ALVARA
Teil von YUVENDA

ALVARA Ergänzungsvereinbarung DORA
Anlage ITK Sicherheitsanforderungen

Präambel

Der Auftraggeber bezieht vom Auftragnehmer IKT-Dienstleistungen im Sinne des Art. 3 Nr. 21 DORA

Hinsichtlich der Begriffe und Systematik dieser Anlage gilt die zwischen den Parteien zu vereinbarende oder bereits vereinbarte " ALVARA Ergänzungsvereinbarung DORA“ (im Folgenden: Ergänzungsvereinbarung).

Die vorausgeschickt werden folgende Sicherheitsanforderungen bestimmt:

Nr.	Gilt für	Anforderung	DORA-Referenz	Umsetzung durch den Auftragnehmer
1	ICC HKSW Pecunia/webAmis (on premise) webAmis (ASP)	Alle internen/externen Mitarbeitenden des Dienstleisters sind angemessen geschult und sensibilisiert, um - ihrer Rolle zur Aufrechterhaltung der Informationssicherheit gerecht zu werden oder - eine Anomalie oder einen IKT-Vorfall erkennen und melden zu können.	Art. 19 RTS 15_16	Jährliche Schulung der Mitarbeiter bezüglich Datenschutz und IT-Sicherheit
2	ICC HKSW Pecunia/webAmis (on premise) webAmis (ASP)	Angemessene Standards für die Informationssicherheit werden nachweislich eingehalten. Der IKT-Drittdienstleister muss in der Lage sein, einschlägige technologische Entwicklungen zu überwachen und führende IKT-Sicherheitspraktiken zu ermitteln und gegebenenfalls umzusetzen, um über einen wirksamen und soliden Rahmen für die digitale betriebliche Widerstandsfähigkeit zu verfügen. Grundsätzlich sollten aber der ISO 27001 Standard oder der BSI-Standard eingehalten werden, wobei der Betrachtungsgegenstand der Standards die vereinbarte Dienstleistung umfassen muss. Die Maßnahmen zur Umsetzung o.g. 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 Auftraggeber in Textform mitzuteilen.	Art. 28.5 DORA	ISO27001 des Rechenzentrums Richtlinien und Maßnahmen: - IT-Sicherheitsleitlinie - IT-Sicherheitskonzept - IT-Richtlinie - Programmierrichtlinie - Jährliche Schulung der Mitarbeiter bezüglich Datenschutz und IT-Sicherheit
3	ICC webAmis (ASP)	Ein übergreifendes Programm für das Testen der digitalen operationalen Resilienz von IKT-Systemen und -Anwendungen, die für die Erbringung der IKT-Dienstleistung eingesetzt werden, wird eingesetzt. Für identifizierte Schwachstellen werden Aktionspläne erstellt und deren Umsetzung verfolgt.	Art. 24.1, Art. 25.1 DORA	Verfahren für Schwachstellentest

K V 146 130325

Nr.	Gilt für	Anforderung	DORA-Referenz	Umsetzung durch den Auftragnehmer
4	ICC HKSW Pecunia/webAmis (on premise) webAmis (ASP)	Ein Prozess für die Behandlung IKT-bezogener Vorfälle ist implementiert. IKT- bezogene Vorfälle und Cyberbedrohungen werden unverzüglich dem Finanzunternehmen gemeldet. Mündliche Unterrichtungen sind in Textform nachzureichen. Insbesondere sind Ausfälle von IKT-Dienstleistungen, die länger als 24 Stunden andauern, zu melden. Der Auftragnehmer stimmt sich zur Behandlung solcher Verletzungen mit dem Auftraggeber ab. Die Parteien treffen die erforderlichen Maßnahmen, einschließlich der Maßnahmen zur Minderung möglicher nachteiliger Folgen. Ein IKT-bezogener Vorfall (oder kurz IKT-Vorfall) ist ein von dem Institut oder Unternehmen nicht geplantes Ereignis (bzw. eine Reihe verbundener Ereignisse), das die Sicherheit der Netzwerk- und Informationssysteme beeinträchtigt und nachteilige Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder auf die vom Finanzunternehmen erbrachten Dienstleistungen hat (Art. 3 Absatz 1 Nr. 8 DORA). Cyberbedrohung bezeichnet einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte.	Art. 17 DORA, Art. 11.1.a RTS 18.3	Eskalationsprozess Die Meldung durch den Auftragnehmer wird ausschließlich per E-Mail erfolgen. Der Auftraggeber wird dem Auftragnehmer per Kontaktformular des Auftragsnehmers entsprechende Ansprechpartner und deren E-Mailadresse melden.
5	ICC webAmis (ASP)	Die IKT-Vermögenswerte werden angemessen verwaltet (Dokumentation der Werte und Abhängigkeiten, mindestens ein Lebenszyklusmanagement). Angemessen bedeutet, dass mindestens ein Inventar existiert, in dem unter anderem auch Altsysteme (Hard- und Software) und deren Betriebsrisiken ersichtlich sind.	Art. 5 RTS 15_16	Backup-Strategie und Scourcecode-Management
6	ICC webAmis (ASP)	Im Rahmen der verschlüsselten Datenverarbeitung werden die jeweils aktuellen BSI-Empfehlungen (BSI TR-02102 Kryptographische Verfahren) eingehalten.	Art. 6.2 RTS 15_16	ICC Sicherheitskonzept
7	HKSW Pecunia/webAmis (on premise)	Kryptographische Verfahren und Schlüssel müssen angemessen verwaltet werden. Hierzu werden risiko und bedrohungsorientiert die jeweils aktuellen BSI Empfehlungen (BSI TR-02102 Kryptographische Verfahren) oder alternativ andere best practices wie NIST SP 800-57 Part 1, NIST 800-175b, ISO 18033, ISO 19772 ausgewählt und eingehalten.	Art. 6.2 RTS 15_16	liegt in der Verantwortung des Kunden, da Betrieb beim Kunden
8	ICC HKSW Pecunia/webAmis (on premise) webAmis (ASP)	Richtlinien zum IKT-Betrieb sind umgesetzt, die mindestens folgendes umfassen: - sichere Installation, Konfiguration, Härtung und Deinstallation von IKT- Systemen - Datenmanagement - Identifizierung und Kontrolle von IKT-Altsystemen - Sicherung und Wiederherstellung (in diesem Zusammenhang sind Anforderungen an zeitliche Abläufe und Interpedenzen zwischen den IKT-Systemen zu berücksichtigen) - Trennung der IKT-Produktionsumgebungen von Entwicklungs-, Test- und anderen Nicht-Produktionsumgebungen - Schutz vor Schadsoftware - Monitoring - Wartung Zur Umsetzung sind Prozesse und Verfahren festgelegt, dokumentiert, und werden regelmäßig gepflegt.	Art. 8.2 RTS 15_16	Aufstellung der Dokumente ist in Arbeit

Nr.	Gilt für	Anforderung	DORA-Referenz	Umsetzung durch den Auftragnehmer
9	ICC HKSW Pecunia/webAmis (on premise) webAmis (ASP)	Verfahren oder Prozesse für ein Schwachstellen- und Patchmanagement sind festgelegt, dokumentiert, umgesetzt und werden regelmäßig gepflegt.	Art. 10.2 RTS 15_16	Software life cycle Arbeitsanweisung Changemanagement Reviewprozess für ein Schwachstellen- und Patchmanagement
10	ICC webAmis (ASP)	Automatische Schwachstellen-Scans werden mindestens monatlich durchgeführt. Für Systeme, die öffentlich zugänglich sind, erfolgen wöchentliche Scans. Die Auswertung der Schwachstellenscans erfolgt, sofern möglich, nach der CVSS-Einstufung. Schwachstellen sind durch die Verantwortlichen zeitnah hinsichtlich ihrer Relevanz, ihrer potenziellen Auswirkungen und ihrer Kritikalität zu bewerten, zu kategorisieren und das Ergebnis ist zu dokumentieren. Zur Behebung der Schwachstellen sind unter Berücksichtigung der damit verbundenen Risiken entsprechende Maßnahmen abzuleiten, zu priorisieren, umzusetzen und nachvollziehbar zu dokumentieren. Die Umsetzung dieser Maßnahmen ist zu überwachen und zu überprüfen. Dem FE werden zumindest die kritischen Schwachstellen sowie Statistiken und Trends gemeldet.	Art. 10.2 RTS 15_16	Verfahren für Schwachstellentest Der Auftragnehmer wird den Auftraggeber bei der Feststellung von kritischen Schwachstellen per E-Mail informieren. Der Auftraggeber wird dem Auftragnehmer per Kontaktformular des Auftragsnehmers entsprechende Ansprechpartner und deren E-Mailadresse melden.
11	ICC HKSW Pecunia/webAmis (on premise) webAmis (ASP)	Verfahren oder Prozesse zur Zugangs- und Zugriffskontrolle, zur Festlegung einer sicheren Konfigurationsbasis und von Sicherheitsmaßnahmen (gegen bösartigen Code), zum ausschließlichen Einsatz zugelassener Software, Datenträger, Systeme und Endgeräte, zur sicheren Nutzung tragbarer Endgeräte sowie zur Telearbeit sind festgelegt, dokumentiert, umgesetzt und werden regelmäßig gepflegt. Dabei sind führende Praktiken und geeignete Techniken zu berücksichtigen.	Art. 11.2 RTS 15_16	ISO27001 des Rechenzentrums Richtlinien und Maßnahmen: - IT-Sicherheitsleitlinie - IT-Sicherheitskonzept - IT-Richtlinie - Programmierrichtlinie
12	ICC HKSW Pecunia/webAmis (on premise) webAmis (ASP)	Verfahren oder Prozesse zur Datensicherung und Wiederherstellung sind festgelegt, dokumentiert, umgesetzt und werden regelmäßig gepflegt. Ein Datensicherungs- und Wiederherstellungskonzept muss Umfang und Vollständigkeit, Häufigkeit, Zeitpunkt, Anzahl der Generationen, Sicherungsarten, Zugriffsberechtigungen, Kontrollen zur Funktionsfähigkeit, Aufbewahrungsdauer regeln. Die Systeme zur Datensicherung müssen physisch und logisch vom Quellsystem getrennt sein und vor unbefugtem Zugriff und Manipulationen geschützt sein.	Art. 12 DORA	ISO27001 des Rechenzentrums Backup-Strategie und Datensicherungskonzept
13	ICC HKSW Pecunia/webAmis (on premise) webAmis (ASP)	Verfahren oder Prozesse zur Sicheren Datenentsorgung und -Löschung sind festgelegt, dokumentiert, umgesetzt und werden regelmäßig gepflegt.	Art. 11.2.g RTS 15_16	IT-Sicherheitskonzept bei HKSW und Pecunia/webAmis(on premise) ist der Kunden verantwortlich, da Betrieb beim Kunden
14	ICC HKSW Pecunia/webAmis (on premise) webAmis (ASP)	Verfahren oder Prozesse zur Verhinderung von Datenverlusten und -lecks sind festgelegt, dokumentiert, umgesetzt und werden regelmäßig gepflegt.	Art. 11.2.i RTS 15_16	ISO27001 des Rechenzentrums Backup-Strategie und Datensicherungskonzept

Nr.	Gilt für	Anforderung	DORA-Referenz	Umsetzung durch den Auftragnehmer
15	ICC webAmis (ASP)	Verfahren oder Prozesse zur Protokollierung sind festgelegt, dokumentiert, umgesetzt und werden regelmäßig gepflegt. Verpflichtende Protokollierungsereignisse sind: Identitätsmanagement (logische/physische Zugangskontrolle), Kapazitätsmanagement, Veränderungsmanagement, IKT-Betrieb einschl. IKT- Systemaktivitäten, Netzverkehrsaktivitäten einschl. der Leistung.	Art. 12 RTS 15_16	ISO27001 des Rechenzentrums Dienstleistungsvertrag mit Rechenzentrum
16	ICC webAmis (ASP)	Verfahren oder Prozesse zum sicheren Management von Netzwerken und Firewalls sind festgelegt, dokumentiert, umgesetzt und werden regelmäßig gepflegt. Die Netzarchitektur ist konzipiert und orientiert sich an führenden Praktiken: - Systeme/Netze sind angemessen segmentiert und getrennt, - alle Netzwerkverbindungen sind dokumentiert, - die Verwaltung von IKT-Assets erfolgt aus einem gesonderten und speziellen Netz, - Netzzugangskontrollen sind implementiert, - Netzverbindungen sind abhängig von der Datenklassifizierung verschlüsselt, - der Netzverkehr zwischen dem internen Netz und dem Internet und möglichen weiteren externen Verbindungen ist gesichert.	Art. 13.1 RTS 15_16	ISO27001 des Rechenzentrums
17	ICC webAmis (ASP)	Netzarchitektur und Netzsicherheitskonzept sowie Firewall-Regeln werden mind. einmal jährlich auf Aktualität und Angemessenheit überprüft	Art. 13.1 RTS 15_16	ISO27001 des Rechenzentrums
18	ICC webAmis (ASP)	Für die Beschaffung, Entwicklung, Änderung und Wartung (neuer) IKT- Systeme sind Verfahren oder Prozesse für Tests und Freigaben festgelegt, dokumentiert, umgesetzt und werden regelmäßig gepflegt.	Art. 16.2 RTS 15_16	ISO27001 des Rechenzentrums
19	ICC webAmis (ASP)	Quellcodeüberprüfungen und Sicherheitstests von Softwarepaketen erfolgen im angemessenen Umfang. Die Ergebnisse der einzelnen Sicherheitsprüfungen sind durch die Verantwortlichen zeitnah hinsichtlich ihrer Relevanz, ihrer potenziellen Auswirkungen und ihrer Kritikalität zu bewerten, zu kategorisieren und das Ergebnis ist zu dokumentieren. Zur Behebung der Schwachstellen sind unter Berücksichtigung der damit verbundenen Risiken entsprechende Maßnahmen abzuleiten, zu priorisieren, umzusetzen und nachvollziehbar zu dokumentieren. Die Umsetzung dieser Maßnahmen ist zu überwachen und zu überprüfen.	Art. 16.2 RTS 15_16	Programmierrichtlinie
20	ICC webAmis (ASP)	Verfahren oder Prozesse für ein Changemanagement sind festgelegt, dokumentiert, umgesetzt und werden regelmäßig gepflegt, bei dem Sicherheitsanforderungen, z.B. hinsichtlich Rollen und Zuständigkeiten, Dokumentation, Rollback, Tests, Planung, Genehmigung, Bewertung Auswirkungen und Risiken Bestandteil sind.	Art. 17.2 RTS 15_16	Arbeitsanweisung Changemanagement
21	ICC webAmis (ASP)	Räumlichkeiten, Rechenzentren und sensible Bereiche mit IKT- Vermögenswerten und Informationswerten sind vor unbefugtem Zugang, Angriffen, Unfällen und vor Umweltbedrohungen und -gefahren zu schützen. Ein Konzept für die physische und umgebungsbezogene Sicherheit, in dem standortabhängige Gefährdungen, Sicherheitszonen innerhalb der Gebäude, Zugangsschutz sowie die Einspeisung von Versorgungsleitungen und Konzepte zur Überbrückung kurzzeitiger (USV) und länger andauernder (NEA) Stromausfälle berücksichtigt werden, ist festzulegen, zu dokumentieren und regelmäßig zu pflegen.	Art. 18.2.b RTS 15_16	ISO27001 des Rechenzentrums IT-Sicherheitskonzept inkl. Anhang

Nr.	Gilt für	Anforderung	DORA-Referenz	Umsetzung durch den Auftragnehmer
22	ICC HKSW Pecunia/webAmis (on premise) webAmis (ASP)	Unter Berücksichtigung des Schutzbedarfs/der Sensitivität der verarbeiteten Informationen sowie dem Need-to-Know- und Least Privilege-Prinzip ist ein Rollen- und Berechtigungskonzept zu erstellen, mit den relevanten Stakeholdern abzustimmen, zu dokumentieren und regelmäßig zu pflegen. Sowohl für die Einrichtung von Benutzerkonten als auch für die Vergabe, die Änderung oder den Entzug von Zugangs- und Zugriffsrechten sind formale Verfahren oder Prozesse festzulegen, zu dokumentieren und zu pflegen. Hierbei ist eine Rollentrennung zwischen den beantragenden, genehmigenden und umsetzenden Personen sicherzustellen. Alle Benutzerkonten sind zu personalisieren und Personen eindeutig zuordenbar zu machen. Für administrative Aufgaben sind gesonderte, personalisierte Benutzerkonten einzusetzen.	Art. 20.2, 21.1 RTS 15_16	Onboarding-Prozess
23	ICC HKSW Pecunia/webAmis (on premise) webAmis (ASP)	Verfahren oder Prozesse, mit denen die Zugangs- und Zugriffsrechte in Verantwortung des IKT-Dienstleisters mind. jährlich überprüft werden, sind festgelegt, dokumentiert, umgesetzt und werden regelmäßig gepflegt.	Art. 21.1 RTS 15_16	Onboarding-Prozess
24	ICC webAmis (ASP)	Für den Fernzugang und privilegierte Zugänge zu IKT-Systemen und Systemen, die diese unterstützen sowie für ITK-Systeme, die öffentlich zugänglich sind, ist eine starke Authentisierung umgesetzt.	Art. 21.1 RTS 15_16	IT-Richtlinie Anhang Allgemein
25	ICC webAmis (ASP)	Verfahren oder Prozesse für die Erkennung anomaler Aktivitäten sind festzulegen, zu dokumentieren und regelmäßig zu pflegen. Hierfür sind geeignete Tools (z.B. SIEM-System) einzusetzen. Die Verfahren und Prozesse sind regelmäßig zu testen. Die aus den Use Cases resultierenden sicherheitsrelevanten Ereignisse sind automatisiert zu melden und durch die Verantwortlichen zeitnah hinsichtlich ihrer Relevanz und potenziellen Auswirkungen zu analysieren, zu bewerten, zu kategorisieren und zu priorisieren. Zur Behandlung sicherheitsrelevanter Ereignisse und zur Einleitung von Reaktionsprozessen bei IKT-bezogenen Vorfällen sind unter Berücksichtigung der damit verbundenen Risiken entsprechende Maßnahmen abzuleiten, umzusetzen und nachvollziehbar zu dokumentieren. Alle Schritte und Ergebnisse sind nachvollziehbar zu dokumentieren.	Art. 10.1 DORA	Dienstleistungsvertrag mit Rechenzentrum
26	ICC webAmis (ASP)	Verfahren oder Prozesse zur IKT-Geschäftsfortführung sind festgelegt, dokumentiert, umgesetzt und werden regelmäßig gepflegt. Kontinuitätspläne und Reaktions- und Wiederherstellungspläne für IKT- Dienstleistungen sind festgelegt und werden risikobasiert regelmäßig getestet.	Art. 25.1, 25.2, 26.1 RTS 15_16	ISO27001 des Rechenzentrums Backup-Strategie und Datensicherungskonzept