Anforderungen gemäß DORA-Verordnung

1. Vorbemerkung

Die TK hat für ihre betriebliche Altersvorsorge die TK Pensionsfonds AG gegründet. Der TK Pensionsfonds ist eine unternehmenseigene Einrichtung der betrieblichen Altersversorgung, die nicht für andere Unternehmen geöffnet ist. Die TK ist die alleinige Aktionärin der TK Pensionsfonds AG. Der TK Pensionsfonds unterliegt der Aufsicht durch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin).

Bei den von dem AN auf der Grundlage des Vertrags erbrachten Leistungen handelt es sich um IKT-Dienstleistungen im Sinne der Verordnung (EU) 2022/2554 (DORA), die kritische / wichtige Funktionen unterstützen. Da diese IKT-Dienstleistungen auch für den TK Pensionsfonds als Finanzunternehmen relevant sind, ergänzen die Parteien den Vertrag gemäß den Anforderungen der DORA-Verordnung und der zugehörigen RTS (relevante technische Regulierungsstandards) an die Gestaltung von Verträgen über IKT-Dienstleistungen, die kritische / wichtige Funktionen unterstützen, nach Maßgabe der folgenden Regelungen. Der AN stimmt der Weitergabe der von ihm nach Maßgabe dieser Anlage bereitzustellenden Informationen an den TK Pensionsfonds zu.

2. Leistungsbeschreibung und Dienstleistungsgüte (Art. 30 Abs. 2 Buchst. a und e DORA)

(1) Die klare und vollständige Beschreibung aller vom AN geschuldeten IKT-Dienstleistungen ergibt sich aus dem Vertrag und den dazugehörigen Anlagen.

(2) Der AN gewährleistet die Einhaltung der im Vertrag vereinbarten Service Level. Stellt die TK fest, dass die vereinbarten Service Level nicht eingehalten werden, kann sie vom AN jederzeit unverzügliche Korrekturmaßnahmen verlangen. Der AN wird der TK in Textform mitteilen, welche Schritte ergriffen werden, um die Service Level wieder einzuhalten.

3. Standorte (Art. 30 Abs. 2 Buchst. b DORA)

Die im Rahmen der vertraglichen Leistungserbringung erfolgende Verarbeitung von Daten (einschließlich deren Speicherung) sowie die Bereitstellung von Funktionen und IKT-Dienstleistungen erfolgen an den in der Anlage V5 (Angebot) zum Vertrag genannten Standorten. Der AN informiert die TK unverzüglich in Textform vorab über jede beabsichtigte Änderung von Standorten.

4. Datenschutz und Datensicherheit (Art. 30 Abs. 2 Buchst. c und d DORA)

(1) Der AN gewährleistet die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit aller Daten, einschließlich personenbezogener Daten. Der AN verpflichtet sich, angemessene, geeignete technische und organisatorische Maßnahmen zum Schutz der Daten zu ergreifen, die dem aktuellen Stand der Technik entsprechen.

(2) Soweit der AN in seinen Systemen Daten der TK (einschließlich personenbezogener Daten) speichert, die der TK nicht selbst vorliegen und auf die die TK nicht jederzeit selbst zugreifen kann, gibt er diese Daten auf Anforderung der TK jederzeit in einem strukturierten, gängigen und maschinenlesbaren Format, das den branchenüblichen Standards entspricht, heraus.

5. IKT-Vorfälle (Art. 30 Abs. 2 Buchst. f DORA) / Meldung und Unterstützung

(1) Sofern der AN von einem IKT-Vorfall in seiner Sphäre mit Relevanz für die vertraglich geschuldeten Leistungen Kenntnis erlangt, wird er die TK unverzüglich benachrichtigen und – auf der Grundlage eines von der TK vorgegebenen Formulars – detailliert über den IKT-Vorfall, dessen potenzielle Auswir-

kungen und die ergriffenen Maßnahmen zur Behebung des IKT-Vorfalls informieren. Bei schwerwiegenden IKT-bezogenen Vorfällen (vgl. Art. 3 Nr. 10 DORA) erfolgt diese Benachrichtigung zudem spätestens innerhalb von 2 Stunden (7x24, auch an Sonn- und Feiertagen) telefonisch an das zentrale IT-Operating der TK (040/6909-1842).

(2) Unabhängig hiervon unterstützt der AN die TK auf Anforderung bei jedem IKT-Vorfall, der in Verbindung mit den vom AN erbrachten Leistungen steht, im Hinblick auf seine Leistungssphäre in dem für die Bewältigung und Aufklärung des IKT-Vorfalls erforderlichen Umfang, insbesondere durch die Bereitstellung der hierfür relevanten Informationen und die Durchführung der in seiner Leistungssphäre erforderlichen Abhilfemaßnahmen. Sofern der AN davon ausgeht, dass es sich um einen schwerwiegenden IKT-bezogenen Vorfall im Sinne von Art. 3 Nr. 10 DORA handeln könnte, der einer Meldepflicht gemäß Art. 19 DORA unterliegt, unterstützt der AN die TK unverzüglich bei der Erfüllung der Melde- und Offenlegungspflichten der TK bzw. des TK Pensionsfonds.

6. Zusammenarbeit mit Behörden (Art. 30 Abs. 2 Buchst. g DORA)

Der AN verpflichtet sich, in vollem Umfang mit den für den TK Pensionsfonds zuständigen Aufsichts- und Abwicklungsbehörden zu kooperieren. Dies umfasst die Bereitstellung von Dokumentationen, Berichterstattungen und die Teilnahme an Besprechungen, die von den Behörden initiiert oder angeordnet werden. Der AN wird die TK unverzüglich über alle Anfragen, Prüfungen oder Ermittlungen von Seiten der Behörden informieren, die sich auf die erbrachten IKT-Dienstleistungen oder die verarbeiteten Daten beziehen. Alle spezifisch auf die TK bezogenen Antworten und ggf. bereitzustellenden Dokumente sind im Vorfeld mit der TK abzustimmen, um sicherzustellen, dass die Interessen der TK und des TK Pensionsfonds gewahrt bleiben.

7. Außerordentliche Kündigung und weitere Kündigungsrechte (Art. 28 Abs. 7 DORA und Art. 6 Abs. 1 RTS SUB)

Die TK hat das Recht, den Vertrag bei Vorliegen eines der in Art. 28 Abs. 7 DORA genannten Fälle – bezogen auf die Berechtigung der TK, die vertraglichen Leistungen auch durch den TK Pensionsfonds zu nutzen – außerordentlich zu kündigen. Die in Art. 28 Abs. 7 DORA genannten Fälle gelten jeweils als wichtiger Grund im Sinne des § 314 BGB. § 314 Abs. 2 BGB bleibt unberührt.

Hiervon unberührt bleibt ein etwaiges auf denselben Sachverhalt gestütztes außerordentliches Kündigungsrecht der TK.

8. Schulungen (Art. 30 Abs. 2 Buchst. i DORA)

Der AN trägt dafür Sorge, dass auf Anforderung der TK – im Hinblick auf die unter dem Vertrag zu erbringenden Leistungen und die Schulungsinhalte – passende Mitarbeitende des Auftragnehmers bzw. der von dem AN eingesetzten Unterauftragnehmer an von der TK bzw. dem TK Pensionsfonds angebotenen Programmen zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz teilnehmen.

9. Unterauftragsvergabe (Art. 30 Abs. 2 Buchst. a DORA; Art. 3 Abs. 1, Art. 4 Abs. 1 und Art. 5 Abs. 1-3 RTS SUB)

(1) Die Regelungen zur Unterauftragsvergabe, insbesondere ein etwaiges Zustimmungserfordernis, ergeben sich – ergänzend zu den folgenden Bestimmungen – aus dem Vertrag.

(2) Der AN informiert die TK rechtzeitig vorab über jede geplante Beauftragung oder wesentliche Änderung („Unterauftragnehmer-Änderung“) von Unterauftragnehmern, die an der Erbringung kriti-

scher/wichtiger IKT-Dienstleistungen mitwirken. Die TK kann der Unterauftragnehmer-Änderung innerhalb einer angemessenen Frist widersprechen oder, falls nach dem Vertrag eine ausdrückliche Zustimmung erforderlich ist, diese verweigern. Hat die TK einer Unterauftragnehmer-Änderung widersprochen oder verweigert sie ihre Zustimmung, darf der AN diese erst umsetzen, wenn entweder eine Einigung über angemessene Anpassungen erzielt oder der ausdrückliche Zustimmungsvorbehalt erfüllt ist.

(3) Der AN bleibt für die Erfüllung der Verpflichtungen aus dem Vertrag verantwortlich, auch wenn die Leistung oder Teile der Leistung durch Unterauftragnehmer erbracht werden. Der AN hat die kontinuierliche Erbringung der IKT-Dienstleistungen sicherzustellen, selbst wenn der Unterauftragnehmer seine Service Level oder andere Pflichten nicht erfüllt.

(4) Der AN überwacht alle (weiter)unterbeauftragten IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, um sicherzustellen, dass die vertraglichen Verpflichtungen durchgehend erfüllt werden.

(5) Der AN informiert die TK über alle wesentlichen Entwicklungen bei Unterauftragnehmern, die die Risikobewertung beeinflussen könnten, insbesondere soweit diese dazu führen könnten, dass der AN seine vertraglichen Verpflichtungen nicht mehr erfüllen kann.

(6) Vor einer Weiterverlagerung von IKT-Dienstleistungen an Unterauftragnehmer prüft der AN insbesondere die damit einhergehenden IKT-Risiken (z. B. Standort, Rechtslage, Sicherheitsniveau).

(7) Der AN stellt sicher, dass sämtliche Unterauftragsverträge in Schriftform oder in einem anderen klar dokumentierten, dauerhaften und zugänglichen Format festgehalten werden und folgende Mindestinhalte umfassen:

- Überwachungs- und Berichtspflichten des Unterauftragnehmers (mindestens entsprechend den Pflichten des AN gegenüber der TK),
- Festlegung der Standorte, an denen Daten verarbeitet und gespeichert werden, sowie Klarstellung des Eigentums an den Daten,
- Verpflichtung des Unterauftragnehmers zur Implementierung und jährlichen Überprüfung eines Notfallkonzepts im Sinne dieser Anlage „Anforderungen gemäß DORA-Verordnung“ (vgl. Ziffer 11),
- Verpflichtung zur Einhaltung der vereinbarten Service Levels,
- Verpflichtung zur Einhaltung der vereinbarten Sicherheitsstandards,
- Einräumung von mindestens denselben Prüfungs- und Zugangsrechten für die TK und die Aufsichtsbehörden, wie sie dem AN selbst obliegen (vgl. Ziffer 13),
- Kündigungsrechte, sofern Service Levels oder sonstige Pflichten nicht eingehalten werden können.

(8) Auf Anforderung der TK wird der AN jederzeit geeignete Nachweise über die Einhaltung und Überwachung der Bestimmungen dieser Ziffer 9 erbringen. Dies umfasst die Offenlegung einschlägiger Informationen und Dokumentationen über den Unterauftragnehmer und das Unterauftragsverhältnis, soweit rechtlich zulässig und erforderlich, damit die TK die Eignung des Unterauftragnehmers beurteilen kann.

10. Berichterstattungspflichten (Art. 30 Abs. 3 Buchst. b DORA)

(1) Zusätzlich zu bestehenden Berichtspflichten aus dem Vertrag wird der AN die TK unverzüglich über jede Entwicklung informieren, die wesentliche nachteilige Auswirkungen auf seine Leistungsfähigkeit zur Bereitstellung der vertraglich geschuldeten IKT-Dienstleistungen (insbesondere die Einhaltung der vereinbarten Service Level) haben könnte. In diesem Fall legt der AN insbesondere dar, wie lange

mögliche Beeinträchtigungen andauern können und gibt auf Anforderung der TK eine realistische Einschätzung über ggf. erforderliche Gegenmaßnahmen ab.

(2) Auf Anforderung der TK hat der AN einmal jährlich (i) Berichte über die vom AN durchgeführten Tests zur Überprüfung der Resilienz der für die Leistungsausführung eingesetzten IT-Systeme, (ii) einen Informationssicherheitsbericht sowie (iii) einen Risikobericht mit für die Leistungserbringung wesentlichen IT- und Informationssicherheitsrisiken vorzulegen und gegebenenfalls zu erläutern.

11. Notfallpläne (Art. 30 Abs. 3 Buchst. c DORA)

(1) Der AN unterhält ein dem Stand der Technik entsprechendes Notfallkonzept (einschließlich Disaster Recovery und Krisenmanagement), um die Kontinuität und Qualität der für die TK zu erbringenden kritischen IKT-Dienstleistungen zu gewährleisten. Der AN hat ein funktionierendes Business Continuity Management nach BSI-Standard 200-4 oder ISO 22301 BCMS etabliert und weist der TK auf Anforderung diesbezügliche Tests nach.

(2) Der AN gewährt der TK auf Anforderung Einblick in sein Notfallkonzept.

(3) Der AN testet mindestens jährlich diejenigen Teile seines Notfallkonzepts, die in ihrer Gesamtheit die Wirksamkeit des Notfallsystems sicherstellen. Der AN stellt der TK auf Anforderung Nachweise über die durchgeführten Tests sowie Einsicht in die Ergebnisse etwaiger Maßnahmenpläne zur Verfügung.

12. Informationssicherheit; Threat-Led Penetration Testing (Art. 30 Abs. 3 Buchst. c und d DORA)

(1) Der AN gewährleistet und überprüft regelmäßig, dass seine technischen und organisatorischen Maßnahmen im Bereich der Informationssicherheit den anerkannten Marktnormen entsprechen (insbesondere ISO/IEC 27001, IT-Grundschutz BSI, ENISA-Empfehlungen).

(2) Der AN hält für die IKT-Dienstleistungen eine vollumfängliche Zertifizierung seines Informationssicherheitsmanagementsystems nach ISO/IEC 27001 aufrecht; der Geltungsbereich der Zertifizierung muss mindestens die vertraglich geschuldeten IKT-Dienstleistungen bzw. eingesetzten IKT-Systeme umfassen. Ein aktuelles Zertifikat nebst aussagekräftigem Statement of Applicability stellt der AN der TK einmal jährlich bereit.

(3) Soweit die TK (bzw. der TK Pensionsfonds) nach Art. 26 DORA verpflichtet ist, Threat-Led Penetration Tests (TLPT) durchzuführen, unterstützt der AN die TK hierbei nach Maßgabe der jeweils anwendbaren DORA-Vorschriften und wirkt an den relevanten Penetrationstests nach besten Kräften mit.

13. Zugangs-, Inspektions- und Audit-Rechte (Art. 30 Abs. 3 Buchst. e DORA)

(1) Die TK ist berechtigt, die Erbringung der Leistungen durch den AN laufend zu überwachen (z. B. durch Audits oder Inspektionen), um die Einhaltung dieser Anlage „Anforderungen gemäß DORA-Verordnung“ und der geltenden regulatorischen Vorgaben zu prüfen. Dazu räumt der AN der TK, dem TK Pensionsfonds sowie von der TK bzw. dem TK Pensionsfonds beauftragten Dritten ein uneingeschränktes Zugangs-, Inspektions- und Auditrecht ein. Dieses umfasst auch das Recht, Kopien von relevanten Unterlagen anzufertigen, sofern diese für die Geschäftstätigkeit des AN entscheidende Bedeutung haben. Dies gilt entsprechend für Prüfungen durch die zuständigen Aufsichtsbehörden des TK Pensionsfonds.

(2) Bei Vor-Ort-Prüfungen und anderen Audits, die von der TK, dem TK Pensionsfonds, den Aufsichtsbehörden oder ausdrücklich von diesen Beauftragten durchgeführt werden, wird der AN uneingeschränkt mitwirken. Die TK wird dem AN Zeitpunkt und Gegenstand einer Prüfung mit angemessenem Vorlauf mitteilen, soweit hierdurch nicht der Prüfzweck gefährdet wird. Vor-Ort-Prüfungen dürfen den Geschäftsbetrieb nicht unzumutbar stören.

14. Beendigungsunterstützung (Art. 30 Abs. 3 Buchst. f DORA)

(1) Endet die Pflicht des AN, die IKT-Dienstleistungen zu erbringen, gleich aus welchem Grund, so wird der AN auf Anforderung der TK über einen von der TK zu bestimmenden Übergangszeitraum (oder gemäß einer gesondert vereinbarten Ausstiegsstrategie) die Leistungen unverändert fortführen, damit keine Unterbrechung der Geschäftstätigkeit der TK bzw. des TK Pensionsfonds entsteht und die Funktionen nahtlos an einen Alternativanbieter oder die TK selbst übergeben werden können. Soweit der AN auf Anforderung der TK nach Maßgabe dieser Regelung die Leistungserbringung fortsetzt, erhält er weiterhin die für die betroffenen Leistungen vertraglich vereinbarte Vergütung.

(2) In der Überleitungsphase wird der AN die TK auf Anforderung in dem für eine reibungslose und effiziente Übernahme der Leistungen durch die TK oder einen Nachfolgedienstleister erforderlichen Umfang unterstützen.

15. Vergütung nach Aufwand

(1) Für Aufwände, die dem AN durch die Erfüllung seiner Pflichten aus den Ziffern 6 (Zusammenarbeit mit Behörden) und 13 (Audit-Rechte) dieses Nachtrags entstehen, erhält der AN eine Vergütung nach Aufwand, soweit die Aufwände nicht ohnehin auch zur Erfüllung der unabhängig von dieser Anlage „Anforderungen gemäß DORA-Verordnung“ bestehenden vertraglichen Pflichten angefallen wären. Der Anspruch auf Vergütung besteht im Hinblick auf Ziffer 13 (Zugangs-, Inspektions- und Audit-Rechte) nur, soweit nicht eine Pflichtverletzung des AN der Anlass ist.

(2) Der Stundensatz für die Abrechnung dieser Aufwände ergibt sich aus der Anlage Preisblatt zu dem Vertrag. Alle Aufwände sind vorab mit der TK abzustimmen und bedürfen deren schriftlicher Zustimmung. Die Abrechnung erfolgt monatlich auf Basis von Leistungsnachweisen. Im Übrigen erfolgt keine gesonderte Vergütung / Erstattung der auf der Grundlage dieser Anlage „Anforderungen gemäß DORA-Verordnung“ zu erbringenden Leistungen und anfallenden Kosten.

16. Sonstiges

(1) Die Bestimmungen dieser Anlage „Anforderungen gemäß DORA-Verordnung“ haben im Falle eines Widerspruchs Vorrang vor den Regelungen im Vertrag. Weitergehende Regelungen/Anforderungen aus dem Vertrag bleiben – auch im Falle eines Widerspruchs – unberührt, sofern sie nicht ausdrücklich durch diese Anlage „Anforderungen gemäß DORA-Verordnung“ modifiziert werden.