

ZUSATZVEREINBARUNG

zum Vertrag vom xx.xx.xxxx

betreffend (Beschreibung der Leistung) - nachstehend „Leistungsvertrag“ -, Zusatzvereinbarung und Leistungsvertrag nachstehend als „Vereinbarung“ bezeichnet

1 Vorliegen einer Auslagerung/Erbringen von IKT-Dienstleistungen

1.1 Die während der Vorbereitung des Vergabeverfahrens durch den Auftraggeber durchgeführte Risikoanalyse hatte zum Ergebnis, dass es sich bei der mit dem Leistungsvertrag vom Auftragnehmer zu erbringenden Leistungen - nachfolgend "**Vertragsleistungen**" genannt - handelt um eine

- ☒ Auslagerung im Sinne der Mindestanforderungen an das Risikomanagement (MaRisk);
- ☒ wesentliche Auslagerung im Sinne der Mindestanforderungen an das Risikomanagement (MaRisk); diese Auslagerung wurde von dem Auftraggeber der BaFin als beabsichtigte wesentliche Auslagerung angezeigt (§ 24 Abs. 1 Nr. 19 Kreditwesengesetz [KWG]). Dem Auftragnehmer ist bekannt, dass die BaFin ihm gegenüber unmittelbar Anordnungen treffen kann;

- ☒ IKT-Dienstleistung im Sinne von Art. 3 Nr. 21 DORA

DORA = VERORDNUNG (EU) 2022/2554 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011

- ☐ diese IKT-Dienstleistung unterstützt kritische und/oder wichtige Funktionen im Sinne von Art. 3 Nr. 22 DORA des Auftraggebers - der Auftraggeber hat die zuständige Aufsichtsbehörde über den beabsichtigten Abschluss der Vereinbarung nach Art. 28 Abs. 3 Unterabs. 5 DORA unterrichtet; dem Auftragnehmer ist bekannt, dass er der behördlichen Überwachung nach Art. 31 ff. DORA unterliegen kann;

1.2 Die Vertragsleistungen und den sie betreffenden Geschäftsbereich, verbleiben im internen Kontrollsystem des Auftraggebers. Dem Auftraggeber stehen die dazu nötigen Auskunfts-, Prüfungs- und Zutrittsrechte sowie Kontroll- und Weisungsbefugnisse zu.

1.3 Der Auftraggeber trägt gegenüber seinen Aufsichtsbehörden weiterhin die Verantwortung für die Vertragsleistungen und den sie betreffenden Geschäftsbereich.

1.4 Die Regelungen in den Nrn. 3. ff. der Zusatzvereinbarung zu Auslagerungen gelten entsprechend für IKT-Dienstleistungen als Vertragsleistungen.

2 Einhalten der für den Auftraggeber geltenden Anforderungen durch den Auftragnehmer

2.1 Die Parteien vereinbaren, an die regulatorischen Anforderungen der BaFin in der jeweils gültigen Fassung im Zeitpunkt des Vertragsschlusses gemäß BaFin Rundschreiben 6/2024 (BA) vom 29.05.2024 - Mindestanforderungen an das Risikomanagement - ("MaRisk"), gebunden zu sein und diese einzuhalten.

2.2 Der Auftragnehmer wird in Bezug auf die von ihm übernommenen Leistungen innerhalb Deutschlands alle rechtlichen und vertraglichen Pflichten, die der Auftraggeber z. B. aufgrund bankenaufsichtsrechtlicher Vorgaben einzuhalten hat, erfüllen. Dies gilt im Hinblick auf allein in der Sphäre des Auftraggebers liegenden Verpflichtungen nur, soweit der Auftraggeber auch über diese informiert hat. Dazu gehören auch technische Standards, die der Auftraggeber in Erfüllung dieser Pflichten anzuwenden hat.

Gesetzliche und bankaufsichtsrechtliche Vorgaben soweit technische Standards sind insbesondere:

- (i) das Kreditwesengesetz (KWG), die aufgrund des KWG erlassenen oder zu erlassenden Rechtsverordnungen, die MARisk,
- (ii) die jeweils für die Buchführung und Geschäftsentwicklung in Kreditinstituten geltenden Rechtsvorschriften, insbesondere handels-, steuer- und aufsichtsrechtliche Vorschriften an eine ordnungsgemäße und sichere Datenverarbeitung (Datenschutzbestimmungen, Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme des Bundesministeriums (GoBS),
- (iii) die im Bankenbereich anerkannten fachlichen und prüferischen Standards, insbesondere die Stellungnahmen und Verlautbarungen der BaFin soweit sie die Vertragsleistungen betreffen,
- (iv) ISO2700x- oder BSI-Standards.

2.3 Der Auftragnehmer wird in Bezug auf die von ihm übernommenen Leistungen alle rechtlichen Pflichten, die der Auftraggeber aufgrund von DORA einzuhalten hat, erfüllen. Dazu gehören über DORA hinaus, insbesondere

- (i) die aufgrund von DORA erlassenen delegierten Verordnungen und Durchführungsverordnungen sowie die Leitlinien der für die Umsetzung von DORA zuständigen Aufsichtsbehörden,
- (ii) die in Deutschland ergänzend zur Anwendung von DORA erlassenen Gesetze, Rechtsverordnungen sowie Rundschreiben der BaFin,
- (iii) die Aufsichtsmitteilung zu Auslagerungen an Cloud-Anbieter der BaFin (aktueller Stand Februar 2024).

3 Vertragsanpassungsklausel

3.1 In dem Falle, dass aufgrund von Änderungen der gesetzlichen Bestimmungen und/oder der regulatorischen Vorgaben die in dieser Vereinbarung getroffenen Regelungen der Ersetzung, Änderung oder Ergänzung bedürfen, werden die Parteien die erforderlichen Anpassungen dieser Vereinbarung einvernehmlich vornehmen. Der Auftraggeber wird den Auftragnehmer unverzüglich über einschlägige Ersetzungen, Ergänzungen oder Änderungen in Kenntnis setzen.

3.2 Voriger Absatz gilt entsprechend, falls aufgrund einer Anordnung einer zuständigen Aufsichtsbehörde oder aufgrund künftiger Verlautbarungen dieser Behörden die Vertragsleistung einer anderen oder zusätzlichen Kategorie als in Nr. 1.1 der Zusatzvereinbarung festgestellt, zuzuordnen sind.

4 Informations-, Prüfungs- und Überwachungsrechte

4.1 Der Auftragnehmer hat,

- (i) dem Auftraggeber sowie dessen Interner Revision oder von ihm gesondert beauftragter Spezialisten, ein jederzeitiges, vollumfängliches und ungehindertes Informations-, Einichts- und Prüfungsrecht einzuräumen, unbeschränkten Zugang zu allen Personen, Räumlichkeiten sowie den unter seiner Kontrolle stehenden Dokumenten, Daten Datenträgern und IT-Systemen, Rechnungsunterlagen und sonstigen Aufzeichnungen und Geschäftsdokumenten (nachfolgend zusammenfassend "**Dokumente**") zu gewähren, die mit den vertragsgegenständlichen Leistungen und der Durchführung der Vereinbarung in Zusammenhang stehen und für die Prüfung dienlich sind. In diesem Zusammenhang hat er allen Personen, die sich ihm gegenüber zur Geheimhaltung verpflichtet haben, von dieser Geheimhaltungsverpflichtung gegenüber den Prüfern freistellen;

Der Auftragnehmer hat den Prüfern zu ermöglichen, Kopien und Abschriften davon anzufertigen bzw. auf dessen Verlangen die Unterlagen/Dokumente per Post/verschlüsselten E-Mail-Verkehr oder sichere Austauschplattform etc. zur Verfügung zu stellen, sofern sie Vertragsleistungen betreffen und von dem Auftraggeber, insbesondere im Rahmen seines

Risikomanagement bzw. im Zusammenhang mit der Prüfung des Jahresabschlusses oder von einer der vorstehend genannten Personen und Aufsichtsbehörden, insbesondere der BaFin im Rahmen ihrer regulären oder sonstigen Prüfungen der Dokumente angefordert werden.

Vorige Absätze von (i) gelten entsprechend für Rechnungsprüfer, Prüfern, die bei dem Auftraggeber aufgrund gesetzlicher Vorschriften tätig werden, Vertretern oder bevollmächtigten Prüfern der BaFin oder einer anderen Aufsichtsbehörde oder der von diesen Behörden zur Durchführung der Prüfung benannten Personen

Der Auftragnehmer ist verpflichtet, mit den zuständigen Aufsichtsbehörden des Auftraggebers, einschließlich von dieser Beauftragten, zusammenzuarbeiten.

- (ii) bei der Durchführung der vorgenannten Prüfungen Unterstützung zu leisten und insbesondere die Durchführung solcher Prüfungen in keiner Weise zu behindern.

Der BaFin sowie der von dieser mit der Prüfung beauftragten Stellen sind in Bezug auf die für den Auftraggeber der Anwendbarkeit der aufsichtlicher Bestimmungen zu Auslagerungen bzw. IKT-Dienstleistungen unterliegenden Leistungen des Auftragnehmers sämtliche Auskünfte zu erteilen und Unterlagen auszuhändigen, die diese für ihre Aufsichtstätigkeit benötigen. Sollte die BaFin ohne vorheriges Einschalten des Auftraggebers unmittelbar an den Auftragnehmer zur Prüfung herantreten und auftraggeberbezogene Daten abfragen, wird der Auftragnehmer den Auftraggeber darüber unverzüglich in Kenntnis setzen

- (iii) in organisatorischer, personeller, technischer und struktureller Hinsicht geeignete Maßnahmen zu treffen, um sicherzustellen, dass der Zugang zu den Dokumenten den Vorschriften der Aufsichtsbehörden entspricht und nur ordnungsgemäß bevollmächtigte Personen Zugang zu den jeweiligen Daten haben
- (iv) sicherzustellen, dass die etablierten, eingerichteten und funktionierenden Schnittstellen zum Auftraggeber durch künftige Veränderungen in Bezug auf die Hard- und Software, die der Auftragnehmer zur Erfüllung seiner vertraglichen Pflichten einsetzt, nicht beeinträchtigt werden

4.2 Die Prüfungs- und Kontrollrechte der Prüfer erstrecken sich auf die Prüfung und Kontrolle der vertragsgemäßen Leistungserbringung und die Einhaltung der vertraglichen Bestimmungen und umfassen insbesondere:

- (i) die Einhaltung der Service Levels sowie die zur Überprüfung der Einhaltung der Service Levels eingesetzten Überprüfungsmethoden sowie die aufgezeichneten Ergebnisse der Überprüfungen,
- (ii) die Richtigkeit der dem Auftraggeber durch den Auftragnehmer in Rechnung gestellten Vergütung und sonstige Beträge,
- (iii) die Sicherheit und den Schutz geheimhaltungsbedürftiger Daten, einschließlich der vom Auftragnehmer zur Gewährleistung der Datensicherheit und des Datenschutzes getroffenen technischen und organisatorischen Maßnahmen,
- (iv) die Einhaltung aller anwendbaren rechtlichen Rahmenbedingungen, insbesondere aufsichtsrechtlicher Anforderungen, durch den Auftragnehmer.

4.3 Vorbehaltlich weiter gehender anwendbarer rechtlicher Rahmenbedingungen, sind die Prüfer bis zwei Jahre nach dem Ende des Geschäftsjahres des Auftraggebers, in dem die Kündigung der Vereinbarung wirksam wurde oder die Vertragslaufzeit endete, zur Prüfung und Kontrolle berechtigt. Der Auftragnehmer stellt sicher, dass während dieses Zeitraumes alle relevanten Dokumente und Datenträger zugänglich bleiben.

- 4.4 Die Funktion der Internen Revision hinsichtlich des ausgelagerten Bereichs kann vollständig oder teilweise durch einen beauftragten qualifizierten Dritten ausgeübt werden, wenn der Auftragnehmer sicherstellt, dass die von dem Dritten für den ausgelagerten Bereich erstellten Dokumente dem Auftraggeber in gleicher Weise zugänglich sind, wie die von einer eigenen internen Revision des Auftragnehmers erstellten Dokumente.
- 4.5 Der Auftragnehmer räumt dem Auftraggeber das Recht ein, jederzeit nach angemessener vorheriger Ankündigung und Abstimmung und unter Berücksichtigung der betrieblichen Belange des Auftragnehmers vollumfänglich und ungehindert eigene Ergänzungsprüfungen durch ihre Interne Revision oder durch vom Auftraggeber gesondert beauftragte Spezialisten im Unternehmen des Auftragnehmers durchzuführen. Absatz (1) (i) gilt entsprechend.
- 4.6 Der Auftraggeber hat das Recht, vom Auftragnehmer durchgeführte Kontrollen mittels eigener Prüfungshandlungen auf ihre Wirksamkeit hin zu überprüfen bzw. die Vollständigkeit und Richtigkeit der regelmäßigen Auswertungen und Berichterstattungen des Auftragnehmers zu überprüfen.
- 4.7 Der Auftragnehmer stellt eine vollständige Geschäftsdokumentation von an ihn ausgelagerten Geschäftstätigkeiten sicher, die eine lückenlose Überwachung des Auftragnehmers durch die BaFin gewährleistet. Erforderliche Aufzeichnungen sind zu diesem Zweck für einen den jeweiligen gesetzlichen (insbesondere § 257 HGB) und aufsichtsrechtlichen Bestimmungen gerecht werdenden Zeitraum aufzubewahren.

5 Weisungsrechte

- 5.1 Der Auftragnehmer ist im Rahmen seiner vertraglichen Pflichten gemäß der Vereinbarung an die Weisungen des Auftraggebers gebunden. Der Auftraggeber kann vorbehaltlich anderslautender Regelungen in Nr. 7 dieser Vereinbarung (Mehrmandantendienstleister) der Geschäftsleitung des Auftragnehmers bei der Durchführung der vom Institut gemäß den aufsichtlichen Bestimmungen zu Auslagerungen ausgelagerten Funktionen unmittelbare Weisungen erteilen. Der Auftragnehmer ist verpflichtet, seinen Geschäftsbetrieb derartig zu organisieren, dass Weisungen des Auftraggebers auf Grundlage der aufsichtlichen Bestimmungen zu Auslagerungen vorrangig vor eventuell bestehenden konkurrierenden Weisungsrechten Dritter beachtet werden.
- 5.2 Der Auftraggeber ist verpflichtet, dem Auftragnehmer die zur Einhaltung der bankspezifischen und bankenaufsichtsrechtlichen Erfordernisse notwendigen Weisungen in geeigneter Darstellung und mit angemessenen zeitlichen Vorlauf zu erteilen. Die Weisungen des Auftraggebers richten sich an den vom Auftragnehmer genannten Ansprechpartner.
- 5.3 Hält der Auftragnehmer Weisungen des Auftraggebers für unzumutbar, so hat er seine Bedenken unverzüglich geltend zu machen.

6 Weiterverlagerung, Einsatz von Subunternehmern

- 6.1 Der Auftragnehmer ist berechtigt, Teile der ihm nach dem Leistungsvertrag obliegenden Leistungen nach vorheriger Zustimmung durch den Auftraggeber auch durch Nachunternehmer erbringen zu lassen. Er kann hierzu Nachunternehmerverträge abschließen, ändern oder beenden.
- 6.2 Die Absicht der Weiterverlagerung ist dem Auftraggeber zuvor – spätestens sechs Wochen vor dem geplanten Weiterverlagerungstermin – schriftlich anzuzeigen. Der Auftragnehmer hat dem Auftraggeber ausreichende Informationen zur Verfügung zu stellen, die diesem eine umfassende Bewertung der Leistungsfähigkeit und Zuverlässigkeit des Subunternehmers sowie der dem Auftragnehmer eingeräumten Überwachungsrechte des Subunternehmers ermöglichen. Hierzu gehören Informationen über die fachliche Eignung sowie die sachliche, technische, personelle und finanzielle Ausstattung des Subunternehmers sowie der Ort seiner Leistungserbringung und der Datenverarbeitung/-speicherung. Der Auftraggeber wird innerhalb von sechs

Wochen ab Zugang der schriftlichen Informationen des Auftragnehmers seine Zustimmung zu dem Einsatz des von dem Auftragnehmer benannten Subunternehmers erteilen, wenn kein wichtiger Grund entgegensteht. Ein wichtiger Grund liegt insbesondere vor, wenn

- (i) Anhaltspunkte dafür bestehen, dass durch die Beauftragung des Subunternehmers die Erbringung der vertragsgegenständlichen Leistungen – vor allem nach den vereinbarten oder den für die ordnungsgemäße Leistungserbringung erforderlichen Standards – oder die Erfüllung der Pflichten des Auftragnehmers aus dieser Zusatzvereinbarung gefährdet oder beeinträchtigt wird,
- (ii) der Auftraggeber in der Vergangenheit mit dem zu beauftragenden Subunternehmer schlechte Erfahrungen gemacht hat,
- (iii) die Zusammenarbeit mit dem Subunternehmer die Erfüllung von gesetzlichen oder vertraglichen Verpflichtungen des Auftraggebers, insbesondere von aufsichtsbehördlichen Vorschriften, gefährdet,
- (iv) der Ort für die Leistungserbringung oder Verarbeitung bzw. Speicherung von Daten des Auftraggebers oder der Sitz des Unterauftragnehmers oder seiner Muttergesellschaft außerhalb der mit dem Auftragnehmer für seine Leistungen und Datenverarbeitung/-speicherung vereinbarten Regionen liegt ,
- (v) die Durchführung der Leistungen durch einen Subunternehmer in dem Leistungsvertrag ausdrücklich ausgeschlossen ist oder aus Gründen des öffentlichen Vergaberechts nicht zulässig ist.

- 6.3 Über seine nach ihrer Bedeutung der Weiterverlagerung entgegenstehenden wichtigen Gründe hat der Auftraggeber den Auftragnehmer innerhalb o. g. Frist zu unterrichten.
- 6.4 Bei jeglicher Weiterverlagerung von Aktivitäten und Prozessen ist seitens des Auftragnehmers zu gewährleisten, dass der auf diese Weise verpflichtete Subunternehmer den zwischen dem Auftraggeber und dem Auftragnehmer bestehenden Verpflichtungen, insbesondere den aufsichtlichen Anforderungen zu Auslagerungen, ebenfalls vollumfänglich nachkommt. Der Auftragnehmer muss auch dafür Sorge tragen, dass der Vertrag mit dem Subunternehmer keine Regelungen enthält, die der Erfüllung der Verpflichtungen des Auftragnehmers gegenüber dem Auftraggeber beeinträchtigen können. Der Vertrag muss insbesondere die Durchsetzbarkeit der in Nrn. 3. und 4. vorgesehenen Rechte (Prüfungs-, Kontroll- und Weisungsrechte, weitere aufsichtsrechtliche Anforderungen) beinhalten und die beim Auftraggeber gültigen Regelwerke gewährleisten (Notfallkonzepte, Datenschutz, Informationssicherheit, etc.). Der Auftragnehmer wird dem Auftraggeber auf Verlangen die Umsetzung seiner Verpflichtungen durch entsprechende Auszüge aus der mit dem jeweiligen Subunternehmer getroffenen Vereinbarungen nachweisen. Weiterhin wird der Auftragnehmer den Auftraggeber umfassend über den Subunternehmer informieren, dem Auftraggeber insbesondere über die technischen und organisatorischen Maßnahmen sowie operativen Möglichkeiten und Erfahrungen des Subunternehmers unterrichten. Weiterhin benennt der Auftragnehmer dem Auftraggeber für jeden Subunternehmer einen Ansprechpartner, der von dem Auftraggeber direkt kontaktiert werden darf.
- 6.5 Der Auftragnehmer bleibt für die Erfüllung der auf den Subunternehmer weiter verlagerten Tätigkeiten in dem gleichen Umfang verantwortlich, als würden diese durch den Auftragnehmer selbst erbracht. Gegenüber dem Auftraggeber wird der Auftragnehmer die einzige Schnittstelle zu dem Subunternehmer bilden. Bestehen Anhaltspunkte dafür, dass die Leistung eines Subunternehmers die Erbringung der Vertragsleistungen beeinträchtigt oder gefährdet, so wird der Auftragnehmer unverzüglich Abhilfe schaffen und ggf. den Subunternehmer ersetzen.
- 6.6 Der Auftragnehmer haftet für die von ihm beauftragten Subunternehmer.
- 6.7 Die zum Zeitpunkt des Vertragsschlusses von dem Auftragnehmer bereits mit der Wahrnehmung von dem Auftraggeber betreffenden Dienstleistungen betrauten Subunternehmer sind vollständig in **Anlage (BITTE ERGÄNZEN)** zu dieser Zusatzvereinbarung aufgeführt. Für diese Subunternehmer gilt die Zustimmung des Auftraggebers als erteilt.

7 Informations- und Berichtspflichten des Auftragnehmers

- 7.1 Der Auftragnehmer hat dem Auftraggeber über die Erbringung der geschuldeten Leistungen regelmäßig Bericht zu erstatten. Dies gilt auch im Falle der Weiterverlagerung.
- 7.2 Der Auftragnehmer ist verpflichtet, den Auftraggeber unverzüglich über alle wesentlichen Fehler und Vorkommnisse bei der Erbringung der Leistungen zu unterrichten. Wesentlich sind insbesondere Fehler und Vorkommnisse, die zu einer erheblichen Schadenshöhe führen können oder die den organisatorischen Arbeitsablauf in erheblicher Weise behindern, weiterhin vorsätzliche Schadenaufügungen von Mitarbeitern, eine Häufung von fahrlässig verursachten Störungen sowie personelle Mängel, die erheblichen Einfluss auf die Leistungserbringung haben.
- 7.3 Der Auftragnehmer unterrichtet den Auftraggeber vorab über eine beabsichtigte Verlagerung des Standorts, an dem aus dem Bereich des Auftraggebers stammende Daten verarbeitet, insbesondere auch gespeichert werden sollen. Davon bleiben Zustimmungsvorbehalte im Leistungsvertrag unberührt.
- 7.4 Der Auftragnehmer verpflichtet sich, die den ausgelagerten Bereich betreffenden Prüfungsergebnisse dem Auftraggeber und dem Abschlussprüfer des Auftraggebers regelmäßig sowie ad-hoc bei besonderen Vorkommnissen zu übergeben.
Ferner hat der Auftraggeber der BaFin eine Abschrift dieser Berichte zu übermitteln.
- 7.5 Der Auftragnehmer ist verpflichtet, im Falle einer Verschlechterung seiner wirtschaftlichen Stabilität den Auftraggeber umgehend zu informieren.
- 7.6 Die folgenden Berichte, Testate und Zertifizierungen des Auftragnehmers werden dem Auftraggeber in elektronischer Form ohne besonderes Entgelt zur Verfügung gestellt.
 - 7.6.1 Jährliche Testate: IDW PS 951 und/oder ISAE 3402 sowie den jeweils geltenden Nachfolgestandards
 - 7.6.2 Einmalig und nach Rezertifizierung: ISO/IEC 27001 Zertifikat oder weitere anerkannte ISMS-Zertifizierungen
 - 7.6.3 Jährliche Berichte
 - (i) Informationssicherheitsbericht
 - (ii) Notfallvorsorgebericht
 - (iii) Datenschutzbericht
 - (iv) Jahresbericht Interne Revision
 - 7.6.4 Quartalsweise Berichte:
 - (i) Risikobericht
 - (ii) Quartalsbericht Interne Revision
 - (iii) aktuelle Ergebnisse und Ereignisse des Quartals, welche die Punkte der Notfallvorsorge betreffen.

8 Dienstleisterbezogenes Internes Kontrollsystem (IKS)

- 8.1 Der Auftragnehmer betreibt und dokumentiert ein dienstleistungsbezogenes internes Kontrollsystem (IKS), welches dem Prüfungsstandard IDW PS 951 Typ B oder ISAE 3402 Typ 2 bzw. dem jeweils geltenden Nachfolgestandard entspricht.
- 8.2 Der Auftragnehmer weist die Erfüllung der hier festgelegten Anforderungen an das IKS des Auftragnehmers dem Auftraggeber nach.

9 Mehrmandantendienstleister

- 9.1 Der Auftragnehmer ist verpflichtet, seine für den Auftraggeber nach dieser Vereinbarung eingerichteten Dienstleistungsbereiche durch geeignete technische und organisatorische Vorkehrungen (Mehrmandantenfähigkeit) entsprechend den banküblichen Anforderungen (z. B. der BaFin) von den Dienstleistungsbereichen anderer Kunden zu trennen sowie sicherzustellen, dass die Dienstleistungen für verschiedene Kunden unabhängig voneinander durchführbar sind und eventuellen Weisungen der verschiedenen Kunden unabhängig voneinander Rechnung getragen werden kann.
- 9.2 Dabei wird der Auftragnehmer Vorkehrungen treffen, dass
- (i) die für unterschiedliche Mandanten des Auftragnehmers gespeicherten und verarbeiteten Datenbestände logisch getrennt sowie wechselseitig abgeschirmt sind
 - (ii) die den jeweiligen Mandanten gegenüber zu erbringenden vertragsgegenständlichen Leistungen unabhängig voneinander durchführbar sind und
 - (iii) Weisungen der verschiedenen Mandanten nach Maßgabe der jeweiligen vertraglichen Regelungen unabhängig voneinander Rechnung getragen werden kann.

10 Business Continuity Management (BCM), Notfallvorsorge

- 10.1 Zur Sicherstellung der Kontinuität des Geschäftsbetriebes hat der Auftragnehmer über ein angemessenes Notfallmanagement zu verfügen, welches sich an den gängigen Standards orientiert. Das Notfallmanagement umfasst dabei Notfallvorsorge- und Notfallbewältigungsmaßnahmen, die regelmäßigen Notfalltests unterliegen. Über die Angemessenheit des Notfallmanagements berichtet der Auftragnehmer entsprechend den geltenden Rechtsvorschriften, mindestens im Rahmen eines Jahresberichtes zum Notfallmanagement an den Auftraggeber. Wesentliche Störungen und Notfälle, welche Auswirkungen auf die vertraglichen Leistungen haben, sind unverzüglich an den Auftraggeber zu melden.
- 10.2 Der Auftragnehmer ist verpflichtet, ein Notfallkonzept zu erstellen, aktuell zu halten und regelmäßig zu testen. Dieses Notfallkonzept
- (i) beinhaltet Maßnahmen und Regelungen für die eigenen zeitkritischen Prozesse und Aktivitäten des Auftragnehmers in branchenüblichen Umfang sowie für Ausfall- und Störfallsituationen der vertragsgegenständlichen Leistungen.
 - (ii) bezieht sich auf die Absicherung aller notwendigen Ressourcen (Infrastruktur, IT, Personal, ggf. Subdienstleister).
- 10.2.1 Ziel dieses Notfallkonzepts ist es, die Kontinuität der Leistungen des Vertragsgegenstandes des Auftragnehmers gegenüber dem Auftraggeber sicherzustellen.
- 10.2.2 Von Seiten des Auftragnehmers sind im Notfallkonzept mindestens zu regeln:
- (i) Notfallmanagement-Aufbauorganisation; Benennung eines Ansprechpartners für alle BCM-relevanten Fragestellungen
 - (ii) Ausfall- und Reaktionszeiten gemäß den vertraglich festgelegten Verfügbarkeitsanforderungen des Auftraggebers sind zu benennen
 - (iii) Notfallbewältigungsstrategien- und Lösungen, die verschiedene relevante Ausfallszenarien abdecken
 - (iv) Beschreibung eines mit dem Auftraggeber abgestimmten Eskalations- und Meldeverfahrens für Störungen und Notfälle
 - (v) Beschreibung eines mit dem Auftraggeber abgestimmter Information/Kommunikation bzw. -wege/-flusses im Störfall oder eines Notfalls
 - (vi) Pläne, wie Geschäftsfortführungs- und Wiederanlaufpläne, mit denen relevante, zeitkritische Geschäftsprozesse bzw. die vertraglichen Leistungen zeitgerecht fortgeführt werden können; Beschreibung der Maßnahmen zur Rückführung in den Normalbetrieb.

- 10.2.3 Der Auftraggeber ist berechtigt/erhält das Recht, die jeweils aktuelle Version des Notfallkonzeptes einzusehen. Änderung von Bedeutung bzw. wesentliche Änderungen des Notfallkonzeptes sind mit dem Auftraggeber abzustimmen und ihm zur Kenntnis zu geben.
- 10.3 Business Impact Analyse, Überprüfung der Notfallpläne und Notfalltest
- Durch den Auftragnehmer ist anlassbezogen sowie regelmäßig (d. h. mindestens jährlich)
- (i) eine Business Impact Analyse (BIA) sowie eine Risikoanalyse durchzuführen
 - (ii) vorhandene Notfallbewältigungsstrategien und -pläne hinsichtlich ihrer Aktualität hin zu überprüfen und die Angemessenheit und Funktionsfähigkeit der darin beschriebenen Maßnahmen in Rahmen von Übungen und Tests zu überprüfen, in die alle für die Leistungserbringung relevanten IT-Anwendungen, IT-Systeme und Prozesse eingebunden werden (Auftragnehmer hat hierzu einen Test- und Übungsplan vorzuhalten, welcher in einem Zeitraum von drei Jahren die Übungs- und Testarten sowie die Häufigkeit der durchgeführten Übungen und Tests regelt. Deren Art und Häufigkeit sind mit dem Auftraggeber gemäß den gültigen Vorschriften des Auftraggebers abzustimmen).
- 10.4 Notfallvorsorgebericht, Quartalsberichte
- 10.4.1 Die im Rahmen der vertragsgegenständlichen Leistung durchgeführten Übungs- und Test-Ergebnisse sind durch den Auftragnehmer zu protokollieren und dem Auftraggeber unverzüglich zur Verfügung zu stellen.
- 10.4.2 Ein Statusbericht zum Business Continuity Management/Notfallkonzept bzw. Notfallvorsorgebericht ist durch den Auftragnehmer regelmäßig, d. h. mindestens jährlich, dem Auftraggeber unaufgefordert mit nachfolgend genannten Mindestinhalt zur Verfügung zu stellen:
- (i) Ergebnisse durchgeführter Übungen und Tests sowie durchgeführter Audits
 - (ii) Reale Sicherheitsvorfälle/Notfälle
 - (iii) Status der Umsetzung von Korrektur- und Verbesserungsmaßnahmen
- 10.4.3 Der Auftragnehmer informiert den Auftraggeber quartalsweise zu aktuellen Ergebnissen und Ereignissen der letzten drei Monate, welche die Punkte des Statusberichtes betreffen.
- 10.5 Kostentragung
- 10.5.1 Für die in dieser Zusatzvereinbarung zum Business Continuity Management (BCM), Notfallvorsorge enthaltenen Verpflichtungen und für Leistungen im Notfall ist der Auftragnehmer nicht berechtigt, eine zusätzliche Vergütung zu verlangen oder bestehende Vergütungen zu erhöhen.
- 10.5.2 Wenn durch einen Notfall, welcher weder durch den Auftraggeber noch durch den Auftragnehmer oder einer seiner Subunternehmer zu vertreten ist, außergewöhnliche Kosten entstehen, so trägt jede Partei die auf ihrer Seite entstehenden Kosten selbst. Für den Fall, dass nachweislich der Notfall durch mangelhafte oder unzureichende Notfallplanung seitens des Auftragnehmers oder eines Subdienstleisters verursacht worden ist, trägt der Auftragnehmer auch die beim Auftraggeber anfallenden Kosten und Schäden (insb. Verluste, Entschädigungen).
- 10.6 Unterstützung bei einem IKT-Vorfall
- Der Auftraggeber unterstützt den Auftragnehmer bei einem IKT-Vorfall, der mit der dem Auftragnehmer erbrachten IKT-Dienstleistung zusammenhängt. Die Kosten hierfür werden dem Auftragnehmer nach Maßgabe der Entgeltregelung im Leistungsvertrag erstattet.

11 Informationssicherheit

- 11.1 Der Auftragnehmer verpflichtet sich, die Sicherheitsvorgaben der ILB unter Berücksichtigung der Schutzbedarfsklassifizierung bzw. Sensibilität/Geschäftskritikalität der ILB-Prozesse und -Daten einzuhalten. Die Sicherheitsvorgaben ergeben sich aus der Art der Dienstleistung sowie dem Schutzbedarf der betroffenen Daten und Prozesse. Diese sind der **Anlage XX** bzw. der Leistungsbeschreibung zu entnehmen.

Schutzziel	Schutzbedarfsklasse
Verfügbarkeit der betroffenen Daten/Prozesse (ILB)	Niedrig/Mittel/Hoch/Sehr hoch
Vertraulichkeit der betroffenen Daten/Prozesse (ILB)	Niedrig/Mittel/Hoch/Sehr hoch
Integrität/Authenzität der betroffenen Daten/Prozesse (ILB)	Niedrig/Mittel/Hoch/Sehr hoch
Gesamtschutzbedarf der betroffenen Daten/Prozesse (ILB)	Niedrig/Mittel/Hoch/Sehr hoch

- 11.2 Der Auftragnehmer verpflichtet sich, dem Auftraggeber die jeweils aktuellen Kontaktdaten der fachlich verantwortlichen Mitarbeitenden (mindestens des Informationssicherheitsbeauftragten) zur Verfügung zu stellen sowie die aktuellen Kontaktdaten des Auftraggebers vorzuhalten.
- 11.3 Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anfrage bei Untersuchungen von Informationssicherheitsvorfällen zu unterstützen und sicherheitsrelevante Informationen auf Anfrage an den Auftraggeber herauszugeben, sofern sie für das Vertragsverhältnis relevant sind.
- 11.4 Der Auftragnehmer informiert den Auftraggeber unverzüglich über alle Informationssicherheits-/IKT-Vorfälle, die die ordnungsgemäße Erbringung der beauftragten Leistung wesentlich beeinträchtigen können und die eine Gefahr für die Verletzung der Schutzziele wie Vertraulichkeit, Integrität, Verfügbarkeit sowie Authentizität der verarbeitenden Daten der ILB zur Folge haben können.
- 11.5 Im Nachgang zu Sicherheitsvorfällen ist eine Ursachenanalyse zu erstellen. Etwaige Maßnahmen zur Vermeidung zukünftiger Sicherheitsvorfälle oder Verbesserung der Sicherheitsvorfallbehandlung sind nachzuhalten.
- 11.6 Der Auftragnehmer verpflichtet sich, sofern erforderlich, bei der Erstellung von Risikoanalysen durch Bereitstellung der notwendigen Informationen zu unterstützen.
- 11.7 Der Auftragnehmer verpflichtet sich, für alle mit der ILB vertraglich vereinbarten Anforderungen auf Nachfrage geeignete Dokumente (z. B. Richtlinien, Arbeitsanweisungen, Konzepte oder Checklisten) unverzüglich als Nachweis zur Verfügung zu stellen.
- 11.8 Die Informationspflichten gelten ebenfalls für die involvierten Dienstleister des Auftragnehmers.
- 11.9 Die Bestimmungen etwaiger weiterer Zusatzvereinbarungen zur Informationssicherheit bleiben hiervon unberührt.

12 Datenschutz

- 12.1 Der Auftragnehmer verpflichtet sich, alle Daten des Auftraggebers, die Gegenstand des Vertragswerkes sind, vertraulich zu behandeln. Des Weiteren verpflichtet sich der Auftragnehmer diese Daten ausschließlich zu Zwecken im Rahmen dieses Vertrages zu verwenden und nur mit vorheriger Zustimmung des Auftraggebers weiterzugeben oder zur Erfüllung gesetzlicher Publizitätspflicht offen zu legen.
- 12.2 Der Auftragnehmer stellt sicher, dass alle Kundendaten des Auftraggebers eindeutig identifiziert werden können, streng von anderen Daten getrennt werden, dass der Zugriff nach einem Berechtigungskonzept nur in Bezug auf Rollen und Rechte erfolgt, und dass starke physische und logische Schutzmaßnahmen implementiert werden.
- 12.3 Der Auftragnehmer ist ferner verpflichtet, die anerkannten Grundsätze ordnungsgemäßer Datenverarbeitung (GoDV) zu beachten, geeignete Sicherungs- und Backupmaßnahmen zu treffen sowie sämtliche angemessenen Maßnahmen zu ergreifen, die nach Auffassung des Auftragnehmers erforderlich sind, um berechtigten Anforderungen des Auftraggebers an Standards ordnungsgemäßer Datenverarbeitung zu entsprechen.
- 12.4 Die Bestimmungen etwaiger weiterer Zusatzvereinbarungen zum Datenschutz (insbesondere Auftragsdatenvereinbarung) bleiben hiervon unberührt.

13 Mitwirkung an Schulungen

- 13.1 Der Auftraggeber ist berechtigt, von dem Auftragnehmer die Teilnahme an den IKT-Sicherheits-sensibilisierungsprogrammen und an Schulungen zur digitalen operationalen Resilienz (umfassend ""IKT-Schulungen"") gemäß Art. 13 Abs. 6 DORA zu verlangen, soweit die IKT-Schulungen für die IKT-Dienstleistungen des Auftragnehmers relevant sind und nur im Hinblick auf die Mitarbeiter des Auftragnehmers, die an der Durchführung der Vereinbarung beteiligt sind.
- 13.2 Der Auftraggeber hat den Auftragnehmer mindestens 4 Wochen vor Beginn einer bestimmten IKT-Schulung zu informieren, einschließlich Termin und Dauer, ob die Schulung online oder in Anwesenheit stattfindet und im Falle der Präsenzs Schulung deren Ort.
- 13.3 Der Auftraggeber ist berechtigt, das Verlangen einmal im Jahr zu stellen. Im Falle von wiederholten und/oder erheblichen Verstößen des Auftragnehmers gegen die Zusatzvereinbarung kann er zusätzliche Schulungen außerhalb des Jahresturnus verlangen.
- 13.4 Die jährlichen Schulungen, die mehr als einen Personentag pro beteiligten Mitarbeiter des Auftragnehmers in Anspruch nehmen, werden gemäß den Entgeltregelungen des Leistungsvertrages abgerechnet. Die außerplanmäßigen Schulungen gemäß vorigem Abs. 3 erfolgen ohne Entgelt und Auslagenersatz.

14 Kündigungsrechte

- 14.1 Der Auftraggeber ist berechtigt, die Vereinbarung außerordentlich kündigen, insbesondere wenn
- (i) ein erheblicher Verstoß des Auftragnehmers gegen geltende Gesetze, sonstige Vorschriften oder Vertragsbedingungen vorliegt;
 - (ii) Umstände, die im Laufe der Überwachung des Auftragnehmers festgestellt wurden und die vom Auftraggeber als geeignet eingeschätzt werden, die Wahrnehmung der im Rahmen der Vereinbarung vorgesehenen Funktionen zu beeinträchtigen, einschließlich wesentlicher Änderungen, die sich auf die Vereinbarung oder die Verhältnisse des IKT-Drittdienstleisters auswirken;
 - (iii) nachweisliche Schwächen des Auftragnehmer 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, vorliegen, und zwar

- unabhängig davon, ob es sich um personenbezogene oder anderweitig sensible Daten oder nicht personenbezogene Daten handelt,
- (iv) die für den Auftraggeber zuständige Behörde diesen infolge der Bedingungen oder Umstände im Zusammenhang mit der Vereinbarung nicht mehr wirksam beaufsichtigen kann,
 - (v) die für den Auftraggeber zuständige Behörde die vorzeitige Beendigung der Vereinbarung anordnet.
- 14.2 Weitergehende Kündigungsrechte beider Vertragsparteien im Leistungsvertrag bleiben unberührt.
- 14.3 Besteht der wichtige Grund in der Verletzung einer vertraglichen Pflicht aus der Zusatzvereinbarung, ist die Kündigung erst nach erfolglosem Ablauf einer zur Abhilfe bestimmten Frist oder nach erfolgloser Abmahnung zulässig. Etwas anderes gilt nur, wenn der Auftragnehmer die Leistung ernsthaft und endgültig verweigert, er die Leistung zu einem im Vertrag bestimmten Termin oder innerhalb einer bestimmten Frist nicht bewirkt, obwohl der Auftraggeber den Fortbestand ihres Leistungsinteresses vertraglich an die Rechtzeitigkeit der Leistung gebunden hat, oder wenn besondere Umstände vorliegen, die unter Abwägung der beiderseitigen Interessen eine sofortige Kündigung rechtfertigen.

15 Übergabephase

- 15.1 Bei Ausübung des Kündigungsrechtes durch eine Vertragspartei oder im Falle einer anderweitigen Beendigung des Leistungsvertrages verpflichtet sich der Auftragnehmer, an einer ordnungsgemäßen Übergabe mitzuwirken. Dafür erbringt der Auftragnehmer die erforderliche Unterstützung, um die Leistungserbringung durch den Auftraggeber oder durch einen Dritten zu ermöglichen (Beendigungsunterstützung). Der Auftraggeber ist berechtigt, ihm im Rahmen der Vertragsleistung eingeräumte Lizenzrechte während der Übergabephase weiterhin zu nutzen. Die Vereinbarung gilt, soweit nicht ein anderes vereinbart wird, während des Unterstützungszeitraumes fort.
- 15.2 Der Auftraggeber ist berechtigt, seine mittels der IKT-Dienstleistungen verarbeiteten Daten, bereits vor Beendigung des Leistungsvertrages zu exportieren und zu sichern. Im Falle einer außerordentlichen Kündigung ermöglicht der Auftragnehmer dem Auftraggeber den Export seiner Daten innerhalb einer angemessenen Frist, die mindestens ein (1) Kalendermonat nach Beendigung des Leistungsvertrages beträgt. Der Auftragnehmer ist verpflichtet, den Auftraggeber beim Datenexport zu unterstützen. Der Zugang des Auftraggebers zu den Daten ist auch im Falle der Insolvenz, Abwicklung oder Einstellung des Geschäftsbetriebs des Auftragnehmers zu gewährleisten.
- 15.3 Unterstützungsleistungen nach Ende des Leistungsvertrages, sowie darüber hinaus gehende Leistungen und deren Entgelt werden gesondert vereinbart. Ist der Vertrag infolge einer außerordentlichen Kündigung durch den Auftragnehmer aus Gründen beendet worden, die der Auftraggeber zu vertreten hat, so ist der Auftragnehmer nur gegen vorab zu leistende angemessene Abschlagzahlungen zur Unterstützung verpflichtet.
- 15.4 Der Auftraggeber wird dem Auftragnehmer die Nutzung der Arbeitsumgebung des Auftraggebers nach Ablauf der Vertragslaufzeit bzw. nach Ablauf des vereinbarten Unterstützungszeitraumes gestatten, soweit dies für die ordnungsgemäße Übergabe erforderlich ist. Die Parteien werden dafür eine gesonderte Vereinbarung schließen.
- 15.5 Der Auftraggeber ist berechtigt, aber nicht verpflichtet, zum Beendigungszeitpunkt Vertragsverhältnisse zu übernehmen, die der Auftragnehmer im Rahmen der Leistungserfüllung ausschließlich zur Erfüllung des Leistungsvertrages mit Unterauftragnehmern geschlossen hat. Der Auftraggeber ist des Weiteren berechtigt, mit Wirkung ab Beendigungszeitpunkt mit den vom Auftragnehmer für die Leistungserbringung beauftragten Unterauftragnehmern für die Erbringung dieser Leistungen unmittelbare Vereinbarungen abzuschließen.

16 Verhaltenskodex und Nachhaltigkeit

Der Auftragnehmer hält sich an die branchenüblichen und für ihn gegebenenfalls verpflichtend geltenden Nachhaltigkeitsstandards und Governancevorgaben.

17 Kosten

- 17.1 Der Auftragnehmer trägt sämtliche mit der Durchführung dieser Vereinbarung verbundenen Kosten. Ausgenommen hiervon sind die eigenen Aufwendungen des Auftraggebers; diese sind jedoch vom Auftragnehmer dem Auftraggeber zu erstatten, soweit dies anderweitig in dieser Vereinbarung bestimmt ist oder Ersatz aufgrund gesetzlicher Bestimmungen verlangt werden kann.
- 17.2 Der Auftragnehmer ist nicht berechtigt, zusätzliche Entgelte für die Ausübung der Informations- und Prüfungsrechte bei den Prüfungshandlungen der ILB oder anderer Prüfer zu verlangen, insbesondere für die Zurverfügungstellung der Prüfungsunterlagen/Berichte oder die Unterstützungsleistungen durch eine Person des Auftragnehmer vor Ort o. Ä..

18 Sonstiges

- 18.1 Mitteilungen, die nach dieser Zusatzvereinbarung abzugeben sind, bedürfen mindestens der Textform, wenn nicht wegen ihrer Eilbedürftigkeit oder vorübergehender technischer Unmöglichkeit der elektronischen Kommunikation die Einhaltung der Textform nicht geeignet oder möglich ist.
- 18.2 Dokumente und Unterlagen sind vom Auftragnehmer und den (Sub-)Subunternehmern dem Auftraggeber in einem elektronischen, allgemein verwendeten Format (pdf, Text-/Bilddatei) zur Verfügung zu stellen, soweit dem nicht berechnigte Geheimhaltungsgründe entgegenstehen.

(Ort, Datum)

(Ort, Datum)

(Auftraggeber)

(Auftragnehmer)

Anlagen:

-
-
-