Security Requirements for Suppliers (SRS) / Sicherheitanforderungen für Lieferanten

of / der

Raiffeisen Informatik GmbH & Co KG
Hollandstraße 11+13, 1020 Wien, Österreich

(subsequently called “CUSTOMER” or “R-IT” / nachfolgend „KUNDE“ oder “R-IT” genannt)

As of June, 15th 2026 / Stand 15. Juni 2026

Delivering trusted services is an integral part of our corporate strategy. Using innovative services and products as well as cooperating with professional partners and suppliers, meeting our security requirements is necessary to stay ahead in a fast-changing industry.

Die Erbringung vertrauenswürdiger Dienstleistungen ist ein integraler Bestandteil unserer Unternehmensstrategie. Der Einsatz innovativer Dienstleistungen und Produkte sowie die Zusammenarbeit mit professionellen und unsere Sicherheitsanforderungen erfüllenden Partnern und Lieferanten ist dabei notwendig, um in einer sich schnell verändernden Branche erfolgreich zu sein.

It is our due diligence to protect our as well as our client’s data, systems and applications with security measures according to leading industry standards as it is expected from an IT-provider, serving international financial institution.

Es gehört zu unserer Sorgfaltspflicht, sowohl unsere als auch die Daten, Systeme und Anwendungen unserer Kunden mit Sicherheitsmaßnahmen nach führenden Industriestandards zu schützen, wie es von einem IT-Provider internationaler Finanzinstitute erwarten wird.

Managing supplier relationships in regard to security is an important part of internal risk management framework, a common praxis (e.g. ISO 27000 series, NIST Cybersecurity Framework) and mandatory for financial institutions (e.g. Digital Operations Act (DORA), § 25 and the Annex to § 25 of the Austrian Banking Act, etc.), together further referred to as the "Security Requirements".

Das Management von Lieferantenbeziehungen in Bezug auf die Sicherheit ist ein wichtiger Teil des internen Risikomanagements, eine gängige Praxis (zB. ISO 27000-Serie, NIST Cybersecurity Framework) und für Finanzinstitute verpflichtend (zB. Verordnung über die digitale operationale Resilienz im Finanzsektor (DORA), § 25 und der Anhang zu § 25 des österreichischen Bankwesengesetzes usw.), die im Folgenden als "Sicherheitsanforderungen" bezeichnet werden.

The Security Requirements are derived from established industry standards and based on best practices, which can be expected from a service provider in the financial sector.

Die Sicherheitsanforderungen leiten sich von etablierten Branchenstandards ab und basieren auf Best Practices, die von einem Dienstleister im Finanzsektor erwartet werden können.

Having regard to the above, the Vendor, Processor or Partner (collectively referred to as “SUPPLIER”) hereby represents and warrants that it has completed all necessary due diligence, is familiar with relevant Security Provisions, and complies with them as commissioned and agreed, in particular when: (a) accessing CUSTOMER facilities, networks or information systems; (b) accessing, processing or storing CUSTOMER information/data; (c) providing infrastructure services or standard software; (d) developing software; (e) using Generative Artificial Intelligence (GenAI)-powered components; and/or (f) providing data or ICT hardware or components. Furthermore, the SUPPLIER undertakes to notify the CUSTOMER at least 30 days in advance before

In Anbetracht des oben Genannten versichert und gewährleistet der Anbieter, Auftragsverarbeiter oder Partner (gemeinsam als „LIEFERANT" bezeichnet), dass er alle erforderlichen Sorgfaltsprüfungen abgeschlossen hat, mit den relevanten Sicherheitsbestimmungen vertraut ist und diese auftragsgemäß und vereinbarungsgemäß einhält, insbesondere wenn: (a) auf Einrichtungen, Netzwerke oder Informationssysteme des KUNDEN zugegriffen wird; (b) Informationen/Daten des KUNDEN abgerufen, verarbeitet oder gespeichert werden; (c) Infrastrukturdienstleistungen oder Standardsoftware bereitgestellt werden; (d) Software entwickelt wird; (e) Komponenten auf Basis generativer künstlicher Intelligenz (GenAI) eingesetzt werden; und/oder (f)

implementing functionalities and/or services with artificial intelligence (“AI”). Such notification shall include a meaningful description of the nature and scope of usage of the envisaged AI functionalities and/or services and shall include a confirmation such implementation will be in line with all applicable laws and regulations, especially with respect to all requirements in accordance with Regulation 2024/1689 of the Eur. Parl. & Council of June 13, 2024 (Artificial Intelligence Act)”.	Daten oder IKT-Hardware oder -Komponenten bereitgestellt werden. Darüber hinaus verpflichtet sich der LIEFERANT, den KUNDEN mindestens 30 Tage im Voraus zu benachrichtigen, bevor er Funktionalitäten und/oder Dienste mit künstlicher Intelligenz („KI") implementiert. Diese Benachrichtigung hat eine aussagekräftige Beschreibung der Art und des Umfangs der Nutzung der vorgesehenen KI-Funktionalitäten und/oder -Dienste zu enthalten sowie eine Bestätigung, dass eine solche Implementierung im Einklang mit allen anwendbaren Gesetzen und Vorschriften steht, insbesondere mit sämtlichen Anforderungen gemäß der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 (Verordnung über künstliche Intelligenz, „KI-Verordnung").
Whenever the term "CUSTOMER" is used in these SRS or any other requirements, it shall refer not only to the respective data (or systems, services, etc.) of R-IT, but also to those of its customers.	Wann immer in diesen SRS oder anderen Anforderungen der Begriff „KUNDE" verwendet wird, bezeichnet dieser nicht nur die jeweiligen Daten (oder Systeme, Dienste usw.) von R-IT, sondern auch die seiner Kunden.
Further security and ICT requirements may be specified in individual agreements (including but not limited to SLA, statement of work).	Weitere Sicherheits- und IKT-Anforderungen können in Einzelvereinbarungen (einschließlich, aber nicht beschränkt auf SLAs, Statements of Work) festgelegt werden.
For the purposes of these Provisions, “ICT Services” shall mean services provided or made available by the SUPPLIER to the CUSTOMER under any agreement. For the provision of the ICT services, the SUPPLIER shall implement appropriate information security, physical and environment-specific security measures at all locations within its control or sphere of influence, based on recognized industry standards and best practices, to ensure the availability, authenticity, integrity, and confidentiality of CUSTOMER data, information assets, and CUSTOMER ICT assets and devices.	Für die Zwecke dieser Bestimmungen bezeichnet „IKT-Dienste" Dienste, die vom LIEFERANTEN dem KUNDEN im Rahmen einer Vereinbarung bereitgestellt oder zur Verfügung gestellt werden. Für die Erbringung der IKT-Dienste hat der LIEFERANT angemessene Maßnahmen zur Informationssicherheit sowie physische und umgebungsspezifische Sicherheitsmaßnahmen an allen Standorten innerhalb seines Einfluss- und Kontrollbereichs einzuführen, die auf anerkannten Branchenstandards und bewährten Verfahren basieren, um die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von KUNDENDATEN, Informationswerten sowie IKT-Assets und -Geräten des KUNDEN zu gewährleisten.
The measures require ICT solutions and processes related to the ICT Services that: (a) establishsecurity of the transfer of data / the means of data transfers; (b) minimize the risk of damage or loss of data, unauthorized access or modification and technical flaws that may hinder the CUSTOMER's business activities; (c) prevent the lack of availability, the impairment of authenticity and integrity, the breach of confidentiality and the loss of data; (d) minimize therisks arising from data management (including poor administration, processing-related risks and human error).	Die Maßnahmen erfordern IKT-Lösungen und -Prozesse im Zusammenhang mit den IKT-Diensten, die: (a) die Sicherheit der Datenübertragung bzw. der Datenübertragungsmittel gewährleisten; (b) das Risiko von Datenschäden oder -verlusten, unbefugtem Zugriff oder unbefugter Änderung sowie technischer Mängel, die die Geschäftstätigkeiten des KUNDEN beeinträchtigen könnten, minimieren; (c) den Mangel an Verfügbarkeit, die Beeinträchtigung der Authentizität und Integrität, die Verletzung der Vertraulichkeit sowie den Datenverlust verhindern; (d) die aus dem Datenmanagement resultierenden Risiken minimieren (einschließlich mangelhafter Verwaltung, verarbeitungsbezogener Risiken und menschlicher Fehler).

The German version is for information purpose only. The English version shall prevail.

Die deutsche Version dient nur zur Information. Die englische Fassung ist maßgebend.

Governance	**Governance**
The SUPPLIER shall: • Implement an information security management system that aligns with recognized industry standards. • Define and regularly review its information security policies and procedures. • Conduct ongoing risk management to identify and mitigate risks effectively. • Provide training and security awareness measures for employees and relevant contractors on practices and their responsibilities.	Der LIEFERANT hat: • Ein Informationssicherheits-managementsystem einzuführen, das anerkannten Branchenstandards entspricht. • Seine Informationssicherheitsrichtlinien und -verfahren zu definieren und regelmäßig zu überprüfen. • Ein kontinuierliches Risikomanagement durchzuführen, um Risiken effektiv zu identifizieren und zu mindern. • Schulungs- und Sicherheitsbewusst-seinsmaßnahmen für Mitarbeiter und relevante Auftragnehmer zu deren Praktiken und Verantwortlichkeiten bereitzustellen.
Testing and Assessments	**Tests und Bewertungen**
The SUPPLIER shall: • Regularly evaluate and test the effectiveness of implemented measures and identify areas for improvement. • Conduct vulnerability assessments and penetration testing to identify and address weaknesses. • Remediate identified weaknesses and vulnerabilities according to their criticality. • Review subcontractors' and service providers' practices to ensure compliance with established security standards.	Der LIEFERANT hat: • Die Wirksamkeit der implementierten Maßnahmen regelmäßig zu bewerten und zu testen sowie Verbesserungspotenziale zu identifizieren. • Schwachstellenbewertungen und Penetrationstests durchzuführen, um Schwachstellen zu identifizieren und zu beheben. • Identifizierte Schwachstellen und Sicherheitslücken entsprechend ihrer Kritikalität zu beheben. • Die Praktiken von Unterauftragnehmern und Dienstleistern zu überprüfen, um die Einhaltung der festgelegten Sicherheitsstandards sicherzustellen.

Technical Measures	Technische Maßnahmen
The SUPPLIER shall: • Implement processes for effective management of human and non-human user accounts/identities. • Review access rights on a regular basis based on the principles of "need-to-know" and least privilege. • Enforce strong password policies and apply strong authentication methods for privileged accounts and accounts with access to CUSTOMER data. • Encrypt data in transit and at rest to ensure protection against unauthorized access. • Implement measures to protect the integrity and authenticity of data throughout its lifecycle. • Implement measures to avoid data loss and leakage. • Follow secure software development principles throughout the development lifecycle. • Process CUSTOMER data only in designated production environments, ensure separation from non-production environments. • Configure ICT assets according to recognized security best practices (system hardening). • Implement protection zones with appropriate physical security measures and access controls. • Restrict physical access to IT systems to authorized personnel only. • Use secure data center facilities which comply with relevant industry standards.	Der LIEFERANT hat: • Prozesse für ein effektives Management von menschlichen und nicht-menschlichen Benutzerkonten/Identitäten einzuführen. • Zugriffsrechte regelmäßig auf Basis der Prinzipien „Need-to-know" und der minimalen Rechtevergabe zu überprüfen. • Starke Passwortrichtlinien durchzusetzen und starke Authentifizierungsmethoden für privilegierte Konten und Konten mit Zugriff auf Kundendaten anzuwenden. • Daten bei der Übertragung und im Ruhezustand zu verschlüsseln, um den Schutz vor unbefugtem Zugriff zu gewährleisten. • Maßnahmen zum Schutz der Integrität und Authentizität von Daten während ihres gesamten Lebenszyklus einzuführen. • Maßnahmen zur Vermeidung von Datenverlust und Datenlecks einzuführen. • Sichere Softwareentwicklungsprinzipien während des gesamten Entwicklungslebenszyklus zu befolgen. • Kundendaten ausschließlich in dafür vorgesehenen Produktionsumgebungen zu verarbeiten und die Trennung von Nicht-Produktionsumgebungen sicherzustellen. • IKT-Assets gemäß anerkannten Best Practices zur Sicherheit zu konfigurieren (System-Hardening). • Schutzzonen mit angemessenen physischen Sicherheitsmaßnahmen und Zugangskontrollen einzurichten. • Den physischen Zugang zu IT-Systemen ausschließlich auf autorisiertes Personal zu beschränken. • Sichere Rechenzentrumseinrichtungen zu nutzen, die relevanten Branchenstandards entsprechen.
Monitoring and Logging	**Überwachung und Protokollierung**
The SUPPLIER shall: • Continuously monitor systems for anomalies and potential security threats. • Maintain and securely store audit logs and access records.	Der LIEFERANT hat: • Systeme kontinuierlich auf Anomalien und potenzielle Sicherheitsbedrohungen zu überwachen. • Prüfprotokolle und Zugriffsnachweise zu pflegen und sicher aufzubewahren.

Incident Response	Reaktion auf Sicherheitsvorfälle
The SUPPLIER shall: • Establish procedures for responding to ICT incidents, including steps for detection, analysis, resolution, documentation, and reporting. • Notify CUSTOMER without undue delay upon becoming aware of any incident related to the ICT services or CUSTOMER data, providing relevant information to assist the CUSTOMER in fulfilling its obligations.	Der LIEFERANT hat: • Verfahren zur Reaktion auf IKT-Vorfälle einzurichten, einschließlich Schritte zur Erkennung, Analyse, Behebung, Dokumentation und Berichterstattung. • Den KUNDEN unverzüglich zu benachrichtigen, sobald der LIEFERANT Kenntnis von einem Vorfall im Zusammenhang mit den IKT-Diensten oder KUNDENDATEN erlangt, und dabei relevante Informationen bereitzustellen, um den KUNDEN bei der Erfüllung seiner Verpflichtungen zu unterstützen.
Business Continuity and Recovery	**Geschäftskontinuität und Wiederherstellung**
The SUPPLIER shall: • Maintain appropriate Business Continuity Plans and Disaster Recovery Plans to mitigate the impact of unplanned disruptions. • Implement procedures to recover and restore the service and data provided to the CUSTOMER within agreed service level. • CUSTOMER data as well as relevant configuration of the CUSTOMER can be restored independently on request of the CUSTOMER. • Ensure the integrity and availability of backups at all times.	Der LIEFERANT hat: • Angemessene Geschäfts-kontinuitätspläne und Notfall-wiederherstellungspläne zu pflegen, um die Auswirkungen ungeplanter Unterbrechungen zu mindern. • Verfahren einzuführen, um den dem KUNDEN bereitgestellten Dienst und die Daten innerhalb des vereinbarten Serviceniveaus wiederherzustellen. • Sicherzustellen, dass Kundendaten sowie relevante Konfigurationen des KUNDEN auf Anfrage des KUNDEN unabhängig wiederhergestellt werden können. • Die Integrität und Verfügbarkeit von Sicherungskopien jederzeit zu gewährleisten.