Supplemental Agreement on Special Provisions Regarding ICT- and Outsourced-Services

entered into by and between

Raiffeisen Informatik Consulting GmbH

Lilienbrunngasse 7-9

1020 Vienna, Austria

(hereinafter “Customer”)

and

[\*\*\*INSERT FULL LEGAL NAME AND ADRESS OF ICT SERVICE/OUTSOURCED SERVICE PROVIDER]

(hereinafter “Service Provider”)

This Supplemental Agreement applies to all existing and future agreements entered into between the Parties and pursuant to the terms of which the Service Provider agrees to perform ICT-Services or Outsourced Services to the Customer and its Affiliates (each an “Agreement”). Any such Agreements shall in any event include the agreements referred to in Annex 3 hereof. However, the Parties can separately agree to opt-out certain Agreements from the applicability of this Supplemental Agreement.

Whenever the terms of an Agreement stand in contrast with the terms of this Supplemental Agreement, the terms of this Supplemental Agreement will take precedence and thus, will amend, supersede and replace any of such terms of such Agreement to the extent so being in contrast with the terms of this Supplemental Agreement.

1. **Terms and Definitions**

Unless defined otherwise hereinafter, capitalized terms used herein shall have the meaning as given to them below:

**Agreement(s)**:shall have the meaning as provided for such term in the first paragraph of this Supplemental Agreement;

**Clause**: a clause of this Supplemental Agreement;

**Critical or Important Service(s)**: shall have the meaning as provided for such term in Clause 5.2 of this Supplemental Agreement;

**Customer**: Raiffeisen Informatik Consulting GmbH;

**ICT-Services**: Services subject to Regulation (EU) 2022/2554 (DORA);

**Outsourced Services**: Services subject to EBA/GL/2019/02 (EBA Guidelines on Outsourcing Arrangements);

**Parties**: The Customer and the Service-Provider which are the parties to the Agreements as well as this Supplemental Agreement;

**Services**: Any ICT and/or Outsourced Service provided under an Agreement;

**Subcontractor**: shall have the meaning as provided for such term in Clause 5.2 of this Supplemental Agreement; and

**Supplemental Agreement**:this Supplemental Agreement on Special Provisions Regarding ICT- and Outsourced-Services.

1. **General Provisions**

Since Customer’s Affiliates qualify as a “financial entity” pursuant to DORA, as well as a “financial institution“ pursuant to EU Regulation 2013/575, the Customer has to comply with certain regulatory provisions. These provisions require (amongst other requirements) the implementation of a 3rd party risk management process and the inclusion of specific contractual provisions in agreements as are being entered into from time to time with the Service Provider.

For as long as any of the terms of an Agreement is applicable (be it because of the terms of this Supplemental Agreement), the Service Provider shall, in relation to any such Agreement:

a) have appropriate and sufficient capabilities, expertise, capacity, resources, organizational structure, and the required regulatory authorizations or registrations required for a proper performance of the Services;

b) fully comply with the Customer’s “Code of Conduct“ specified in Annex 4 and the Customers’ “Security Requirements for Suppliers” specified in Annex 5; and

c) apply the same due diligence and service quality criteria, as the Customer would have to apply if it provided the Service itself.

1. **Locations**

The Service Provider shall provide the Services to the Customer and process the data including the data storage exclusively at the locations specified in Annex 2. These locations may only be changed by mutual agreement.

1. **Business Contingency Management**

The Service Provider shall always implement and have available during the term of any Agreement a business contingency plan aimed at:

a) preventing situations, in which the Service Provider will not be able to provide the Services at all or at the agreed level; and

b) implementing such measures that will lead to the prompt restoration of the provision of the Services to the agreed level if the provision of the Services fails or the quality of the Services deteriorates.

The Service-Provider shall provide the Customer upon its request with evidence that an adequate business contingency plan for the respective Services as well as the IT systems required to perform such Services is in place.

The Service Provider undertakes to test the business contingency plan at least annually for practicability and technical feasibility and update the business contingency plan accordingly. The Service Provider shall evidence to the Customer upon its request that the business contingency plan was tested and updated.

1. **Service Provider’s Performance Reporting Duties**

5.1 The Service Provider undertakes to provide the Customer in each case at its own costs:

a) as soon as practicable upon the Customer’s request, with the Service Provider’s financial statements;

b) at least annually with a written report, giving details about:

(i) the performance level achievement in accordance with the terms of each Agreement; and

(ii) any ICT incidents (always including in respect of any data protection breach) or service interruptions, whether, or not, earlier reported or risks identified which could trigger ICT incidents or service interruptions in the future, together with the measures the Service Provider has put into effect to avoid any future ICT incidents or service interruptions and to cope with any such risks so being identified (and if any such risk can only be mitigated by risk acceptance this shall be identified and stated so in such report);

c) and at least annually with a report setting out the Service Provider’s ICT-Security and business contingency measures taken and tests made, including the test results; and

d) all other relevant information.

5.2 In case of subcontracting critical or important services or material parts of it, the report referred to in Clause 5.1 above also has to contain respective reports and information in respect of any subcontracted services (to the extent supporting critical or important ICT Services and herein referred to as “Critical or Important Services”) and each relevant subcontracted service provider (each a “Subcontractor”).

5.3 The Supplier must report ad-hoc without undue delay on:

a) ICT-related incidents;

b) Operational or security payment-related incidents;

c) about any change in name, corporate seat, delivery address, unique identifier details, any of its other registration details, or any change in its ownership structure; and

d) any intention to change the locations of the Services, namely the regions or countries, where contracted or subcontracted Services are to be provided and where data is to be processed and stored, in each instance.

1. **Subcontracting**

6.1 Subcontracting for any Critical or Important Services is only permitted with the Customer´s prior written consent.

6.2 The Service Provider is obliged to provide the Customer with all required information and data in connection with the intended subcontracting for any Critical or Important Services, in particular name and location of the Subcontractor, location of data in rest and data processing and the parent company of the Subcontractor. The Service Provider shall assess all risks, including ICT risks, associated with the location of any potential or actual Subcontractor and its parent company and the location where a Critical or Important Service is provided from. The Service Provider ensures that its due diligence process can address, select and assess the operational and financial abilities of a potential or actual Subcontractor to provide the Critical or Important Services, including by participating in digital operational resilience testing as referred to Chapter IV of DORA as required by the Customer.

6.3 If the Customer authorises the Service Provider to use a Subcontractor for any Critical or Important Services, the Service Provider shall:

a) be liable for all acts and omissions of any such Subcontractor as for its own;

b) require written consent from the Customer prior any material changes of any Critical or Important Services or the Subcontractor;

c) inform the Customer of changes of subcontracting with sufficient lead time for the Customer to assess the impact of the changes and the risk the Customer is or might be exposed to, as well as whether such changes might affect the ability of the Service Provider to meet its obligations under the relevant Agreement. In order to carry out such risk assessment, the Service Provider shall provide the Customer with all information required;

d) have adequate abilities, expertise, financial, human and technical resources, apply appropriate information security standards, and have an appropriate organizational structure, including risk management and internal controls, incidents reporting and responses, to monitor its Subcontractors and Critical or Important Services;

e) monitor all Subcontracted Services to ensure that its contractual obligations with the Customer are continuously met;

f) continuously assess all risks associated with the location of each relevant Subcontractor and its parent company and the location from where any Critical or Important Service is provided;

g) include in its written contractual agreement with each Subcontractor all provisions necessary to ensure that:

(i) such Subcontractor owes the same level of performance and quality as the Service Provider; and

(ii) the Customer and the authorities responsible for the Customer can exercise the same rights with each Subcontractor as with the Service Provider. In any case for each Service permitted by the Customer for subcontracting the written contractual agreement concluded between the Service Provider and the Subcontractor shall at the minimum specify:

A) the monitoring and reporting obligations of each Subcontractor towards the Service Provider, and where agreed, towards the Customer;

B) the obligation to comply with the Customers’ “Security Requirements for Suppliers” and any additional security requirements, where relevant;

C) an incident response plan so that each Subcontractor will be obliged to comply with the incident reporting requirements as set out in the “Security Requirements for Suppliers”, and a business contingency plan as referred to in Clause 4 above as well as Art 11 DORA and the service levels to be met by the Subcontractor in relation to these plans;

D) the location and ownership of data processed or stored by the Subcontractor, where relevant; and

E) an obligation to grant to the Customer and relevant competent and resolution authorities the same rights of access, inspection and audit as granted to the Customer and relevant competent and resolution authorities by the Service Provider under this Supplemental Agreement;

h) be able to identify, notify and inform the Customer of any Subcontractor in the chain of subcontracting providing Services, and to provide all relevant information that may be necessary for the assessment by the Customer; and

i) ensure the contingency of the Services throughout the chain of subcontractors in case of failure by a subcontractor to meet its contractual obligations.

6.4 The Customer shall have the right to request a copy of the subcontracting agreement with a Subcontractor. The Service Provider may black out financial information and other confidential information, if such information is not required by the Customer to evidence that the terms of the subcontracting agreement fulfil the requirements referred to herein.

6.5 The Customer will inform the Service Provider about its risk assessment results on planned subcontracting, and, in case it exceeds the Customer’s risk tolerance, the Customer shall be entitled to disagree with the proposed subcontracting, or to demand changes being made to the terms of any such proposed subcontracting prior to their implementation.

6.6 The Service Provider will, in the relevant agreement for any such subcontracting agree with the Subcontractor that the Customer has direct termination rights in accordance with Clause 9 of this Supplemental Agreement and in accordance with the circumstances set out under Art 28(7) DORA.

6.7 The list of Subcontractors approved (if any) by the Customer as of the date of signing this Supplemental Agreement is listed for each Agreement in Annex 1.

1. **Audit, Inspection and Access Rights**

7.1 The Service Provider acknowledges and agrees that the Customer and any competent supervising authority of the Customer as well as the competent Lead Overseer (as defined in the DORA and in this Clause 7.1 each hereinafter a “Competent Authority”) has the right to monitor the performance of the Service Provider at any time and for this purpose the Customer and any Competent Authority or the persons/third party nominated by the Customer or a Competent Authority have:

a) unrestricted rights of access to all relevant business premises (head offices and operating centres), including relevant facilities, systems, networks, information and data used for the performance of the Services;

b) rights of inspection and audit; and

c) the right to take copies of relevant documentation on-site if they are critical to the operations of the Service Provider. The Service Provider undertakes to fully co-operate with and assist during the onsite inspections and audits performed by the Customer’s internal audit units, Competent Authorities or any third party appointed by any of them.

The aforementioned rights shall not be impeded or limited by other contractual arrangements or implementation policies.

7.2 The Customer has the right to choose on alternative assurance levels where appropriate. The Customer may, at its sole discretion, use the following methods to monitor the Service Provider´s performance:

a) its own internal audit or an audit by an appointed third party;

b) where appropriate, pooled audits and pooled ICT testing, including threat-led penetration testing, that are organized jointly with other contracting financial entities or firms that use Services of the Service Provider and that are performed by those contracting financial entities or firms or by a third party appointed by them;

c) where appropriate, third-party certifications;

d) where appropriate, internal or third-party audit reports made available by the Service Provider; and

e) the use of other relevant information available to the Customer or other information provided by the Service Provider.

7.3 The Service Provider herewith permits that its IT systems and IT infrastructure may be tested against (internationally accepted industry) IT security quality standards, including, but not limited to, penetration tests. If it is required for any such internal or external audit to be performed in accordance with its terms to also gain access to any client data which is unrelated to the data processed, stored or generated, for the Customer, any such other client data (only) will be either segregated from the data processed, stored or generated, for the Customer or will be made illegible prior to granting access to any such data.

7.4 On Customer’s request, the Customer and the Service Provider shall agree on an audit plan which shall be updated periodically. The Customer has the right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls; whereas the number and frequency of such requests for scope modification shall be reasonable and legitimate from a risk management perspective.

7.5 The Service Provider will, at any time upon demand of the Customer provide the Customer with any license or authorization required to have or available with the Service Provider to conduct its business.

7.6 The Service Provider will, at least on an annual basis, submit to the internal audit unit of the Customer or any independent quality audit firm reasonably selected by the Customer, its internal audit report so that the Customer will receive such report no later than fourteen days after its issuance.

1. **Data Protection**

The requirements and measures on availability, authenticity, integrity and confidentiality in relation to the data protection, including personal data are contained in the Customer`s “Security Requirements for Suppliers” and in the Agreement(s). In particular, the Service Provider guarantees that the Services are set up and structured and that all operating processes and requirements for security elements are designed in such a way that no access to systems of other clients or third parties and vice versa is possible from a system operated for the Customer. In case of conflict between the provisions of this Supplemental Agreement and the provisions of a Data Processing Agreement (DPA) as referred to in Art 28 GDPR, the DPA shall prevail over the provisions of this Supplemental Agreement.

1. **Termination Rights and Termination assistance**

9.1 The Customer shall be entitled to terminate an Agreement in accordance with the provisions of the respective Agreement.

9.2 In addition to, and separate from the above, the Customer shall also be entitled to terminate at any time an Agreement with immediate effect also for any of the following reasons:

a) in the event of a significant breach by the Service Provider of applicable laws, regulations or contractual terms;

b) in the event of circumstances identified throughout the monitoring of ICT third-party risk that are deemed capable of altering the performance of the functions provided through the contractual arrangement, including material changes that affect the arrangement or the situation of the Service Provider;

c) in the event of the Service Provider’s evidenced weaknesses pertaining to its overall ICT risk management and in particular in the way it ensures the availability, authenticity, integrity and confidentiality, of data, whether personal or otherwise sensitive data, or non-personal data;

d) if the competent authority can no longer effectively supervise the Customer as a result of the conditions of, or circumstances related to, the respective contractual arrangement;

e) if any of the Customer’s competent supervising authorities is asking for a termination of an Agreement (and in the event such authority asks for a suspension of the application of all or only some terms of an Agreement, the applicability of any such terms shall be suspended upon the Service Provider receiving notice);

f) if legal acts coming into force, or court (including administrative court) rulings are being issued and which require (whether directly or indirectly) to terminate an Agreement (and in the event such legal act or court asks for a suspension of the application of all or only some terms of an Agreement, the applicability of any such terms shall be suspended upon the Service Provider receiving notice);

g) if the Service Provider implements material changes to subcontracting arrangements regarding the provision of Services supporting critical or important functions despite the objection or request for modifications to the changes by the Customer; or

h) when the Service Provider subcontracts a Critical or Important Service not explicitly permitted to be subcontracted hereunder.

9.3 In the event an Agreement is being terminated, the Service Provider undertakes to continue performing the Services until the point in time when the Customer confirms to the Service Provider that the Customer is performing such Services on its own or that such Services have been transferred to another service provider. Until the time when the Service Provider actually (but in accordance with the terms of this Supplemental Agreement) discontinues with the performance of the Services (until which point in time the Customer will pay the fees as originally agreed under the relevant Agreement (as if the same were not terminated)), the Service Provider further undertakes to put the Customer back into a position in which the Customer will be enabled again (and where such enablement shall include the return of all data, the migration of all data which is intended to be generated, collected, or processed for or on behalf of the Customer when performing the Services under the Agreement, information and all other auxiliary material) to fully perform the Services on its own or to transfer the duty to perform such Services to another service provider whereas the Customer shall use reasonable endeavors to ensure such period will be as short as possible. The Service Provider is obliged to follow the Customer’s instructions on the transfer of the Services.

1. **Cooperation with Competent authorities**

The Service Provider undertakes, in addition to the otherwise agreed obligations, to co-operate fully with the competent authorities and resolution authorities responsible for the Customer, including persons appointed by these authorities.

1. **Access Rights**

11.1 The Service Provider warrants that the Customer is able to access all personal and non-personal data stored by or for the Customer at or through the Service Provider or its Subcontractors (e.g. hosting providers) at any time.

11.2 Back-up, restoration, recovery and return of the Customer's data must be possible at any time in an easily accessible format by the Service Provider and must be carried out immediately upon request.

11.3 The Customer shall at any time have access to personal and non-personal data and the Service Provider shall put, immediately upon the written request of the Customer, all codes (including any source codes) and all personal data (each in an easily accessible format, and in this Clause 11.3 referred to as “Resilience Data”) required for the Customer to continuously perform by itself or through a replacement service provider the Services in the event the Service Provider becomes insolvent, is resolved or otherwise discontinues with its business into escrow (together with any subsequent modifications to it) and instructing (unless agreed otherwise in the Agreement, at the Service Provider’s costs) an escrow agent acceptable to the Parties to hand over to the Customer, immediately upon the Customer’s demand for doing so in writing, such Resilience Data, provided that in such demand the Customer confirms that the conditions for such hand over have been met. Any such escrow conditions shall be reasonably acceptable for the Parties and shall in any event include that a demand for such hand over, transfer and release shall be justified in the event of the Service Provider’s insolvency, inability to pay its debt, dissolution, or any party filing for the Service Provider to be put out of business or being otherwise dissolved (voluntarily or involuntarily) and where such filing has not been finally revoked or dismissed within two weeks’ after such filing has been made (and nothing herein shall prevent the Principal to make such filing unless such filing is made in bad faith).

1. **Miscellaneous**

12.1 Transmittal of data will be done in a logged manner so that there will be a protocol available indicating who has transmitted to or received from which party which data at which times. The Service Provider also undertakes to store data which is related to the Service in a segregated silo and hence separate from any of its own data or data processed or stored for any of its other clients.

12.2 The Service-Provider undertakes to:

a) participate in the Customer’s ICT security awareness programs and digital operational resilience training to the extent defined as compulsory by the Customer and subject to it having received at least one month prior to such programs or trainings a written invitation provided by the Customer to participate; Art 30(2) (i) of DORA; and

b) participate and fully cooperate in the Customer’s threat-led penetration testing (TLPT) as referred to and in accordance with Art. 26 and 27 DORA.

12.3 The Service-Provider shall at all times of the contractual period have taken out a professional indemnity insurance on terms reasonably acceptable to the Customer. Any time upon request the Service Provider will provide the Customer with a copy of the respective insurance certificate.

12.4 This Supplemental Agreement can be terminated by either Party by giving the other Party a written termination notice whereupon this Supplemental Agreement shall terminate on the last day of the calendar month falling three months after giving of such notice, always provided that the Service Provider will not be entitled to terminate this Supplemental Agreement for as long as any Agreement is effective.

12.5 For this Supplemental Agreement the same choice of law and dispute resolution provisions as agreed between the Parties pursuant to the most recent Agreement applicable and as entered into between the Parties prior to the date of this Supplemental Agreement shall apply.

For and on behalf of:

Raiffeisen Informatik Consulting GmbH

|  |  |
| --- | --- |
| ……………………………………………………………….. | ……………………………………………………………….. |
| ARNO GRUBER | MARTIN SCHÖNHOFER |

[\*\*\*INSERT FULL LEGAL NAME OF SERVICE PROVIDER]

|  |  |
| --- | --- |
| ……………………………………………………………….. | ……………………………………………………………….. |
| [\*\*\*INSERT NAME OF AUTHORIZED SIGNATORY] | [\*\*\*INSERT NAME OF AUTHORIZED SIGNATORY] |

ANNEX 1

List of Approved Subcontractors

|  |  |  |
| --- | --- | --- |
| LEGAL NAME OF SUBCONTRACTOR | IDENTIFICATION CODE | RELEVANT AGREEMENT |
| [\*\*\*FILL IN FULL LEGAL NAME AND ADDRESS] | [\*\*\*FILL IN LEI OR EUID] | [\*\*\*INCLUDE REFERENCE TO AGREEMENT AS PER ANNEX 3] |
|  |  |  |
|  |  |  |

ANNEX 2

Locations

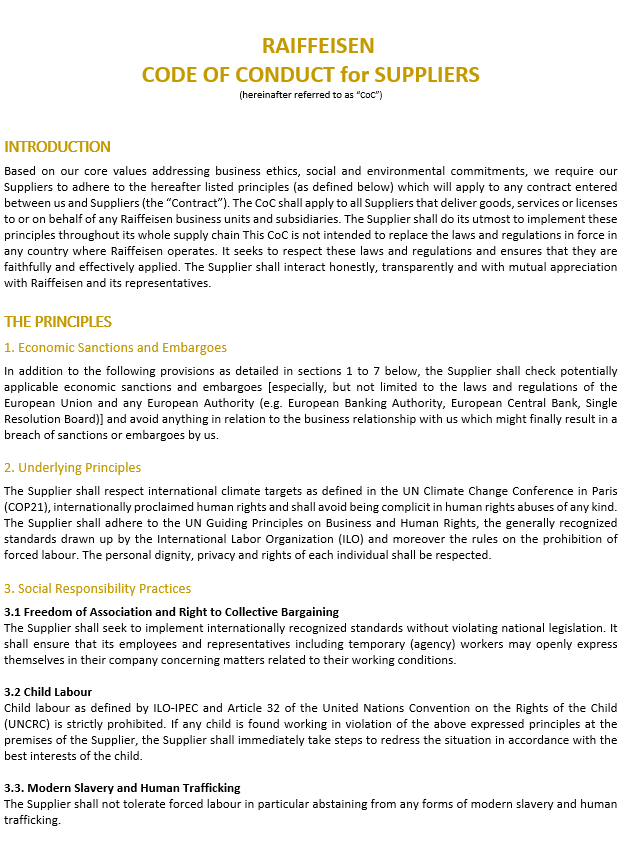
|  |  |  |  |
| --- | --- | --- | --- |
| [\*\*\*FILL IN COUNTRY OR REGION] | Service provided (mark with “x” if applicable) | Data processed (mark with “x” if applicable) | Data stored (mark with ”x” if applicable) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

ANNEX 3

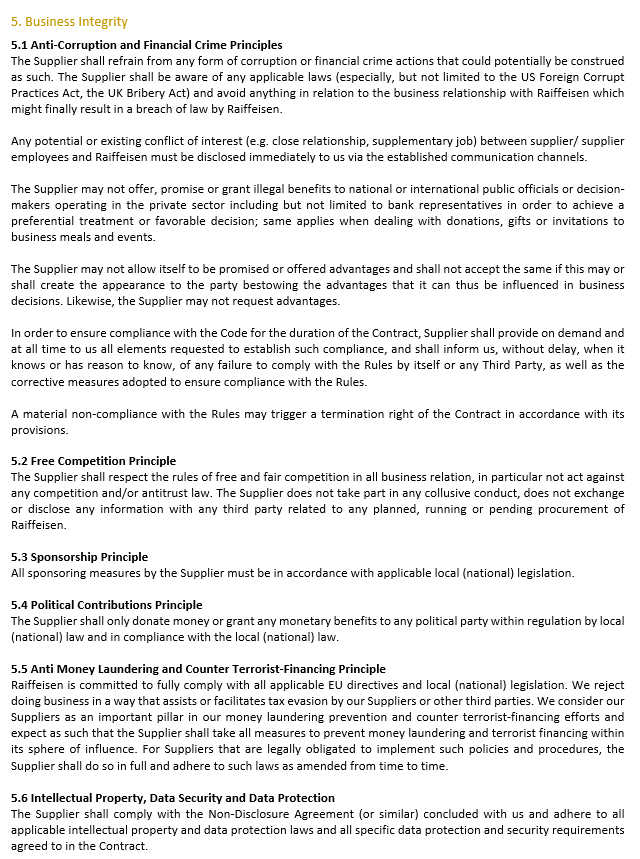
Applicable Agreements

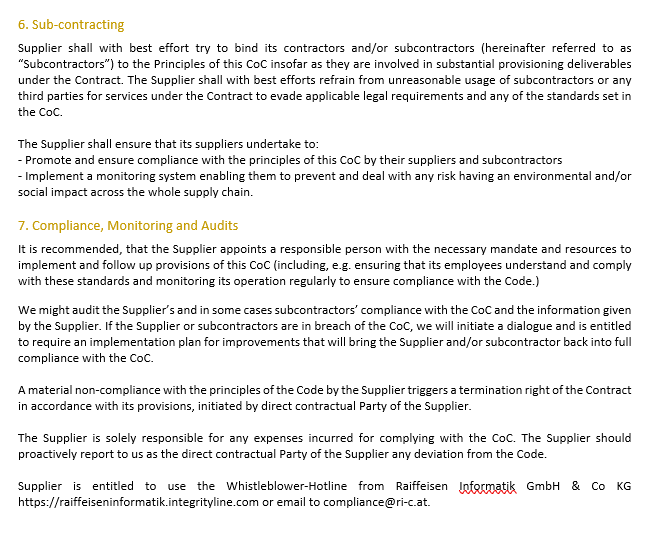
|  |  |  |
| --- | --- | --- |
| Date of agreement | Title of Agreement | Brief description of purpose |
| [\*\*\*INSERT DATE] |  | [\*\*\*INSERT PURPOSE] |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

ANNEX 3



|  |
| --- |
|  |





ANNEX 5

Security Requirements for Suppliers

Trust in Raiffeisen (“CUSTOMER”) services is an integral part of our corporate culture. Using innovative services and products as well as cooperating with professional partners and suppliers is necessary to stay ahead in a fast-changing industry.

It is our due diligence to protect our as well as our client’s data, systems and applications with security measures, together further referred to as the "Security Requirements". 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.

Managing supplier relationships in regard to security is an important part of Raiffeisen’s internal risk management framework, a common praxis (e.g. ISO 27000 series, NIST Cybersecurity Framework) and mandatory for financial institutions (e.g. the EBA Guidelines on ICT and security risk management dated 29 November 2019, § 25 and the Annex to § 25 of the Austrian Banking Act, etc.).

Having regard to the above, the Vendor, Processor or Partner (collectively referred to as “SUPPLIER”) represents and warrants that it has made all necessary due diligence and is familiar with and acknowledges the Security Requirements and agrees to comply with the Security Requirements in general, as well when (a) accessing CUSTOMER facilities, Networks and/or Information Systems, or (b) accessing, processing, or storing CUSTOMER information/data, or (c) providing infrastructure services and/or standard software, or (d) developing software.

Additional security requirements may be specified in individual agreements (e.g. SLA, statement of work).

|  |
| --- |
|  |
| **ICT Governance** |
| **Guidelines** |
| The SUPPLIER maintains an information security management system including a continuous improvement process based on recognized industry standards. |
| Information security policies, procedures, roles, responsibilities and accountabilities are defined in accordance with SUPPLIER`s business requirements, relevant laws and regulations. Information security policies are approved by management, published and communicated to employees and relevant external parties. |
| The SUPPLIER regularly reviews its compliance to established security policies, standards and any other security requirements. |
| **Risk Management** |
| The SUPPLIER has an industry standard security risk management program in place. Risks are identified, assessed, treated, and documented. |
| **Contractual Agreement** |
| The SUPPLIER must include responsibilities for information security in contractual agreements with their employees and contractors. |
| **Background Checks** |
| Background verification checks on candidates for employment are carried out in accordance with relevant laws and regulations. The level of verification performed must be proportional to the risk associated with the candidate's role. |
| **Awareness Program** |
| All employees of the SUPPLIER and, where relevant, contractors receive awareness education and trainings appropriate for their job function. Additionally, updates of SUPPLIER`s policies and procedures are communicated to employees as well. All personnel must have adequate skills related to their roles and responsibilities. |
| **Sub-Contractors** |
| **Sub-Contractors** |
| The SUPPLIER has contractual agreements with subcontractors who process, store or transmit CUSTOMER data in order to state their responsibility for the security of CUSTOMER data. The SUPPLIER requires that security measures implemented by beforementioned subcontractors have an equivalent level of security as stated within this document. The SUPPLIER verifies the effectiveness of the measures as part of their supplier management process. |
| **ICT Project and Change management** |
| **Change Management** |
| The SUPPLIER has a change management process that includes reasonable security testing and documentation of request initiation and approvals. Cybersecurity reviews for new system designs or changes to systems, and security testing prior to deployment must be part of the processes. |
| **Secure Software Development Lifecycle** |
| The SUPPLIER has secure software development lifecycle policies and procedures in place and implements among others following security measures:   * Usage of secure software development methods as part of the secure software development process * Secure coding guidelines based on international standards * Mechanisms to detect and protect against unauthorized changes to source code * Periodically carry out secure code reviews (Static Application Security Testing and Dynamic Application Security Testing) * Vulnerability scanning which also includes used third-party code and open-source components (e.g. libraries) * Penetration tests which are performed by either an independent third party or by persons who were not involved in the development of the security measures. Testers must have sufficient knowledge, skills, and expertise to perform penetration tests. * Appropriate trainings for internal and external software developers.   Findings and known vulnerabilities are mitigated before release to production. |
| The SUPPLIER maintains an up-to-date Software Bill of Materials (SBOM) according to industry standards for CUSTOMER used software components.  The SBOM includes but is not limited to:   * Open-source libraries that an application imports or depends on. * Plugins, extensions or other add-ons that an application uses. * Proprietary application packages written in-house by developers. * Information about the versions, licensing status and/or patch status of these components. * APIs or third-party services required to run the service. |
| **Information Security** |
| **Identity and Access Management** |
| The SUPPLIER has access controls in place in order to verify identities and restrict access to authorized users only. Access rights are based on "need to know" and "least privilege" principles. Additionally, the principle of "separation of duties" is adhered to. |
| The SUPPLIER shall review the access rights of its staff on regular intervals and shall change (i.e. restrict or revoke) the access rights if necessary. |
| The SUPPLIER has implemented authentication mechanisms to protect accesses to systems, according to best practices which include but are not limited to:   * password policies (minimum lengths, complexity, avoiding re-use) * unique user identification (generic and shared users are avoided) * secure storage/management/transmission of credentials |
| The SUPPLIER has implemented strong controls for privileged accounts (e.g. system administrators) by means of strong authentication (e.g. multi-factor authentication), limitation to a minimum and closely supervised usage. |
| SUPPLIER ensures that accounts which are used for access over the internet are protected by strong authentication mechanisms (e.g. multi-factor authentication). |
| **Patch Management** |
| The SUPPLIER periodically analyses systems (operating systems, applications, network components) for known vulnerabilities. Patches are applied in a consistent, standardized manner and prioritized based on criticality. If the root cause of vulnerabilities could not be mitigated within reasonable time, alternative risk mitigation measures must be implemented until the root cause is remedied. The SUPPLIER has implemented an emergency change process. |
| **Network Security** |
| The SUPPLIER has implemented and maintained network security infrastructure components such as firewalls, intrusion detection/prevention systems (IDS/IPS) and other security controls, providing detection, continuous monitoring, and restrictive network traffic flow to assist in limiting the impact of attacks. Systems with a higher risk level (e.g. externally exposed) must have stricter measures in place. |
| The SUPPLIER ensures that a formal remote access policy is in place. |
| The SUPPLIER ensures segregation and segmentation of the environments according to industry standards, when:   1. environments are shared with other customers; and/or 2. SUPPLIER implements test, quality and production environments. |
| **Encryption** |
| The SUPPLIER must consider measures for data in transit, data in memory and data at rest, such as the use of encryption technologies in combination with a key management architecture. The encryption is compliant to leading standards and guidelines or equivalent (e.g., National Institute of Standards and Technology – NIST). |
| The SUPPLIER protects mobile devices and external electronic media (e.g. USB memory storage, tape) against unauthorized access, through adequate physical and logical security measures. Data-at-rest encryption on these devices must be enforced. |
| **Malware Protection** |
| The SUPPLIER protects servers and endpoints with malware protection which is kept up to date. The software must detect if anti-virus/malware software on devices has been disabled or not receiving regular updates. |
| **Security Testing, Monitoring & Reporting** |
| The SUPPLIER has security measures in place to protect data, applications and systems against cyber threats. The SUPPLIER periodically evaluates the effectiveness of security measures related to known cyber threats and frauds as well as respective models (e.g. based on up-to-date threat catalogues like National Institute of Standards and Technology, Bundesamt für Sicherheit in der Informationstechnik). |
| The SUPPLIER has periodic plans and executes vulnerability assessments and penetration tests on systems used to provide services to the CUSTOMER. Penetration tests on these systems have to be conducted in the following manner:   1. at least once a year 2. in case of a major release/updates of applications/software/information services 3. Penetration tests are carried out by testers with sufficient knowledge, skills and expertise and were not involved in the development of the security measures.   The discovered vulnerabilities and findings must be managed appropriately: Analysis, classification and remediation. Mitigation actions must be performed according to their criticality in a timely manner. |
| During the term of this Agreement and not more than once per year (unless circumstances warrant additional audits as described below), CUSTOMER may assess the SUPPLIER’s security posture to ensure compliance (e.g., security questionnaires, security assurance reports) with the here listed Security Requirements. Notwithstanding the foregoing, the parties agree that CUSTOMER may conduct an audit at any time, in the event of:   1. audits required by CUSTOMER’s supervisory or regulatory authorities, 2. investigations of claims of misappropriation, fraud, or business irregularities of a potentially criminal nature, or 3. CUSTOMER reasonably believes that an audit is necessary to address a material operational problem or issue that poses a threat to CUSTOMER’s business.   In the rare case of an on-site audit, the CUSTOMER notifies the SUPPLIER sufficiently in advance, signs necessary confidentiality agreements, adheres to established house rules, ensures that the audit is performed during business hours, and with minimal disruption to the SUPPLIER’s business operations. |
| Upon request, the SUPPLIER must provide non-sensitive/non-confidential documents or extracts from documents to verify compliance with the here listed Security Requirements. Such requests may include, but are not limited to:   * CUSTOMER questionnaires * Security Assurance Reports:   + SOC2 type 2 report   + Internal audit reports * Certifications:   + ISO/IEC 27001 certification incl. Statement of Applicability (SoA)   + ISO/IEC 22301 certification   + PCI DSS * Penetration tests: independent attestation for   + execution of penetration tests   + remediation of found vulnerabilities * Business Continuity and Disaster Recovery Management:   + summaries of its Business Continuity and Disaster Recovery Plans   + test execution summaries (incl. scope, approach, significant findings and lessons learned) of service relevant Business Continuity Plans or Disaster Recovery Plans * Responses to requests as to whether the provided service / product is affected by specific vulnerabilities |
| The SUPPLIER ensures that security issues identified and reported by the CUSTOMER are validated and resolved within a reasonable timeframe if issue is confirmed. |
| **System Hardening** |
| The SUPPLIER has configured and deployed their ICT assets (e.g. databases, applications, operating systems, network devices) using a secure baseline (hardening). The secure baseline is based on best practices (e.g. CIS standards) or equivalent. The hardening configurations on the ICT assets are periodically reviewed and updated. |
| **ICT Operations** |
| **Asset Lifecycle** |
| The SUPPLIER ensures that information security is part of ICT assets across their entire lifecycle. The lifecycle of information includes creation, processing, storage, transmission, decommissioning, deletion and destruction. |
| The SUPPLIER classifies, documents, stores and maintains ICT assets in an up-to-date inventory. |
| The SUPPLIER ensures that provided software is supported by operating systems and middleware versions, which receive security updates and are not end-of-life. The SUPPLIER provides regular, in time security updates over the entire contract lifecycle. |
| **Data Management** |
| The SUPPLIER must not replicate CUSTOMER production data or use it in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from the CUSTOMER. |
| The SUPPLIER has measures against data loss and leakage in place. |
| **Backup & Recovery** |
| The SUPPLIER ensures that backup and data retention concepts exist for each relevant platform/component under the responsibility of the SUPPLIER. Backups have defined retention periods and recovery tests are performed. Backup concepts and recovery procedures are suitable to ensure agreed availability levels. |
| **Logging & Monitoring** |
| The SUPPLIER has adopted appropriate measures in order to ensure accountability and traceability of operations carried out. Logs must provide sufficient details to assist in the identification of the source of an (security) issue and enable a series of events to be recreated.  Logs must record access attempts, system and network security event information, alerts, failures and errors. Integrity of log files must be ensured. Access to log files must be restricted. |
| **Incident Management & Reporting** |
| The SUPPLIER must have documented information Security Incident procedures, enabling effective and orderly management of Security Incidents. The procedures must cover the reporting, analysis, monitoring, resolution and documentation of Security Incidents.  SUPPLIER notifies CUSTOMER without undue delay after becoming aware of an Incident which is in connection with CUSTOMER related services and data and provide reasonable information (such as log files, etc.) in its possession to assist CUSTOMER to meet CUSTOMER’S obligations. SUPPLIER provides such information in phases as it becomes available.  After verification of a security incident in connection with CUSTOMER related services or data, the SUPPLIER shall:   1. provide written notification to the CUSTOMER´s business units and additionally to vendor-incidents@ri-c.at and in time-critical cases or imminent danger also call +43 1 71707-5800 (information security on-call duty) without undue delay. 2. the notification shall include at least following details, if initially not all information is available, the SUPPLIER should provide details as soon as they are known in a staged reporting: 3. Contact information of SUPPLIER incident responsible 4. What occurred 5. How occurred 6. Why occurred 7. Components/assets affected 8. CUSTOMER services/data affected 9. Date and time the incident occurred 10. Date and time the incident was discovered 11. Business impact/effect for CUSTOMER services/data 12. Incident resolution 13. Action taken to resolve incident 14. Action planned to resolve incident 15. use reasonable efforts to avoid and detect such incidents in future; 16. regularly update the CUSTOMER of the measures the SUPPLIER is taking or intends to take; and 17. coordinate further activities with the CUSTOMER. |
| **Physical Security** |
| **Physical Security** |
| The SUPPLIER has categorized its premises into different protection zones, reflecting certain security measures and access rights according to the relevant security needs. |
| Access to IT systems such as servers is further restricted with special protection zones for authorized personnel only. |
| Only secure data center facilities must be used to store CUSTOMER data. |
| **Resilience** |
| **Business Continuity Management** |
| The SUPPLIER has up to date and maintained Disaster Recovery Plans and Business Continuity Plans in place. The Disaster Recovery Plans and Business Continuity Plans must be designed to prevent negative impacts by unplanned disruptions to maximum possible extend and to ensure, that the SUPPLIER can continue to function through operational interruption and continue to provide services as specified in its agreement with the CUSTOMER. |
| The scope of SUPPLIER’s Business Continuity Plans and Disaster Recovery Plans encompasses locations, personnel and information systems used to perform or provides services for the CUSTOMER. |
| The SUPPLIER performs annual, adequate tests of their own Business Continuity Plans and Disaster Recovery Plans. A service relevant test execution summary (incl. scope, approach, significant findings and lessons learned) must be provided to the CUSTOMER. |
| **Security Conditions** |
| **Security Conditions** |
| Following security conditions resulting from the "Vendor Assessment" must be fulfilled within the aligned timeline: |