

## **Kritisch oder wichtige Funktionen - Stand: 20.10.2025**

### **Ergänzungsvereinbarung über die Mindestinhalte nach Art. 30 Abs. 3 DORA**

zu

#### **betroffener Vertrag**

nachfolgend „Vertragswerk“ genannt

zwischen der

#### **LfA Förderbank Bayern**

Königinstraße 17  
80539 München

nachfolgend „LfA“ genannt

und der

#### **Name des Auftragnehmers**

Straße, Hausnummer  
PLZ, Ort

nachfolgend „Auftragnehmer“ genannt

nachfolgend gemeinsam „Vertragspartner“ genannt

# Inhaltsverzeichnis

Inhaltsverzeichnis.....	2
Präambel .....	4
1    Geltungsbereich und Rangfolge.....	4
2    Leistungsinhalte (Art. 30 Abs. 2 (a) DORA) .....	5
2.1  Leistungsbeschreibung .....	5
2.2  Leistungsgüter / Service Level und KPIs (Art. 30 Abs. 2 (e), Art. 30 Abs. 3 (a) DORA) .....	6
2.3  Vertragsänderung.....	6
3    Einsatz von Subunternehmern (Art. 30 Abs. 2 (a) DORA).....	7
3.1  Zustimmungsvorbehalt und Risikobewertung.....	7
3.1.1  Zustimmungsvorbehalt.....	7
3.1.1  Risikobewertung .....	7
3.2  Vertragsgestaltung .....	8
3.3  Verantwortung des Auftragnehmers.....	8
3.4  Weiterverlagerungskette.....	9
4    Standorte / Leistungsorte (Art. 30 Abs. 2 (b)) .....	10
4.1  Leistungsorte .....	10
4.2  Änderung der Leistungsorte .....	10
5    Berichtspflichten (Art. 30 Abs. 3 (b) DORA).....	11
5.1  IKT-Risikoprozess und -identifikation .....	11
5.1.1  Selbstaudit/Auditierung .....	11
5.1.2  Informationspflicht.....	12
6    Aufsichtsrechtliche Prüf- und Auditrechte (Art. 30 Abs. 3 (e) DORA) .....	12
6.1  Prüfungs- und Kontrollrechte der LfA, der Revision und der Bundesanstalt für Finanzdienstleistungsaufsicht („BaFin“) .....	12
6.1.1  Einräumung von Prüfungs- und Kontrollrechten.....	12
6.1.2  Risikomanagement und Internes Kontrollsystem des Auftragnehmers .....	14
6.1.3  Zusammenarbeit der internen Revisionen.....	14

6.2	Fortbestand von Prüfungs- und Kontrollrechten .....	14
6.3	Beanstandungen und Mängelbeseitigung .....	15
6.4	Externe Prüfungen .....	15
6.4.1	Abschlussprüfung .....	15
6.4.2	Duldung von Maßnahmen der Aufsichtsbehörden .....	15
6.4.3	Prüfungen Dritter .....	16
6.4.4	Umfassende Unterstützung .....	16
6.4.5	Weitergehende Reporting- und Informationspflichten .....	16
7	Datenschutz (Art. 30 Abs. 2 (c) DORA) .....	17
7.1	Zweckbestimmung und Schutzmaßnahmen .....	17
7.2	Verarbeitung Personenbezogener Daten im Auftrag .....	17
8	Zugang zu Daten, Wiederherstellung und Rückgabe von Daten (Art. 30 Abs. 2 (d) DORA) .....	17
9	IKT-Sicherheit (Art. 30 Abs. 3 (c), Art. 28 Abs. 5 DORA) .....	18
9.1	Selbstauskunft .....	18
9.2	Allgemeine Grundsätze .....	18
9.3	Informationssicherheitsmanagement .....	19
9.3.1	Anforderungen an das Informationssicherheitsmanagement .....	19
9.3.2	Weiterentwicklung des Informationssicherheitsmanagements .....	19
9.3.3	Überwachung und Kontrollen .....	19
9.4	IKT-Vorfälle (Art. 30 Abs. 2 (f) DORA) .....	20
9.4.1	Meldung und Dokumentation .....	20
9.4.2	Unterstützung der LfA .....	21
9.4.3	IT-Sicherheitsüberprüfung (TLPTs) (Art. 30 Abs. 3 (d) DORA) .....	21
10	Notfallmanagement (Art. 30 Abs. 3 (c) DORA) .....	22
10.1	Allgemeine Grundsätze .....	22
10.1.1	Durchführung von Notfallübungen .....	22
10.1.2	Sofortmaßnahmen .....	22
11	Laufzeit und Kündigung (Art. 30 Abs. 2 (h), Art. 30 Abs. 3 (b) DORA) .....	22

11.1.1	Ordentliche Kündigung.....	22
11.1.2	Außerordentliche Kündigung .....	22
12	Exit Management (Art. 30 Abs. 3 (f)) .....	24
12.1.1	Verlängerungsoption.....	24
12.1.2	Exit Management.....	25
12.1.3	Wissenstransfer.....	26
13	Sensibilisierung und Schulung (Art. 30 Abs. 2 (i) DORA) .....	27
14	Ansprechpartner .....	28
15	Schlussbestimmung.....	28
16	Anlagen .....	28
	Unterschriften.....	28

## Präambel

Die LfA ist das Landesförderinstitut des Freistaats Bayern und ist eine Anstalt des öffentlichen Rechts mit Sitz in München. Die LfA ist verpflichtet, ab dem 17. Januar 2025 die Vorschriften der „Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor“ (Digital Operational Resilience Act; im Folgenden „DORA“) einzuhalten.

Die LfA hat eine Risikoanalyse durchgeführt, wonach der Auftragnehmer als IKT-Drittdienstleister einzustufen ist und die von ihm erbrachten Vertragsleistungen als IKT-Dienstleistung im Sinne von Art. 3 Nr.21 DORA zu qualifizieren sind, die zur Unterstützung von kritischen und wichtigen Funktionen dienen.

Aus diesem Grund vereinbaren die Vertragspartner zusätzlich zu den zwischen den Vertragspartnern bestehendem Vertragswerk Folgendes:

## 1 Geltungsbereich und Rangfolge

Die in dieser Ergänzungsvereinbarung vereinbarten Regelungen ergänzen das Vertragswerk samt Anlagen und gelten für sämtliche vom Auftragnehmer unter dem Vertragswerk zu erbrin-

genden Leistungen („Vertragsleistungen“), insbesondere werden die Regelungen der geltenden übergeordneten Vertragsdokumente ergänzt. Die Regelungen der Ergänzungsvereinbarung haben bei Widersprüchen Vorrang vor den Regelungen des Vertragswerkes.

Ausnahmen der vorstehenden Regelungen sind in diesem Dokument ausdrücklich für den Einzelfall zu vereinbaren.

## **2 Leistungsinhalte (Art. 30 Abs. 2 (a) DORA)**

### **2.1 Leistungsbeschreibung**

Die vom Auftragnehmer zu erbringenden Vertragsleistungen sind in dem Vertragswerk beschrieben und genügen hinreichenden Best Practices. Leistungsbestandteil sind auch ohne ausdrückliche Beschreibung solche Leistungen, die typischerweise Bestandteil der beschriebenen Vertragsleistungen, Aufgaben, Verfahren und Verantwortlichkeiten sind, oder die benötigt werden, um diese wirtschaftlich sinnvoll nutzen zu können.

Grundsätzlich haben sämtliche vom Auftragnehmer zu erbringende Vertragsleistungen dem Stand der Technik zu entsprechen. Der Auftragnehmer wird die Vertragsleistungen in Übereinstimmung mit einschlägigen Best-Practices, technischen Fachvorschriften, allgemeinen Normen und (Sicherheits-) Standards und entsprechend dem Stand der Technik erbringen.

Zudem hat der Auftragnehmer angemessene Best Practices zu Sicherheit, Nachhaltigkeit und Datenschutz implementiert. Ferner wird der Auftragnehmer die in den Leistungsbeschreibungen im Speziellen genannten Qualitäts- bzw. Sicherheitsstandards einhalten.

Im Übrigen erbringt der Auftragnehmer die Vertragsleistungen so, wie sie allgemein von einem professionellen, erfahrenen IKT-Drittdienstleister erwartet werden können. Der Auftragnehmer wird diese Qualitäts- bzw. Sicherheitsstandards in ihrer jeweiligen aktuellen Fassung befolgen. Soweit sich die Anforderungen der Qualitäts- bzw. Sicherheitsstandards ändern oder Qualitäts- bzw. Sicherheitsstandards durch neue Qualitäts- bzw. Sicherheitsstandards ersetzt werden, wird der Auftragnehmer diese Anforderungen auf eigene Kosten umsetzen. Der Auftragnehmer wird der LfA auf deren Verlangen die Zertifikate und Testate vorlegen, die die Konformität des Auftragnehmers mit den Qualitäts- bzw. Umweltstandards belegen. Im Falle eines Cloud-Betriebs sind vom Auftragnehmer die marktüblichen spezifischen Zertifikate vorzulegen (insbesondere BSI C5 und BSI AIC4). Die LfA ist berechtigt, in einer aus der Perspek-

tive des IKT-Risikomanagements angemessenen Häufigkeit Änderungen des Umfangs der Zertifizierungen oder Auditberichte mit Blick auf einschlägige Systeme und Kontrollen zu verlangen.

## **2.2 Leistungsgüte / Service Level und KPIs (Art. 30 Abs. 2 (e), Art. 30 Abs. 3 (a) DORA)**

Die Vertragspartner prüfen das Vertragswerk regelmäßig gemeinsam auch während der Vertragslaufzeit, um sicherzustellen, dass die Leistungsgüte durch die LfA beurteilt werden kann. Die Vertragspartner überprüfen oder vereinbaren im Wege des vertraglichen Änderungsverfahrens angemessene messbare Leistungskriterien, in der Regel in Form von Key Performance Indikatoren (KPI) und / oder Service Levels sowie zugehöriger Messkriterien und Berichte.

Der Auftragnehmer wird – unabhängig von den sonstigen vereinbarten Anforderungen an die Vertragsleistungen – die vereinbarten Service Level einhalten. Soweit für bestimmte Vertragsleistungen keine Service Level vereinbart wurden, wird der Auftragnehmer zumindest die Qualität sicherstellen, die von einem professionellen Dienstleister im Finanzdienstleistungssektor erwartet werden kann.

Die Service Level stellen eine qualitative Festlegung der Vertragsleistungen dar und schränken die Pflicht des Auftragnehmers zur kontinuierlichen Leistungserbringung nicht ein. Der Auftragnehmer kann sich auf das Erreichen der Service Levels nicht berufen, wenn der LfA durch eine Pflichtverletzung des Auftragnehmers im Rahmen der Leistungserbringung trotz Erreichens der Service Levels ein Schaden entsteht. Die Verfehlung von Service Levels hat unbeschadet weitergehender Ansprüche der LfA die vertraglich beschriebenen Rechtsfolgen.

Der Auftragnehmer wird die Einhaltung der Service Level und der vereinbarten KPIs kontinuierlich gemäß den vertraglichen Vereinbarungen messen und der LfA die vertraglich vereinbarten Berichte in elektronischer Form liefern.

## **2.3 Vertragsänderung**

Der Auftragnehmer wird Änderungsanträge der LfA hinsichtlich der Anpassung bzw. der Ergänzung der Leistungsbeschreibung sowie der Vereinbarung angemessener KPIs und/oder Service Level nicht unbillig verweigern.

## **3 Einsatz von Subunternehmern (Art. 30 Abs. 2 (a) DORA)**

### **3.1 Zustimmungsvorbehalt und Risikobewertung**

#### **3.1.1 Zustimmungsvorbehalt**

Dritte dürfen nur dann als Subunternehmer zur Erbringung der Vertragsleistungen eingesetzt werden, wenn und soweit die LfA hierzu zuvor schriftlich ihre Zustimmung erteilt hat. Der Zustimmungsvorbehalt erstreckt sich auch auf Umfang und Details der Weiterverlagerung. Die LfA ist berechtigt ihre Zustimmung im billigen Ermessen zu verweigern. Aus **Anlage 1 (Leistungsorte und Subunternehmer)** ergeben sich die im Zeitpunkt der Unterzeichnung des Vertragswerkes genehmigten Subunternehmer.

Der Auftragnehmer informiert die LfA mit einem Vorlauf von mindestens 3 Monaten über einen beabsichtigten Subunternehmereinsatz oder die Änderung eines bereits genehmigten Subunternehmereinsatzes in Textform unter Angabe der Firma, der Leistungsbeschreibung, des Leistungsortes, des Orts der Datenhaltung und Datenverarbeitung sowie des anwendbaren Rechts der Subunternehmervereinbarung.

#### **3.1.1 Risikobewertung**

Die LfA ist berechtigt, weitere Informationen zu dem geplanten Subunternehmereinsatz zu verlangen, die die LfA im Rahmen ihrer eigenen Risikobewertung benötigt. Weiterhin stellt der Auftragnehmer die Ergebnisse seiner Risikobewertung bereit, die insbesondere etwaige Risiken aus dem Standort des Subunternehmers (einschließlich Muttergesellschaft) sowie den Orten der Leistungserbringung für die LfA nachvollziehbar bewertet. Die vorgenannte Risikobewertung durch den Auftragnehmer beinhaltet einen Auswahl- und Bewertungsprozess hinsichtlich des Subunternehmens. Dabei bewertet der Auftragnehmer insbesondere (i) etwaige Interessenskonflikte (einschließlich deren Behandlung) beim Einsatz des Subunternehmers und (ii) die Ressourcen des Subunternehmens, einschließlich des Fachwissens und der angemessenen finanziellen, personellen und technischen Ressourcen, die Informationssicherheit, seine Organisationsstruktur, einschließlich des Risikomanagements und der internen Kontrollen, prüfen. Dabei sind auf Verlangen der LfA auch weitere Informationen jederzeit unverzüglich zur Verfügung zu stellen.

Unbeschadet der in dieser Ergänzungsvereinbarung genannten Voraussetzungen für den Einsatz von Subunternehmern hat die LfA das Recht, ihre Zustimmung zum Einsatz eines Dritten

als Subunternehmer jederzeit, auch nach Aufnahme der Tätigkeit durch den Subunternehmer, aus wichtigem Grund zurückzunehmen.

### **3.2 Vertragsgestaltung**

Voraussetzung für den Einsatz des Subunternehmers ist zudem, dass der Auftragnehmer dafür Sorge trägt, dass zwischen dem Auftragnehmer und dem Dritten schriftliche vertragliche Vereinbarungen bestehen, durch die sichergestellt ist, dass während der gesamten Zeit der Erbringung der Subunternehmerleistung

- a) die Pflichten des Dritten im Einklang mit den in diesem Vertragswerk geregelten Pflichten des Auftragnehmers stehen; dies gilt insbesondere für die Rechte der LfA für eine Kündigung nach Maßgabe von Art.28 Abs. 7 DORA, den Service Levels/KPI und Berichtspflichten nach dieser Ergänzungsvereinbarung sowie für die Pflichten des Auftragnehmers in Bezug auf Vertraulichkeit, Datenschutz, Sicherheit, Notfallvorsorge und die Steuerung und Kontrolle der Vertragsleistungen, und dass
- b) der Dritte zur Einhaltung aller relevanten Gesetze und aufsichtsrechtlichen Anforderungen, datenschutzrechtlichen Bestimmungen, des Bankgeheimnisses und der Wahrung von Geschäftsgeheimnissen verpflichtet ist, und dass
- c) der Auftragnehmer mit diesem Dritten eine Auftragsverarbeitungsvereinbarung gemäß Art. 28 Abs. 3 DSGVO nebst den gegebenenfalls nach Art. 44 ff. DSGVO erforderlichen Garantien abgeschlossen hat oder der Auftragnehmer nachweisen kann, dass der Dritte keinen Zugang zu oder Zugriff auf personenbezogene Daten aus der Sphäre der LfA hat.

Der Auftragnehmer wird der LfA die Einhaltung dieser Anforderungen auf Verlangen in geeigneter Form nachweisen und der LfA bei wesentlichen Änderungen des Vertrags mit dem Subunternehmer informieren.

### **3.3 Verantwortung des Auftragnehmers**

Der Auftragnehmer bleibt für die Erfüllung der auf den Subunternehmer übertragenen Tätigkeiten in dem gleichen Umfang verantwortlich, als würden diese durch den Auftragnehmer selbst ausgeführt.

Der Auftragnehmer steuert und überwacht den Subunternehmereinsatz gemäß den Vorgaben der LfA nachvollziehbar. Zu der regelmäßigen Steuerung gehört mindestens die monatliche Bewertung und Dokumentation der Service Level Einhaltung, die Würdigung von Berichten,



einschließlich Berichten über IKT-Vorfälle, Betriebsstabilität, IKT-Sicherheit und Business Continuity, und Zertifikaten und die regelmäßige Abstimmung mit dem Subunternehmer. Stellt der Auftragnehmer im Rahmen der Steuerung und Überwachung bei einem Subunternehmer fest, wird er den Auftraggeber unverzüglich informieren, Maßnahmen zur Behebung mit dem Subunternehmer definieren und die Umsetzung der Maßnahmen nachhalten.

### **3.4 Weiterverlagerungskette**

Sofern die LfA dem Einsatz eines Subunternehmers zur Erbringung der Vertragsleistungen zustimmt, gelten die Vorgaben dieser Ziffer 3.4 für die Einschaltung weiterer nachgelagerter Subunternehmer entsprechend.

Bei der Einschaltung von nachgelagerten Subunternehmern hat der Auftragnehmer nachfolgende Verpflichtungen:

- a) Der Auftragnehmer ermöglicht der LfA die regelmäßige Aktualisierung ihres Informationsregisters, in dem er der LfA sämtliche Informationen zur Weiterverlagerungskette unaufgefordert einmal jährlich, spätestens zum 30.11 eines Kalenderjahres, in Textform zur Verfügung stellt.
- b) Der Auftragnehmer stellt durch angemessene vertragliche Vereinbarungen mit den Dienstleistern in seiner Weiterverlagerungskette sicher, dass die LfA und die für sie zuständigen Aufsichtsbehörden ihren in dieser Ergänzungsvereinbarung enthaltenen Steuerungs-, Prüfungs- und Kontrollrechten auch in der Weiterverlagerungskette, also auch unmittelbar gegenüber den Subunternehmern, nachkommen kann.
- c) Der Auftragnehmer stellt der LfA unaufgefordert einmal jährlich, spätestens zum 30.11 sämtliche Informationen zur Verfügung, die es der LfA ermöglichen zu beurteilen, ob und wie die potenziell lange oder komplexe Kette von Unterauftragnehmern, die wesentliche Bestandteile der Leistungen erbringen, die Fähigkeit, die Vertragsleistungen vollständig zu überwachen, und die Fähigkeit der zuständigen Behörde, die LfA in dieser Hinsicht wirksam zu beaufsichtigen, beeinflussen kann.
- d) Der Auftragnehmer stellt der LfA unaufgefordert einmal jährlich, spätestens zum 30.11 alle relevanten Informationen zu den vertraglichen Vereinbarungen (insbesondere Leistungsbeschreibungen, Service Levels und KPIs) zur Verfügung, damit die LfA ihren aufsichtsrechtlichen Steuerungs-, Prüfungs- und Kontrollrechten nachkommen kann.

## 4 Standorte / Leistungsorte (Art. 30 Abs. 2 (b))

### 4.1 Leistungsorte

Der Auftragnehmer, einschließlich der von ihm eingesetzten Subunternehmen, wird die Vertragsleistungen von den in **Anlage 1 (Leistungsorte und Subunternehmer)** genannten Standorten aus erbringen. Sofern der Auftragnehmer die Vertragsleistungen gemäß den vertraglichen Vereinbarungen an den Standorten der LfA erbringt, bedarf dies keiner Aufführung in **Anlage 1 (Leistungsorte und Subunternehmer)**.

**Anlage 1 (Leistungsorte und Subunternehmer)** enthält darüber hinaus die Standorte, an denen maßgebliche Daten gespeichert und/oder verarbeitet werden.

### 4.2 Änderung der Leistungsorte

Der Auftragnehmer ist frei, innerhalb der jeweiligen, in **Anlage 1 (Leistungsorte und Subunternehmer)** aufgeführten Länder (nicht jedoch länderübergreifend) Standorte zu verlegen oder zu verändern, vorausgesetzt, die Interessen und Rechte der LfA, insbesondere die Qualität der geschuldeten Vertragsleistungen (einschließlich der Informationssicherheit), werden hierdurch nicht negativ beeinträchtigt und der Auftragnehmer hat die LfA über die Verlegung oder Veränderung mit angemessenem zeitlichem Vorlauf von mindestens drei (3) Monaten schriftlich unterrichtet und sich mit der LfA über die möglichen Folgen der Verlegung oder Veränderung verständigt.

Sofern es sich bei der Änderung des Leistungsortes um die Nutzung eines anderen Rechenzentrums für die Vertragsleistungen oder um die Verlagerung von Vertragsleistungen ins EU-Ausland handelt, bedarf dies der vorherigen ausdrücklichen schriftlichen Zustimmung der LfA. Die LfA wird die Zustimmung zu einer solchen Verlagerung nicht unbillig verzögern und nur bei Vorliegen eines wichtigen Grundes verweigern. Ein wichtiger Grund liegt insbesondere vor, wenn die Verlagerung nach der vernünftigen Einschätzung der LfA

- a) die in dieser Ergänzungsvereinbarung vereinbarten Prüfungsrechte oder Steuerungs- und Kontrollmöglichkeiten der LfA oder die Prüfungsrechte und Kontrollmöglichkeiten der Bankenaufsicht oder der Finanzverwaltung einschränkt,
- b) die von der Änderung betroffenen Vertragsleistungen und damit verbundenen Risiken der LfA in einem erheblichen Maße zum Nachteil der LfA verändert,
- c) sich mehr als nur unwesentlich auf die Geschäftsprozesse der LfA auswirkt,

- d) eine Rück- oder Weiterverlagerung der Vertragsleistungen durch die LfA im Falle der Beendigung dieses Vertrages erschwert oder ausschließt.

Die Verlagerung von Vertragsleistungen in Länder außerhalb der EU bedarf der vorherigen ausdrücklichen schriftlichen Zustimmung der LfA, die in deren freien Ermessen steht.

Der Auftragnehmer trägt die eigenen Kosten sowie die Kosten der LfA, die durch die Verlegung oder Veränderung eines Standortes verursacht werden.

## **5 Berichtspflichten (Art. 30 Abs. 3 (b) DORA)**

### **5.1 IKT-Risikoprozess und -identifikation**

#### **5.1.1 Selbstaudit/Auditierung**

Der Auftragnehmer ist verpflichtet, einen Prozess zu implementieren, der die Identifizierung der IKT-Risiken im Rahmen der Vertragsleistungen für seine Erbringung der Vertragsleistungen zum Gegenstand hat („IKT-Risikoprozess“). Der IKT-Risikoprozess muss weiterhin vorsehen, dass identifizierte IKT-Risiken in angemessenem Zeitraum, bei außergewöhnlichen Ereignissen unverzüglich bewertet und Maßnahmen festgelegt werden, die eine Kontrolle der IKT-Risiken und deren unverzügliche Einleitung von Gegenmaßnahmen zum Ziel haben. Im Falle gemäß dem IKT-Risikoprozess identifizierter IKT-Risiken ist die LfA zu informieren.

Als Teil des IKT-Risikoprozesses ist der Auftragnehmer außerdem verpflichtet, jährlich ein Selbstaudit oder eine Auditierung durch Dritte im Wege einer

☐ Typ 2 Prüfung gem. Prüfungsstandard ISAE 3402 (INCLUSIVE-Methode) oder IDW PS 951 Typ B

☐ Prüfung gemäß ISO27001 in der jeweils gültigen Fassung

☐ [...]

durchzuführen und Richtlinien und Prozesse zu implementieren, die dies sicherstellen („Selbstauditberichte“) und die Auditierungen der LfA hierzu angemessen zu unterstützen. Hierbei ist besonders eine Schnittstelle der IKT-Risikoprozesse zwischen dem Auftragnehmer und der LfA zu etablieren. Im Falle der Identifizierung des IKT-Risikoprozesses als nicht effizient oder identifizierten Verstoß gegen die Bestimmungen dieser Ergänzungsvereinbarung ist der Auftragnehmer verpflichtet, den Prozess so zu ändern, dass er effizient und vertragskonform ist.

### **5.1.2 Informationspflicht**

Der Auftragnehmer informiert die LfA gemäß dem vereinbarten IKT-Risikoprozess in angemessenem Zeitraum, bei außergewöhnlichen Ereignissen unverzüglich über im Rahmen des IKT-Risikoprozesses gemäß vorstehenden Bestimmungen oder auf sonstigem Wege identifizierte Risiken hinsichtlich der Erbringung der Vertragsleistungen.

Der Auftragnehmer stellt der LfA die vollständigen Selbstauditberichte innerhalb von vier (4) Wochen nach Abschluss des jeweiligen Audits zur Verfügung. Der Auftragnehmer ist berechtigt, diese Berichte in dem Umfang zu anonymisieren, wie es zwingend erforderlich ist, damit er nicht gegen Vertraulichkeitsvereinbarungen mit Dritten oder gesetzliche Bestimmungen verstößt. Jegliche Auditberichte sind streng vertraulich und unterfallen den Regelungen der Vertraulichkeitsbestimmungen des Vertragswerkes.

## **6 Aufsichtsrechtliche Prüf- und Auditrechte (Art. 30 Abs. 3 (e) DORA)**

### **6.1 Prüfungs- und Kontrollrechte der LfA, der Revision und der Bundesanstalt für Finanzdienstleistungsaufsicht („BaFin“)**

#### **6.1.1 Einräumung von Prüfungs- und Kontrollrechten**

Unter Bezugnahme auf die anwendbaren rechtlichen Rahmenbedingungen vereinbaren die Vertragspartner, dass der LfA, deren interner Revision, deren Compliance- und Datenschutzbeauftragten, Erfüllungsgehilfen, deren Risikomanagement und Abschlussprüfern, den für die LfA zuständigen Aufsichts- und Abwicklungsbehörden, einschließlich der Bundesanstalt für Finanzdienstleistungsaufsicht („BaFin“) oder einer von dieser zur Prüfung beauftragten Stelle (nachfolgend einzeln oder zusammen „Prüfer“) Auskunfts-, Einsichts-, Prüfungs- und Zutrittsrechte sowie Kontrollbefugnisse (nachfolgend zusammen die „Prüfungs- und Kontrollrechte“) wie nachfolgend beschrieben zustehen.

Der Auftragnehmer wird den Prüfern jederzeit zu Prüfungs- und Kontrollzwecken umfassenden und unbeschränkten Zugang zu allen Personen, Räumlichkeiten sowie den unter seiner Kontrolle stehenden Dokumenten, Daten, Datenträgern, Rechenzentren, Geräten, Systemen, Netzwerken sowie Unterlagen gewähren, die mit den Vertragsleistungen in Zusammenhang stehen und für die Prüfung dienlich sind. Die Prüfungs- und Kontrollrechte der Prüfer umfassen auch

die Anfertigung von Abschriften einschlägiger Unterlagen und die Vervielfältigung von Dokumenten und Datenträgern.

Die Prüfungs- und Kontrollrechte erstrecken sich auf die Prüfung und Kontrolle der Einhaltung der anwendbaren rechtlichen Rahmenbedingungen (einschließlich der aufsichtsrechtlichen Regelungen, insbesondere DORA) sowie der vertragsgemäßen Leistungserbringung und die Einhaltung der vertraglichen Bestimmungen und umfassen insbesondere:

- a) die Leistungsorte und sämtliche vom Auftragnehmer zur Erbringung der Vertragsleistungen eingesetzten IT-Systeme, einschließlich deren Sicherheit,
- b) die Einhaltung der Service Levels sowie die zur Überprüfung der Einhaltung der Service Levels eingesetzten Messinstrumente und die aufgezeichneten Messergebnisse,
- c) die Richtigkeit der der LfA durch den Auftragnehmer in Rechnung gestellten Vergütung und sonstigen Beträge,
- d) die Sicherheit und den Schutz von Daten, einschließlich der vom Auftragnehmer zur Gewährleistung der Datensicherheit und des Datenschutzes getroffenen technischen und organisatorischen Maßnahmen,
- e) die Einhaltung aller anwendbaren rechtlichen Rahmenbedingungen, insbesondere aufsichtsrechtlicher Anforderungen, durch den Auftragnehmer, insbesondere der versicherungsaufsichtsrechtlichen Bestimmungen und Aufbewahrungspflichten für relevante Dokumente,
- f) die Erfüllung gesetzlicher oder von den zuständigen Aufsichtsbehörden auferlegten Verpflichtungen der LfA, und
- g) sonstige Prüfungspunkte, die eine zuständige Aufsichtsbehörde für prüfungsrelevant erachtet.

Den Prüfern stehen dabei mindestens die Auskunfts-, Einsichts-, Prüfungs- und Zutrittsrechte sowie Kontrollbefugnisse zu, die sich aus den anwendbaren rechtlichen Rahmenbedingungen ergeben. Insbesondere beinhalten diese die Verpflichtung des Auftragnehmers, sämtliche Auskünfte zu erteilen und Unterlagen auszuhändigen, die die Prüfer für ihre Aufsichts- und Prüfungstätigkeiten benötigen.

Der Auftragnehmer wird alle Personen, die sich ihm gegenüber zur Geheimhaltung verpflichtet haben, von dieser Verpflichtung gegenüber den Prüfern entbinden.

Hat die LfA mit der Überprüfung eine Wirtschaftsprüfungsgesellschaft beauftragt, so kann die LfA die Prüfung jederzeit wieder selbst übernehmen.

Der Auftragnehmer wird insbesondere dafür sorgen, dass die LfA ihrer Pflicht gem. Art. 11 Abs. 8 DORA jederzeit nachkommen kann.

### **6.1.2 Risikomanagement und Internes Kontrollsystem des Auftragnehmers**

Der Auftragnehmer ist verpflichtet, ein angemessenes internes Kontrollsystem vorzuhalten sowie ein angemessenes Risikomanagement zu betreiben und die Vertragsleistungen in diese Systeme einzubeziehen. Insbesondere ist der Auftragnehmer verpflichtet, eine funktionsfähige Organisationsstruktur einzurichten, die in Bezug auf die Vertragsleistungen sämtliche Prozesse im Zusammenhang mit der Erbringung der Vertragsleistungen und IT-Systeme, die für die Erbringung von Vertragsleistungen genutzt werden gemäß den Vorgaben der anwendbaren rechtlichen Rahmenbedingungen laufend prüft und überwacht.

### **6.1.3 Zusammenarbeit der internen Revisionen**

Der Auftragnehmer sichert zu, bei der Organisation seiner internen Revision die aufgrund der anwendbaren rechtlichen Rahmenbedingungen, insbesondere des Bankaufsichtsrechts, zu beachtenden Grundsätze zur Ausgestaltung der internen Revision zu erfüllen. Die interne Revision des Auftragnehmers wird mit der internen Revision der LfA vertrauensvoll zusammenarbeiten. Die Berichte der internen Revision des Auftragnehmers über den ausgelagerten Bereich sind, insbesondere zur Kontrolle festgestellter Mängel, an die interne Revision der LfA weiterzuleiten. Der Auftragnehmer verpflichtet sich weiterhin, die die Vertragsleistungen betreffenden Prüfungsergebnisse seiner internen Revision der BaFin und dem Abschlussprüfer der LfA – jeweils auf Anforderung – zur Verfügung zu stellen. Der Auftragnehmer räumt der LfA das Recht ein, eigene Ergänzungsprüfungen durch deren interne Revision im Unternehmen des Auftragnehmers durchzuführen.

## **6.2 Fortbestand von Prüfungs- und Kontrollrechten.**

Die Prüfungs- und Kontrollrechte, wie vorstehend näher beschrieben, bestehen nach Beendigung der von der LfA beauftragten Vertragsleistungen für einen Zeitraum von fünf (5) Jahren fort, beginnend mit dem Ablauf des Geschäftsjahres der LfA, in dem sämtliche Vertragsleistungen nach dem Vertragswerk beendet werden. Relevante Unterlagen müssen, unbeschadet sonstiger gesetzlicher Aufbewahrungsfristen, ebenso lange verfügbar bleiben.

## **6.3 Beanstandungen und Mängelbeseitigung**

Der Auftragnehmer ist verpflichtet, die durch die Prüfer, insbesondere auch solche durch Aufsicht und Wirtschaftsprüfer, festgestellten Beanstandungen und Mängel auszuräumen und unverzüglich angemessene Maßnahmen zur Beseitigung der Mängel zu ergreifen. Die Prüfer und/oder die LfA können dem Auftragnehmer eine angemessene Frist zur Beseitigung der Mängel setzen. Der Auftragnehmer trägt sämtliche direkten und indirekten Kosten der Mängelbeseitigung.

## **6.4 Externe Prüfungen**

### **6.4.1 Abschlussprüfung**

Die vom Auftragnehmer erbrachten Vertragsleistungen sind Gegenstand der Abschlussprüfung bei der LfA. Der Auftragnehmer verpflichtet sich, auf Verlangen der LfA den Prüfern insoweit alle erforderlichen Prüfungshandlungen zu ermöglichen. Die LfA wird den Prüfern insbesondere alle für ihre Tätigkeit benötigten Auskünfte erteilen, den Zutritt zu Geschäftsräumen und den Zugang zu allen benötigten Dokumenten, Daten, Datenträgern, Rechenzentren, Geräten, Systemen, Netzwerken sowie Unterlagen ermöglichen, Einsicht in diese sowie die Anfertigung von Abschriften gewähren und sie bei ihrer Prüfungstätigkeit unterstützen.

### **6.4.2 Duldung von Maßnahmen der Aufsichtsbehörden**

Der Auftragnehmer ist in Bezug auf die Vertragsleistungen zur Zusammenarbeit mit den für die LfA zuständigen Aufsichts- und Abwicklungsbehörden, einschließlich der BaFin, verpflichtet. Der Auftragnehmer ist insbesondere verpflichtet, unmittelbar oder mittelbar an ihn gerichtete Fragen der Aufsichtsbehörden unverzüglich und vollständig zu beantworten und nach den anwendbaren rechtlichen Rahmenbedingungen zulässige und rechtmäßige Anordnungen der Aufsichtsbehörden zu befolgen.

Der Auftragnehmer verpflichtet sich, durch die Aufsichtsbehörden gegenüber der LfA oder dem Auftragnehmer angeordnete Prüfungen sowie sonstige gesetzlich vorgesehene Prüfungen und aufsichtsrechtliche Maßnahmen, die zur Überwachung des Geschäftsbetriebes der LfA oder des Auftragnehmers angeordnet werden, zu dulden. Dies gilt auch für Prüfungen, die in den Geschäftsräumen des Auftragnehmers stattfinden. Der Auftragnehmer wird die LfA unverzüglich - vorbehaltlich etwaiger Verschwiegenheitspflichten - schriftlich unterrichten, sofern der Auftragnehmer von einer Behörde um Auskunft ersucht oder von bevorstehenden auf-

sichtsrechtlichen Maßnahmen unterrichtet oder solchen Prüfungen oder Maßnahmen unterworfen wird oder werden soll, sofern sich solche Auskunftsverlangen, Prüfungen oder Maßnahmen auf die Vertragsleistungen beziehen, und sich im Anschluss daran über das weitere Vorgehen abstimmen.

#### **6.4.3 Prüfungen Dritter**

Die Prüfer sind im Rahmen ihrer Tätigkeit auch berechtigt, auf die Prüfungsergebnisse aus Prüfungen Dritter beim Auftragnehmer zurückzugreifen, soweit diese die Vertragsleistungen betreffen und nicht exklusiv für einen Kunden des Auftragnehmers durchgeführt wurden.

#### **6.4.4 Umfassende Unterstützung**

Der Auftragnehmer ist verpflichtet, bei sämtlichen Tätigkeiten im Rahmen der in dieser Ziffer 6.4 vorgesehenen Prüfungen und Kontrollen, Unterstützung in einem ihm zumutbaren Umfang zu leisten. Der Auftragnehmer ist darüber hinaus verpflichtet, die LfA auf Verlangen auch bei jeglichen Prüfungen in zumutbarem Umfang zu unterstützen, die in Bezug oder im Zusammenhang mit den Vertragsleistungen bei der LfA stattfinden.

Der Auftragnehmer ist insbesondere verpflichtet, die LfA ohne zusätzliche Vergütung jeweils bei der Erstellung, Implementierung und dauerhafter Umsetzung (i) eines IKT-Risikomanagementrahmens i.S.v. Art. 6 DORA, (ii) einer IKT-Geschäftsfortführungsleitlinie i.S.v. Art. 11 DORA und/oder (iii) bei der Umsetzung und Einhaltung der Pflichten der LfA gem. Art. 17 DORA zu unterstützen.

#### **6.4.5 Weitergehende Reporting- und Informationspflichten**

Der Auftragnehmer wird der LfA auf deren Anforderung jederzeit uneingeschränkt und unverzüglich alle Auskünfte und Informationen erteilen, die zur umfassenden Beurteilung der Durchführung der Vertragsleistungen aus Sicht der LfA erforderlich sind. Der Auftragnehmer wird in diesem Rahmen der LfA insbesondere ermöglichen, zu überprüfen, ob die Qualitätsanforderungen eingehalten werden. Der Auftragnehmer wird der LfA bzw. von dieser beauftragten Dritten alle hierzu erforderlichen Informationen erteilen und Unterlagen vorlegen.



## **7 Datenschutz (Art. 30 Abs. 2 (c) DORA)**

### **7.1 Zweckbestimmung und Schutzmaßnahmen**

Der Auftragnehmer legt besonderen Wert auf den Schutz sämtlicher Daten seiner Kunden, einschließlich der Personenbezogenen Daten (gemeinsam nachfolgend auch „Daten“).

Der Auftragnehmer verarbeitet Daten ausschließlich zu den mit der LfA vereinbarten Zwecken, nur in Übereinstimmung mit den Bestimmungen des Vertragswerkes, auf Weisungen des Kunden sowie zur Erfüllung seiner Verpflichtungen aus dem Vertragswerk.

Der Auftragnehmer implementiert angemessene technische und organisatorische Maßnahmen zur Sicherung der Verfügbarkeit, Integrität und Authentizität sämtlicher Daten.

### **7.2 Verarbeitung Personenbezogener Daten im Auftrag**

Der Auftragnehmer hält bei der Verarbeitung von Personenbezogenen Daten alle einschlägigen datenschutzrechtlichen Bestimmungen der DSGVO und anderer anzuwendender Datenschutzgesetze ein.

Für die Verarbeitung Personenbezogener Daten im Auftrag gelten die Bestimmungen der zwischen den Vertragspartnern geschlossenen Auftragsverarbeitungsvereinbarung gemäß Art 28. DSGVO.

## **8 Zugang zu Daten, Wiederherstellung und Rückgabe von Daten (Art. 30 Abs. 2 (d) DORA)**

Alle Auftraggeber-Daten stehen der LfA zu. „Auftraggeber-Daten“ sind alle Daten, die die LfA oder ein mit der LfA verbundenes Unternehmen oder deren jeweiligen Kunden oder Geschäftspartner betreffen, sowie sonstige Daten, zu denen der Auftragnehmer im Zusammenhang mit den Vertragsleistungen Zugang hat oder die im Zusammenhang mit den Vertragsleistungen durch die LfA oder im Auftrag der LfA geschaffen werden, mit Ausnahme von Daten, die der Auftragnehmer unabhängig von den vorstehend beschriebenen Daten zu internen Zwecken der Erbringung der Vertragsleistungen selbst generiert.

Auf Verlangen der LfA wird der Auftragnehmer jederzeit während der Vertragslaufzeit sowie nach der Beendigung der vertraglichen Vereinbarung die Auftraggeber-Daten in einem ge-

bräuchlichen Datenformat (wieder-)herstellen und herausgeben, auch mehrfach sowie in Teilen. Eine Konvertierung in ein anderes Datenformat kann die LfA gegen Vergütung beim Auftragnehmer beauftragen. Für die Datenübertragung werden entsprechende Tests von der LfA geplant und durchgeführt, bei denen der Auftragnehmer beratend und unterstützend zur Verfügung steht.

Hat der Auftragnehmer im Rahmen der Vertragsleistungen Besitz an Auftraggeber-Daten erlangt, ist der LfA auch im Falle der Insolvenz, Liquidation oder Abwicklung des Auftragnehmers ungehinderter Zugriff insbesondere durch (Wieder-)Herstellung und Rückgabe dieser Auftraggeber-Daten in einem gebräuchlichen Dateiformat zu gewähren.

Zurückbehaltungsrechte des Auftragnehmers in Bezug auf die Herausgabe von Auftraggeber-Daten sind ausgeschlossen.

## **9 IKT-Sicherheit (Art. 30 Abs. 3 (c), Art. 28 Abs. 5 DORA)**

### **9.1 Selbstauskunft**

Alle dem Auftragnehmer zur Verfügung gestellten Zusatzdokumente zu Informationssicherheit und Datenschutz (z.B. „Selbstauskunft Informationssicherheit“, Maßnahmenkatalog) sind zu befüllen und im jährlichen Turnus zu bestätigen oder bei wesentlichen Änderungen (z.B.: kein gültiges Zertifikat mehr vorhanden, Verschlechterung des vorhandenen Reifegrads) neu abzustimmen.

### **9.2 Allgemeine Grundsätze**

Der Auftragnehmer ergreift angemessene technische und organisatorische Maßnahmen, die zur Gewährleistung eines dem Stand der Technik entsprechenden Niveaus an IT-Sicherheit in Bezug auf die Vertragsleistungen und die vom Auftragnehmer für deren Erbringung genutzten Systeme erforderlich sind. Die IT-Systeme des Auftragnehmers stellen die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der im Rahmen der Vertragsleistungen verarbeiteten Daten sicher.

Der Auftragnehmer verpflichtet sich, alle empfangenen oder von ihm generierten Informationen und Daten im Zusammenhang mit dem Vertragswerk nach dem Stand der Technik sofort wirksam gegen unberechtigten Zugang und Zugriff, unberechtigte Veränderung, Zerstörung oder Verlust, unerlaubte Übermittlung, anderweitige unerlaubte Verarbeitung und sonstigen Missbrauch zu sichern.

## **9.3 Informationssicherheitsmanagement**

### **9.3.1 Anforderungen an das Informationssicherheitsmanagement**

Der Auftragnehmer ist verpflichtet, die von ihm gegenüber der LfA zu erbringenden Vertragsleistungen in sein Informationssicherheitsmanagement einzubeziehen. Im Rahmen seines Informationssicherheitsmanagements trifft der Auftragnehmer unter anderem geeignete technische und organisatorische Maßnahmen, um ein dem Risiko für die Informationssicherheit angemessenes Schutzniveau zu gewährleisten. Dabei wird der Auftragnehmer in Bezug auf die Daten und Informationen der LfA die Schutzziele der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit auf Basis aktueller und höchster Qualitätsstandards der Informationssicherheit (Artikel 28 Abs. 5 DORA) wahren. Zudem sind die Eintrittswahrscheinlichkeit und die Schwere eines aus einer möglichen Verletzung der Informationssicherheit resultierenden Risikos sowie der Stand der Technik, gängige Marktstandards (z.B. IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI), der internationale Sicherheitsstandard ISO 27001) zu berücksichtigen. Dies beinhaltet auch Maßnahmen, die darauf ausgerichtet sind, Cyberrisiken angemessen zu steuern.

### **9.3.2 Weiterentwicklung des Informationssicherheitsmanagements**

Der Auftragnehmer wird die technischen und organisatorischen Maßnahmen entsprechend dem technischen Fortschritt und des Bekanntwerdens neuer Risiken für die Informationssicherheit stetig weiterentwickeln. Wesentliche Änderungen der technischen und organisatorischen Maßnahmen, die Einfluss auf die Integrität, Vertraulichkeit, Authentizität oder Verfügbarkeit der im Kontext der Leistungserbringungen betroffenen Daten und Informationen haben können, wird der Auftragnehmer der LfA mitteilen, wobei die LfA solchen Änderungen nur aus wichtigem Grund widersprechen kann. Als wichtiger Grund gilt insbesondere, wenn begründeter Anlass zu Zweifeln bezüglich des ordnungsgemäßen Schutzes der Informationen der LfA besteht. Die LfA kann jederzeit eine aktuelle Beschreibung der vom Auftragnehmer konkret getroffenen technischen und organisatorischen Maßnahmen anfordern.

### **9.3.3 Überwachung und Kontrollen**

Der Auftragnehmer wird der LfA mindestens einmal jährlich durch geeignete Nachweise belegen, dass er geeignete technische und organisatorische Maßnahmen implementiert hat, um ein dem Risiko für die Informationssicherheit angemessenes Schutzniveau zu gewährleisten. Die LfA oder ein von ihm beauftragter Dritter, sowie die zuständigen Behörden haben unein-

geschränkte Zugangs-, Inspektions- und Auditrechte sowie das Recht auf Anfertigung von Kopien einschlägiger Unterlagen vor Ort. Die LfA ist berechtigt, nach vorheriger Abstimmung mit dem Auftragnehmer zu seinen üblichen Geschäftszeiten ohne Störung des Betriebsablaufs diese Rechte auszuüben. Vertragliche Vereinbarungen, Umsetzungsrichtlinien oder interne Vorgaben des Auftragnehmers, die die tatsächliche Ausübung dieser Rechte behindern oder einschränken, sind unwirksam. Die LfA und der Auftragnehmer haben das Recht, alternative Bestätigungsniveaus zu vereinbaren, wenn die Rechte anderer Kunden betroffen sind. Der Auftragnehmer verpflichtet sich zur uneingeschränkten Zusammenarbeit bei Vor-Ort-Inspektionen und Audits, die von den zuständigen Behörden, der federführenden Überwachungsbehörde, der LfA oder einem beauftragten Dritten durchgeführt werden.

## **9.4 IKT-Vorfälle (Art. 30 Abs. 2 (f) DORA)**

### **9.4.1 Meldung und Dokumentation**

Der Auftragnehmer hat Unregelmäßigkeiten in der Verarbeitung von Informationen, sowie alle sicherheitsrelevanten Vorfälle, die zu einer Verletzung mindestens eines der Schutzziele Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit führen (nachfolgend gemeinsam „IKT-Vorfall“) unverzüglich, d.h. ohne schuldhaftes Zögern nach Bekanntwerden zu melden und zu dokumentieren. Der Auftragnehmer hat zur Erkennung, Abwehr und Behandlung von IKT-Vorfällen angemessene Systeme, Prozesse und Verantwortlichkeiten implementiert. Die Dokumentation und Meldung eines Informationssicherheitsvorfalls enthält mindestens folgende Informationen:

- a) eine Beschreibung der Art des IKT-Vorfalles, der betroffenen Informationen, der voraussichtlichen Folgen und der von dem Auftragnehmer ergriffenen oder beabsichtigten Maßnahmen zur Behebung des IKT-Vorfalles und der nachteiligen Auswirkungen sowie
- b) den Namen und die Kontaktdaten des Informationssicherheitsbeauftragten oder eines anderen Ansprechpartners.

Der Auftragnehmer wird die LfA über die Behebung des IKT-Vorfalles fortlaufend informieren. Auf Anfrage wird der Auftragnehmer die LfA über Meldungen informieren, die der Auftragnehmer an für die ihn zuständige Behörden abgegeben hat. Nach Abschluss des IKT-Vorfalles wird der Auftragnehmer der LfA eine Root-Cause-Analyse zugänglich machen und daraus Maßnahmen zur Vermeidung künftiger vergleichbarer Vorfälle ableiten.

#### **9.4.2 Unterstützung der LfA**

Der Auftragnehmer ist verpflichtet, die LfA beim Eintritt eines IKT-Vorfalles im Rahmen des Zumutbaren zu unterstützen.

Zu dieser Unterstützung gehört insbesondere die Umsetzung aller erforderlichen Maßnahmen zur Analyse der Ursachen (einschließlich forensischer Analysen) sowie zur Sicherung der Auftraggeber-Daten und zur Umsetzung aller Sicherheitspatches.

Der Auftragnehmer ist im Übrigen verpflichtet, der LfA innerhalb angemessener Frist alle Auskünfte zu erteilen oder Informationen zur Verfügung zu stellen, die für die Behandlung und Behebung des IKT-Vorfalles notwendig sind.

Diese Unterstützungsleistungen sind mit der vereinbarten Vergütung abgegolten.

#### **9.4.3 IT-Sicherheitsüberprüfung (TLPTs) (Art. 30 Abs. 3 (d) DORA)**

Der Auftragnehmer erteilt der LfA mit Abschluss dieser Ergänzungsvereinbarung die unwiderrufliche Einwilligung zur Durchführung von IT-Sicherheitsüberprüfungen (insb. von bedrohungsorientierten Penetrationstests (TLPT – Threat-Led Penetration Testing) auf bzw. von den zur Leistungserbringung bereitgestellten bzw. eingesetzten Systemen und Zugängen.

Der Auftragnehmer verpflichtet sich, die Durchführung von IT-Sicherheitsüberprüfungen zu ermöglichen, sich zu beteiligen, uneingeschränkt mitzuwirken und zu unterstützen.

Die IT-Sicherheitsüberprüfungen können dabei auch Testangriffe z. B. auf Firewalls und passwortgeschützte Bereiche (Penetrationstests) umfassen. Der Auftragnehmer ist verpflichtet, alle Daten auf seinen IT-Systemen in Hinblick auf mögliche Penetrationstests so zu sichern, dass die Gefahr eines Datenverlusts auch im Falle eines erfolgreichen Penetrationstests ausgeschlossen ist. Die LfA kann sich für die Durchführung der IT-Sicherheitsüberprüfungen qualifizierter Dritter bedienen.

Die LfA wird die Durchführung von Prüfungen vor Ort und destruktive IT-Sicherheitsüberprüfungen mit einem Vorlauf von zehn (10) Werktagen ankündigen. Die Vertragspartner werden sodann einvernehmlich einen Termin festlegen, zudem der Auftragnehmer die erforderlichen Ressourcen bereitstellen und sich eng mit der LfA und/oder mit dem von der LfA beauftragten Dritten abstimmen wird.

## **10 Notfallmanagement (Art. 30 Abs. 3 (c) DORA)**

### **10.1 Allgemeine Grundsätze**

Der Auftragnehmer verfügt über ein Notfallhandbuch mit geeigneten Notfallplänen und Sicherheitsmaßnahmen, die die vertragsgemäße Fortführung der Vertragsleistungen bei Notfällen sicherstellen („Notfallhandbuch“). Das Notfallhandbuch wird vom Auftragnehmer regelmäßig aktualisiert und ist der LfA auf Anforderung zur Einsichtnahme vorzulegen. Der Auftragnehmer muss für die autorisierte und rechtzeitige Einleitung von Notfallmaßnahmen einen Notfallverantwortlichen benennen. Der Auftragnehmer hat dabei insbesondere die Schnittstellen zur Notfallvorsorge durch die LfA zu bedienen.

#### **10.1.1 Durchführung von Notfallübungen**

Durch regelmäßige, stichprobenartige Notfallübungen steigert der Auftragnehmer die Effizienz der Einsatzbereitschaft und gewährleistet die Durchführbarkeit der Notfallmaßnahmen. Die Regelungen bezüglich des Umfangs der Notfallübungen sind im Notfallhandbuch festzulegen.

#### **10.1.2 Sofortmaßnahmen**

Der Auftragnehmer ist dafür verantwortlich, dass nach der Ausrufung des Notfalls die im Notfallhandbuch aufgeführten Maßnahmen unverzüglich umgesetzt werden. Die Sofortmaßnahmen müssen die Alarmierung der entsprechenden Institutionen beinhalten, die gemäß Notfallhandbuch gefordert sind.

## **11 Laufzeit und Kündigung (Art. 30 Abs. 2 (h), Art. 30 Abs. 3 (b) DORA)**

#### **11.1.1 Ordentliche Kündigung**

Die Bestimmungen in dem Vertragswerk zur ordentlichen Kündigung bleiben unberührt.

#### **11.1.2 Außerordentliche Kündigung**

Jeder Vertragspartner kann das Vertragswerk außerordentlich aus wichtigem Grund kündigen.

Ist die LfA zur Kündigung aus wichtigem Grund berechtigt, kann die LfA in der Kündigungserklärung eine angemessene Kündigungsfrist, längstens 12 Monate, bestimmen.

Ist der Auftragnehmer zur Kündigung aus wichtigem Grund berechtigt, beträgt die Kündigungsfrist 12 Monate, es sei denn dies ist für den Auftragnehmer unzumutbar. Dessen ungeachtet ist die LfA berechtigt auf die Einhaltung einer Kündigungsfrist ganz oder vollständig zu verzichten.

Ein wichtiger Grund, der die LfA zur außerordentlichen Kündigung berechtigt, liegt insbesondere dann vor, wenn

- a) beim Auftragnehmer eine wesentliche Vermögensgefährdung oder Vermögensverschlechterung eintritt, die zu einem Creditreform-Bonitätsindex von 420 oder schlechter führt, oder
- b) sich die Eigentumsverhältnisse beim Auftragnehmer im Sinne eines Change of Control verändern, oder
- c) der Auftragnehmer eine wesentliche Pflicht des Vertragswerkes trotz vorheriger Abmahnung nicht einhält, hierzu gehört auch der vertragswidrige Einsatz von Subunternehmern oder die vertragswidrige Verlegung von Leistungsorten, oder
- d) der Auftragnehmer wiederholt mangelhaft leistet, insbesondere wiederholt Service Level(s) nicht einhält oder die Betriebssicherheit oder Betriebsstabilität kritischer Systeme gefährdet ist, oder
- e) die Art und/oder Häufigkeit von Schadensfällen den Betriebsablauf bei der LfA so beeinträchtigt, dass ihr ein Festhalten an dem Vertragswerk nicht mehr zugemutet werden kann, oder
- f) ein erheblicher Verstoß des Auftragnehmers gegen geltende Gesetze, sonstige Vorschriften oder Bestimmungen der vertraglichen Regelungen vorliegt; oder
- g) ein nicht nur geringfügiger Verstoß gegen Datenschutz- und/oder Vertraulichkeitsbestimmungen vorliegt, oder
- h) nachweisliche Schwächen des Auftragnehmers in Bezug auf sein allgemeines 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, vorliegen; oder
- i) die Kündigung zur Erfüllung aufsichtsrechtlicher, gesetzlicher oder gerichtlicher Anordnungen gegenüber der LfA oder aufgrund einer Feststellung von Missständen durch die BaFin geboten ist.

Jede Kündigung bedarf der Schriftform. Vor einer Kündigung aus wichtigem Grund ist diese schriftlich anzudrohen. Der vertragsbrüchige Vertragspartner ist schriftlich abzumahnern und

ihm ist Gelegenheit zu geben, innerhalb von 30 Kalendertagen nach Erhalt der Abmahnung die den wichtigen Grund begründenden Missstände zu beheben. Einer Abmahnung bedarf es nicht, wenn

- a) der vertragsbrüchige Vertragspartner die Leistung ernsthaft und endgültig verweigert, und/oder
- b) besondere Umstände vorliegen, die unter Abwägung der beiderseitigen Interessen die sofortige Kündigung rechtfertigen.

Die Kündigung kann nur binnen einer Frist von 3 Monaten erklärt werden, nachdem der zur Kündigung berechnete Vertragspartner Kenntnis vom Kündigungsgrund erlangt hat. Berechnet die Gesamtbetrachtung einer Reihe von Ereignissen einen Vertragspartner zur Kündigung, so ist die Frist ab dem letzten dieser Ereignisse zu berechnen.

## **12 Exit Management (Art. 30 Abs. 3 (f))**

### **12.1.1 Verlängerungsoption**

Der Auftragnehmer ist verpflichtet, die Vertragsleistungen für einen Zeitraum von bis zu 12 Monaten über den jeweiligen Beendigungszeitpunkt hinaus („Übergangszeit“) zu erbringen, falls die LfA dies verlangt („Verlängerungsverlangen“). Ein Verlängerungsverlangen hat schriftlich mit einem Vorlauf von möglichst drei (3) Monaten zu erfolgen und soll Angaben über Art und Umfang der fortzuführenden Vertragsleistungen enthalten.

Im Verlängerungsverlangen ist die Dauer der Übergangszeit anzugeben. Veränderungen wird die LfA dem Auftragnehmer jeweils unverzüglich mitteilen. Wenn die LfA das Recht zur Verschiebung des Beendigungszeitpunkts mit einem Vorlauf von weniger als drei (3) Monaten vor dem zuletzt geltenden Beendigungszeitpunkt ausübt und soweit der Auftragnehmer nachweist, dass sich durch die Verschiebung des Beendigungszeitpunkts ohne Beachtung dieser Vorlaufzeit der Aufwand für die weitere Erbringung der betroffenen Vertragsleistungen nachweislich erhöht, kann der Auftragnehmer von der LfA verlangen, dass diese den zusätzlichen Aufwand gegen Nachweis erstattet.

Auf Verlangen der LfA werden die Vertragspartner eine Verlängerung der Übergangszeit über den Zeitraum von maximal 6 Monaten hinaus vereinbaren

Für die Dauer der Übergangszeit gelten die Bestimmungen des Vertragswerks fort, soweit sich nicht aus den sonstigen Abreden der Vertragspartner etwas anderes ergibt. Dies gilt insbesondere für die Erbringung der Vertragsleistungen und die Einhaltung der Service Level. Die



fortzuführenden Vertragsleistungen werden während der Übergangszeit zu den unmittelbar vor dem Beendigungszeitpunkt gültigen Konditionen abgerechnet.

### **12.1.2 Exit Management**

Der Auftragnehmer wird dafür Sorge tragen, dass die Vertragsleistungen im Falle einer vollständigen oder teilweisen Beendigung des Vertragswerks reibungslos ganz oder teilweise durch den Folgeanbieter übernommen werden können.

Der Auftragnehmer verpflichtet sich, innerhalb eines zwischen den Vertragspartnern abgestimmten Zeitplans einen Plan für die Überleitung („Exit-Plan“) zu erstellen. Jede Fassung des Exit-Plans bedarf der Abnahme durch die LfA.

Der Exit-Plan nimmt alle nachfolgend genannten Punkte zu Hardware, Software, sonstigen Verträgen etc. auf. Der Auftragnehmer muss im Exit-Plan detailliert beschreiben, auf welche Weise und mit welchen Methoden die betroffenen Vertragsleistungen und die ihnen zugrundeliegenden Prozesse des Auftragnehmers im Falle einer Beendigung aus der Sphäre des Auftragnehmers herausgelöst und an die LfA oder an Folgeanbieter übergeben werden können; dies schließt ein Migrationskonzept ein. Die LfA sowie ein etwaiger Folgeanbieter muss mit diesem Plan in die Lage versetzt werden, die Vertragsleistungen in ihre bzw. seine Sphäre zu übernehmen. Daraus dürfen sich nur unwesentliche Einschränkungen hinsichtlich der Kontinuität und Qualität der Unterstützung der kritischen oder wichtigen Funktion ergeben. Der Exit-Plan enthält insbesondere Folgendes:

- a) eine detaillierte Beschreibung der zu übergebenden Vertragsleistungen (insb. Beschreibung der Prozesse, einschließlich der verwendeten Standards etc.);
- b) eine Beschreibung von Mitwirkungsleistungen der LfA oder des Folgeanbieters;
- c) einen detaillierten Meilensteinplan für die Überleitung;
- d) einen detaillierten Ressourcenbedarf, aufgeteilt nach Ressourcen, die vom Auftragnehmer, der LfA, einem etwaigen Folgeanbieter oder einem sonstigen von der LfA benannten Dritten zu stellen sind;
- e) eine Beschreibung der erforderlichen Zusammenarbeit (z.B. Zeitrahmen, Rollen, Skills) zwischen den an der Überleitung Beteiligten;
- f) alle Daten, Hardware, Software, Lizenzen, Verträge mit Subunternehmern des Auftragnehmers und/oder anderen Dritten sowie alle anderen Gegenstände, die vom Auftragnehmer für die Erbringung der Vertragsleistungen genutzt werden und deren Übertragung an die LfA im Hinblick auf die Überleitung erforderlich oder nützlich sein könnten (Asset-Liste);

- g) jegliche anderen wesentliche Informationen in Bezug auf die Überleitung; und
- h) das Format aller vom Auftragnehmer im Zuge der Überleitung zur Verfügung gestellten Informationen.

Der Auftragnehmer verpflichtet sich, im Rahmen des Zumutbaren sämtliche Aufgaben zu erledigen, die ihm im Exit-Plan zugewiesen werden, und zwar zu den in der jeweils aktuellen Fassung des Exit-Plan vorgesehenen Terminen. Die Überleitung ist so auszuführen, dass insbesondere (i) damit verbundene operative Risiken soweit wie möglich minimiert werden, (ii) die Qualität der Vertragsleistungen vor und nach dem Überleitungszeitpunkt unbeeinträchtigt bleibt und (iii) die LfA oder ein Folgeanbieter objektiv in der Lage ist, die Vertragsleistungen ab dem Überleitungszeitpunkt in einem stabilen Zustand zu übernehmen.

Der Auftragnehmer ist verpflichtet, den Exit-Plan jederzeit auf Wunsch der LfA, mindestens aber unaufgefordert zu Beginn eines jeden Kalenderjahrs, zu aktualisieren und die so aktualisierte Fassung der LfA zur Abnahme vorzulegen. Der Auftragnehmer hat dabei detaillierte Maßnahmen vorzuschlagen, um den Exit-Plan auf dem neuesten Stand zu halten. Der Auftragnehmer wird der LfA den Vorschlag für den aktualisierten Exit-Plan zur Prüfung und Kommentierung durch die LfA vorlegen.

Ferner ist der Auftragnehmer verpflichtet, der LfA innerhalb von 15 Arbeitstagen, nachdem er eine Kündigung erhalten hat, oder bei ordentlicher Beendigung 6 Monate vor dem regulären Vertragsende, der LfA einen Vorschlag für eine überarbeitete Version des Exit-Plans zu unterbreiten, der alle Änderungen enthält, die erforderlich sind, um die besonderen Anforderungen der anstehenden Überleitung zu erfüllen.

### **12.1.3 Wissenstransfer**

Der Auftragnehmer wird der LfA im Zusammenhang mit der Beendigung des Vertragswerks rechtzeitig alle Informationen und Unterlagen (soweit der Auftragnehmer darüber verfügen darf und nur Kopien, soweit der Auftragnehmer die Original-Unterlagen selbst weiterhin benötigt) zur Verfügung stellen), die sich auf die Vertragsleistungen beziehen oder die erforderlich und/oder nützlich sind, um die LfA in die Lage zu versetzen, die Durchführung der Vertragsleistungen selbst zu erbringen oder durch Folgeanbieter erbringen zu lassen. Der Auftragnehmer verpflichtet sich insbesondere, der LfA und (potenziellen) Folgeanbietern auf Verlangen der LfA in einem Detailgrad, der es möglichen Folgeanbietern erlaubt, ein fundiertes Verständnis über die Vertragsleistungen zu erlangen, Folgendes zur Verfügung zu stellen:

- a) eine aktualisierte Dokumentation der Vertragsleistungen sowie der diesbezüglichen Systeme und Prozesse, einschließlich etwaiger Schnittstellen sowie der IT-Architektur, jeweils soweit zur reibungslosen Überleitung erforderlich oder zweckdienlich;
- b) die System- und Anwendungsdokumentation für die vom Auftragnehmer für die LfA betriebenen oder betreuten Anwendungen;
- c) alle sonstigen Dokumentationen, Daten, Datenbanken, Systeme und Informationen, die der LfA gehören, für diese erstellt wurden oder diesen auf sonstige Weise nach dem Vertragswerk zustehen, wobei dies jeweils in einem elektronischen Format zu geschehen hat, das mit zu diesem Zeitpunkt marktüblichen Standard-Tools gelesen werden kann;
- d) eine aussagekräftige Darstellung der Tools und Prozesse, die zur Gewährleistung der IT-Sicherheit und des Managements der Vertragsleistungen (z.B. IAM, Konfiguration, Deployment) eingesetzt werden, soweit zur ordnungsgemäßen Überleitung erforderlich;
- e) sämtliche LfA-spezifischen Policies, Prozesse, Standards und Betriebsabläufe im Zusammenhang mit den Vertragsleistungen im Rahmen der Leistungserbringung zu erläutern;
- f) in angemessenem Umfang Schulungen von Mitarbeitern der LfA und von Folgeanbietern durchzuführen, um zu gewährleisten, dass der Folgeanbieter die Vertragsleistungen nach dem Überleitungszeitpunkt ohne operative Einschränkungen fortführen kann; und
- g) in angemessenem Umfang und unter Wahrung der operativen Leistungsfähigkeit Zugang zu Mitarbeitern und Betriebsstätten des Auftragnehmers bzw. seiner von der LfA genehmigten Subunternehmer (z.B. im Rahmen eines sogenannten Shadowing), soweit diese für Vertragsleistungen eingesetzt werden, zu verschaffen;

Die Lieferungen im Rahmen des Wissenstransfers müssen jeweils so beschaffen sein, wie es von einem führenden Anbieter von IKT-Leistungen erwartet werden kann.

## **13 Sensibilisierung und Schulung (Art. 30 Abs. 2 (i) DORA)**

Auf Verlangen der LfA wird der Auftragnehmer an den von der LfA gemäß Art. 13 Abs. 6 DORA angebotenen Programmen zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz teilnehmen. Die LfA informiert Auftragnehmer in Textform über Termine und Schulungsinhalte. Der Auftragnehmer trägt die Aufwände seiner Mitarbeiter, die durch die Teilnahme an den Schulungen entstehen. Mitarbeiter des Auftragnehmers, die mit-

tels eines Accounts direkten Zugriff auf das Netzwerk und die Systeme der LfA besitzen, müssen zusätzlich entsprechend ihrer Tätigkeiten an Schulungs- und Sensibilisierungsmaßnahmen teilnehmen, die von der LfA zugewiesen werden, um die Sicherheit der verarbeiteten Informationen der LfA während der Vertragslaufzeit zu gewährleisten.

## 14 Ansprechpartner

Auftragnehmer: [bitte ausfüllen, Name, Vorname, Position, Email Adresse und ggf. Telefonnummer]

LfA: [bitte ausfüllen, Name, Vorname, Position, Email Adresse und ggf. Telefonnummer]

## 15 Schlussbestimmung

Die vorliegende Ergänzungsvereinbarung unterfällt im Übrigen den Regelungen des Vertragswerkes.

## 16 Anlagen

Anlage 1      Leistungsorte und Subunternehmer

## Unterschriften

**LfA**

München, den \_\_\_\_\_

München, den \_\_\_\_\_

\_\_\_\_\_

Unterschrift

\_\_\_\_\_

Unterschrift

\_\_\_\_\_  
Name des Unterzeichnenden

\_\_\_\_\_  
Name des Unterzeichnenden

**Auftragnehmer**

[Ort], den \_\_\_\_\_

[Ort], den \_\_\_\_\_

\_\_\_\_\_  
Unterschrift

\_\_\_\_\_  
Unterschrift

\_\_\_\_\_  
Name des Unterzeichnenden

\_\_\_\_\_  
Name des Unterzeichnenden