustellen. Das Geschäftsfortführungsmanagement von Microsoft unterliegt einer Prüfung und ISO 22301-Zertifizierung. Die Kontrollen, die solche Pläne unterstützen, werden zusätzlich durch ISO 27001- und SSAE 18 SOC 2 Typ II-Audits überprüft, die für jeden Onlinedienst mindestens jährlich initiiert und von qualifizierten, unabhängigen, externen Prüfern durchgeführt werden. Microsoft stellt dem Kunden über das Kunden-Compliance-Programm Informationen zur Verfügung, um die Ansätze von Microsoft für Geschäftsfortführung und Notfallwiederherstellung zu verstehen. Weitere Informationen findet der Kunde unter https://learn.microsoft.com/de-de/compliance/regulatory/offering-iso-22301 und https://learn.microsoft.com/de-de/compliance/ oder auf Nachfolgeseiten, wie von Microsoft festgelegt.

f. **Geschäftsfortführungs- und Notfallwiederherstellungspläne des Kunden.**

   1. Der Kunde ist dafür verantwortlich, seine eigenen Geschäftsfortführungs- und Betriebsresilienzpläne zu entwickeln, indem er die verfügbaren Funktionen und Merkmale der Onlinedienste nutzt. Der Kunde bleibt für das Entwerfen, Testen und Bereitstellen seiner Pläne verantwortlich. Soweit Microsoft in der Lage ist, Unterstützung zu leisten, kann Microsoft den Kunden bei der Entwicklung und dem Testen seiner Geschäftsfortführungs und Betriebsresilienzpläne unterstützen. Diese Unterstützung kann der Kunde direkt von einem Microsoft-Partner erhalten, oder sie kann über die Professional Services-Organisation von Microsoft zum jeweils aktuellen Tarif für diese Dienste oder einen Teil davon bereitgestellt werden.

   2. Der Kunde ist dafür verantwortlich, einen eigenen Plan für den ordnungsgemäßen Übergang und Ausstieg aus den Onlinediensten zu entwickeln, indem er die verfügbaren Funktionen und Merkmale der Onlinedienste nutzt. Der Kunde bleibt für seinen eigenen Plan für den ordnungsgemäßen Übergang und Ausstieg aus den Onlinediensten verantwortlich, vorausgesetzt, dass Microsoft auf Wunsch des Kunden und in dem Umfang, in dem Microsoft in der Lage ist, Unterstützung zu leisten, diesen Übergang über die Professional Services-Organisation von Microsoft zum derzeit geltenden Tarif für solche Dienste oder Teile davon unterstützen kann, um i) den Kunden bei der Entwicklung eines Plans für den ordnungsgemäßen Übergang und Ausstieg aus den Onlinediensten zu unterstützen und/oder ii) dem Kunden angemessene Unterstützung beim Testen des oben genannten Plans des Kunden zu bieten. Diese Unterstützung kann der Kunde auch direkt von einem Microsoft-Partner erhalten.

9. Sonstiges

a. **Vertraulichkeit**. Diese Zusatzvereinbarung, die Prüfungsberichte und alle damit verbundenen Informationen stellen vertrauliche Informationen von Microsoft dar. Der Kunde ist berechtigt, diese Komponenten gegenüber einem Prüfer des Kunden oder einem Berater oder einer Aufsichtsbehörde offenzulegen, vorausgesetzt, dass (1) der Kunde zunächst alle Bestimmungen unkenntlich macht, die nicht der regulatorischen Aufsicht und Genehmigung unterliegen, einschließlich Preisinformationen und Bestellmengen; und (2) der Kunde (ausgenommen Offenlegungen gegenüber einer Aufsichtsbehörde) die Vertraulichkeitsbestimmungen des Rahmenvertrags so einhält, als ob es sich um eine Offenlegung vertraulicher Informationen von Microsoft gegenüber einem Kundenvertreter handeln würde, die ausschließlich auf der Grundlage der Notwendigkeit der Kenntnisnahme und im Rahmen von Geheimhaltungsverpflichtungen erfolgen darf, die mindestens so schützend sind wie die Vertraulichkeitsbestimmungen im Rahmenvertrag zwischen dem Kunden und Microsoft. Microsoft behält sich das Recht vor, bestimmte Informationen als vertrauliche Informationen festzulegen, die der Kunde auch bei Abschluss einer Vertraulichkeitsvereinbarung nicht ohne vorherige schriftliche Zustimmung von Microsoft weitergeben darf.

b. Laufzeit und Kündigung. Vorbehaltlich der Abschnitte 8(c) und 8(d) weiter oben endet diese Zusatzvereinbarung automatisch mit jeder Kündigung oder jedem Ablauf des Vertrags.

c. Konflikt und Koordination. Mit Ausnahme von Änderungen, die durch diese Zusatzvereinbarung vorgenommen werden, bleibt der Vertrag unverändert und vollständig wirksam. Bei Konflikten zwischen einer Bestimmung in dieser Zusatzvereinbarung und einer Bestimmung im Vertrag hat diese Zusatzvereinbarung Vorrang. Für den Fall, dass der Kunde Onlinedienste von Microsoft oder einem Microsoft-Partner separat erworben hat, gelten die in diesem Zusatz vorgesehenen Rechte und Pflichten in Bezug auf die Prüfungsrechte des Kunden, die Prüfungsrechte seiner Aufsichtsbehörden und andere Anforderungen des Kunden zur Einhaltung von Vorschriften in den Abschnitten 2, 3 und 4 dieses Zusatzes.

d. Angemessene Versicherung. Microsoft erhält durch eine kommerzielle Versicherung, Bildung von Rücklagen, eine Kombination aus beiden oder durch eine andere ähnliche, das Risiko finanzierende Alternative angemessenen Versicherungsschutz aufrecht. Auf Anfrage kann Microsoft dem Kunden einen Nachweis über diesen Versicherungsschutz zur Verfügung stellen.

Gerichtsstandsspezifische Zusatzvereinbarung zu Companion (Deutschland)

Die Geschäftsbestimmungen dieser Zusatzvereinbarung zu Companion ergänzen die in der Zusatzvereinbarung zu Finanzdiensten im Microsoft-Kundenvertrag („**FSA**") genannten Bestimmungen, die für die Nutzung der Onlinedienste durch den Kunden gelten („**Zusatzvereinbarung zu Companion**"). Der Kunde unterliegt der Aufsicht einer Finanzdienstleistungsaufsichtsbehörde in Deutschland sowie den Konformitäts- und regulatorischen Anforderungen Deutschlands. Alle in dieser Begleitvereinbarung verwendeten Begriffe, die hierin nicht definiert sind, haben dieselbe Bedeutung, die in der FSA für sie festgelegt wurde. Soweit die Bestimmungen dieser Zusatzvereinbarung zu Companion mit den Bestimmungen des FSA in Konflikt stehen, haben die Bedingungen dieser Zusatzvereinbarung zu Companion Vorrang, soweit der Kunde oder der Klient der Aufsicht einer Finanzaufsichtsbehörde in Deutschland unterliegt.

Die folgenden Begriffe werden dem FSA in den jeweiligen Abschnitten hinzugefügt wie unten angegeben:

1. Definierte Begriffe

1.1 Die folgende Definition wird Ziffer 1 („Definierte Begriffe") der FSA hinzugefügt:

„**Kunde**" bezeichnet den Kunden des Kunden, der der behördlichen Aufsicht oder Aufsichtsbehörde durch eine Regulierungsbehörde unterliegt.

1.2 Die Definition des Begriffs „Regulierungsbehörde" in Abschnitt 1 („Definierte Begriffe") des FSA wird gänzlich gestrichen und durch Folgendes ersetzt:

Aufsichtsbehörde bezeichnet eine Aufsichts- oder Verhaltensaufsichtsbehörde für Finanzdienstleistungen mit Aufsichts-, Vergleichs- oder Abwicklungsrechten nach geltendem Recht oder geltenden Vorschriften, einschließlich der Verwahrstelle im Sinne der Richtlinie 2011/61/EU, gegenüber dem Kunden oder Microsoft im Zusammenhang mit der Nutzung der Onlinedienste durch Kunden oder Klienten.

2. Unterstützung der Kunden-Compliance

2.1 Abschnitt 2.a („Allgemeines Zugriffsrecht") des FSA wird gänzlich gelöscht und durch Folgendes ersetzt:

a. **Kundenzugriff auf Daten.** Der Kunde hat jederzeit direkt Zugriff auf Kundendaten, einschließlich der in den Onlinediensten bereitgestellten virtuellen Computer und Anwendungen. Die Nutzung der Onlinedienste erfolgt auch in Übereinstimmung mit dem zugrunde liegenden Microsoft-Kundenvertrag (einschließlich DPA, Produktbestimmungen, insbesondere Datenschutz- und Sicherheitsbestimmungen sowie anderer Bestimmungen, die durch Bezugnahme darin enthalten sind).

2.2 Abschnitt 2.c („Prüfungen von Onlinediensten durch Microsoft") des FSA wird gänzlich gelöscht und durch Folgendes ersetzt:

c. **Prüfungen von Onlinediensten durch Microsoft**. Für jeden Onlinedienst veranlasst Microsoft die Durchführung von Prüfungen bezüglich der Sicherheit der Computer, Datenverarbeitungsumgebungen und physischen Rechenzentren, die sie zur Verarbeitung von Kundendaten (einschließlich personenbezogener Daten) verwendet. Diese Überprüfungen werden alle zwölf Monate von Microsoft initiiert und von qualifizierten unabhängigen externen Prüfern durchgeführt. Die Prüfungen bestehen aus jährlichen Prüfungen anhand des „Cloud Computing Compliance Controls Catalogue" („C5") des Bundesamtes für Sicherheit in der Informationstechnik („BSI") in der Fassung vom April 2020. Jede Prüfung führt zur Erstellung eines Microsoft-Prüfberichts, wie in der DPA festgelegt, und wird dem Kunden über das Dienstvertrauensstellungsportal (Service Trust Portal; https://servicetrust.microsoft.com/ oder eine von Microsoft definierte Nachfolgewebsite) zur Verfügung gestellt.

2.3 Abschnitt 2.d („Logische Trennung") des FSA wird gänzlich gelöscht und durch Folgendes ersetzt:

ci. **Logische Trennung.** Microsoft verwendet bei der Speicherung und Verarbeitung von Kundendaten eine logische Trennung, um eine Vermischung dieser Daten mit den Daten anderer Microsoft-Kunden zu verhindern und die gegenseitige Abschirmung (keine Zugriffs- und Änderungsrechte) der für die jeweiligen Kunden gespeicherten und verarbeiteten Daten zu gewährleisten.

2.4 Am Ende von Abschnitt 2 („Durchsetzung der Einhaltung von Vorschriften durch Kunden") des FSA werden folgende Bestimmungen als neue Abschnitte 2.f bis 2.k. hinzugefügt:

f. **Kontrolle der Nutzung von Onlinediensten durch Weisung**. Der Kunde kontrolliert die Nutzung der Onlinedienste durch eigene Anweisungen, die über die Nutzung und Konfiguration von Funktionen und Verwaltung in den Onlinediensten oder anderweitig gemäß den Vereinbarungen erteilt werden, wobei ein Eingreifen von Microsoft nicht erforderlich ist. Die Weisungsrechte des Kunden sind auch in Übereinstimmung mit den zugrunde liegenden Volumenlizenzverträgen des Kunden (einschließlich DPA, Produktbestimmungen, insbesondere Datenschutz- und Sicherheitsbestimmungen und anderer Bestimmungen, die durch Bezugnahme darin enthalten sind). Weitere Weisungsrechte richten sich nach den nachfolgenden Kapiteln und dem DPA.

g. **Informationssicherheitsrichtlinie für Onlinedienste**. Wie im DPA und in den Produktbestimmungen, insbesondere den Datenschutz-. und Sicherheitsbestimmungen ausgeführt, gilt für jeden Onlinedienst eine schriftliche zentrale Datensicherheitsrichtlinie („Informationssicherheitsrichtlinie"), die bestimmte Kontrollstandards und Rahmenbestimmungen einhält. Microsoft stellt den Kunden diese Informationssicherheitsrichtlinie zusammen mit Beschreibungen der Sicherheitskontrollen für den jeweiligen Onlinedienst und anderen vom Kunden vernünftigerweise angeforderten Informationen zu Microsoft-Sicherheitspraktiken und -richtlinien über das Service Trust Portal (https://servicetrust.microsoft.com/ oder eine von Microsoft festgelegte Nachfolgewebsite) zur Verfügung.

h. **Informationen über Ereignisse**. Microsoft stellt dem Kunden unverzüglich Mitteilungen zur Verfügung über (1) die Art, häufige Ursachen und Lösungen von Sicherheitsvorfällen und andere Umstände, bei denen davon ausgegangen werden kann, dass sie einen wesentlichen Einfluss auf die Nutzung der Onlinedienste durch den Kunden haben, über (2) Risikobedrohungsbewertungen von Microsoft und über (3) wesentliche Änderungen bzgl. Microsofts Geschäftswiederaufnahme- und Krisenpläne oder andere Umstände, die einen wesentlichen Einfluss auf die Nutzung der Onlinedienste durch den Kunden haben könnten. Dies gilt zusätzlich zu verschiedenen Funktionen, die bereits in den Onlinediensten bereitgestellt werden.

i. **Informationen zu Verfügbarkeit und Sicherheit**. Microsoft berichtet dem Kunden kontinuierlich über die aktuelle Verfügbarkeit der Onlinedienste durch eine genaue Darstellung der jeweiligen Dienstverfügbarkeit in einem „Dienststatus-Dashboard" des Kunden (oder durch funktional gleichwertige Nachfolgeberichte). Microsoft stellt kontinuierlich einen Informationsfeed für Ergebnisse des Sicherheitsinformations- und Ereignismanagements (SIEM) über verschiedene kundenseitige Portale in den Onlinediensten und auch über eine Verwaltungs-API bereit, die von Drittanbietersoftware verwendet werden kann, die der Kunde optional erwerben und betreiben kann.

j. **Angemessenes Geschäftsverhalten**. Microsoft hat einen individuellen Verhaltenskodex für angemessenes Geschäftsverhalten eingeführt, beispielsweise ethische Geschäftspraktiken und die Einhaltung gesetzlicher Vorschriften. Den aktuellen Verhaltenskodex von Microsoft („Microsoft Standards of Business Conduct") finden Sie hier: https://www.microsoft.com/en-us/legal/compliance/sbc/ (oder auf einer von Microsoft ausgewählten Nachfolgewebsite).

k. **Nachhaltigkeit**. Microsoft verfolgt Nachhaltigkeitsziele, die regelmäßig in einem „Umweltschutz- und Nachhaltigkeitsbericht" zusammengefasst und veröffentlicht werden. Den Bericht finden Sie hier: https://www.microsoft.com/en-us/corporate-

responsibility/sustainability/report (oder auf einer von Microsoft ausgewählten Nachfolgewebsite).

3. Uneingeschränkte Rechte auf Zugriff, Untersuchung und Audit durch die Regulierungsbehörde

3.1 Der Titel von Abschnitt 3 „Uneingeschränkte Untersuchungs- oder Prüfungsrechte der Aufsichtsbehörde" des FSA wird gänzlich gelöscht und durch Folgendes ersetzt:

„Uneingeschränktes Recht auf Zugang, Untersuchung und Prüfung durch die Aufsichtsbehörde".

3.2 In Abschnitt 3.a des FSA wird der erste Satz vollständig gelöscht und durch Folgendes ersetzt:

Für den Fall, dass die Aufsichtsbehörde eine Untersuchung oder Prüfung der Abläufe und Kontrollen der Onlinedienste verlangt, um die Aufsichtspflichten der Aufsichtsbehörde, unter anderem die Prüfung oder Untersuchung von Microsoft als direktem Dienstanbieter des Kunden oder indirektem Dienstanbieter von Klienten, zu erfüllen, gewährt Microsoft der Aufsichtsbehörde ein uneingeschränktes Recht zur Untersuchung oder Prüfung der Onlinedienste.

3.3 Am Ende von Abschnitt 3.a des FSA wird folgende Bestimmung hinzugefügt:

Diese Tätigkeiten werden unter der Koordination und Aufsicht von Microsoft und ohne Beschränkung auf die Bestimmungen dieses Zusatzes durchgeführt.

3.4 Abschnitt 3.d des FSA wird hiermit gänzlich gestrichen und durch Folgendes ersetzt:

d. Microsoft stimmt zu, mit Regulierungsbehörden für die Zwecke der Aufsichtstätigkeiten der Regulierungsbehörde zusammenzuarbeiten, einschließlich wenn der Kunde die Onlinedienste direkt von Microsoft lizenziert oder wenn der Kunde eine Drittanbieterlösung lizenziert, die Onlinedienste nutzt, bzw. wenn die Regulierungsbehörde in Bezug auf Klienten agiert. Microsoft und der Kunde bestätigen, dass mit den Bestimmungen in Bezug auf das Recht der Aufsichtsbehörde auf Untersuchung nicht beabsichtigt wird, anwendbaren Gesetzen oder Vorschriften zuwiderzuhandeln oder ihre Ausführung zu beeinträchtigen, und dass keine Bestimmung in diesem Abschnitt dahingehend ausgelegt werden darf, die Aufsichtsbehörde bei der Untersuchung der Onlinedienste zu behindern.

3.5 Abschnitt 3.g des FSA wird hiermit gänzlich gestrichen und durch Folgendes ersetzt:

g. Microsoft erklärt sich bereit, mit den Aufsichtsbehörden des Kunden zusammenzuarbeiten, einschließlich der Möglichkeit, dass die Aufsichtsbehörden Fragen zum Zwecke der Aufsicht direkt an Microsoft richten können. Microsoft wird die besagte Zusammenarbeit gemäß den Bestimmungen dieser Zusatzvereinbarung leisten.

3.6 Am Ende von Abschnitt 3 des FSA wird folgende Regelung als neuer Abschnitt 3.h angefügt:

h. Aus Gründen der Klarheit: Die Parteien erkennen die Befugnisse der Aufsichts- und Abwicklungsbehörde insbesondere gemäß Art. 63 Abs. 1 a), 68 und 71 der Richtlinie 2014/59/EU und Art. 65 Abs. 3 der Richtlinie 2013/36/EU und der jeweiligen nationalen Gesetzgebung, die die genannte Richtlinie umgesetzt hat.

4. Uneingeschränkte Rechte auf Zugriff, Untersuchung und Audit durch den Kunden

4.1 Der Titel von Abschnitt 4 „Uneingeschränkte Prüfungsrechte des Kunden" des FSA wird gänzlich gelöscht und durch Folgendes ersetzt:

„Uneingeschränkte Rechte auf Zugang, Untersuchung und Prüfung durch den Kunden".

4.2 In Abschnitt 4.a des FSA wird folgender Satz gänzlich gestrichen:

„Die Ausübung dieser Rechte unterliegt dem Grundsatz der Verhältnismäßigkeit in Bezug auf die Kritikalität dieser Onlinedienste bei der Ausübung wesentlicher Funktionen des Kunden."

4.3 Abschnitt 4.b des FSA wird hiermit gänzlich gestrichen und durch Folgendes ersetzt:

b. **Umfang der Prüfung durch den Kunden.** Der Kunde hat das Recht, bei sich selbst, seinen regulierten Partnern, den Kundenprüfern, der Regulierungsbehörde oder einem externen Prüfer auf alle Informationen zuzugreifen, die erforderlich sind, um die Einhaltung der einschlägigen rechtlichen Verpflichtungen zu gewährleisten und sicherzustellen, dass:

1. Die Onlinedienste entsprechen den Produktbedingungen, dem DPA und dieser Zusatzvereinbarung.
2. die Vereinbarungen zum Servicelevel eingehalten werden;
3. die Integrität und Vertraulichkeit der Kundendaten in Übereinstimmung mit den Geschäftsbestimmungen des DPA und dieses Zusatzes geschützt werden und
4. Die dem Kunden zur Verfügung gestellten Onlinedienste sicher sind.

4.4 Abschnitt 4.c.1 des FSA wird hiermit gänzlich gestrichen und durch Folgendes ersetzt:

1. Nach angemessener schriftlicher Vorankündigung gestattet Microsoft dem Kunden die Durchführung einer Kundenprüfung der Geschäftsräume von Microsoft und der vom Kunden genutzten Onlinedienste. Datum, Uhrzeit und Ort der Kundenprüfung werden einvernehmlich zwischen dem Kunden und Microsoft vereinbart. Dies kann auch die Prüfung von Zulieferern einschließen, die die Leistungen des Onlinedienstes bieten und vollbringen. Diese Tätigkeiten werden unter der Koordination und Aufsicht von Microsoft und vorbehaltlich aller Bestimmungen dieses Zusatzes durchgeführt. Aus Gründen der Klarheit: In diesem Absatz soll nicht das Recht des Kunden auf Prüfung eingeschränkt werden, und Microsoft bestätigt, dass ein Vertrag über Datum, Uhrzeit und Ort der Prüfung unter Berücksichtigung des Umfangs und der Gründe für die Anforderung der Prüfung nicht unangemessen zurückgehalten oder verzögert wird, dass in einer Not- oder Krisensituation eine begrenzte vorherige angemessene Benachrichtigung möglich ist und dass eine solche Terminplanung nicht dazu verwendet wird, das Ziel der Prüfung zu gefährden.

4.5 Abschnitt 4.c.2 des FSA wird hiermit gänzlich gestrichen und durch Folgendes ersetzt:

2. Der Kunde erklärt sich damit einverstanden, dass er die Microsoft im Zusammenhang mit der Kundenprüfung entstandenen Kosten auf der Grundlage eines Tagessatzes für jeden Microsoft-Mitarbeiter zuzüglich angemessener Reisekosten trägt. Diese Kosten werden in einer Leistungsbeschreibung ausgewiesen. Eine Microsoft-Engineering-Quelle, die nur für einen Teil eines einzigen Tags benötigt wird, wird dem Kunden anteilig in Rechnung gestellt. Microsoft berechnet nur Gebühren für Leistungen, die nach Zeitsätzen erbracht werden. Außerdem berechnet Microsoft keine Gebühren für administrative Tätigkeiten, die von Microsoft-Mitarbeitern ausgeübt werden, wie die Organisation von Meetings, die Begleitung von Besuchern oder das Kopieren von Unterlagen. Falls es Streitigkeiten über Kosten im Zusammenhang mit einer Kundenprüfung gibt, werden die Parteien die Angelegenheit an ihre zuständigen Führungskräfte zwecks Schlichtung weiterleiten.

4.6 Abschnitt 4.c.3.d des FSA wird hiermit gänzlich gestrichen und durch Folgendes ersetzt:

d. Die Kundenprüfung wird in Übereinstimmung mit den sicherheitsbezogenen Richtlinien und Verfahren von Microsoft durchgeführt, um die Integrität und Sicherheit der beteiligten Personen zu gewährleisten und die Sicherheit und Vertraulichkeit der Kundendaten aller Microsoft-Kunden zu schützen, ohne die Rechte des Kunden einzuschränken.

4.7 Am Ende von Abschnitt 4.c.3 des FSA wird folgende Regelung als neuer Abschnitt 4.c.3.g angefügt:

g. **Gruppen- oder Pool-Prüfungen.** Der Kunde kann sich dafür entscheiden, Microsoft als Mitglied einer Gruppe mit anderen beaufsichtigten Microsoft-Kunden zu prüfen. Für diese

Gruppenprüfung gelten die zwischen der Gruppe und Microsoft vereinbarten Teilnahmeregeln für den Kunden. Die Lösung wesentlicher Abweichungen durch Microsoft, die im Rahmen von Gruppen- oder Pool-Prüfungen entdeckt wurden, wird zwischen Microsoft und der Gruppe vereinbart, und dies ist die einzige Lösung des Kunden für solche Abweichungen im Rahmen der Prüfung. Das Vorstehende soll nicht a) den Kunden daran hindern, eine unabhängige Lösung angeblicher technischer oder vertraglicher Nichtübereinstimmungen in Bezug auf seine Nutzung der Onlinedienste zu beantragen; oder b) den Kunden daran hindern, von Microsoft Lösungen für Probleme zu erhalten, die von Aufsichtsbehörden gemäß Abschnitt 3 aufgeworfen werden.

4.8 Abschnitt 4.c.4 des FSA wird gänzlich und ersatzlos gestrichen.

4.9 Am Ende von Abschnitt 4 des FSA wird folgende Regelung als neuer Abschnitt 4.d angefügt:

d. Um Zweifel auszuschließen: Dieser Abschnitt 4 „Uneingeschränkte Rechte auf Zugriff, Untersuchung und Audit durch den Kunden" soll nicht dazu dienen, den Kunden im Vergleich zu den Rechten einer Aufsichtsbehörde weniger vorteilhaft zu behandeln.

5. Zusätzliche Kundenvorteile

5.1 Abschnitt 5.a des FSA wird hiermit gänzlich gestrichen und durch Folgendes ersetzt:

a. Für den Fall, dass die Aufsichtsbehörde neue oder aktualisierte Leitlinien veröffentlicht, die sich auf die Onlinedienste beziehen, wird Microsoft auf schriftliche Anfrage des Kunden eine schriftliche Antwort auf diese Leitlinien angemessen vorbereiten, einschließlich der Art und Weise (und des Umfangs), wie die Onlinedienste die Leitlinien entweder durch bestehende Funktionen, geplante Änderungen am Leitplan für die Onlinedienste oder Änderungen an diesem Zusatz berücksichtigen.

5.2 Am Ende des Abschnitts 5.b des FSA wird folgender zusätzlicher Satz hinzugefügt:

Wenn dem Antrag von Microsoft nach vernünftigen Gesichtspunkten nicht stattgegeben werden kann, übermittelt Microsoft dem Kunden eine schriftliche Begründung für die Ablehnung des Antrags.

5.3 Abschnitt 5.d des FSA wird hiermit gänzlich gestrichen und durch Folgendes ersetzt:

d. Microsoft stellt sicher, dass ihre Verträge mit Vertragspartnern, die in ihrem Namen bestimmte eingeschränkte oder ergänzende Dienste für die Bereitstellung der Onlinedienste erbringen, Bestimmungen enthalten, die diese Vertragspartner verpflichten, alle Gesetze und behördlichen Anforderungen einzuhalten, die für die ausgelagerten Onlinedienste relevant sind und von Microsoft gemäß der DPA verlangt werden. Microsoft stellt sicher, dass die Verträge mit solchen Vertragspartnern im Einklang mit den vertraglichen Vereinbarungen zwischen Microsoft und dem Kunden für die Onlinedienste stehen und dass die Zugriffs-, Untersuchungs- und Prüfungsrechte des Kunden und der Regulierungsbehörde gemäß den Abschnitten 2, 3 und 4 dieser Zusatzvereinbarung durch die Vergabe von Unteraufträgen nicht beeinträchtigt werden und in vollem Umfang auf derartige Vertragspartner ausgedehnt werden. Bei der Bereitstellung der Onlinedienste verpflichtet sich Microsoft, diese Vertragspartner in dem Umfang zu beaufsichtigen, der zur Erfüllung der im Rahmen des DPA und dieser Zusatzvereinbarung für Microsoft geltenden Verpflichtungen erforderlich ist. Microsoft ist für die Handlungen und Unterlassungen dieser Vertragspartner verantwortlich und haftet so, als wären es die eigenen Handlungen und Unterlassungen.

5.4 Am Ende von Abschnitt 5 des FSA werden folgende Bestimmungen als neue Abschnitte 5.e und 5.f angefügt:

e. Im Rahmen der Bereitstellung von Microsoft-Onlinediensten gemäß Definition im FSA kann Microsoft auch zusätzliche Drittanbieter beauftragen, die Microsoft bestimmte Funktionen anbieten, die für ihre Kunden als wesentlich oder wichtig erachtet werden können („Wichtige Anbieter"). Diese wichtigen Anbieter sind eine Ergänzung zur Liste der Microsoft-Unterauftragsverarbeiter (https://servicetrust.microsoft.com/) und von diesen getrennt. Sie sind

in der Liste „Wichtige Drittanbieter für Microsoft-Onlinedienste" von Microsoft aufgeführt. Vorbehaltlich der Bestimmungen in diesem Absatz 5.e hätte ein Leistungsausfall eines wichtigen Anbieters keine Auswirkungen auf die Fähigkeit von Microsoft, Microsoft-Onlinedienste in Übereinstimmung mit den geltenden Vereinbarungen zum Servicelevel bereitzustellen. Microsoft wird in Zukunft möglicherweise auch neue wichtige Anbieter einsetzen. Sollte Microsoft einen neuen wichtigen Anbieter einsetzen, dessen Leistungsausfall die Fähigkeit von Microsoft beeinträchtigen würde, Microsoft-Onlinedienste im Einklang mit geltenden Vereinbarungen zum Servicelevel bereitzustellen (einen „Microsoft Material Sub-Outsourcer"), wird Microsoft den Kunden mindestens 30 Tage im Voraus über die Nutzung eines Microsoft Material Sub-Outsourcers benachrichtigen. Wenn der Kunde einen neuen Microsoft Material Sub-Outsourcer zur Verwendung in einem Onlinedienst ablehnt, ist der Kunde berechtigt, jedes Abonnement für den betroffenen Core-Onlinedienst ohne Strafe oder Gebühr für die Kündigung zu kündigen, indem er vor Ablauf der entsprechenden Kündigungsfrist eine schriftliche Kündigung einreicht. Nach der Kündigung wird Microsoft Zahlungsverpflichtungen für Abonnements oder andere anwendbare, unbezahlte Arbeiten für die gekündigten Produkte aus nachfolgenden Rechnungen an den Kunden oder seinen Handelspartner entfernen.

Der Kunde kann Fragen bezüglich der Kategorisierung der beteiligten Vertragspartner für bestimmte Verwendungszwecke der Dienste an Microsoft richten.

f. **Ernennung eines Prozessvertreters**. Der Kunde erkennt an und stimmt zu, dass die Microsoft Corporation die Microsoft Deutschland GmbH, Walter-Gropius-Straße 5, 80807 München, Deutschland, als ihren inländischen Zustellungsbevollmächtigten gemäß § 25b (3) Satz 4 Kreditwesengesetz (KWG) benannt hat, an den Mitteilungen und Zustellungen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) erfolgen können. Darüber hinaus fungiert die Microsoft Deutschland GmbH gemäß Abschnitt 25b(3) Satz 4 KWG im Namen ihrer Sub-Outsourcer als Zustellungsbevollmächtigter für Mitteilungen, die sie von der BaFin erhält und die (i) für den jeweiligen externen Sub-Outsourcer der Microsoft Corporation bestimmt sind, der seinen Sitz in einem Drittland außerhalb des Europäischen Wirtschaftsraums hat, (ii) dieser externe Sub-Outsourcer wichtige oder kritische Funktionen im Zusammenhang mit der Bereitstellung der im Rahmen der Microsoft-Kundenvereinbarung des Kunden erworbenen Onlinedienste wahrnimmt und (iii) dieser externe Sub-Outsourcer keinen anderen Zustellungsbevollmächtigten in Deutschland benannt hat, der die von der BaFin übermittelten Mitteilungen direkt entgegennimmt. Zur Klarstellung: Dies betrifft die Bereitstellung von Onlinediensten, die in den entsprechenden Produktbestimmungen als „Kerndienste" bezeichnet werden. Zur Klarstellung: Für die jeweiligen Pflichten zur Bestellung von Prozessbevollmächtigten gemäß Abschnitt 26 (1) Satz 5 ZAG (*Gesetz über die Beaufsichtigung von Zahlungsdiensten*), Abschnitt 32 (4) Satz 3 VAG (*Gesetz über die Beaufsichtigung der Versicherungsunternehmen*), Abschnitt 40 (2) Satz 2 WpIG (Wertpapierinstitutsgesetz) und Abschnitt 36 (1) Satz 1 Nr. 7 KAGB (*Kapitalanlagegesetzbuch*) gelten die vorstehenden Regelungen dieses Absatzes entsprechend der Beaufsichtigung der Versicherungsunternehmen.

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.