Zusatzvereinbarungen “Security Audit”

“Weiterentwicklung und Betrieb der Software für die Datentreuhänder-Plattform EuroDaT sowie des AML-Anwendungsfalls safeAML”

1. Präambel

Die Auftraggeberin erbringt durch die Bereitstellung der EuroDaT-Plattform und der safeAML-Anwendung IKT-Dienstleistungen für Finanzunternehmen, die aufsichtsrechtlich verpflichtet sind, mit Auftragnehmerinnen, die digitale Dienste oder Datendienste erbringen, die über Informations- und Kommunikationstechnologie („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“), Regelungen zu vereinbaren, insbesondere auch um die digitale operationale Widerstandsfähigkeit von EU-Finanzunternehmen und ihren IKT-Drittdienstleistern zu verbessern.

Soweit es sich bei den Leistungen um IKT-Dienstleistungen zur Unterstützung einer oder mehrerer Funktionen handelt, deren Ausfall die finanzielle Leistungsfähigkeit dieser Finanzunternehmen oder die Solidität oder Fortführung ihrer Geschäftstätigkeiten und Dienstleistungen erheblich beeinträchtigen würde oder deren unterbrochene, fehlerhafte oder unterbliebene Leistung die fortdauernde Einhaltung der Zulassungsbedingungen und -verpflichtungen der Finanzunternehmen oder ihrer sonstigen Verpflichtungen nach dem anwendbaren Finanzdienstleistungsrecht erheblich beeinträchtigen würde („IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen“), haben die Parteien dies in der Rahmenvereinbarung oder einem Einzelauftrag vereinbart, oder aber es besteht die Möglichkeit, dass auf Basis der Rahmenvereinbarung ein Einzelauftrag geschlossen wird, der dies vereinbart.

Die Auftragnehmerin erbringt Leistungen für die Auftraggeberin, die deren Leistungserbringung gegenüber Finanzunternehmen unterstützt. In diesem Zusammenhang ist die Auftragnehmerin auch für den Schutz der zu diesem Zwecke eingesetzten Anwendungen und Daten vor Wissen oder Veränderung Dritter, insbesondere durch sogenannte Hackerangriffe oder „Denial of Service“ (DoS)-Angriffe, verantwortlich.

Die Auftraggeberin hat ein großes Interesse daran, dass die von der Auftragnehmerin betriebenen Hard- und Softwarekomponenten, sowie die Datenspeicherung und Datenübertragung gegen den unbefugten Zugriff Dritter geschützt sind. Die Auftraggeberin ist bestrebt, die Sicherheit der Leistungen der Auftragnehmerin in unregelmäßigen Abständen zu überprüfen bzw. den Finanzunternehmen, die ihre Kunden sind, die Möglichkeit einzuräumen, eine solche Überprüfung durchzuführen.

Die Auftraggeberin bzw. die Finanzunternehmen verfolgen mit der Überprüfung insbesondere folgende Ziele:

1) Identifizierung von Schwachstellen
2) Erhöhung oder Bestätigung der Sicherheit der technischen Systeme
3) Erhöhung oder Bestätigung der Sicherheit der organisatorischen und menschlichen Infrastruktur

Um diese Überprüfungen sicherzustellen, schließen die Parteien folgende Zusatzvereinbarung:

2. Durchführung von Tests durch die Auftragnehmerin

Erbringt die Auftragnehmerin IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen für die Auftraggeberin bzw. für Fnanzunternehmen, die ihre Kunden sind, gemäß des Digital Operational Resilience Act (Verordnung (EU) 2022/2554, „DORA-Verordnung“), führt die Auftragnehmerin für vertraglich vereinbarte IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen mindestens jährlich selbstständig Tests zur Überprüfung der Resilienz durch. Die Berichte der Tests inkl. zugehörigem Maßnahmenplan der identifizierten Schwachstellen werden während der Laufzeit des Vertrags jährlich oder auf Verlangen der Auftraggeberin dieser unverzüglich ausgehändigt. Sollte die Auftragnehmerin bei einem von ihm durchgeführten Test eine kritische Schwachstelle feststellen, ist dies der Auftraggeberin unverzüglich aufzuzeigen.

Diese durch die Auftragnehmerin erstellten Testberichte und Maßnahmenpläne nutzen die Finanzunternehmen, die Kunden der Auftraggeberin sind, zur Erfüllung ihrer Pflichten gemäß Artikel 25 der DORA-Verordnung. Die durchzuführenden Tests („Resilienztests“) umfassen daher mindestens Schwachstellenbewertung und -scans, Open-Source-Analysen, Netzwerksicherheitsbewertungen, Lückenanalysen, Überprüfung der physischen Sicherheit, Fragebögen und Scans von Softwarelösungen, Quellcodeüberprüfungen soweit durchführbar, szenariobasierte Tests, Kompatibilitätstests, Leistungstests, End-to-End-Tests und Penetrationstests.

Die Testberichte der Auftragnehmerin beinhalten mindestens eine Management Summary der Testergebnisse, sowie eine detaillierte Auflistung und Beschreibung der während des Resilienztest aufgedeckten Schwachstellen, als auch deren Kritikalitätseinwertung. Die auf Basis der Testberichte von der Auftragnehmerin zu erstellenden Maßnahmenpläne zur Behebung der Schwachstellen und Sicherheitsmängel haben die Kritikalität der festgestellten Sicherheitsmängel und deren Fristen zur Behebung angemessen zu berücksichtigen. Die Auftraggeberin ist zur Weitergabe der Testergebnisse an die betroffenen Finanzunternehmen berechtigt.

Soweit erforderlich, arbeiten die Parteien zusammen, um Sicherheitsmängel zu beheben. Die Auftragnehmerin berichtet regelmäßig und der Kritikalität angemessen, mindestens jedoch wöchentlich bei im Testbericht als kritisch eingestuften Sicherheitsmängeln, über den Fortschritt der Behebung.

Die Auftragnehmerin hat die im Testbericht festgestellten Schwachstellen und Sicherheitsmängel innerhalb der Fristen auf ihre Kosten zu beheben.

3. Durchführung von Resilienztests durch die Finanzunternehmen

Um ihren Verpflichtungen zur Durchführung von Resilienztests gemäß Artikel 25 DORA-Verordnung nachzukommen, sind die Finanzunternehmen, die Kunden der Auftraggeberin sind, oder eine von ihnen beauftragte Dritte jederzeit berechtigt, mit einer unter Einhaltung einer angemessenen Frist ausgesprochenen Vorankündigung über die Nutzung von Telekommunikationsleitungen, insbesondere des Internets, zu überprüfen, ob die von der Auftragnehmerin zur Erbringung von Leistungen im Rahmen des Vertrags bereitgestellten oder betriebenen Webserver und sonstigen technischen Einrichtungen sowie Softwareanwendungen gegen Eindringen von außen und Manipulationen geschützt sind, oder ob die IT-Sicherheit derzeit durch die eingesetzten Sicherheitsmaßnahmen gewährleistet ist.

Vor Beginn des Resilienztests legen die Parteien und das durchführende Finanzunternehmen gemeinsam die Rahmenbedingungen für die Überprüfung fest (z.B. Testzeitraum, Testobjekt und Testtiefe). Auf Verlangen der Auftraggeberin oder des Finanzunternehmens stellt die Auftragnehmerin die für den Resilienztests erforderlichen Informationen und sichere Kommunikationswege unverzüglich, vollständig und korrekt zur Verfügung. Dazu gehören z.B. DNS-Namen, IP-Adressen, Sicherheitsrichtlinien, Systemkonfigurationen, Firewall-Regeln und Systeme von Drittanbietern (z. B. Router eines Anbieters, Webserver eines Hosts).

Vor Durchführung eines Resilienztests hat die Auftragnehmerin eine potenziell betroffene Dritte (z.B. Subunternehmerin) rechtzeitig über den geplanten Resilienztest zu informieren. Im Übrigen gilt Ziffer 10.

Bei ihren Penetrationstests orientieren sich die Finanzunternehmen an den Open Web Application Security Project („OWASP“) Testing Guides und prüfen unter anderem die OWASP Top 10 Schwachstellen, sind aber nicht darauf beschränkt. Insbesondere ist die Finanzunternehmen berechtigt, die dort dargestellten und aktuellen Tools, Techniken und Verfahren zum Nachweis von Schwachstellen zu verwenden, die dem Ausrüstungsniveau potenzieller Angreifer:innen entsprechen. Dieses Recht erstreckt sich auch auf die Anwendung von Verfahren des Reverse Engineering zur Überprüfung von Sicherheitsmaßnahmen.

Die Auftragnehmerin hat sicherzustellen, dass während der vereinbarten Prüfungszeit keine Wartungsarbeiten an den betroffenen IT-Systemen durchgeführt werden. Die Auftragnehmerin hat die Auftraggeberin und das ausführende Finanzunternehmen unverzüglich zu benachrichtigen, wenn während des Resilienztests ein Systemausfall oder ein sonstiger Notfall eintritt, z. B. eine schwere Systemstörung.

4. Sorgfalt; Daten anderer Kunden

Bei den Resilienztests, insbesondere den Penetrationstests, wendet das Finanzunternehmen die übliche Sorgfalt an, um Schäden an den Systemen und Daten der Auftragnehmerin oder anderer Kundinnen der Auftragnehmerin, insbesondere der Auftraggeberin, zu vermeiden. Die Bank wird die Daten anderer Kundinnen der Auftragnehmerin, die mit Hilfe der geprüften Systeme Leistungen erhalten, nicht verändern, zerstören oder anderweitig beeinträchtigen. Gezielte DoS-Angriffe, die den gesamten Systembetrieb lahmlegen können, werden nicht durchgeführt.

5. Vertraulichkeit

Das ausführende Finanzunternehmen und die Auftraggeberin werden alle Informationen, die ihnen im Rahmen einer Prüfung offengelegt wurden, geheim halten und vor dem Zugriff Dritter schützen. Dazu gehören Daten anderer Kundinnen, die während der Resilienztests unbeabsichtigt angezeigt werden.

Das ausführende Finanzunternehmen und die Auftraggeberin wird die auf ihren Systemen gespeicherten Daten anderer Kundinnen unverzüglich löschen, spätestens jedoch, wenn der Testbericht gemäß Ziffer 7 dieses Anhangs an die Auftragnehmerin übermittelt wurde oder die Auftragnehmerin die Löschung verlangt.

Die Bank ist berechtigt, von ihr selbst oder von der Auftragnehmerin erstellte Testberichte und Maßnahmenpläne, sowie damit zusammenhängende Informationen, an zuständige Behörden weiterzugeben. Die Auftraggeberin ist berechtigt, von ihr selbst oder von der Auftragnehmerin erstellte Testberichte und Maßnahmenpläne, sowie damit zusammenhängende Informationen, an betroffene Finanzunternehmen weiterzugeben.

6. Ansprechpartner

Die Parteien und das ausführende Finanzunternehmen benennen Ansprechpartner:innen für die gesamte Kommunikation im Zusammenhang mit der Durchführung dieses Anhangs, die insbesondere während der Durchführung der Resilienztests erreicht werden und wichtige Entscheidungen für die Parteien treffen können.

Die Auftragnehmerin identifiziert auch Kontakte Dritter, insbesondere mit den entsprechenden Subunternehmerinnen. Jede Änderung der Kontaktpersonen ist unverzüglich der anderen Partei bzw. dem ausführenden Finanzunternehmen zu melden.

7. Testbericht und Maßnahmenplan

Die Auftragnehmerin erhält einen vertraulichen Bericht, in dem die beim Resilienztest festgestellten Schwachstellen oder Sicherheitsmängel beschrieben werden. Die Auftragnehmerin darf den Testbericht nur an beteiligte Dritte (die Auftraggeberin, Subunternehmerinnen oder Dritte, die zur Behebung von Sicherheitsmängeln eingebunden werden) und zuständige Behörden weitergeben. Die Auftragnehmerin erstellt innerhalb von 30 Kalendertagen nach Versand des Testberichts an den Auftragnehmer einen einvernehmlich abgestimmten Maßnahmenplan zur Behebung der Schwachstellen und

Sicherheitsmängel, der die Kritikalität der festgestellten Sicherheitsmängel und deren Fristen zur Behebung angemessen berücksichtigt.

Soweit erforderlich, arbeiten die Parteien und das durchführende Finanzunternehmen zusammen, um Sicherheitsmängel zu beheben. Die Auftragnehmerin berichtet regelmäßig und der Kritikalität angemessen, mindestens jedoch wöchentlich bei im Testbericht als kritisch eingestuften Sicherheitsmängeln, über den Fortschritt der Behebung.

Die Auftragnehmerin hat die im Testbericht festgestellten Schwachstellen und Sicherheitsmängel innerhalb der abgestimmten Fristen auf ihre Kosten zu beheben.

8. Kündigung

Stellt ein Finanzunternehmen im Falle eines Resilienztests fest, dass die Sicherheit der Systeme der Auftragnehmerin erheblich von den technischen Sicherheitsstandards abweicht und 30 Kalendertage nach Versand des Testberichts an die Auftragnehmerin kein einvernehmlich abgestimmter Maßnahmenplan vorliegt oder die dort festgelegten Fristen mehr als 15 Kalendertage überschritten sind, so hat die Auftraggeberin zusätzlich zu sonstigen vereinbarten Kündigungsrechten das Recht, den Vertrag außerordentlich zu kündigen. Diese Kündigung kann innerhalb von sechs Monaten nach Vorliegen des Kündigungsgrundes erfolgen und wird an dem in der Kündigungsbekanntmachung genannten Tag wirksam.

9. Haftung

1) Die Auftraggeberin haftet für Vorsatz und grobe Fahrlässigkeit im Rahmen dieser Zusatzvereinbarung. Bei leichter Fahrlässigkeit ist die Haftung auf die Höhe der Vergütung beschränkt, die die Auftraggeberin der Auftragnehmerin für die Dauer von einem Jahr nach dem Vertrag zahlt.
2) Bei Feststellung des entstandenen Schadens bleiben mittelbare Schäden und Folgeschäden außer Betracht. Dies sind insbesondere, aber nicht abschließend, Schadensersatzforderungen wegen entgangenen Gewinns, Betriebsunterbrechungen, personeller Mehraufwand und vergebliche Aufwendungen beim Auftragnehmer, Nutzungsausfall und Umsatzeinbußen. Der Haftungsausschluss für mittelbare Schäden und Folgeschäden gilt nicht bei Vorsatz, grober Fahrlässigkeit oder bei der Verletzung des Lebens, des Körpers oder der Gesundheit.
3) Eine Haftung nach diesem Anhang besteht nicht, soweit der Schaden dadurch entsteht, dass die Auftragnehmerin vertragliche Verpflichtungen nicht erfüllt hat und der Schaden aus dieser Pflichtverletzung resultiert.
4) Um Schäden zu vermeiden, ist die Auftragnehmerin verpflichtet, in angemessenen Zeitabständen Sicherungen der gefährdeten und relevanten Systeme anzufertigen, so dass im Bedarfsfall die Wiederherstellbarkeit der Daten sichergestellt ist.

10. Einsatz von Subunternehmerinnen

Im Falle des Einsatzes von Subunternehmerinnen hat die Auftragnehmerin insbesondere dafür Sorge zu tragen, dass die Finanzunternehmen, die Kundinnen der Auftraggeberin sind, und für die IKT-Dienstleistungen erbracht werden, die kritische oder wichtige Funktionen unterstützen, das durch diesen Anhang erworbene Recht zur Durchführung von Resilienztests gegenüber den Subunternehmerinnen frei und rechtmäßig ausüben können.

11. Threat-Led Penetration Tests gemäß Artikel 26 DORA-Verordnung

Erbringt die Auftragnehmerin IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen für die Auftraggeberin bzw. Finanzunternehmen, die deren Kunden sind, so ist sie verpflichtet, sich an Threat-Led Penetration Tests („TLPT“) der Auftraggeberin bzw. deren Kundinnen gemäß Artikeln 26 und 27 DORA-Verordnung zu beteiligen und uneingeschränkt daran mitzuwirken. Die Vereinbarungen nach diesem Anhang gelten auch für die Durchführung eines TLPT gemäß Artikel 26 DORA-Verordnung. Insbesondere sind die Auftraggeberin bzw. deren Kundinnen berechtigt, alle Taktiken, Techniken und Prozeduren der für den Test ausgewählten Angreifenden in Bezug auf die Anwendungen, Systeme und für die Kundinnen tätigen Mitarbeiter:innen der Auftragnehmerin zu simulieren. Stehen die Anwendungen und Systeme der Auftragnehmerin im Fokus der TLPT und sind nicht nur beiläufig von den TLPT betroffen, wird das die TLPT durchführende Finanzunternehmen die Auftragnehmerin am übergreifenden Risiko-Management für den TLPT auf die betroffenen IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen der Auftragnehmerin angemessen beteiligen.

Die Auftragnehmerin beteiligt sich nach Aufforderung durch die Auftraggeberin oder deren Kundinnen an der Bewertung der Testergebnisse im von der DORA-Verordnung und dem zugehörigen Regulatory Technical Standard („RTS“) vorgegebenen Zeitrahmen. Ebenso sichert sie die Behebung auf eigene Kosten von Schwachstellen gemäß Ziffer 7 zu.

12. Pooled Tests gemäß Artikel 26 DORA-Verordnung

Erbringt die Auftragnehmerin IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen für die Auftraggeberin oder ein Finanzunternehmen, das ein Kunde der Auftraggeberin ist, und ist vernünftigerweise davon auszugehen, dass sich die Einbindung der Auftragnehmerin in einen TLPT gemäß Ziffer 11 nachteilig auf die Qualität oder die Sicherheit von Dienstleistungen der Auftragnehmerin an Kundinnen, bei denen es sich um nicht in den Anwendungsbereich der DORA-Verordnung fallende Unternehmen handelt, oder auf die Vertraulichkeit in Bezug auf die mit diesen Dienstleistungen verbundenen Daten auswirkt, kann das Finanzunternehmen von der Auftragnehmerin unbeschadet Artikel 26 Absatz 2 Unterabsätze 1 und 2 der DORA-Verordnung schriftlich verlangen, dass die Auftragnehmerin unmittelbar vertragliche Vereinbarungen mit einem externen Tester schließt, um unter der Leitung eines benannten Finanzunternehmens einen gebündelten

TLPT durchzuführen, an dem mehrere Finanzunternehmen beteiligt sind („gebündelter Test“ / „Pooled Test“), für die die Auftragnehmerin oder die Auftraggeberin IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen erbringt.

Diese Pooled Tests erstrecken sich auf das relevante Spektrum von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von den Finanzunternehmen per Vertrag an die jeweiligen IKT-Drittdienstleisterinnen vergeben wurden. Die Pooled Tests gelten als TLPT, die von den an den Pooled Tests beteiligten Finanzunternehmen durchgeführt werden.

Die Zahl der Finanzunternehmen, die sich an den Pooled Tests beteiligen, wird unter Berücksichtigung der Komplexität und der Art der betreffenden Dienstleistungen angemessen austariert.

Führt die Auftragnehmerin sogenannte Pooled Tests gemäß DORA-Verordnung durch, prüfen die durchführenden Finanzunternehmen, die Kunden der Auftraggeberin sind, die Teilnahme und Ergebnisse. Soweit diese geeignet sind, um eigene Prüfungen zu ersetzen, können diese Finanzunternehmen auf die Ausübung ihrer Rechte gemäß Ziffer 11 verzichten.

13. Unterschriften

Auftraggeberin

_____ _____

_____

Auftragnehmerin

_____ _____

_____