

**Zusatzvereinbarung der Verpflichtungen aufgrund der  
Verordnung (EU) Nr. 2022/2554 des Europäischen Parlaments  
und des Rates vom 14. Dezember 2022 über die digitale operationale  
Resilienz des Finanzsektors (DORA)**

durch die

**XXXXX**

(als „Lieferant“)

mit der

**XXXXX**

(als „Kunde“)

- Kunde und Lieferant werden im Folgenden einzeln als "Partei" oder gemeinsam als "Parteien" bezeichnet.

## Präambel

Diese Zusatzvereinbarung dient der Erfüllung der Mindestanforderungen aus DORA und ist zwischen den Parteien dahingehend auszulegen.

*Bemerkung: Wir möchten darauf hinweisen, dass aus Gründen der leichteren Lesbarkeit auf diesen Seiten die männliche Sprachform verwendet wird. Sämtliche Aussführungen gelten natürlich in gleicher Weise für die weibliche.*

## 1. Zweck der Zusatzvereinbarung

- (A) Die Parteien schlossen folgende/n Vertrag/Verträge:  
**VERTRAG ##### vom ##.##.####** (im Folgenden jeweils „Vertrag“ oder „Verträge“),
- (B) Der Lieferant erbringt IKT-Dienstleistungen für den Kunden, der gemäß der Verordnung (EU) Nr. 2022/2554 („DORA“) als Finanzunternehmen gilt und daher in Bezug auf die nach dem Vertrag erbrachten Dienstleistungen unter die entsprechenden Verpflichtungen fällt. Der Kunde ist verpflichtet, Anforderungen aus der DORA auf seine IKT-Dienstleister zu überbinden.
- (C) Daher schließen die Vertragsparteien diese Zusatzvereinbarung ab, um den Anforderungen aus der DORA zu genügen. Diese Zusatzvereinbarung ergänzt die Bestimmungen in dem Vertrag/den Verträgen.
- (D) Die in dieser Zusatzvereinbarung verwendeten Begriffe haben, sofern hierin nicht anders definiert, die in DORA festgelegte Bedeutung.
- (E) Im Anhang befinden sich (*Checkliste bei Bedarf*)
  - (i) #####
  - (ii) #####
  - (iii) #####
  - (iv) #####

*Die Anhänge i - iv gelten für den Fall, dass der Hauptvertrag keine entsprechenden Elemente enthält.*

## 2. Festlegung der Kritikalität gemäß Artikel 8 (5) und 28 (4) a und c DORA

Nach der Unternehmensrisikobewertung des Kunden handelt es sich bei den erbrachten Leistungen des Lieferanten nicht um solche, die nach Artikel 8 (5) und 28 (4) a und c DORA als kritisch oder wichtig im Sinn von Artikel 3 Ziffer 22 eingestuft werden.

Daher vereinbaren der Kunde und der Lieferant das Folgende:

*Weitere Ausführungen je nach Vertragsinhalt.*

### 3. Definitionen

Es gelten die Begriffsbestimmungen gemäß Artikel 3 der Verordnung (EU) Nr. 2022/2554.

"DORA" bezeichnet die Verordnung (EU) Nr. 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale Robustheit des Finanzsektors.

"Kundendaten" sind alle im Eigentum des Kunden befindlichen Daten/Informationen (einschließlich personenbezogener Daten), die der Lieferant im Auftrag des Kunden im Zusammenhang mit der Erbringung der IKT-Dienstleistungen erhält, verarbeitet, speichert, abruft oder erstellt.

### 4. Beschreibung der IKT Dienstleistung gemäß Art. 30 Abs. 2 lit. a und der Dienstleistungsgüte gemäß Art. 30 Abs. 2 lit. e DORA

Die IKT-Dienstleistung und Beschreibungen der Dienstleistungsgüte, einschließlich Aktualisierungen und Überarbeitungen des Lieferanten, werden in folgenden Verträgen dargelegt:

- \_\_\_\_\_
- \_\_\_\_\_

*Hinweis: Verweis auf ein SLA wenn abgeschlossen, sonst auf den Vertrag.*

### 5. Orte der Leistungserbringung und der Kundendatenverarbeitung gemäß Art. 30 Abs. 2 lit. b DORA

#### 5.1. Zulässige Standorte

Die Durchführung der Leistungen sowie die Verarbeitung der Daten einschließlich ihrer Speicherung erfolgt durch den Auftragnehmer und gegebenenfalls durch seine Unterauftragnehmer ausschließlich an den im Vertrag/in den Verträgen aufgeführten Standorten.

*Hinweis: Wenn nicht im Hauptvertrag angeführt, dann hier zusätzlich anführen.*

Die IKT-Dienstleistungen werden von folgender Region aus erbracht

- **EWR**

*Hinweis: Sofern Leistungen außerhalb EWR erbracht werden, ist die Einhaltung der DSGVO zu gewährleisten. Bei unterschiedlichen Standorten wird eine tabellarische Auflistung empfohlen.*

Die Kundendaten werden in folgendem Land verarbeitet und gespeichert

- **EWR**

*Hinweis: Sofern Leistungen außerhalb EWR erbracht werden, ist die Einhaltung der DSGVO zu gewährleisten. Bei unterschiedlichen Standorten wird eine tabellarische Auflistung empfohlen.*

## 5.2. Änderungen der zulässigen Standorte

Der Lieferant teilt dem Kunden mindestens **XX** Tage im Voraus schriftlich mit, wenn er beabsichtigt, einen Standort der Leistungserbringung zu wechseln oder einen zusätzlichen Standort zur Leistungserbringung zu eröffnen.

## 6. Bestimmungen über Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit in Bezug auf den Datenschutz gemäß Art. 30 Abs. 2 lit. c DORA

Die Bestimmungen über Verfügbarkeit, Authentizität, Integration und Vertraulichkeit in Bezug auf den Datenschutz (einschließlich personenbezogener Daten) sind in den bestehenden Verträgen geregelt.

- Vertrag XYZ

*Hinweis: Verträge anführen, z.B. Auftragsverarbeitungsvertrag AVV*

**6.1.** In Bezug auf die Erbringung der IKT-Dienstleistungen ergreift der Lieferant an seinen Standorten / in seiner Einflusssphäre angemessene Maßnahmen zur Informationssicherheit sowie zur physischen und umgebungsbedingten Sicherheit, um die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit in Bezug auf den Schutz von Kundendaten, Informationsvermögen, IKT-Assets des Kunden und Zugangskontrollvorrichtungen zu gewährleisten.

- 6.1.1.** Die Sicherheitsmaßnahmen gemäß Punkt 6.1 umfassen folgende Punkte:
- Einsatz von IKT-Lösungen und -Prozessen, die
- a. die Sicherheit der  Datenübertragung /  des Datenübertragungsmittels gewährleisten,
  - b. das Risiko der Beschädigung oder des Verlusts von Daten, des unbefugten Zugriffs und technischer Mängel, die die Geschäftstätigkeit des Kunden beeinträchtigen könnten, minimieren,
  - c. mangelnde Verfügbarkeit, die Beeinträchtigung der Authentizität und Integrität, die Verletzung der Vertraulichkeit und den Verlust von Daten verhindern,
  - d. den Schutz der Daten vor Risiken aus der Datenverwaltung (einschließlich schlechter Verwaltung, verarbeitungsbedingter Risiken und menschlicher Fehler) gewährleisten.

## 7. Zugang zu Kundendaten gemäß Art. 30 Abs. 2 lit. d DORA

Unbeschadet einer allenfalls bestehenden Datenschutzvereinbarung zwischen den Vertragsparteien wird der Lieferant im Falle von Insolvenz, Abwicklung oder Einstellung seiner Geschäftstätigkeit dem Kunden ohne Verzögerung Zugriff zu den in seinem Besitz befindlichen Daten des Kunden gewähren sowie die Wiederherstellung und Rückgabe der Daten in einem allgemein lesbaren digitalen Format gewährleisten.

## 8. Zusammenarbeit mit der Aufsichtsbehörde Art. 30 Abs. 2 lit. g DORA

Der Lieferant und seine Mitarbeiter werden mit der für den Kunden zuständigen Aufsichtsbehörde, einschließlich der von dieser benannten Personen, in Bezug auf den Vertrag und/oder dessen Gegenstand uneingeschränkt zusammenarbeiten.

## 9. Programme und Schulungen gemäß Art. 30 Abs. 2 lit. i DORA

Gemäß Artikel 30 (2) vereinbaren die Parteien, dass das Personal des Lieferanten nach Aufforderung durch den Kunden an Programmen des Kunden zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz laut Artikel 13 (3) teilnimmt, sofern

- die handelnden Personen Zugang zu den Systemen des Kunden haben,
- durch die Schulung zusätzliche Fertigkeiten oder Erkenntnisse erlangen können,
- im Rahmen ihrer Tätigkeit für den Lieferanten eine derartige Schulung nicht erfolgt ist und
- die Kosten vom Kunden getragen werden.

Bestätigungen der erfolgten Schulungen können bei Bedarf vom Kunden angefordert werden.

Der Kunde und der Lieferant können in einem zusätzlichen Vertrag vereinbaren, dass

- nur bestimmte Mitarbeiter oder Arten/Gruppen von Mitarbeitern an einer solchen Schulung teilnehmen;
- der Lieferant eine entsprechende Schulung für seine Mitarbeiter durchführt.

Folgende Vereinbarungen wurden getroffen:

**XXX (konkrete Vereinbarung oder Referenz auf zusätzlichen Vertrag)**

## 10. Prüfung der digitalen operationalen Resilienz des Kunden gemäß Artikel 24 bis 27 DORA

Auf Verlangen und Kosten des Kunden wird der Lieferant am Programm zum Testen der digitalen Betriebsfestigkeit des Kunden (einschließlich Krisenkommunikation) teilnehmen. Dies umfasst auch die IKT-Assets des Lieferanten, die zur Unterstützung der IKT-Dienste dienen, sowie die Zusammenarbeit mit beteiligten Dritten. Die Teilnahme und Zusammenarbeit erfolgt insbesondere dann, wenn der Kunde berechtigterweise feststellt, dass dies zur Sicherstellung der Einhaltung geltender Gesetze erforderlich ist, oder wenn die Aufsichtsbehörde eine solche Teilnahme anordnet oder empfiehlt.

Der Lieferant ist verpflichtet, dem Kunden im Voraus einen Stundensatz für die geplanten Leistungen mitzuteilen und ihn rechtzeitig bei der Planung der benötigten Ressourcen zu unterstützen.

## **11. Erkennung und Management von Vorfällen im Zusammenhang mit dem für den Kunden bereitgestellten IKT-Dienst gemäß Art. 30 Abs. 2 lit. f DORA**

Der Lieferant verpflichtet sich, den Kunden im Falle eines IKT Sicherheitsvorfalls, der mit den Dienstleistungen in Verbindung steht, zu unterstützen. Die Unterstützung erfolgt bei Verschulden durch den Lieferanten ohne zusätzliche Kosten sowie in allen anderen Fällen entgeltlich zu den im Vertrag/in den Verträgen festgesetzten Stundensätzen oder falls solche nicht im Vertrag/in den Verträgen geregelt sind, zu vorab zwischen den Vertragsparteien festzusetzenden Kosten.

## **12. Außerordentliche Kündigung des Vertrages**

### **12.1. Beendigung aus wichtigem Grund**

Der Vertrag gemäß Punkt 1(A) kann von jeder Vertragspartei aus wichtigem Grund mit sofortiger Wirkung schriftlich gekündigt werden, wenn die andere Vertragspartei eine wesentliche Vertragsverletzung begeht, die entweder nicht behoben werden kann oder die andere Vertragspartei trotz einer schriftlichen Aufforderung zur Behebung des Verstoßes nicht innerhalb von dreißig (30) Kalendertagen nach Erhalt der schriftlichen Aufforderung behoben wird. Sollte die Behebung nicht binnen der dreißig (30) Kalendertage behoben werden können, so ist eine angemessene Nachfrist zu vereinbaren.

### **12.2. Der Kunde hat insbesondere unter den in 12.1 genannten Voraussetzungen ein Kündigungsrecht und kann den Vertrag durch schriftliche Mitteilung in nachfolgenden Fällen kündigen, sofern diese Umstände nicht durch eine angemessene Vertragsanpassung bzw. im Falle eines Verstoßes durch eine Nachbesserung behoben werden können:**

**12.2.1. wenn der Lieferant in erheblichem Maße gegen geltende Gesetze, sonstige Vorschriften oder Vertragsbedingungen verstößt;**

**12.2.2. wenn im Laufe der Überwachung des IKT-Drittunternehmenrisikos Umstände festgestellt wurden und die als geeignet eingeschätzt werden, die Wahrnehmung der im Rahmen der vertraglichen Vereinbarung vorgesehenen Funktionen zu beeinträchtigen, einschließlich wesentlicher Änderungen, die sich auf die Vereinbarung oder die Verhältnisse des IKT-Drittunternehmers auswirken; Art. 28 Abs.7 lit.b**

**12.2.3. wenn es sich um nachweisliche Schwächen des IKT-Drittunternehmers in Bezug auf sein allgemeines IKT-Risikomanagement und insbesondere bei der Art und Weise, in der er die Verfügbarkeit, Authentizität, Sicherheit und Vertraulichkeit von Daten gewährleistet, unabhängig davon, ob es sich um personenbezogene oder anderweitig sensible Daten oder nicht personenbezogene Daten handelt; Art. 28 Abs.7 lit.c**

12.2.4. wenn die zuständige Behörde den Kunden aufgrund der Bedingungen oder Umstände im Zusammenhang mit diesem Vertrag oder dieser Zusatzvereinbarung nicht mehr wirksam beaufsichtigen kann.

## 13. Vergabe von Unteraufträgen

Der Lieferant ist berechtigt, für die Ausführung der ausgelagerten Tätigkeiten bzw. Teilen davon Unterauftragnehmer heranzuziehen.

Der Lieferant ist jedenfalls für die Erbringung der von dessen Unterauftragnehmern bereitgestellten Dienstleistungen bzw. erbrachten Leistungen verantwortlich und überwacht die Erfüllung aller Verpflichtungen aus den Unteraufträgen.

Falls der Kunde aus begründeten schwerwiegenden Sicherheits- oder Compliancegründen Einwände gegen eine Untervergabe an IKT-Unterauftragnehmer hat, wird er diese dem Lieferanten schriftlich mitteilen. Sollte der Lieferant den Einwänden nicht nachkommen, steht dem Kunden das Recht zu, den Vertrag innerhalb von **XXX** Wochen nach Mitteilung der Einwände außerordentlich zu kündigen.

Die Vertragsparteien kommen überein, dass konzernmäßig verbundene Unternehmen des Lieferanten als Unterauftragnehmer im Sinne der DORA akzeptiert sind, da alle Inhalte dieser Zusatzvereinbarung auch auf sie zutreffen und der Lieferant die Erfüllung der Verpflichtungen überwacht.

## 14. Datum des Inkrafttretens und Laufzeit dieser Zusatzvereinbarung

Diese Zusatzvereinbarung tritt an dem Tag, an dem beide Parteien diese Zusatzvereinbarung unterzeichnet haben ("Datum des Inkrafttretens") in Kraft.

Diese Zusatzvereinbarung wird für die Dauer des Vertrages/der Verträge abgeschlossen und endet automatisch mit der Beendigung des Vertrages/der Verträge, mit der Ausnahme der Bestimmungen dieser Zusatzvereinbarung, die ausdrücklich über ihre Laufzeit hinaus wirksam sind.

## 15. Verhältnis zum Vertrag

Der übrige Teil des Vertrages/der Verträge laut Pkt 1 (A) bleibt unverändert, es sei denn, er wird ausdrücklich durch diese Zusatzvereinbarung geändert.

Wenn und soweit Widersprüche zwischen dem Vertrag/der Verträge, ggf. der Datenverarbeitungsvereinbarung und dieser Zusatzvereinbarung bestehen, haben die Bestimmungen dieser Zusatzvereinbarung Vorrang.

## 16. Salvatorische Klausel

Sollte eine Bestimmung dieser Änderung unwirksam sein oder werden oder versehentlich unvollständig sein, so wird dadurch die Wirksamkeit der übrigen Bestimmungen dieser Zusatzvereinbarung nicht berührt. Die unwirksame oder unvollständige Bestimmung ist durch eine rechtswirksame Regelung zu ersetzen oder zu ergänzen, die dem entspricht, was die Vertragsparteien gewollt haben oder nach den Zielen dieser Zusatzvereinbarung gewollt hätten, wenn sie die Unwirksamkeit bzw. Unvollständigkeit erkannt hätten.

## 17. Gerichtsstand, anwendbares Recht, Schriftlichkeit, Gerichtsstand, anwendbares Recht, Schriftlichkeit

Gerichtsstand und anwendbares Recht richten sich nach dem Vertrag gem. Pkt 1A.

*Beim Fehlen einer solchen Klausel im Vertrag wird die ausschließliche Zuständigkeit des sachlich zuständigen Gerichts für XXX, vereinbart.*

Für Änderungen dieser Zusatzvereinbarung wird Schriftlichkeit vereinbart.

Für den Lieferanten

Für den Kunden

Ort, Datum