

Anlage 04b – Bankenaufsichtliche Anforderungen

Inhaltsverzeichnis

Inhaltsverzeichnis	1
Präambel	2
1 Vereinbarungsgegenstand/Dienstleistungsgüte	2
2 Leistungsort / Ort der Datenspeicherung und Datenverarbeitung	3
3 Zusammenarbeit der Parteien	3
4 Zusammenarbeit mit den Behörden	4
5 Vergütung	4
6 Kündigung	5
7 Zugriff auf Daten	6
8 Internes Kontrollsystem	7
9 Datenschutz	8
10 Informationssicherheit (IKT-Sicherheit)	9
11 Haftung und Versicherung	10
12 Revisionsdienstleistungen durch den Auftragnehmer	10
13 Schlussbestimmungen	14
14 Definitionen und Auslegung	15

Präambel

Die von dem Dienstleister zu erbringenden Dienstleistungen stellen IKT-Dienstleistungen im Sinne von Art. 3 Nr. 21 DORA dar, die **nicht** kritische oder wichtige Funktionen des Instituts im Sinne von Art. 3 Nr. 22 DORA unterstützen. Das Institut und der Dienstleister sind sich einig und bewusst, dass in Bezug auf die Auslagerung von Vertragsleistungen die Letztverantwortung für eine ordnungsgemäße Geschäftsorganisation beim Institut verbleibt. Insofern ist das Vertragsverhältnis so zu verstehen und auszulegen, dass es dem Institut jederzeit und vollumfänglich möglich sein muss, alle Maßnahmen zu ergreifen, die erforderlich sind, um seiner aufsichtsrechtlichen Verantwortung gerecht zu werden und alle aufsichtsrechtlichen Anforderungen zu erfüllen. Der Dienstleister ist verpflichtet, das Institut dabei zu unterstützen und entsprechend alle Leistungen so auszuführen, dass dies gewährleistet ist.

Die Dienstleistungen sind in die Geschäfts- und Risikostrategie sowie in das IKS und Risikomanagement des Instituts eingebunden.

Mit Zuschlagserteilung vereinbaren die Parteien die folgenden aufsichtsrechtlich begründeten Verpflichtungen als Mindeststandards (sollten Anforderungen aus den weiteren Anlagen des Vergabeverfahrens über die Anforderungen aus diesem Dokument hinausgehen, gelten jeweils die höheren Anforderungen):

1 Vereinbarungsgegenstand/Dienstleistungsgüte

- 1.1 Das klare und vollständige Vertragsverhältnis („Dienstleistungen“) im Einzelnen ergibt sich aus den Vergabeunterlagen (insb. der Leistungsbeschreibung) und dem gem. Vergabeverfahren bezuschlagten Angebot sowie den zugehörigen Nachträgen. Die Beschreibung der zwischen den Parteien vereinbarten Dienstleistungsgüte, inklusive etwaiger Aktualisierungen und Überarbeitungen, ergibt sich ebenso daraus. Der Dienstleister ist verpflichtet, in jedem Fall eine für die Erbringung von IKT-Dienstleistungen im Finanzdienstleistungssektor angemessene Dienstleistungsgüte sicherzustellen.
- 1.2 Die Tätigkeiten qualifizieren sich ferner als digitale Dienste und Datendienste, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern dauerhaft bereitgestellt werden, einschließlich Hardware als Dienstleistung und Hardwaredienstleistungen, wozu auch technische Unterstützung durch den Hardwareanbieter mittels Software- oder Firmware-Aktualisierungen gehört, mit Ausnahme herkömmlicher analoger Telefondienste („IKT-Dienstleistungen“).

- 1.3 Im Falle der Nichteinhaltung der vertraglich vereinbarten Dienstleistungsgüte kann das Institut vom Dienstleister die unverzügliche Umsetzung von Korrekturmaßnahmen verlangen, die für das Erreichen der vertraglich vereinbarten Dienstleistungsgüte notwendig sind.

2 Leistungsort / Ort der Datenspeicherung und Datenverarbeitung

- 2.1 Der Dienstleister erbringt die Vertragsleistungen (einschließlich der Speicherung oder Verarbeitung von Daten) ausschließlich an den in der Leistungsbeschreibung und den Anlagen genannten Standorten. Der Ort der zu erbringenden Leistungen ist der beigefügten Anlage Standortliste NBank zu entnehmen. Die Vereinbarungen schreiben auch die Leistungsorte und Standorte der Unterauftragnehmer und Back-Ups fest.
- 2.2 Eine Verlagerung des Ortes der Leistungserbringung (einschließlich der Speicherung und/oder Verarbeitung von Daten) setzt die vorherige Information des Instituts voraus. Der Dienstleister wird vor einer möglichen Verlagerung das Institut so rechtzeitig vorher informieren, dass dem Institut eine Risikobewertung der geplanten Verlagerung möglich ist, mindestens jedoch 90 Tage im Voraus. Dies gilt unabhängig davon, ob die Verlagerung innerhalb des Inlands oder ins Ausland erfolgen soll. Eine Verlagerung des Ortes der Leistungserbringung (einschließlich der Speicherung und/oder Verarbeitung von Daten) außerhalb des EWR ist nicht erlaubt.
- 2.3 Hat der Dienstleister seinen Sitz in einem Drittstaat, hat es einen inländischen Zustellungsbevollmächtigten zu benennen, an den unter anderem Bekanntgaben und Zustellungen durch die BaFin bewirkt werden können.

3 Zusammenarbeit der Parteien

- 3.1 Die Parteien werden hinsichtlich der Dienstleistung vertrauensvoll zusammenarbeiten. Insbesondere werden die Parteien, soweit erforderlich, daran mitwirken, dass die in den Leistungsbeschreibungen und in den Serviceverträgen beschriebenen Leistungen in der dort festgelegten Art und mit der dort festgelegten Qualität sowie in Einklang mit den aufsichtsrechtlichen Anforderungen an das Institut erfüllt werden können („**Mitwirkungspflichten**“). Dies gilt insbesondere bei Änderungen der einschlägigen aufsichtsrechtlichen Vorgaben oder bei Einwendungen der zuständigen Aufsichtsbehörden.

- 3.2 Zur Erfüllung der Mitwirkungspflichten werden sich die Parteien die erforderlichen Ressourcen und Informationen gegenseitig kostenfrei zur Verfügung stellen. Hierzu zählt insbesondere die gegenseitige Zurverfügungstellung einer inhaltlich ausreichenden, strukturierten und verarbeitbaren Datengrundlage. Soweit erforderlich und nach den allgemeinen aufsichtsrechtlichen Organisationsanforderungen an eine Bank zulässig, umfassen die Mitwirkungspflichten auch die gegenseitige Gewährung des Zugangs zu den Räumlichkeiten der Parteien. Vorbehaltlich abweichender Regelungen in den Serviceverträgen umfassen die Mitwirkungspflichten auch die Einräumung von Nutzungsrechten an den Programmen, Verfahren und am geistigen Eigentum der Parteien, soweit dies zu Erbringung der Dienstleistungen erforderlich ist.
- 3.3 Die Parteien sind sich einig darüber, dass das Institut für die Einhaltung der gesetzlichen Bestimmungen für Banken nach deutschem und europäischem Aufsichtsrecht verantwortlich bleibt und die letztendliche aufsichtsrechtliche Verantwortung für die Funktionen trägt, die Gegenstand der Dienstleistung sind. Im Übrigen wird der Dienstleister das Institut, sofern angemessen und dem Dienstleister möglich, jederzeit bei der Erfüllung seiner Pflichten aus der DORA, den begleitenden Rechtsakten und aus anderen einschlägigen nationalen und europarechtlichen Rechtsvorschriften unterstützen. Zu diesem Zweck wird das Dienstleister dem Institut auf Anfrage die ihm vorliegenden Informationen zur Verfügung stellen, die für die Erfüllung dieser Pflichten notwendig sind.
- 3.4 Die Parteien vereinbaren, bei einem Notfall vertrauensvoll nach dieser Ziffer zusammenzuarbeiten, um die Folgen des Notfalls schnellstmöglich zu überwinden und die weitere Erbringung der geschuldeten Dienstleistungen sicherzustellen. Ein Notfall liegt insbesondere im Fall einer Katastrophe oder eines teilweisen oder vollständigen Verlusts der Infrastruktur der Parteien durch Feuer, Überschwemmung, Erdbeben, Kabelbruch oder ähnliche Ereignisse vor. Die Parteien implementieren und überwachen Maßnahmen, um bei einem Systemausfall die Speicherung der Daten zu gewährleisten und regelmäßige Daten-Backups sicherzustellen.
- 3.5 Die Parteien koordinieren und testen regelmäßig ihre notfallbezogenen Maßnahmen und stimmen diese aufeinander ab.

4 Zusammenarbeit mit den Behörden

- 4.1 Der Dienstleister wird vollumfänglich mit den für das Institut zuständigen Behörden und Abwicklungsbehörden, einschließlich der von diesen benannten Personen, zusammenarbeiten.

5 Vergütung

- 5.1 Die Vergütung richtet sich ausschließlich nach dem Preisblatt (Anlage 07) und dem bezuschlagten Angebot. Diese Anlage begründet keine zusätzlichen Vergütungsansprüche des Dienstleisters, soweit nicht ausdrücklich etwas Abweichendes durch das Institut beauftragt wird.
- 5.2 Die Vergütung ist - soweit die erbrachten Dienstleistungen nicht von der Umsatzsteuer befreit sind - zzgl. der gesetzlichen Umsatzsteuer zu entrichten. Der Dienstleister erteilt dem Institut eine ordnungsgemäße Rechnung im Sinne des § 14 UStG.
- 5.3 Fälligkeit, Zahlungsweise und Rechnungsstellung richten sich nach dem Preisblatt (Anlage 07), dem EVB-IT Instandhaltungsvertrag (Anlage 04) sowie dem bezuschlagten Angebot. Rechnungen sind als PDF-Datei an rechnungen@nbank.de zu senden.

6 Kündigung

- 6.1 Die Vertragslaufzeit richtet sich ausschließlich nach der Leistungsbeschreibung (Anlage 03), dem EVB-IT Instandhaltungsvertrag (Anlage 04) sowie dem bezuschlagten Angebot. Eine darüberhinausgehende Grundlaufzeit, automatische Verlängerung oder Verlängerungsoption wird durch diese Anlage nicht begründet.
- 6.2 Eine Kündigung einer etwaig vorliegenden Rahmenvereinbarung beendet auch alle unter ihm abgeschlossenen Serviceverträge, sollte nicht explizit eine andere Regelung getroffen werden. Die Parteien sind jedoch im Rahmen einer ordnungsgemäßen Abwicklung dazu verpflichtet, die gemäß den Serviceverträgen noch offenen Leistungen ungeachtet der Kündigung dieses Vertragsverhältnisses für einen zur Abwicklung angemessenen Zeitraum, längstens aber bis zum nächstmöglichen Kündigungszeitpunkt, zu erbringen.
- 6.3 Wird eine unter diesem Vertragsverhältnis abgeschlossene Leistung gekündigt, so bleiben der etwaig vorliegende Rahmenvertrag und die übrigen Leistungen hiervon unberührt, sofern die Parteien nicht eine andere Vereinbarung getroffen haben.
- 6.4 Jede Partei kann dieses Vertragsverhältnis ohne Einhaltung einer Kündigungsfrist aus wichtigem Grund kündigen.
- 6.5 Jede Kündigung dieses Vertrages oder eines Servicevertrages bedarf der Schriftform. Das Institut kann diesen Vertrag jederzeit ohne Einhaltung einer Kündigungsfrist kündigen, wenn einer der folgenden Umstände vorliegt:
 - 6.5.1 bei einem Verstoß des Dienstleisters gegen geltende Gesetze, sonstige Vorschriften oder Vertragsbedingungen;

- 6.5.2 wenn Umstände vorliegen, die im Laufe der Überwachung des IKT-Drittparteienrisikos festgestellt wurden und als geeignet eingeschätzt werden, die Wahrnehmung der im Rahmen der vertraglichen Vereinbarung vorgesehenen Funktionen zu verändern oder beeinträchtigen, einschließlich wesentlicher Änderungen, die sich auf die Vereinbarung oder die Verhältnisse des Dienstleisters auswirken;
- 6.5.3 bei nachweislichen Schwächen des Dienstleisters 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;
- 6.5.4 wenn die zuständige Behörde das Institut infolge der Bedingungen der vertraglichen Vereinbarung zwischen den Parteien oder der mit der vertraglichen Vereinbarung verbundenen Umstände nicht mehr wirksam beaufsichtigen kann;
- 6.5.5 wenn die für das Institut zuständige Behörde oder Abwicklungsbehörde die Beendigung der vertraglichen Vereinbarung verlangt;
- 6.5.6 wenn Hindernisse identifiziert wurden, die die wirksame Bereitstellung der Dienstleistungen gemäß dem vereinbarten Leistungsniveau wesentlich beeinträchtigen können;
- 6.5.7 wenn ein Dienstleister mit Sitz in einem Drittland als kritischer IKT-Dienstleister nach Art. 31 DORA eingestuft wurde und nicht innerhalb von 12 Monaten ab dieser Einstufung ein Tochterunternehmen in der Europäischen Union gegründet hat und die vertraglich vereinbarte IKT-Dienstleistung über dieses Tochterunternehmen erbringt.
- 6.6 Der Dienstleister kann diesen Vertrag nicht aufgrund einer Umstrukturierung oder Abwicklung des Instituts kündigen, aussetzen oder ändern, solange das Institut seinen Zahlungspflichten nachkommt.

7 Zugriff auf Daten

- 7.1 Der Dienstleister hat dafür Sorge zu tragen, dass die in ihrem Besitz oder unter ihrer Kontrolle befindlichen personenbezogenen und nicht-personenbezogenen Daten auch im Falle der Insolvenz, Abwicklung, der Auflösung oder der Einstellung des Geschäftsbetriebs oder einer Beendigung der vertraglichen Vereinbarung zugänglich bleiben. Auf jederzeitiges Verlangen des Instituts hin ist der Dienstleister verpflichtet, die Daten in einem leicht zugänglichen, für die Art der jeweiligen Daten branchenüblichen (leicht zugänglichem) Format an das Institut oder einen von diesem benannten Dritten herauszugeben. Der Dienstleister ist verpflichtet, alle erforderlichen Vorkehrungen zu treffen, um dem Herausgabeverlangen des Instituts jederzeit unmittelbar entsprechen zu können. Die Verpflichtung nach Satz 1 gilt für solche Daten, die der Dienstleister im Zusammenhang mit oder infolge der Erbringung der Dienstleistungen erhebt oder speichert und die im Eigentum des Instituts stehen oder zu deren Besitz oder Zugriff das Institut nach Ablauf oder Beendigung dieses Vertrages nach geltendem Recht verpflichtet ist.

8 Internes Kontrollsystem

- 8.1 Die Pflicht zu prozessbegleitenden, internen Kontrollen wird vom Dienstleister übernommen. Der Dienstleister verpflichtet sich, ein funktionsfähiges Internes Kontrollsystem für die Bereiche vorzuhalten, die von den vereinbarten IT-Services betroffen sind.
- 8.2 Der Dienstleister etabliert ein dienstleistungsbezogenes Internes Kontrollsystem (nachfolgend „IKS“). Dieses ist funktional von dem Risikomanagement getrennt.
- 8.3 Das IKS umfasst sowohl die Geschäfts- und Service-Prozesse in der Organisation als auch die kundenbezogene Leistungserbringung. Die Bestandteile des IKS sind in die technischen und organisatorischen Abläufe integriert (Prozesslandkarte) und werden von der Geschäftsführung, den Prozess- bzw. Kontrollverantwortlichen sowie den operativen Fachbereichen gemeinsam aktiv ausgeübt.
- 8.4 Der Dienstleister verfügt im Rahmen des IKS über eine Standard-Kontrollmatrix. Die in der Standard-Kontrollmatrix enthaltenen Kontrollen werden dem Institut entsprechend des mit ihm vereinbarten Leistungsschnitts zugeordnet.
- 8.5 Dem Institut wird jährlich ein Bericht nach dem IDW-Prüfungsstandard 951 Typ 2 über die „Prüfung des internen Kontrollsystems beim Dienstleistungsunternehmen für auf das Dienstleistungsunternehmen ausgelagerte Funktionen“ zur Verfügung gestellt. Der Bericht wird von einer externen Wirtschaftsprüfungsgesellschaft ausgestellt.
- 8.6 Erweiterte Kontrollen zur Standard-Kontrollmatrix des IKS treten auf, wenn nach Beauftragung durch das Institut von den standardisierten Kontrollaktivitäten und den definierten Verfahren im IKS abgewichen wird. Die Aufnahme und Durchführung von kundenindividuellen Kontrollen im IKS sowie der damit verbundene Aufwand sind gesondert zu vereinbaren und werden zusätzlich in Rechnung gestellt.

9 Datenschutz

- 9.1 Die Parteien sind sich der besonderen Bedeutung des Datenschutzes und der Informationssicherheit bewusst. Sie werden insoweit die datenschutzrechtlichen Bestimmungen, insbesondere der EU-DSGVO und des BDSG, einhalten, durch geeignete Maßnahmen für die Zugänglichkeit, die Vertraulichkeit, die Verfügbarkeit und die Richtigkeit/Integrität und Authentizität der Daten sorgen, die praktische Handhabung der datenschutzrechtlichen Bestimmungen fortlaufend überprüfen und diese bei Bedarf anpassen.
- 9.2 Personenbezogene Daten sind durch angemessene technische und organisatorische Maßnahmen vor unbefugtem Umgang zu schützen. Die für die Erbringung der Leistungen eingesetzten Systeme sind insbesondere gegen unbefugte oder zufällige Vernichtung, zufälligen Verlust, technische Fehler, Fälschung, Diebstahl, widerrechtliche Verwendung, unbefugtes Ändern, Kopieren, Zugreifen und andere unbefugte Bearbeitungen zu schützen.
- 9.3 Soweit die Parteien im Rahmen ihrer Zusammenarbeit unter diesem Vertrag oder unter den jeweiligen Leistungsbeschreibungen oder Serviceverträgen personenbezogene Daten für die jeweils andere Partei im Auftrag verarbeiten, schließen sie einen Auftragsverarbeitungsvertrag ab. Soweit die Parteien im Rahmen ihrer Zusammenarbeit unter diesem Vertrag oder unter den jeweiligen Leistungsbeschreibungen oder Serviceverträgen personenbezogene Daten als gemeinsame Verantwortliche verarbeiten, schließen sie eine Vereinbarung über die gemeinsame Verantwortlichkeit ab. Die Vereinbarungen im Sinne des Satzes 1 und 2 regeln abschließend die zwischen den Parteien bestehenden datenschutzrechtlichen Rechte und Pflichten.
- 9.4 Die Parteien haben durch geeignete organisatorische, personelle, technische und bauliche Maßnahmen sicherzustellen, dass alle vertraulichen Informationen über die Parteien, ihre Kunden und Geschäftspartner geschützt werden. Die Zugriffsregelungen auf die von den Parteien in Erfüllung ihrer vertraglichen Verpflichtungen nach diesem Vertrag eingesetzten Datenverarbeitungssysteme müssen diesen Anforderungen entsprechen, wobei der Zugriff auf die betreffenden Daten auf entsprechend befugte Personen beschränkt sein muss.
- 9.5 Die Parteien legen sich gegenseitig jährlich einen Datenschutzbericht vor, der insbesondere die im Berichtszeitraum aufgetretenen datenschutzrelevanten Vorfälle, durchgeführte Datenschutz- und IT-Sicherheitsmaßnahmen, Audit- und Kontrollergebnisse zum Datenschutz und zur IT-Sicherheit, Bewertungen des Datenschutzniveaus und geplante Datenschutz- und IT-Sicherheitsmaßnahmen enthält.

- 9.6 Die Parteien werden diesen Vertrag und die Leistungsbeschreibungen und Serviceverträge streng vertraulich behandeln und nur mit Zustimmung der anderen Partei Dritten zugänglich machen. Dies gilt nicht, soweit eine Partei aufgrund geltendem Recht oder einer behördlichen Anordnung zur Offenlegung verpflichtet ist. In diesem Fall wird sie die jeweils andere Partei vor der Offenlegung oder, soweit dies nicht möglich ist, unverzüglich nach Offenlegung über die Umstände der Offenlegung informieren

10 Informationssicherheit (IKT-Sicherheit)

- 10.1 Der Dienstleister verpflichtet sich über die Dauer des Vertragsverhältnisses zwischen den Parteien fortlaufend angemessene Qualitätsstandards für die Informationssicherheit einzuhalten. Die konkreten vom Dienstleister umzusetzenden Maßnahmen ergeben sich aus den Anlagen gem. Vergabeverfahren und insb. aus dem („Sollmaßnahmenkatalog“). Die ausgefüllte Anlage ist dem Institut innerhalb von 4 Wochen nach Vertragsschluss zu übermitteln. Der Dienstleister wird die Einhaltung dieser Qualitätsstandards für Informationsstandards kontinuierlich überwachen.
- 10.2 Ergänzend zu den Maßnahmen der Anlage Sollmaßnahmenkatalog muss das der Dienstleister in der Lage sein, einschlägige technologische Entwicklungen zu überwachen, führende IKT-Sicherheitspraktiken umzusetzen, Bedrohungen zu identifizieren und zu bewerten und IKT-Risiken zu managen, um über einen wirksamen und soliden Rahmen für die digitale betriebliche Widerstandsfähigkeit zu verfügen. Grundsätzlich sollen der ISO 27001-Standard oder der BSI-Standard eingehalten werden, wobei der Betrachtungsgegenstand der Standards die vereinbarte Dienstleistung umfassen muss. Die Maßnahmen zur Umsetzung der oben genannten Standards haben dem jeweils aktuellen Stand der Technik und den geltenden gesetzlichen und regulatorischen Anforderungen zu entsprechen. Dabei ist sicherzustellen, dass das vertraglich vereinbarte Schutzniveau insgesamt nicht unterschritten wird. Wesentliche Änderungen, welche die Informationssicherheit nachteilig beeinträchtigen könnten, sind dem Institut in Textform mitzuteilen.
- 10.3 Der Dienstleister wird ein übergreifendes Programm für das regelmäßige, anlassbezogene und risikoorientierte Testen der digitalen operationalen Resilienz von IKT-Systemen und -Anwendungen einsetzen, welche für die Erbringung der IKT-Dienstleistung eingesetzt werden. Für identifizierte Schwachstellen wird der Dienstleister Aktionspläne erstellen und deren Umsetzung verfolgen.

- 10.4 Im Falle eines IKT-Vorfalles, welcher in Verbindung mit der für das Institut erbrachten IKT-Dienstleistung steht, wird der Dienstleister dem Institut ohne zusätzliche Kosten vollumfänglich unterstützen. Verschuldet das Institut den IKT-Vorfall, hat das Institut der Dienstleister (für die nachgewiesenen Kosten für die Unterstützungsleistung) angemessen zu entschädigen. Der Dienstleister wird das Institut in jedem Fall unverzüglich über den IKT-Vorfall informieren, damit das Institut seiner Meldepflicht nach Art. 19 DORA nachkommen kann. Mündlich erfolgte Meldungen sind dem Institut in Textform nachzureichen.
- 10.5 Der Dienstleister stellt sicher, dass seine internen und externen Mitarbeiter angemessen geschult und sensibilisiert sind, um ihrer Rolle zur Aufrechterhaltung der Informationssicherheit gerecht zu werden und um eine Anomalie oder einen IKT-Vorfall erkennen und melden zu können. Der Dienstleister wird, sofern das Institut ihn hierzu auffordert, an den vom Institut angebotenen Programmen zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz im Sinne von Art. 13 Abs. 6 DORA teilnehmen. Sofern der Dienstleister zur Erbringung der vertraglich geschuldeten IKT-Dienstleistungen IKT-Systeme des Instituts nutzt, ist er verpflichtet, die hierfür geltenden Anweisungen und Nutzungsbedingungen des Instituts zu beachten.

11 Haftung und Versicherung

- 11.1 Der Dienstleister haftet für alle vorsätzlichen und fahrlässigen Pflichtverletzungen.
- 11.2 Ebenfalls haftet der Dienstleister dafür, dass durch seine Vertragsleistungen Urheberrechte, Lizenzrechte oder vergleichbare Rechte Dritter nicht verletzt werden. Es stellt das Institut von derartigen Ansprüchen Dritter frei.
- 11.3 Der Dienstleister ist verpflichtet, eine Betriebshaftpflichtversicherung zu unterhalten, die Personen-, Sach- und Vermögensschäden abdeckt. Es hat dem Institut vor Unterzeichnung den genauen Deckungsumfang schriftlich nachzuweisen. Sollten sich während der Laufzeit dieses Vertrages im Zusammenhang mit der Betriebshaftpflicht Änderungen ergeben, ist der Dienstleister verpflichtet, das Institut unverzüglich schriftlich darüber zu informieren. Vor Ablauf ist der jeweils aktualisierte Versicherungsnachweis unaufgefordert vorzulegen. Die in den Bewerbungsbedingungen definierten Mindestdeckungssummen dürfen nicht unterschritten werden.
- 11.4 Für Subunternehmen und Erfüllungsgehilfen haftet der Dienstleister wie für eigenes Tun respektive für eigene Mitarbeiter.
- 11.5 Die Parteien haben sich jeweils gegenseitig über Schäden unverzüglich nach Kenntnis zu informieren.

12 Revisionsdienstleistungen durch den Auftragnehmer

12.1 Leistungsbeschreibung

Die Funktion der Internen Revision wird in Bezug auf die ausgelagerte Leistung durch die Interne Revision des Auftragnehmers wahrgenommen. Die Interne Revision führt als Organisationseinheit objektive und unabhängige Prüfungen im Rahmen der vertragsgemäßen Leistungserbringung durch, insbesondere hinsichtlich des Risikomanagements, des internen Kontrollsystems sowie der Aufbau- und Ablauforganisation. Die Revision des Auftragnehmers ist weisungsfrei, prozessunabhängig und hat ein uneingeschränktes Informationsrecht in der Organisation. Der Auftragnehmer stellt sicher, dass seine Interne Revision den gegenwärtigen und künftigen aufsichtsrechtlich zu beachtenden Grundsätzen zur Ausgestaltung der Internen Revision (insbesondere nach Maßgabe des jeweils geltenden BaFin-Rundschreibens zu den MaRisk in der jeweils aktuellen Fassung entspricht. Die Parteien sind sich bewusst, dass die BaFin auch unmittelbar gegenüber dem Auftragnehmer im Einzelfall Anordnungen treffen kann.

12.2 Wahrnehmung der Revisionsfunktion

Risikoorientiert und prozessunabhängig sind beim Auftragnehmer und bei allen zur Leistungserbringung vom Auftragnehmer eingesetzten Subunternehmern die Wirksamkeit und Angemessenheit des Risikomanagements im Allgemeinen und des internen Kontrollsystems im Besonderen sowie die Ordnungsmäßigkeit grundsätzlich aller für die Leistungserbringung relevanter Aktivitäten und Prozesse durch die Interne Revision zu prüfen und zu beurteilen.

Die Funktion der Internen Revision wird in Bezug auf die Vertragsleistungen durch die Interne Revision des Auftragnehmers wahrgenommen. Die Interne Revision des Auftragnehmers und des jeweiligen Auftraggebers werden vertrauensvoll zusammenarbeiten. Der Auftragnehmer stellt sicher, dass seine Interne Revision den gegenwärtigen und künftigen aufsichtsrechtlich zu beachtenden Grundsätzen zur Ausgestaltung der Internen Revision (insbesondere nach Maßgabe des jeweils geltenden BaFin-Rundschreibens zu MaRisk in der jeweils aktuellen Fassung entspricht. Die Parteien sind sich bewusst, dass die BaFin auch unmittelbar gegenüber dem Auftragnehmer im Einzelfall Anordnungen treffen kann.

12.3 Prüfung durch Auftragnehmer

Der Auftragnehmer wird den Auftraggebern unverzüglich und unaufgefordert alle für die vertraglichen Leistungen relevanten Prüfungsberichte der Internen Revision zuleiten. Der Auftragnehmer wird die vertraglichen Leistungen nach dem Prüfungsstandard IDW PS 951 durch einen inländischen Wirtschaftsprüfer prüfen lassen. Die Prüfung beinhaltet auch die Beurteilung der Funktionsfähigkeit der Internen Revision des Auftragnehmers im Sinne der MaRisk. Die Prüfung darf sich hierbei nicht auf die beauftragten Sachverhalte beschränken, sondern soll auch die zu dessen Erfüllung benötigten Ressourcen und Prozesse einschließen.

12.4 Grundsatz der Abstimmung

Die Interne Revision des Auftragnehmers wird sich mit der Internen Revision des jeweiligen Auftraggebers über den Prüfungsplan (Jahres- bzw. Mehrjahresplan) abstimmen, und die Auftraggeber über Anpassungen des Prüfungsplans in Kenntnis setzen. Zur Prüfung der ordnungsgemäßen Revisionsfunktion durch den Auftragnehmer stehen der Internen Revision des jeweiligen Auftraggebers hinreichende Zugangs-, Zutritts-, Zugriffs-, Informations- und Prüfungsrechte gemäß § 15 dieser Anlage zu.

12.5 Abstimmungs-Meetings

Die Parteien halten mindestens quartalsweise ein Meeting zur Abstimmung ab, dessen Termine zwischen den Parteien abzustimmen sind. Die Meetings finden grundsätzlich per Video- oder Telefonkonferenz statt. Auf Wunsch einer Partei ist ein Service-Meeting als Präsenz-Meeting durchzuführen.

12.6 Inhalte der Meetings

Im Rahmen der Meetings werden Themen betreffend die Arbeitsweise der Internen Revision der jeweiligen Partei behandelt. Insbesondere handelt es sich hierbei um Themen:

- neue Revisionsberichte,
- Stand Prüfungsplan,
- Wesentliche Feststellungen,
- Tracking-Status.

Eine Dokumentation der Inhalte und Ergebnisse der Service-Meetings in Form eines Protokolls erfolgt unverzüglich nach den Meetings. Das Protokoll ist von dem Auftragnehmer in Textform zu erstellen und zwischen den Parteien abzustimmen.

12.7 Follow-Up Prozess

Der Auftragnehmer wird einen transparenten und für Dritte nachvollziehbar dokumentierten Prozess etablieren, um den Abarbeitungsfortschritt von in Prüfungen festgestellten Mängeln bzw. der hierzu vereinbarten Maßnahmen zu verfolgen („Follow-Up Prozess“). Die Dokumentation zum Follow-Up Prozess hat mindestens die Informationen über Anzahl und Gewicht offener Mängel sowie Erledigungstermine, etwaige Fristüberschreitungen und Prolongationen darzustellen. Hierzu wird der Auftragnehmer einen entsprechenden Bericht zur Verfügung stellen.

12.8 Prüfungen und Anordnungen

Die Auftraggeber beabsichtigen, von dem vertraglich vereinbarten Prüfungsrecht themen- oder anlassbezogen, auch durch den Einsatz externer Prüfungsgesellschaften, zur Prüfung des Auftragnehmers Gebrauch zu machen. Hierzu werden die Auftraggeber dem Auftragnehmer Zeitraum und Inhalt der jeweiligen Prüfung zeitnah vor Prüfbeginn mitteilen.

12.9 Revisionsberichterstattung

Die Berichte sind von der vertraglichen Vergütung für die Vertragsleistungen umfasst und sind nicht gesondert zu vergüten. Sofern in dieser Anlage nichts anderes bestimmt ist, sind die Berichte spätestens innerhalb von 2 Wochen nach dem jeweiligen Monats-, Quartals- bzw. Jahresende zu liefern. Der Auftragnehmer verpflichtet sich, der Internen Revision und der für die Leistungserbringung zuständigen Stelle des jeweiligen Auftragnehmers die in Anhang 3 definierten Berichte in elektronischer Form zur Verfügung zu stellen. Soweit nicht anders angegeben, sind die Berichte zu gegebenen Daten oder nach ihrer Erstellung unverzüglich zu übersenden.

Revision		
Ergebnisse der Prüfungen der Internen Revision des Auftragnehmers	Vollständige Revisionsberichte inklusive der Einzelfeststellungen; die Berichterstattung muss auch Prüfungsergebnisse zu Nebenpflichten (z. B. Datenschutz, BCM, IKS, Informationssicherheit, Personal, ISMS) und Basisleistungen (Infrastruktur, Gebäude, Clouddienste) enthalten. Die Interne Revision des Auftragnehmers wird insbesondere auch unverzüglich und unaufgefordert über ihre Erkenntnisse berichten, soweit die Ordnungsmäßigkeit, Sicherheit und Verfügbarkeit der Leistungserbringung durch den Auftragnehmer maßgeblich berührt sind.	Unverzüglich nach Fertigstellung der jeweiligen Berichte

Quartalsbericht	Berichterstattung zur Einhaltung des Prüfungsplans, neuen wesentlichen Feststellungen, Follow-up Status und anderen Aktivitäten der Internen Revision.	Quartalsweise
Prüfungsplan der Internen Revision des Auftragnehmers	Übersendung des Prüfungsplans (Mehrjahres- und Jahresplan) der Internen Revision des Auftragnehmers sowie bei Änderungen einen aktualisierten Prüfungsplan mit Begründung der Änderung nebst Nachweis des entsprechenden Geschäftsleitungsbeschlusses des Auftragnehmers	Jährlich; anlassbezogen
Prüfungsbericht des IKS	Übersendung des Berichts der Prüfung nach IDW PS 951. n.F. Typ 2 oder ISAE 3402 bezüglich des Auftragnehmers; in dem Bericht ist die Funktionsfähigkeit der Internen Revision des Auftragnehmers ausdrücklich zu bestätigen.	Jährlich, jeweils nach Prüfung
Ergebnisse aufsichtsrechtlicher Prüfungen	Bekanntgabe der Ergebnisse aufsichtsrechtlicher Prüfungen (z. B. nach Art. 12 der EU-Verordnung 1024/2013 oder § 44 Abs. 1 KWG) mit Relevanz für den ausgelagerten Bereich	Unverzüglich
Bewertungsmethode	Bekanntgabe der Bewertungsmethode der Internen Revision des Auftragnehmers für Berichte und Feststellungen	Aufnahme in Quartalsbericht
Meldung bei behördlichen Auskunftersuchen oder bevorstehenden aufsichtsrechtlichen Prüfungen oder Maßnahmen	Der Auftragnehmer wird die Auftraggeber unverzüglich – vorbehaltlich etwaiger Verschwiegenheitspflichten – unterrichten, sofern es selbst von einer Behörde um Auskunft ersucht oder von bevorstehenden aufsichtsrechtlichen Maßnahmen unterrichtet oder solchen Prüfungen oder Maßnahmen unterworfen wird, sowie sofern sich solche Auskunftsverlangen, Prüfungen oder Maßnahmen auf die vertragsgegenständlichen Leistungen beziehen	Unverzüglich

13 Schlussbestimmungen

- 13.1 Der Dienstleister bestätigt, notwendige Maßnahmen gemäß § 2 Abs. 7 Nr. 2 der IVV vorzunehmen. Hierzu ist der Dienstleister während der Dauer dieses Vertragsverhältnisses verpflichtet, erforderliche Vorkehrungen zu treffen, wonach ein möglicherweise variabel ausgestalteter Vergütungsanteil an in die Erbringung der Vertragsleistungen unmittelbar einbezogene Mitarbeiter den Anforderungen der IVV nicht zuwiderlaufen darf.
- 13.2 Die Vereinbarung unterliegt dem deutschen Recht unter Ausschluss des UN-Kaufrechts.
- 13.3 Gerichtsstand ist Hannover.

- 13.4 Jede Änderung oder Ergänzung dieser Anlage und/oder der unter dieser Vereinbarung abzuschließenden Servicevertrag bedarf zu ihrer Wirksamkeit der Schriftform, soweit nicht nach zwingendem Recht eine strengere Form vorgeschrieben ist. Sie sind durch alle Parteien zu datieren und unterzeichnen.
- 13.5 Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam oder nichtig sein oder werden, so wird hierdurch die Gültigkeit der übrigen Bestimmungen nicht berührt. In einem solchen Fall sollen die unwirksamen oder nichtigen Bestimmungen vielmehr so ausgelegt, umgedeutet oder ersetzt werden, dass der mit ihnen beabsichtigte rechtliche und wirtschaftliche Zweck erreicht wird.
- 13.6 Diese Anlage gilt mit Zuschlagserteilung.
- 13.7 Die Parteien werden im Falle einer Veränderung des Aufsichtsrechts sowie im Falle einer Änderung der Verwaltungspraxis der zuständigen Behörden nach Treu und Glauben über eine Vertragsanpassung verhandeln, um die geänderte Anforderungslage vertraglich abzubilden. Dasselbe gilt im Falle einer Änderung von internen Leit- oder Richtlinien beim Institut, welche eine Anpassung des Vertragsverhältnisses notwendig machen.

14 Definitionen und Auslegung

- 14.1 Begriffe, die in dieser Anlage definiert wurden, haben die Bedeutung, die in dieser Anlage festgelegt wird.

Aufsichtsmitteilung Cloud-Anbieter	Aufsichtsmitteilung der BaFin zu Auslagerungen an Cloud-Anbieter in der Fassung vom Februar 2024
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BDSG	Bundesdatenschutzgesetz
BCM	Business Continuity Management
BGB	Bürgerliches Gesetzbuch in seiner jeweils gültigen Fassung
BSI	Bundesamt für Sicherheit in der Informationstechnik

BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik in seiner jeweils gültigen Fassung
EU-DSGVO	Verordnung (EU) 2016/679 vom 27. April 2016 (Datenschutz-Grundverordnung).
DORA	Verordnung (EU) 2022/2554 vom 14. Dezember 2022 (Digital Operational Resilience Act)
EBA	European Banking Authority
EBA-Leitlinien zu Auslagerungen	Leitlinien der EBA zu Auslagerungen (EBA/GL/2019/02 „EBA Guidelines on Outsourcing Arrangements“) in ihrer jeweils gültigen Fassung
EU	Die Europäische Union
EWR	Der Europäische Wirtschaftsraum
EZB	Europäische Zentralbank
IKS	Internes Kontrollsystem
IKT	Informations- und Kommunikationstechnologie
ISMS	Informationssicherheitsmanagementsystem
IT	Informationstechnik bzw. Informationstechnologie
KWG	Kreditwesengesetz in seiner jeweils gültigen Fassung
MaRisk	Rundschreiben 06/2024 der BaFin „Mindestanforderungen an das Risikomanagement der Kreditinstitute“ in seiner jeweils gültigen Fassung

MB	Megabyte
MiLoG	Mindestlohngesetz in seiner jeweiligen Fassung
PDF	Portable Document Format
PSD2	Payment Services Directive 2
SAG	Sanierungs- und Abwicklungsgesetz in seiner jeweils gültigen Fassung
SLA	Service Level Agreement
SREP	Leitlinien der EBA zu gemeinsamen Verfahren und Methoden für den aufsichtlichen Überprüfungs- und Bewertungsprozess (Supervisory Review and Evaluation Process, SREP) sowie für die aufsichtlichen Stresstests (EBA/GL/2018/03) in ihrer jeweils gültigen Fassung
UStG	Umsatzsteuergesetz in seiner jeweils gültigen Fassung