

DORA-VEREINBARUNG

zum Dienstleistungsvertrag über xxx vom tt.mm.jjj

zwischen

der Hamburgische Investitions- und Förderbank
(nachfolgend „**IFB Hamburg**“ oder „**Auftraggeber**“)

und

xxx

(nachfolgend „**Auftragnehmer oder IKT-Drittdienstleister**“)

Die IFB Hamburg und der Auftragnehmer werden gemeinsam auch „**Parteien**“ genannt. Die Begriffsbestimmungen in Art. 3 DORA gelten für die DORA-Vereinbarung entsprechend.

Vorbemerkung:

Die IFB Hamburg schließt mit dem Auftragnehmer den obig bezeichneten Dienstleistungsvertrag zur Durchführung von IKT-Dienstleistungen ab.

Unter dem Vertrag stellt der Auftragnehmer insbesondere IKT-Dienstleistungen i.S.d. Art. 3 Nr. 21 der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor (nachfolgend „**DORA**“ oder „**DORA-Verordnung**“) bereit. Mit der DORA-Verordnung hat die Europäische Union eine finanzsektorweite Regulierung für die Themen Cybersicherheit, IKT-Risiken und digitale operationale Resilienz geschaffen. Die DORA-Verordnung nebst den damit verbundenen technischen Regulierungsstandards und technischen Durchführungsstandards soll wesentlich dazu beitragen, den europäischen Finanzmarkt gegenüber Cyberrisiken und Vorfällen der Informations- und Kommunikationstechnologie (nachfolgend „IKT“) zu stärken. Insbesondere enthält die DORA-Verordnung neue Anforderungen, wie die vertraglichen Vereinbarungen, auf deren Grundlage IKT-Dienstleistungen an Finanzunternehmen erbracht werden, ausgestaltet sein müssen.

Dazu vereinbaren die Parteien Folgendes:

§ 1 Klassifizierung

Die Parteien sind sich darüber einig, dass die Dienstleistungen, die der IKT-Drittdienstleister für das Finanzunternehmen bereitstellt, IKT-Dienstleistungen im Sinne des Art. 3 Nr. 21 DORA-Verordnung sind.

Die IFB Hamburg hat die Dienstleistungen, die der IKT-Drittdienstleister unter dem Dienstleistungsvertrag erbringt, als IKT-Dienstleistung klassifiziert

☒ die ausschließlich **keine** kritische oder wichtige Funktion im Sinne des Art. 3 Nr. 22 DORA betreffen.

oder

☐ die zumindest auch eine **kritische oder wichtige Funktion** i.S.d. Art. 3 Nr. 22 DORA betreffen.

§ 2 Verschiedenes

(1) Die Bedingungen dieser DORA-Vereinbarung sind von und zwischen den Parteien in Übereinstimmung mit dem Sinn und Zweck dieser DORA-Vereinbarung

auszulegen, der darin besteht, sicherzustellen, dass die vertragliche Vereinbarung zwischen den Parteien den Anforderungen entspricht, die DORA vorgibt.

(3) Sollten einzelne Bestimmungen dieser DORA-Vereinbarung unwirksam sein oder eine Lücke aufweisen, so wird die Wirksamkeit der übrigen Bestimmungen dieser DORA-Vereinbarung davon nicht berührt. Die unwirksame oder unvollständige Bestimmung ist durch eine rechtswirksame Regelung zu ersetzen oder zu ergänzen, die dem entspricht, was die Parteien gewollt haben bzw. nach den Zielen dieser DORA-Vereinbarung gewollt hätten, wenn sie die Unwirksamkeit oder die Lücke erkannt hätten.

(4) Sofern der Auftragnehmer zur Erbringung der vertraglich geschuldeten IKT-Dienstleistung IKT-Systeme des Auftraggebers nutzt, ist er verpflichtet, die hierfür geltenden Anweisungen und Nutzungsbedingungen des Auftraggebers zu beachten.

§ 3 Beschreibung der Funktionen und Dienstleistungsgüte

(Art. 30 Abs. 2 lit. a und e der DORA)

(1) Die Rechte und Pflichten der Parteien im Hinblick auf die IKT-Dienstleistungen werden im Dienstleistungsvertrag eindeutig zugewiesen und schriftlich dargelegt. Die Auftragnehmerin erbringt die IKT-Dienstleistungen wie im Dienstleistungsvertrag und dessen sämtlichen Anlagen und sonstigen Anhängen näher beschrieben.

Soweit im Dienstleistungsvertrag keine besondere Dienstleistungsgüte festgelegt ist, wird der Auftragnehmer zumindest die Qualität sicherstellen, die von einem professionellen IKT-Drittdienstleister im Finanzdienstleistungssektor im Zusammenhang mit den IKT-Dienstleistungen erwartet werden kann.

(2) Der Auftragnehmer wird die IKT-Dienstleistungen im Einklang mit den jeweils maßgeblichen geltenden gesetzlichen, aufsichtlichen und sonstigen Anforderungen, insbesondere der DORA-Verordnung, erbringen und behördliche Vorschriften sowie vereinbarte Qualitäts-, Sicherheits- und Vertraulichkeitsniveaus einhalten und über alle Genehmigungen, Zulassungen, Verifizierungen und Erlaubnisse verfügen, die für die Erfüllung seiner vertraglichen Verpflichtungen erforderlich sind.

(3) Weiter wird der Auftragnehmer die IFB Hamburg bei der Einhaltung ihrer Verpflichtungen gemäß der DORA-Verordnung angemessen unterstützen. Der Auftragnehmer wird der IFB Hamburg auf Verlangen insbesondere alle Informatio-

nen und Dokumentationen zur Verfügung stellen, die die IFB Hamburg vernünftigerweise für die Erfüllung ihrer Pflichten gemäß der DORA-Verordnung benötigt, soweit diese bei dem Auftragnehmer vorhanden sind.

§ 4 Leistungsstandorte und Verarbeitungsorte

(Art. 30 Abs.2 lit b. DORA)

(1) Der Auftragnehmer (und etwaige Subunternehmer) erbringen die IKT-Dienstleistungen, einschließlich der Speicherung und Verarbeitung von Daten, ausschließlich von und an den im Dienstleistungsvertrag vereinbarten Standorten („**Leistungsstandorte**“).

(2) Der Auftragnehmer wird die IFB Hamburg über eine beabsichtigte Verlegung eines Leistungsstandortes an einen anderen Standort, einschließlich der Speicherung und Verarbeitung von Daten an einem anderen Standort, innerhalb angemessener Frist, mindestens aber [6 Monate] vorab, in Textform informieren. Gleiches gilt bei der Verlegung eines Leistungsstandortes eines Subunternehmers.

Er stellt dabei ausreichende Informationen zur Verfügung, damit die IFB Hamburg die Risiken und Auswirkungen auf die IKT-Dienstleistungen, die Datenverarbeitung und die Speicherorte (einschließlich der Auswirkungen auf die vereinbarten Service-Levels und die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Datenverarbeitung) beurteilen kann. Für - sofern vorhanden - personenbezogene Daten gelten zudem die in der Auftragsverarbeitungsvereinbarung dargelegten Anforderungen.

§ 5 Informationssicherheit

(Art. 28 Abs. 5, Art. 30 Abs. 2 lit. c, d, f und i DORA)

(1) Der Auftragnehmer hält angemessene Standards für die Informationssicherheit ein. Insoweit gelten die im Vertrag, insbesondere in der Anlage *Informationssicherheit* festgelegten Vorgaben für Maßnahmen zur Gewährleistung der Informationssicherheit.

Im Rahmen der IT-Sicherheitsmaßnahmen hat der Auftragnehmer auch die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit in Bezug auf die im Rahmen der IKT-Dienstleistung verarbeiteten Daten sicherzustellen.

(2) Der Auftragnehmer erbringt

- a) die IKT-Dienstleistungen im Einklang mit geltendem Datenschutzrecht, insbesondere den Vorgaben der EU-Datenschutz-Grundverordnung und den geltenden Datenschutzgesetzen an den Leistungsstandorten, jeweils soweit anwendbar, und weist dies entsprechend nach;
- b) ist zur Verschwiegenheit über alle auf die Kunden der IFB Hamburg bezogenen Tatsachen und Wertungen, von denen sie Kenntnis erlangt (Bankgeheimnis), verpflichtet; und
- c) stellt die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit in Bezug auf die im Rahmen der IKT-Dienstleistung verarbeiteten Daten sicher und setzt die hierfür erforderlichen sowie etwaige zwischen den Parteien vereinbarten Maßnahmen zur Gewährleistung der Informationssicherheit um.

§ 6 Zugang zu Daten

(Art. 30 Abs. 2 d) DORA)

Im Falle der Insolvenz, Abwicklung oder Einstellung des Geschäftsbetriebs des IKT-Drittdienstleisters oder im Falle der Beendigung des Vertrages („**Beendigungsereignis**“) wird der IKT-Drittdienstleister der IFB Hamburg nach Eintritt des Beendigungsereignisses Zugang zu allen personenbezogenen und nicht personenbezogenen Daten, die im Rahmen der IKT-Dienstleistung verarbeitet werden, mit der Möglichkeit zum Download der Kundendaten in einem mit allgemein verfügbarer Standardsoftware lesbaren Format gewähren. Der Auftragnehmer ist insbesondere verpflichtet, für eine insolvenz sichere Datenhaltung zu sorgen.

§ 7 Mitwirkungspflicht bei einem IKT-Vorfall

(Art. 30 Abs. 2 f) DORA)

Der Auftragnehmer wird die IFB Hamburg bei einem IKT-bezogenen Vorfall gem. Art. 3 Ziff. 8 DORA-Verordnung, der mit den IKT-Dienstleistungen in Verbindung steht, ohne zusätzliche Kosten in Textform unverzüglich informieren und angemessen unterstützen. Dies umfasst unter anderem die Unterstützung bei den von der IFB Hamburg geforderten Abhilfemaßnahmen.

§ 8 Zusammenarbeit mit Aufsichtsbehörden

(Art. 30 Abs. 2 lit. g DORA)

(1) Der IKT-Drittdienstleister wird mit den für die IFB Hamburg zuständigen Abwicklungsbehörden und sonstigen Behörden einschließlich der von diesen benannten Personen in vollem Umfang zusammenarbeiten. Dazu gehört unter anderem, dass der IKT-Drittdienstleister Anfragen der Aufsichtsbehörden beantwortet und sein Personal und – soweit von den Aufsichtsbehörden gefordert – seine externen Prüfer anweist, mit den Aufsichtsbehörden in vollem Umfang zu kooperieren.

(2) Wenn eine Aufsichtsbehörde im Zusammenhang mit den IKT-Dienstleistungen Maßnahmen gegen den IKT-Drittdienstleister ergreift oder eine Anordnung, ein Ersuchen oder eine Mitteilung an den IKT-Drittdienstleister richtet, wird der IKT-Drittdienstleister die IFB Hamburg unverzüglich informieren und die Kommunikation an die Aufsichtsbehörden vorab mit der IFB Hamburg abstimmen.

§ 9 Kündigungsrechte

(Art. 28 Abs. 7, Art. 30 Abs. 2 lit. h DORA)

Der Vertrag kann von jeder Partei aus wichtigem Grund mit sofortiger Wirkung durch Mitteilung gekündigt werden, wenn die andere Partei in erheblichem Maße gegen die Vertragsbestimmungen verstößt.

(1) Für die IFB Hamburg liegt ein wichtiger Kündigungsgrund insbesondere dann vor, wenn

- a. ein erheblicher Verstoß des Auftragnehmers gegen geltende Gesetze, sonstige Vorschriften oder Vertragsbedingungen vorliegt;
- b. Umstände vorliegen, die im Laufe der Überwachung des IKT-Drittparteienrisikos 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 diesen Vertrag oder die Verhältnisse des Auftragnehmers auswirken;
- c. nachweisliche Schwächen des Auftragnehmers in Bezug auf sein allgemeines IKT-Risikomanagement vorliegen, 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;

- d. die Aufsichtsbehörde die IFB Hamburg infolge der Vereinbarungen des Vertrages oder der mit dem Vertrag verbundenen Umstände nicht mehr wirksam beaufsichtigen kann; oder
 - e. die Aufsichtsbehörde die Beendigung des Vertragsverhältnisses verlangt.
- (2) Im Übrigen gelten für Kündigungen die im Ursprungsvertrag vereinbarten Kündigungsfristen.

§ 10 Schulungen

(Art. 30 Abs. 2 i) DORA)

Auf Verlangen der IFB Hamburg werden Mitarbeiter des IKT-Drittdienstleisters, die Zugang zum Netz oder zu den IKT-Systemen der IFB Hamburg haben oder für die die IFB Hamburg anderweitig vernünftigerweise festgestellt hat, dass eine Teilnahme erforderlich ist, an Schulungen der IFB Hamburg zur digitalen operationalen Resilienz gemäß Art. 13 Abs. 6 DORA-Verordnung teilnehmen.

§ 11 Informationsregister

(Art. 28. Abs. 3 DORA)

(1) Die IFB Hamburg ist nach Art. 28 Abs. 3 DORA-Verordnung dazu verpflichtet, ein Informationsregister zu führen, das sich auf alle vertraglichen Vereinbarungen über die Nutzung von durch IKT-Drittdienstleister bereitgestellten IKT-Dienstleistungen bezieht.

(2) Der IKT-Drittdienstleister wird der IFB Hamburg diejenigen Informationen zur Verfügung stellen, die die IFB Hamburg zur Befüllung des Informationsregisters benötigt. Dies ist insbesondere der Legal Entity Identifier (LEI) oder der European Unique Identifier (EUID). Das gleiche gilt im Hinblick auf Informationen betreffend mögliche Unterauftragnehmer des IKT-Drittdienstleisters.