GENERAL CONTRACTUAL CONDITIONS
for the Procurement of Goods and Services

by Raiffeisen Informatik Consulting GmbH and the Raiffeisen Group

I. Introduction

I.1 These General Contractual Conditions („GCC“) shall govern all goods and services rendered to or supplied to Raiffeisen Informatik Consulting GmbH, A-1020 Vienna, and the Raiffeisen Group Members (together “CUSTOMER”) by a third party (“SUPPLIER”). Any detailed provisions concerning such Goods and Services shall be agreed in individual agreements (“Individual Agreements”) Agreement.

I.2 Unless explicitly agreed otherwise in an Individual Agreement, general business conditions of the SUPPLIER and of any third party supplier shall not become part of the Individual Agreement between the CUSTOMER and the SUPPLIER, even if the CUSTOMER does not expressly object to them.

I.3 These GCC also apply to all modifications, supplements and enhancements developed/prepared in the context of the Individual Agreement, unless the Parties agree otherwise in writing; the requirement of the written form can only be waived in writing.

I.4 Prior to making an offer for the supply of goods and services, the SUPPLIER must carefully familiarize itself with the technical and functional requirements and the relevant situation of the CUSTOMER and the concerned Raiffeisen Group Members. Based on such knowledge, the SUPPLIER shall submit its offers.

I.5 Capitalized terms used in these GCC shall have the meaning set out in Definitions included in these GCC, unless defined otherwise in these GCC. The terms “include” or “including” shall not be construed as terms of limitation.

A) GENERAL CONDITIONS

1 Application of the GCC/Object

1.1 These GCC govern (i) the delivery of goods, (ii) works contracts, as well as (iii) services. Where applicable, special provisions with respect to Software licensing and Software maintenance are included in Chapters B, C and D of these GCC.

1.2 The Goods and Services shall be specified in, and shall be in accordance with, the terms of mutually agreed-upon Individual Agreements signed by authorized representatives of both Parties. The CUSTOMER may provide a form for Individual Agreements to be used under these GCC. In case of contradictions between an Individual Agreement and these GCC, the Individual Agreement shall prevail.

1.3 The Individual Agreement shall provide for the details concerning description, content and extent of the Goods and Services, timeframes and deadlines, remuneration, manner and extent of particular obligations of the CUSTOMER to provide cooperation and assistance, project management, acceptance procedures, limitations on use, term of the agreement and other conditions. An Individual Agreement can also be a Purchase order issued by CUSTOMER’s ordering system with reference to this GCC or a frame contract and shall be effective without signature.

1.4 If the Individual Agreement is concluded between the SUPPLIER and the CUSTOMER, other Raiffeisen Group Members of the CUSTOMER may also be beneficiaries of the Individual Agreement. In such case, the SUPPLIER shall be obliged vis-à-vis such Group Members directly to comply with the provisions of these GCC.

1.5 If applicable special provisions which are required due to regulatory and legal regulations are included in Exhibits and are integrated parts of the Individual Agreement based on this GCC.

2 Principles of Performance

2.1 In performing the Services, the SUPPLIER shall at all times

(i) perform the agreed Services including services which can reasonably be considered inherent to the explicitly agreed services, act diligently and exercise due and proper care;
(ii) comply with Applicable Law and Regulatory Requirements applicable to the SUPPLIER;
(iii) comply with Commonly Acknowledged Industry Standards and Practices;
(iv) comply with the Compliance Rules and Policies of the CUSTOMER including its Code of Conduct as agreed in the respective Individual Agreement (which may be reasonably modified by the CUSTOMER from time to time)
(v) comply with the Data Protection and Security Standards of the CUSTOMER as agreed in the respective Individual Agreement (which may be reasonably modified by the CUSTOMER from time to time)
(vi) obtain and maintain during the term of the Individual Agreements all consents and rights necessary to perform its obligations under the Individual Agreement.

2.2 In performing the Services, the SUPPLIER shall not interfere with, and/or adversely impact the business of the CUSTOMER.

3 Delivery/Time of Performance/Delay

3.1 The place of delivery of Goods and/or rendering the Services shall be set forth in the Individual Agreement.

3.2 The SUPPLIER may not withhold the delivery of Goods as security for claims against the CUSTOMER.

3.3 The delivery terms for Goods shall be D.D.P at the site agreed in the relevant Individual Agreement, as per the Incoterms 2010. Partial deliveries and partial services shall not entail the passage of risk from the SUPPLIER to the CUSTOMER.

3.4 All Goods shall be suitably packed in a way that the packaging is safe and fit for the respective transport. Packing slips, labels, tags, etc. shall be provided by the SUPPLIER in order to secure an unmistakable identification of the items delivered and an unmistakable quantitative ascertainment. SUPPLIER shall ensure disposal of the packaging material immediately after delivery, at SUPPLIER´s cost.

3.5 The SUPPLIER shall perform and complete the Services in a timely manner, and in accordance with any appli-cable time schedules set out in the Individual Agreement. Deadlines and terms for the provision of Services shall be binding, unless the SUPPLIER and the CUSTOMER have expressly agreed in writing that they shall be not binding in any individual case.

3.6 If the SUPPLIER has not duly performed and completed the agreed Services in time, the SUPPLIER shall be in default.

3.7 If an agreed delivery/performance date or deadline is not complied with for reasons, which fall primarily within the responsibility of the SUPPLIER, then the SUPPLIER shall pay to the CUSTOMER – as of the beginning of the 2nd week of delay – a compensation, irrespective of culpability or fault, in the amount of 1 % of the remuneration for the respective Services per commenced week of delay, with a maximum of 15 %. The SUPPLIER shall bear the burden of proof that the delay does not fall within the primary responsibility of the SUPPLIER. Any further or other rights or claims the CUSTOMER may have shall not be limited thereby.
3.8 If a default exceeds 4 weeks, the CUSTOMER shall have the right to withdraw from or – at its discretion fully or partially – terminate the respective Individual Agreement for material cause (extraordinary termination), this being without prejudice to any other rights the CUSTOMER may have under the Individual Agreement or Applicable Law.

3.9 In case of Force Majeure or other circumstances not falling within the sphere of the SUPPLIER and its Subcon-tractors, in particular if a delay has been caused by the CUSTOMER, such shall not be considered as a delay for which the SUPPLIER is responsible. In such cases, the deadlines and terms shall be extended by the duration of the hindrance, provided, however, that the SUPPLIER has immediately and in writing informed the CUSTOMER of any default, for which the SUPPLIER is not responsible, including information on the consequences of such default (e.g. term of delay). If the SUPPLIER does not comply with such duty to inform, it cannot rely thereupon at a later time.
3.10 Generally, if the SUPPLIER cannot meet an agreed deadline, such shall be notified in writing to the CUS-TOMER without delay together with information on the reasons for such delay and its expected term; such notification shall, however, not prejudice any rights the CUSTOMER may have due to the default.

4 Documentation

4.1 Any Services shall include the delivery of state-of-the-art documentation related to the Services, including (de-pending on the kind of Service) but not limited to (i) user documentation; (ii) technical documentation; (iii) develop-ment documentation in case of Individual Software; (iv) documentation concerning customizations, configuration, implementation, integration and migration; (v) maintenance documentation and reports; and (vi) Project documen-tation. Details concerning documentation shall be set forth in the respective Individual Agreement.

4.2 The supply of documentation shall be deemed a material obligation of the SUPPLIER.

4.3 All documentation shall be in English, unless agreed otherwise in writing.

5 Personnel, Governance and Subcontracting

5.1 The SUPPLIER shall assign an adequate number of Personnel to perform the Services, who are properly edu-cated, trained, skilled and familiar with the Services they are assigned to perform and have the required know-how, competence and skills. Upon CUSTOMER´s request, the SUPPLIER shall promptly provide to the CUSTOMER a written confirmation of the skills and experiences of the SUPPLIER´s and/or Subcontractor´s Personnel, including resumes.

5.2 The SUPPLIER shall ensure that, whilst present at the CUSTOMER's premises, the SUPPLIER itself and SUPPLIER's personnel will comply with the reasonable rules and regulations of the CUSTOMER, including but not limited to health, safety, security and confidentiality, applicable at the location at which the work is taking place ("work location"); observe all lawful regulations of the CUSTOMER and the laws of the country, in which the work is taking place; take reasonable security precautions with materials and information under the SUPPLIER´s control. The SUPPLIER shall indemnify and keep the CUSTOMER indemnified against any liability for making any payments or deductions, which may be due in respect of the SUPPLIER's personnel by way of national insurance contributions and income tax or other similar statutory deductions on any fees or expenses or other remuneration paid to the SUPPLIER or on behalf of the SUPPLIER's personnel;

5.3 The SUPPLIER shall provide to the CUSTOMER a certificate concerning the applicable European Union legislation form (Form A1) - or an equivalent certificate - for each of its Personnel for purposes of social insurance.

5.4 The SUPPLIER, but not the CUSTOMER, shall bear any risk regarding work permits, trading licence of the SUPPLIER, tax or social security payments in connection with the performance of the Services. The SUPPLIER shall ensure that the SUPPLIER itself and SUPPLIER's personnel observe all lawful regulations of the CUSTOMER and the laws of the country in which the work is taking place, in particular, but not limited to:
(i) labour laws
(ii) tax laws
(iii) social security regulations
(iv) residence permit
(v) trading licence

5.5 The SUPPLIER shall provide to the CUSTOMER a copy of its registration form. Work permits are to be applied for directly by the SUPPLIER or, as the case may be, by the Subcontractors as the CUSTOMER does not employ the Personnel.

5.6 The Parties shall specify in the Individual Agreement which individuals/roles are considered to be key for the performance of the respective Services ("Key Personnel" and "Key Persons"). If the SUPPLIER wishes to substitute any Key Person by another individual, the substitute must have similar qualifications and a similar level of experi-ence as the person the SUPPLIER intends to replace. In addition, any such exchange is only permitted for important reasons (such as sickness or termination of the employment relationship), and requires the prior written consent of the CUSTOMER, which consent, however, shall not be withheld unreasonably.

5.7 The CUSTOMER shall be entitled to request the immediate removal and replacement of any SUPPLIER's or Subcontractor´s Personnel from any CUSTOMER facility, if such person (i) is threatening or abusive, (ii) commits a crime, breaks any law or regulation or engages in an act of dishonesty, which makes it unacceptable for the CUSTOMER to continue dealing with such a person; or (iii) materially violates the Compliance Rules and Policies and/or the Data Protection and Security Standards of the CUSTOMER.

5.8 The SUPPLIER shall promptly remove any SUPPLIER or Subcontractor´s Personnel in performing Services, if the CUSTOMER, in good faith, finds such SUPPLIER or Subcontractor´s Personnel´s performance to be insufficient
for the fulfilment of the tasks assigned to him/her and so notifies the SUPPLIER. In such cases, the SUPPLIER shall promptly provide an appropriate replacement, whose appointment shall be subject to CUSTOMER´s prior approval.

5.9 With respect to Project Services, the following shall apply:

5.9.1 In the Individual Agreement or at the beginning of a Project, each Party will nominate a project manager ("Project Manager"). The Project Managers shall have the authority to make decisions on short notice.
5.9.2 Each Project Manager is responsible for the steering, management and supervision of its own project team; to the extent necessary, the Project Manager will be assisted by the Project Manager of the other Party.

5.9.3 Unless agreed differently in the Individual Agreement, the SUPPLIER´s Project Manager shall in regular intervals document the progress of the rendering of the Services and shall make appropriate status reports available to the CUSTOMER. Such status reports shall inform, in particular, about the then-current status of the Services, about any deviations from project plans, about any pending Change Requests and other relevant circumstances.

5.9.4 The Parties shall institute a project steering committee ("Steering Committee") to steer and supervise the Project implementation. The Steering Committee shall be responsible for making decisions on issues submitted by the Project Managers, furthermore for the supervision of the project progress. The Steering Committee shall meet whenever requested by a Project Manager, in addition periodic meetings can be provided for in the respective Individual Agreement.

5.9.5 Specific provisions concerning governance may be provided for in the respective Individual Agreement.

5.9.6 Unless agreed otherwise in the Individual Agreement, any technical, functional and other requirements of the CUSTOMER for the Services shall be at least roughly described and provided by the CUSTOMER in writing, for example, in the form of specification requirements ("Specification Requirements"). The SUPPLIER is obliged to carefully examine any Specification Requirements provided by the CUSTOMER and to inform the CUSTOMER in writing about any possible perceivable deficiencies/objections relating to such Specification Requirements without delay, so that the CUSTOMER can, as the case may be, correct/modify the concerned Specification Requirements.

5.9.7 Unless agreed otherwise in the Individual Agreement, on the basis of the Specification Requirements, the SUPPLIER shall, particularly in connection with works contracts, prepare an implementation specification ("Implementation Specification"), which shall be reviewed by the CUSTOMER. The Implementation Specification shall become an integral part of the Individual Agreement only after its written acceptance, in the hierarchy of agreements it shall prevail over the Individual Agreement. The Implementation Specification shall also include any specifics concerning the cooperation duties of the CUSTOMER including its required resources (plan concerning resources) as well as a detailed project plan and other relevant requirements necessary for the implementation of the Services.

5.9.8 The Parties may also agree on a detailed analysis phase, the purpose of which is the review of specifications and/or requirements, the outcome of which are detailed analysis documents, which may also become part of the Implementation Specification.

5.9.9 Should the Parties decide explicitly in an Individual Agreement on an agile or hybrid project approach (method) the Parties shall – in deviation from/modification of the relevant provisions of this Chapter – describe the applicable methods, roles and responsibilities as well as the project organization and management, the remuneration model, the termination rights, the acceptance rules and other specifics in the respective Individual Agreement.

5.10 If services (as opposed to works), such as consulting services and trainings, are the object of the Individual Agreement, no project organization as set forth in Section 5.9 is required. In such case, both Parties will, either in the Individual Agreement or at the beginning of the Services, nominate a service manager ("Service Manager"). The Service Managers shall have the authority to make decisions on short notice.

5.11 Any decisions made, whether by the Project Managers, the Service Managers or the Steering Committee or any other body, shall only become binding if they have been made or confirmed in writing. In case of e-mails, the receipt thereof must explicitly be confirmed by the recipient by mail in order to become effective.

5.12 Even if Personnel of the SUPPLIER provide Services at the location of the CUSTOMER, exclusively the SUP-PLIER shall have the authority to give instructions to these employees and the SUPPLIER shall have the exclusive organizational control of such employees.

5.13 The SUPPLIER may only engage Subcontractors in the performance of the Services, which have been pre-approved by the CUSTOMER in writing.

5.14 The SUPPLIER shall ensure and procure that all Subcontractors have, at a minimum, committed to and are bound to the relevant provisions of the Individual Agreement, in particular the provisions concerning Confidentiality, Data Protection, Security, Compliance including audit rights and Intellectual Property Rights. Upon request of the CUSTOMER, the SUPPLIER shall make available to the CUSTOMER without delay the respective agreements with its Subcontractors and any additional information the CUSTOMER may reasonably request from the SUP-PLIER in this connection.

5.15 The SUPPLIER shall assume the full responsibility for any Services rendered or supplied by its Subcontractors.

6 Security

6.1 When present at CUSTOMER´s facilities or accessing CUSTOMER´s systems, or accessing and/or processing CUSTOMER´s data and CUSTOMER´s records, the SUPPLIER shall observe and comply with (i) the CUSTOMER´s Compliance Rules and Policies and its Data Protection and Security Standards, and (ii) any reasonable instructions from the CUSTOMER´s Personnel.

6.2 The SUPPLIER shall enforce and maintain appropriate technical, organizational and/or logical security measures to protect (i) CUSTOMER´s and SUPPLIER´s facilities from unauthorized access; and (ii) CUSTOMER´s data and CUSTOMER´s records against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.

6.3 Upon becoming aware of any actual or potential security breach in connection with the Services, the SUPPLIER shall (i) notify the CUSTOMER in writing without delay; (ii) use all reasonable efforts to avoid such breach or reduce its consequences; (iii) continuously inform the CUSTOMER of the measures the SUPPLIER is taking or intends to take; (iv) obtain the CUSTOMER´s prior written approval pursuant to Applicable Law in connection with any notification or public information with respect to such breach, and (v) coordinate any further activities with the CUSTOMER.

6.4 The SUPPLIER and its Subcontractors shall produce, keep, maintain and monitor at all times during the contractual relationship with the CUSTOMER a back-up, security and emergency concept, as required by Applicable Law, Regulatory Requirements, and the Commonly Acknowledged Industry Standards and Practices for supplies of services for the banking industry, if and to the extent they concern or may concern the Services.

7 Confidentiality and Data Protection

7.1 The Parties shall be obliged to keep all information received concerning data, documentation and other information, of which they have obtained knowledge or which has become available to them in connection with the contractual relationship, in confidence, and shall safeguard Confidential Information from unauthorized disclosure, reproduction or use according to Commonly Acknowledged Industry Standards and Practices.

7.2 The obligation of confidentiality pursuant to Section 7.1 above shall not apply to information which (i) is publically available or was already known to the other Party earlier; (ii) has been developed by one of the Parties independently without knowledge of the relevant information of the other Party or without use thereof; or (iii) has been made public by a third party, which is not subject of the confidentiality obligation.

7.3 Each Party shall use Confidential Information of the disclosing Party only for the purpose and to the extent necessary for the performance of its tasks under the respective Individual Agreement or as explicitly allowed under such Individual Agreement.

7.4 Notwithstanding Sections 7.2 and 7.3 above, each Party may:

(i) make available Confidential Information to Raiffeisen Group Members and/or a third party, provided such third party is subject to confidentiality obligations comparable to those applicable to the Parties and for the purpose and to the extent necessary for the performance of the receiving Party´s obligations under an Individual Agreement; and/or to enable a third party to perform legal, accounting or audit services for a Party;
(ii) make disclosures as required by Applicable Law and Regulatory Requirements, relevant stock exchange rules and/or applicable accounting rules, or are required by any court of competent jurisdiction, or any competent governmental, supervisory or regulatory body, provided that the receiving Party takes reason-able measures to limit such disclosures to the extent necessary; and notifies the disclosing Party reason-ably in advance to enable the disclosing Party to participate in such efforts, unless prohibited by mandatory Applicable Law to do so.

7.5 The SUPPLIER shall ensure that its employees, the Personnel, other representatives, and Subcontractors hav-ing access to CUSTOMER´s Confidential Information
(i) are bound by a written agreement, containing confidentiality and non-disclosure obligations comparable to those applicable to the SUPPLIER under the respective Individual Agreement; and
(ii) promptly execute and provide the CUSTOMER, at CUSTOMER´s request, any additional documents or agreements containing confidentiality and non-disclosure obligations as may be required by Applicable Law and Regulatory Requirements or CUSTOMER´s Compliance Rules and Data Protection and Security Rules.

7.6 The Parties and its Subcontractors shall comply with the applicable data protection laws and provisions. Should the provision of Services require the SUPPLIER or its Subcontractors to act as Data Processors, the SUPPLIER and its Subcontractors shall enter into a separate data processing agreement as provided by the CUSTOMER.
7.7 Nothing in this section shall be construed as obligating a Party to disclose its Confidential Information to the other Party, or as granting to a Party any rights to the Confidential Information of the other Party.
7.8 This section shall remain in full force and effect for an indefinite period after termination of the respective Individual Agreement.

8 Compliance/Audits

8.1 The CUSTOMER and its concerned Raiffeisen Group Members, their (internal and external) auditors, regulators and other authorized representatives may be required or deem it necessary to review whether the SUPPLIER and its Sub-contractors – in performing the Services (fulfilling an Individual Agreement) – comply with compliance, security, documentation and reporting requirements as provided for by Applicable Law and Regulatory Requirements, Com-monly Acknowledged Industry Standards and Practices in the banking industry, the Individual Agreement, in par-ticular the agreed Compliance Rules and Policies and the Data Protection and Security Standards.

8.2 For the purposes of Section 8.1, the CUSTOMER, its concerned Group Members, their internal and external auditors, and the competent regulatory authorities shall have the right to request information/documentation/reports from the SUPPLIER and its Subcontractors for any of the following purposes; (i) to verify the accuracy of invoices; (ii) to examine data and records with respect to the compliance with Applicable Law, Regulatory Requirements and the Individual Agreement, in particular the applicable Compliance, Security and Data Protection rules, which affect the Services; (iii) to review operations and procedures applied in performing the Services; (iv) and to verify SUP-PLIER´s performance in rendering the Services. Not later than 10 days after the request of the CUSTOMER and/or the Group Members, the SUPPLIER shall submit any requested documents.

8.3 In addition to the rights mentioned in Section 8.2, if so requested by the CUSTOMER, the concerned Group Members, their auditors or the competent regulatory authorities, such bodies shall have the right to examine and audit SUPPLIER´s information and systems on site. Audits by regulatory authorities may be conducted without prior notice.

8.4 The SUPPLIER and its Subcontractors shall (i) fully cooperate with the CUSTOMER, the Group Members, the auditors and the regulatory authorities in conducting audits; (ii) provide such assistance as the CUSTOMER, the Group Members, the auditors and the regulatory authorities reasonably require to carry out the audits, and (iii) provide access to and disclose any information needed for such audits, including copies of relevant documents, which they require.

8.5 The CUSTOMER shall ensure that the persons authorized to carry out the audit will (i) oblige themselves to not disclose Confidential Information pursuant to the corresponding obligations of the CUSTOMER; and (ii) to the extent reasonable, comply with the security and access requirements and observe the relevant written instructions issued by the SUPPLIER in advance.

8.6 The SUPPLIER, the CUSTOMER and the concerned Group Members shall bear their own costs for any audits performed under an Individual Agreement. If an audit reveals any material deficiencies, a material breach of the applicable rules, or any overcharge for the period being audited, then the SUPPLIER shall reimburse the CUS-TOMER and/or the concerned Group Members, without any prejudice to any other rights the CUSTOMER and/or the Group Members may have, for the respective audit costs incurred by the CUSTOMER and/or the concerned Group Members.

8.7 After an audit, the CUSTOMER may provide the SUPPLIER and the concerned Affiliate with a written report including the audit´s findings as to any actual or potential deficits or breaches with respect to the Services. In this case, the SUPPLIER shall promptly provide, for CUSTOMER´s approval, a corrective action plan describing the measures the SUPPLIER has taken or intends to take to rectify the audit findings, including a timetable for each step.

9 Acceptance and Warranty

9.1 All Deliverables shall be accepted by the CUSTOMER, unless agreed otherwise by the Parties in the Individual Agreement. There shall be no implied acceptance (for example by any payments made by the CUSTOMER) for any Services, which are subject to CUSTOMER´s acceptance. Any acceptances shall be made explicitly in writing, e.g. in the form of a statement of acceptance. Upon completion of the respective Services, the acceptance procedure shall be commenced by a written declaration of readiness of acceptance (“DRA”). After receipt of the DRA, the CUSTOMER shall commence with the acceptance procedure without delay.

9.2 If Material Defects occur during the acceptance, such shall be described in a protocol prepared by the CUS-TOMER. The acceptance procedure shall be discontinued if a Material Defect occurs and therefore a meaningful continuation of the acceptance is not reasonably possible. In case of a discontinuance of the acceptance procedure, the SUPPLIER shall commence without delay with the remedy of the defects and shall again declare its readiness for acceptance within a reasonable term following the discontinuance, which term shall not exceed 10 working days. After notification of a remedy of defect by the SUPPLIER, a new acceptance shall be undertaken. Such shall be without prejudice to the rights and claims of the CUSTOMER in case of any delay as set forth in these GCC and the Individual Agreement or provided for by Applicable Law.

9.3 Unless explicitly agreed otherwise, all Deliverables under an Individual Agreement including, if any, Standard Software, Individual Software, the documentation and any other agreed Services are subject to a final acceptance ("Final Acceptance"). Partial acceptances are only permitted if provided for in the respective Individual Agreement. Unless explicitly agreed otherwise or in case the CUSTOMER declares the Services under an Individual Agreement as divisible, all Services shall, for the purpose of acceptance and warranty, be considered as indivisible. The Final Acceptance shall be confirmed by the CUSTOMER in writing (statement of acceptance). Upon the Final Acceptance, the warranty period for all Services under the respective Individual Agreement shall commence.
9.4 Interim acceptances can be provided for by the Parties in the Individual Agreement. Interim acceptances do not substitute for the Final Acceptance. Final Acceptances shall be made regardless of whether any Services have already been subject to interim acceptances. The main purpose of interim acceptances is not only to identify any defects as soon as possible during project implementation and to remedy the same, but also to document the continuous developments of the project results and to optimize the continuation and realization of the respective Project. The results of interim acceptances shall be considered as the basis for the continuation of project implementation.

9.5 The acceptance by the CUSTOMER (e.g. by issuing a statement of acceptance) shall be without prejudice to any claims in respect of any deficiencies and/or defects that may subsequently become apparent or be discovered.

9.6 In case of the delivery of Goods there shall be no acceptance procedure. The acceptance shall be substituted by a confirmation of receipt of the Goods by the CUSTOMER.

9.7 In addition to any other agreed warranties, the SUPPLIER warrants that the Services are free of defects and will perform in a manner that meets any agreed quality standards.

9.8 The CUSTOMER shall notify the SUPPLIER of defects without undue delay. However, the provisions of §§ 377,378 of the Austrian Commercial Code shall not apply. The SUPPLIER shall remedy defects at its own costs. The SUPPLIER shall commence with the remedy of defects immediately after receipt of the notice of defect.

9.9 If a Material Defect is not remedied within a reasonable period of time, which shall not exceed 4 weeks after receipt of the notice of defect, then after such term the CUSTOMER may grant an additional cure period of 10 days. The CUSTOMER may, in its discretion, extend such 10 days period. After expiration of any additional time periods, in case of a Material Defect the CUSTOMER has the right to withdraw from and/or extraordinarily terminate – at its discretion fully or partially – of the respective Individual Agreement, this being without prejudice to any other or additional rights and claims the CUSTOMER may have under an Individual Agreement or Applicable Law.

9.10 The SUPPLIER shall document all defects as well as the status of remedy and shall make available to the CUSTOMER such reports upon request of the CUSTOMER at any time.

10 Damage Claims

10.1 For damages caused intentionally or by gross negligence of the SUPPLIER, and for damages in connection with injury to life, limb or health, the SUPPLIER shall be liable in accordance with Applicable Law.
10.2 In case of slight negligence, the liability of the SUPPLIER shall in total be limited to the contractual value of the respective Individual Agreement. However, the CUSTOMER acknowledges and agrees that the SUPPLIER shall, in case of slight negligence, not be liable for any indirect, incidental or punitive damages.
10.3 Any liability of the SUPPLIER based on the Austrian Product Liability Act remains unaffected by the liability exclusions and limitations set forth above.
10.4 The liability exclusions and limitations contained in this Section shall also apply to damages caused by the CUSTOMER, respectively.

11 Remuneration/Payment Conditions/Taxes

11.1 It is to be agreed in the respective Individual Agreement whether the remuneration shall be a fixed price or be determined on the basis of time and materials ("T&M") or by a combined system.

11.2 If – as at the time of the conclusion of the respective Individual Agreement – the SUPPLIER is able to make an estimate of T&M, the Parties shall agree on a fixed price; the amount and due dates of any partial payment (which shall be linked to the achievement of certain milestones) shall also be set forth in the Individual Agreement. If the Parties agree that an estimate of time and materials requires additional analyses and the Parties have agreed on a detailed analysis phase following the conclusion of the Individual Agreement, then the remuneration for the Services of the SUPPLIER during the analysis phase shall be a fixed price or be based on T & M, which shall be set forth in the respective Individual Agreement. At the end of such analysis phase the SUPPLIER shall offer a fixed price for the Services, which offer may be accepted or rejected by the CUSTOMER. Until acceptance of such offer, the CUSTOMER is at any time entitled to terminate the respective Individual Agreement, without having to give reasons. In case of such termination, the SUPPLIER shall be proportionally

compensated by the CUSTOMER for the work performed by and the expenses incurred until the termination at the rates and fees and up to the maximum amount agreed upon in the respective Individual Agreement, without prejudice to any other cancellation and termination rights (for example for cause) the CUSTOMER may have pursuant to Applicable Law or other contractual provisions.

11.3 In case the Parties agree on a T&M remuneration, the SUPPLIER shall provide work and expense sheets for the services rendered/expenses incurred, which shall contain detailed information on the services rendered by the respective employees, their working times, activities, and expenses.
11.4 The up-to-date work and expense sheets shall be submitted to the CUSTOMER at the end of each month or be included in a time-recording system as designated by the Parties; such shall be the basis of invoicing. Upon request of the CUSTOMER, the SUPPLIER shall prepare more detailed work and expense sheets and shall give all necessary information in connection with such work sheets as may be reasonably requested by the CUSTOMER. Payment on the basis of the invoices shall not be considered as consent of the CUSTOMER to the accuracy and completeness of the work sheets.

11.5 The applicable remuneration rates and rates for out-of-pocket expenses, also for Changes, and other details shall be set forth in the Individual Agreement.

11.6 The following travel policy shall apply:
Travel time remuneration is applicable only for the business travel days agreed with CUSTOMER. For travel time between the home location and the agreed normal place of work there will be no remuneration for travel time. Travel time will be remunerated based on the number of actual hours of travel time at 50% of the normal hourly rate agreed, up to a maximum of 4 hours each way (valid for any travel destination worldwide).
Travel expenses shall be remunerated as follows

- Air travel: Economy class flights
- Train travel: 2nd Class
- Accommodation: CUSTOMER's preferred hotel
- Taxi and public transportation

11.7 The factoring of claims of the SUPPLIER against the CUSTOMER to third parties by the SUPPLIER is prohibited.

11.8 All payments shall be in EURO. Unless set forth differently, value-added-tax in the legal amount shall be added to all prices.

11.9 In case the CUSTOMER is required by law to deduct withholding taxes for the SUPPLIER, the CUSTOMER may deduct such withholding taxes from payments to the SUPPLIER. Any such deduction will be notified to the SUPPLIER.

11.10 If a double tax treaty is applicable between the states of the Parties (= states in which the CUSTOMER and the SUPPLIER are considered residents) which reduces the withholding tax rate, the CUSTOMER is allowed to deduct such reduced withholding tax amount, provided that the SUPPLIER submits to the CUSTOMER a valid certificate of residence as required by law for such payment before the date of the first invoice and for each subsequent calendar year.

11.11 The SUPPLIER is obliged to act in compliance with the tax law applicable to the CUSTOMER, in particular, to comply with registration and documentation requirements. If the CUSTOMER has to pay withholding taxes for the SUPPLIER caused by violation against the tax law applicable to the CUSTOMER, the SUPPLIER shall reimburse the withholding taxes so paid to the CUSTOMER forthwith upon receipt of the CUSTOMER's notice.

11.12 During the contractual relationship between the CUSTOMER and the SUPPLIER, the SUPPLIER is required to inform the CUSTOMER of all tax registrations (e.g. permanent establishment) effected in the state, where the CUSTOMER is considered resident.

11.13 Payments shall be due within 30 days after receipt of the respective invoice.

11.14 The CUSTOMER shall make payments only upon receipt of invoices which include all information required under the relevant provisions of the applicable tax laws.

11.15 In case of payment delays the SUPPLIER has the right, after written reminder and non-payment within 30 days after the reminder, to charge interest rates in the amount of 4 percent per annum.

11.16 In case of non-payment of any invoices of the SUPPLIER, the SUPPLIER is only entitled to terminate or suspend Services if the payment claims are not disputed by the CUSTOMER or a competent court has finally confirmed the payment claim of the SUPPLIER.

12. Intellectual Property Rights of Third Parties

12.1 If the Intellectual Property Rights of third parties have been violated by the agreed use of the Services, or if the CUSTOMER and/or the Group Members have been prohibited from using in full or in part such Services, or if – in the opinion of CUSTOMER or its Third-Party Licensors – such is threatened, SUPPLIER shall at its own expense and, if applicable, after consultation with the producer of the Software/Third Party Licensors either (i) obtain for the CUSTOMER/Group Members the necessary right of use, or (ii) create the respective Services free of Intellectual Property Rights of third parties, or (iii) substitute the respective Results by others which create similar outcomes, but do not violate any third-party Intellectual Property Rights.

12.2 The SUPPLIER shall defend the CUSTOMER/Group Members against all claims, which arise out of a violation of an Intellectual Property Rights by the contractual use of the Services made available or supplied by SUPPLIER. The SUPPLIER shall assume any costs and damages imposed on the CUSTOMER/Group Members by a court to the extent the CUSTOMER notifies the SUPPLIER or the Group Members of such claims raised without undue delay and in writing and the SUPPLIER has been accorded all rights of defense and settlement negotiations. The CUSTOMER/Group Members may not, on its own accord, acknowledge any claims of third parties.

12.3 The SUPPLIER shall indemnify the CUSTOMER/Group Members and hold them harmless against any claim or action on the ground that the Services infringe a copyright, patent right or other intellectual property right of a third party. In such a case, the liability exclusions and limitations in Section 10 above shall not apply.

13 Rights to Results

13.1 All copyrights and other Intellectual Property Rights to all works including concepts, documents and other results individually developed/prepared by the SUPPLIER for the CUSTOMER in the context of an Individual Agree-ment (“Results”) shall exclusively and without restrictions be accorded to the CUSTOMER.

13.2 If the SUPPLIER, in the context of rendering Services, supplies programs or documentation, which have been developed/prepared outside of the contractual relationship with the CUSTOMER (“External Results”), the SUP-PLIER or the concerned third party shall remain the owner of the copyright and other Intellectual Property Rights in such External Results, provided, however, the SUPPLIER has informed the CUSTOMER in advance about such External Results and has included them explicitly in the Individual Agreement; in such case, the CUSTOMER shall obtain a time unlimited, non-exclusive right to use the External Results as agreed in the Individual Agreement.

14 Information Duties

The SUPPLIER shall keep the CUSTOMER informed without delay concerning circumstances of any kind, which could substantially hinder the rendering of the Services irrespective of whether such lies within its own scope of responsibility, within the scope of the CUSTOMER or of a third party. Circumstances are excluded from this obligation of information, which are obviously known to the CUSTOMER.

15 Changes

15.1 During the term of an Individual Agreement, the CUSTOMER may require changes or additions in particular to the scope of the respective Services (“Changes”).

15.2 Requests for Changes (“Change Requests”) shall be submitted in writing to the Contact Person of the SUP-PLIER.

15.3 Change Requests by the CUSTOMER shall be reviewed by the SUPPLIER for any possible effects on Deliv-erables, deadlines/milestones, Personnel, cooperation duties, costs and other respects without delay, but not later than 5 working days after receipt of a Change Request.

15.4 If a Change Request has no effect on Deliverables, deadlines/milestones, Personnel, cooperation duties or costs, the SUPPLIER shall confirm the Change Request and realize it. Should the Change Request of the CUS-TOMER be considered by the SUPPLIER as not appropriate or suitable in a technical or other sense, in particular if such may even be detrimental to the contractual objectives, the SUPPLIER shall be obliged to inform the respective Contact Person of the CUSTOMER in writing and suggest alternatives, which in the opinion of the SUPPLIER have no negative effects within the term set forth in Section 15.3 above.

15.5 Also the Contact Person of the SUPPLIER can make Change Requests addressed to the Contact Person of the CUSTOMER. The Change Requests shall contain, in a binding matter, in particular information on any effects on Deliverables, deadlines/milestones, Personnel, cooperation duties or costs.

15.6 If, in the opinion of the SUPPLIER, the Change Request of the CUSTOMER may have an effect on Delivera-bles, deadlines/milestones, Personnel, cooperation duties or costs, such shall be notified to the CUSTOMER

within 5 working days under detailed and binding indication of the effect on Deliverables, deadlines/milestones, Personnel, cooperation duties and/or costs, together with a binding reasonable offer.

15.7 Work on a Change Request, for which a supplementary offer is required, may not be commenced until an agreement concerning the Change has been concluded or the CUSTOMER has in writing confirmed the Change offer of the SUPPLIER.

16 Cooperation of the CUSTOMER

16.1 Certain Services, in particular Project Services, require the cooperation/assistance of the CUSTOMER.
16.2 The CUSTOMER shall, as specifically agreed and specified in the respective Individual Agreement, assist the SUPPLIER at the location of the CUSTOMER, including the making available of necessary technical equipment and shall further make any agreed work space and resources available.

16.3 Details concerning cooperation tasks of the CUSTOMER shall be provided in the Individual Agreement.

16.4 Should the SUPPLIER be of the opinion that the CUSTOMER is not or not sufficiently complying with its duties of cooperation, such shall be reported by the SUPPLIER in writing and without delay to the respective Contact Person of the CUSTOMER. If the SUPPLIER fails to give immediate written notice of the – in its opinion – insufficient cooperation of the CUSTOMER, it can later not effectively rely thereon nor base claims (e.g. for additional remuneration) thereon nor can it use such as a defense (duty to warn).

17 Insurance

The SUPPLIER shall have and maintain business insurance coverage proportionately to the extent of the Individual Agreement and the risk entailed by rendering the Services and present to the CUSTOMER on demand the appropriate proofs of insurance prior to commencing the respective Services.

18 Term

18.1 The term of the Services, timelines and deadlines shall be agreed in the Individual Agreement.

18.2 If no fixed term is agreed, the contractual relationship can be terminated by either Party in writing under observation of a notice period of 6 months as of the end of each month. Irrespective thereof, if no fixed term is agreed, any Individual Agreement can be terminated for material reasons within the sphere of responsibility of the other Party (extraordinary termination). However, prior to an extraordinary termination, such must be threatened in writing and opportunity must be given to the other Party to cure such violation within a reasonable period of time.

18.3 In the case an Individual Agreement is terminated, SUPPLIER shall, upon request of the CUSTOMER, continue to perform the Services at the agreed prices after the termination so that the CUSTOMER is enabled to perform the respective services on its own or such services can be taken over/continued by another supplier. SUP-PLIER further undertakes to put CUSTOMER (with CUSTOMER´s assistance, and at CUSTOMER´s cost and expense) into a position in which CUSTOMER will be enabled (and where such enablement shall include the return of data, information and other auxiliary material) to fully perform the Services on its own (or to transfer such services to another supplier). The maximum duration of the post-termination support shall be 180 days.

19 Governing Law, Arbitration

19.1 All disputes or claims arising out of or in connection with these GCC or an Individual Agreement, including disputes related to its violation, breach, termination or nullity shall be subject to the final jurisdiction the competent court in Vienna, Innere Stadt.

19.2 The substantive Austrian laws under exclusion of its conflicts-of-law provisions and under exclusion of the United Nation Convention on Contracts for the International Sale of Goods shall be applicable to these GCC and to any Individual Agreements, unless expressly provided otherwise in writing.

20 Final general provisions

20.1 No omission, delay or forbearance on the part of a Party in enforcing any right or remedy arising in connection with an Individual Agreement shall be construed or operate as waiver of either that or any other right or remedy.

20.2 Unless otherwise required by an Individual Agreement or mandatory Applicable Law, the SUPPLIER may not assign or transfer any rights or obligations under the Individual Agreement without the prior written consent of the CUSTOMER, which shall not be unreasonably withheld. The CUSTOMER may transfer the Individual Agreement fully or partly to another member of the Group.

20.3 The invalidity of any individual provision hereof or of an Individual Agreement shall not lead to the invalidity of the these GCC or of the entire Individual Agreement. The invalid provision shall be replaced by a valid and enforce-able provision, which approximates the invalid provision as closely as possible.

20.4 Any modifications or amendments to these GCC or to any Individual Agreement must be in the written form, this also applies to any waiver of the written form.

20.5 SUPPLIER is only entitled to use the CUSTOMER´s name and the Services subject to an Individual Agreement as reference in its marketing activities, if and to the extent the CUSTOMER has explicitly agreed thereto in writing.

21 DEFINITIONS

Acceptance: Rules and procedures as described in Section 9 above.

Affiliate: Any legal entity that directly or indirectly through one or more intermediaries controls a party, or is controlled by a party, or is under common control of a party. For the purpose of this definition, the term “control” shall be understood as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of a legal entity, whether through the ownership of voting stock, by contract or otherwise.

Applicable Law: The laws governing these GCC and any Individual Agreement.

Change and Change Request shall have the meaning as described in Section 15 above.

Code of Conduct: The Code of Conduct of the CUSTOMER.

Commonly Acknowledged Industry Standards: Practices, methods and procedures which are established or recognized industry standards for provision of Services in the banking industry, as modified from time to time.

Compliance, Security and Data Protection Rules/Compliance Rules and Policies/Data Protection and Security Standards: The respective rules of the CUSTOMER, which may be amended from time to time.

Confidential Information: All information relating to the other Party´s trade and business secrets and information and documentation regarding such Party´s business or information to the Individual Agreement whether technical or commercial, including without limitation all specifications, drawings, designs and computer software or other information disclosed or otherwise acquired by the Parties which is in a tangible, oral or visible form and/or clearly marked or designated in writing by the disclosing Party as being confidential or which an experienced business person would consider as confidential or any information, which is to be treated confidential pursuant to Applicable Law, Regulatory Provisions or standards in the banking industry.

Contact Person: A person nominated by a Party to contact or be contacted (by) the other Party in a specific context, for example the Project Managers.

Deliverable: A tangible or intangible but verifiable work, product or other result that must be produced to complete a process, Project or Service pursuant to an Individual Agreement.

Force Majeure: Any event, in which a Party´s performance of any of its obligations under an Individual Agreement is prevented, hindered or delayed directly or indirectly by fire, flood, earthquake, elements of nature, acts of war, terrorism, riots, civil disorders, strikes, power outages, rebellions, pandemic, or any similar cause beyond the rea-sonable control of such Party.

GCC: These General Contractual Conditions.

Goods: Any tangible products.

Group/Raiffeisen Group/Raiffeisen Group Members: All Affiliates and any legal entity

(i) that is a member of the Oesterreichischer Raiffeisenverband;
(ii) that is audited by a Raiffeisen Revisionsverband;
(iii) that is authorized to use the “Raiffeisen” trademark;
(iv) in which a Raiffeisen Group Member as per subsections (i), (ii) or (iii) above solely or together with one or more other Raiffeisen Group Members per subsections (i), (ii) or (iii) above jointly controls the majority of either the shares or the voting rights;
(v) that has control over the majority of the shares or the voting rights of a Raiffeisen Group Member as per subsections (i), (ii) or (iii) above; or
(vi) that is provided with IT services by a Raiffeisen Group Member as per subsections (i) to (v) above on a service bureau basis (e.g. Raiffeisen Informatik GmbH & Co KG, RAITEC GmbH). Raiffeisen

Group Members as per this subsection (vi) may use the software as part of the provided IT services. Raiffeisen Group Members acting as service bureau may use the software also for the internal business purposes of Raiffeisen Group Members as per this subsection (vi).

Individual Agreement: An agreement concluded between the SUPPLIER and the CUSTOMER which governs the cooperation between the Parties under these GCC. The basis of Individual Agreements can also be purchase orders issued, with reference to these GCC or a frame contract based on these GCC by CUSTOMER's ordering system; such purchase orders do not require a signature in order to become effective.

Intellectual Property Rights: Any patents, trademarks, copyrights or other intellectual property rights.

Individual Software: Any modifications and enhancements of Standard Software code and any software code individually developed for the CUSTOMER (as opposed to Standard Software including customizations such as parametrizations).

Material Defect: Defect(s) materially preventing/hindering the use of the Services by the CUSTOMER, with respect to Software Critical and/or Serious Defects as described in Chapter D are considered as Material Defects.

Party or Parties: The contractual parties as specified in an Individual Agreement

Personnel: The employees or other individuals engaged in the performance of Services.

Project: The supply of works and Services connected therewith.

Project Manager: The person(s) nominated by the Party as responsible for the management of a Project.

Project Services: Services, the object of which are work contracts.

Regulatory Requirements: Any lawful requirement, order or demand, as amended from time to time, of any competent authority.

Services: The Goods, Deliverables and services to be delivered/performed by the SUPPLIER under an Individual Agreement.

Software: Software, which is the object of an Individual Agreement.

Standard Software: Software, which is made available to a substantial number of CUSTOMERs.

Subcontractors: Any subcontractors engaged by the SUPPLIER for the performance of Services.

Third Party Licensor: Producers or third parties copyright owners of Software.

B) SPECIAL CONDITIONS FOR SOFTWARE LICENSING (STANDARD SOFTWARE)

1 Subject Matter

1.1 This Chapter B) governs the licensing of Standard Software by the SUPPLIER to the CUSTOMER and Raiffeisen Group Members as agreed in an Individual Agreement. The producer/owner and the description of the Standard Software, the scope of the license, the use environment and the use conditions for the Standard Software, as well as other special conditions shall be provided in the respective Individual Agreement.

1.2 These GCC apply both to Standard Software, of which the SUPPLIER is the producer or owner, as well as to Third-Party Software. If the SUPPLIER is not the producer or owner of the Standard Software (Third-Party Software), the SUPPLIER shall acquire a non-exclusive right of use (as specified in an Individual Agreement) for the CUSTOMER from the producer/owner or from the Third-Party Licensor as set forth in the Individual Agreement.

1.3 Unless agreed differently in an Individual Agreement, the Standard Software shall be supplied in machine code (object code) in the version current at the time of the conclusion of the Individual Agreement, together with the documentation generally made available by the SUPPLIER to its customers.

1.4 The SUPPLIER shall supply the Standard Software at the place of delivery agreed in an Individual Agreement or make it available by download. The supply shall be undertaken up to the date agreed in the Individual Agreement. The relevant point in time in respect of meeting potentially scheduled delivery dates is the point in time when the Software has been made available for electronic download by the SUPPLIER and the CUSTOMER

has received the information of such availability together with a download link including the required access data ("Delivery").

2 Copyright/Kind of License

2.1 The CUSTOMER acknowledges that all rights to the Standard Software, in particular the encompassing copyrights, patent rights and other Intellectual Property Rights together with all ancillary rights to all programs and documentation made available to the CUSTOMER under these GCC shall belong to the SUPPLIER, to the producer of the Standard Software or to the Third-Party Licensor; the CUSTOMER shall only have the right to the use of the Standard Software as defined in an Individual Agreement including these GCC.

2.2 SUPPLIER grants to the CUSTOMER and Raiffeisen Group Members a non-exclusive right to use the Standard Software in the contractually agreed scope either against a one-time payment for an unlimited perpetual term (= License Purchase) or for a limited term with the possibility of termination (= Rental License or SaaS). It shall be agreed in the Individual Agreement whether the license is acquired on a purchase or on a rental basis. The right to use shall begin with the date provided in the Individual Agreement, in the absence thereof with the Delivery.

2.3 The right to use Standard Software, which the CUSTOMER receives in the context of remedy (corrections) or maintenance, shall commence at such time, in which the CUSTOMER processes such on a CPU, or has received access to it via a SaaS or a cloud model.

2.4 The CUSTOMER shall use the programs only in the agreed use environment (e.g. CPU, place of installation, SaaS environment, etc.) and only within the scope of the agreed use conditions (e.g. named users, number of concurrent users, etc.). The use environment and use conditions shall be provided in the respective Individual Agreement. The use environment may be changed by the CUSTOMER at no additional cost, provided that the scope of the agreed use conditions (e.g. number of users) is complied with.

2.5 The Standard Software may only be used by the CUSTOMER and Raiffeisen Group Members for its own purposes and/or for the purposes of members of the Group. In addition, the use of the Standard Software in an external data center for the CUSTOMER or a member of the Group by a third-party provider (outsourcing) is permissible.

2.6 The CUSTOMER may use the Standard Software pursuant to the mandatory provisions of § 40 d Austrian Copyright Act.

2.7 Any re-translation of the Software into any other form of code (decompilation) and any reconstruction of its various manufacturing stages (e.g. by reverse engineering or disassembling) are only permissible, if such measures are indispensable to achieve interoperability with other independently created computer programs, and if the necessary interface information has not been published by the SUPPLIER or if the CUSTOMER cannot easily obtain such information without delay in another way (e.g. from the user documentation or by requesting it from the SUPPLIER).

2.8 The granting of sublicenses of the Standard Software is not permissible, except to members of the Group, without the express consent from the SUPPLIER.

2.9 Irrespective of the reason for the termination of a license, upon the ending thereof the CUSTOMER must return all copies of the Standard Software to the SUPPLIER or must destroy them upon request of the SUPPLIER. In such case, the CUSTOMER is obliged to cease all use of the Standard Software. Excluded from the obligation to destroy/delete is the retention of an archive copy to be retained according to legal provisions for the legally required term, which, however, may no longer be put into productive use by the CUSTOMER. Upon request of the SUPPLIER the CUSTOMER shall confirm in writing to the SUPPLIER that the above measures have been undertaken.

2.10 If the CUSTOMER receives Updates or Upgrades of the Standard Software, for example in the context of maintenance, for such new software versions the same license rights and provisions shall apply as for the original Standard Software.

2.11 In order to secure the further correction, enhancement and maintenance of the Standard Software, in case of insolvency and similar proceedings concerning the SUPPLIER or in case that the SUPPLIER discontinues the further development and maintenance services ("Release Events"), the SUPPLIER shall within three months following the first Delivery of the respective Standard Software, make available the Standard Software source code including any reasonably required development and technical documentation to the escrow agent nominated by the CUSTOMER according to its standard deposit conditions so that in case a Release Event occurs the escrow agent is obliged to immediately provide the CUSTOMER with the complete and actual source code and documentation. Details may be specified in the Individual Agreement. This depositing and/or handing over shall be repeated together with each delivery of a new version of the Standard Software, however no more than once every six calendar months.

2.12 The SUPPLIER and its Subcontractors are prohibited from furnishing the Software with any keys or other devices, which could prevent or hinder the CUSTOMERS from fully using the agreed Software.

3 License Fees/Payment Conditions

3.1 The license fee is the remuneration for the agreed use of the Software. The amount of the remuneration shall be agreed in the respective Individual Agreement.

3.2 In case of a License Purchase, the license fee does not include the maintenance fee, in case of a Rental License, the license fee includes both the remuneration for the use as well as the maintenance fee.

3.3 Unless agreed differently, in case of a License Purchase, the license fee shall be due for payment within 30 days after the conclusion of the Individual Agreement, the rental fee is due for payment quarterly in advance, for the first month within 30 days after the conclusion of the Individual Agreement.

4 Term and Termination

4.1 In case of a License Purchase, the respective right of usage is granted for an unlimited and perpetual term.

4.2 In case of a Rental License, the term of the rental (license term) including, if any, the notice period for ordinary termination, shall be specified in the Individual Agreement. Any termination of a license for cause shall be only permitted in the event of a material violation of the provisions of the respective Individual Agreement concerning the license rights, which have been caused by the CUSTOMER by gross negligence or intent. Prior to the extraordinary termination of any such rights, such must be threatened by the SUPPLIER in writing and opportunity must be given to cure such violation within a reasonable time period.

C) SPECIAL CONDITIONS FOR SOFTWARE LICENSING (INDIVIDUAL SOFTWARE)

1 Subject Matter

This Chapter C) governs Individual Software.

2 Rights in Individual Software

2.1 Unless explicitly agreed otherwise in an Individual Agreement, all copyrights, patent- and other Intellectual Property Rights in Individual Software including the source codes and the respective documentation belong to the CUSTOMER/are granted by the SUPPLIER to the CUSTOMER. The CUSTOMER therefore has the exclusive and unlimited right to use, transfer, modify and exploit the Individual Software without restrictions.

2.2 The SUPPLIER shall be prohibited to use, transfer or otherwise exploit any Individual Software without the express prior written consent of the CUSTOMER.

2.3 However, the SUPPLIER is permitted to use pre-existing know-how for other customers and projects, which the SUPPLIER has used in connection with the development of the Individual Software.

2.4 The remuneration for the development of Individual Software shall be agreed in the respective Individual Agreement.

D) SPECIAL CONDITIONS FOR MAINTENANCE OF STANDARD SOFTWARE AND INDIVIDUAL SOFTWARE

1 Subject Matter (Standard Software Maintenance)

Sections 1 to 5 govern the maintenance of Standard Software including customizations, which are not Individual Software. Unless expressly agreed differently in the Individual Agreement, in case of a License Purchase, the maintenance of Standard Software shall be offered to the CUSTOMER separately from the granting of rights to use the Standard Software (license), it shall not be part of the grant of rights to use the Software. However, in case of a Rental License including SaaS, the Software maintenance is an integral part of the software license.

2 Scope of Maintenance (Standard Software)
2.1 If provided for in the respective Individual Agreement, the Software shall be maintained by the SUPPLIER. The scope of maintenance and the service levels shall be included in the respective Individual Agreement. Unless agreed otherwise in an Individual Agreement, maintenance includes the following services:

2.1.1 Corrective maintenance: The SUPPLIER shall correct defects in the Standard Software.
Defects are classified into 3 categories as follows:
(i) Critical (Category 1):
- one or more core functionalities are not working and no workaround is available (e.g. payments cannot be received, account reporting is not available)
- defects, which prevent the CUSTOMER and/or the concerned Group Members communicating with its customers.
- defects, which prevent data from being received by CUSTOMER and/or its Group Members, or a digital signature cannot be generated.
- serious malfunction causing loss or corruption of data
- substantial impact on performance, resulting in CUSTOMERS and/or the its Group Members being unable to work with the system
- Functionality causing serious overload of system
- Security issues and potential threats (e.g. a customer is able to see/download data of another client)

(ii) Serious (Category 2):
- one or more core functionalities are not working but an easy, well-documented, already available worka-round is available (e.g. executing some additional steps which allow payments to be received, account reporting is available after executing some additional steps)
- individual functional areas cannot be used, and no workaround is available (e.g. display of payment files for authorization is not working, statement information cannot be exported); and

(iii) Minor (Category 3):
- there are specific errors in individual functions, which do not affect the proper functioning of the functional area or the system as a whole (e.g. a field check for valid characters is not implemented, a reference field for a transaction is not correctly displayed)
- misspellings and cosmetics
- these include by default any minor faults or incompletion in non-functional components (training, layouts, etc.)
- issues causing small annoyances without a need for workaround

The relevance of these defect categories, for example in connection with Service Levels, is in particular set out in the Individual Agreement.

2.1.2 First Level Support: Within the agreed service times, the SUPPLIER shall in the context of the First-Level Support be available to the persons nominated by the CUSTOMER by telephone or remote for consultation in case of problems arising in connection with the use of the respective Standard Software. The specifics (e.g. the nomi-nated persons, any technical or organizational prerequisites to be created by the CUSTOMER, the service levels such as the reaction times, etc.) shall be set forth in the respective Individual Agreement. If the completion of a training for the nominated users to be provided by the SUPPLIER is a prerequisite for the use of First Level Support, such shall be specified in the respective Individual Agreement. The Parties may agree in the Individual Agreement that the First Level Support is undertaken by the CUSTOMER.

2.1.3 Second Level Support: In case of technical error messages and system errors in connection with the use of the Standard Software, or problems, which the First Level Support cannot solve, the SUPPLIER shall be available to the persons nominated by the CUSTOMER within the agreed service times in the context of Second Level Sup-port by telephone or remotely (e.g. via a ticket system). The nominated persons of the CUSTOMER, which shall be the contact persons for the SUPPLIER in the context of Second Level Support, the service levels such as the reaction and repair times and other specifics (e.g. the technical or organizational prerequisites to be created by the CUSTOMER) shall be set forth in the Individual Agreement. If the completion of a training for the nominated persons to be provided by the SUPPLIER is a prerequisite for the use of Second Level Support, such shall be specified in the respective Individual Agreement.

2.1.4 Update Service: The SUPPLIER shall regularly improve its Software and make available Updates and Up-grades to its customers including the CUSTOMER. Subject to the Update Service is the making available and installation of Updates and Upgrades, which are generally made available to the customers of the SUPPLIER in the context of maintenance by the SUPPLIER during the term of maintenance. Formerly agreed/included function-alities and features must not be deleted by the SUPPLIER (or the relevant third party) in Updates or Upgrades. The SUPPLIER declares that the installation of new Updates or Upgrades do not require substantial modifications of the IT-systems, on which the Software is permitted to run.

2.1.5 Troubleshooting on Location: If a problem cannot be solved by telephone or remotely, then the SUPPLIER shall render the required services at the use environment of the CUSTOMER, which service is included in the respective maintenance fees.

2.1.6 Regulatory Maintenance: Any modifications required to ensure that the Standard Software complies during the maintenance term with current Applicable Law and Regulatory Requirements in the jurisdictions in which the Software is agreed to be used. Such modifications shall be provided by the SUPPLIER within a reasonably period

of time and are included in the scope of maintenance and in the regular maintenance fees. The SUPPLIER is obliged to inform itself about any relevant amendments of Applicable Law and Regulatory Requirements.

2.2 Which of the above maintenance services (2.1.1 to 2.1.6) are available to the CUSTOMER shall be set forth in the respective Individual Agreement.

2.3 The CUSTOMER is under no obligation to accept and install Updates or Upgrades provided by the SUPPLIER in the context of maintenance.

2.4 Any increased efforts/expenditures for the maintenance of Standard Software shall be excluded from maintenance and shall be paid additionally in accordance with the agreed rates of remuneration and expenses, if such have become necessary due to use beyond the contractually agreed scope or manner, by a use environment different than contractually agreed, incorrect usage, or for other reasons falling within the scope of responsibility of the CUSTOMER, further for work on Software, which the CUSTOMER has itself altered or which has been maintained by persons other than SUPPLIER's technicians without prior written consent of SUPPLIER ("Events"). The SUPPLIER has the obligation to prove that an Event occurred and has caused additional costs.

2.5 If Third-Party Software shall be included in the maintenance the conditions with respect to maintenance shall also apply for Third-Party Software.

3 Service Levels (Standard Software)/Penalties (Service Credits)

3.1 At least the following categories of service levels shall be included and specified in the respective Individual Agreement: (i) Service Times, (ii) Availabilities, (iii) Reaction Times, and (iv) Repair Times.

3.2 The specifics concerning service levels (each also including rules concerning measurement of the service level and the reporting thereof as well as Service Credits/penalties in case of non-compliance) shall be included in the respective Individual Agreement.

4 Maintenance Fees (Standard Software)

4.1 The maintenance fee is the remuneration for the agreed maintenance of the Software. The amount of the fees for the Services described in 2.1 shall be agreed in the respective Individual Agreement.

4.2 The maintenance fees shall be due for payment at the beginning of each maintenance year/month, for the first time with the Delivery, in case of a License Purchase independent of the license fees.

5 Maintenance Term and Termination (Standard Software)

5.1 The agreement concerning maintenance – in case of a License Purchase independent of the software license, in case of a Rental License together with the software license – is concluded for an indefinite term; however, in the Individual Agreement also a fixed term can be agreed. To the extent no fixed term is agreed, the maintenance relationship can be terminated by either of the Parties in writing under observation of a notice period of 6 months as of the end of any calendar year. The SUPPLIER waives its right to terminate the agreement concerning maintenance for a period of five years, beginning with the conclusion of the respective Individual Agreement. In case of a Rental License, this shall also apply to the license grant, which is inseparable from maintenance.

5.2 Irrespective of 5.1 above an agreement concerning maintenance can be terminated with immediate effect by either Party for material reasons within the sphere of responsibility of the other party, in case of a Rental License together with the right of use (license). Any repeated violation of material contractual provisions shall be considered as material reason, which entitle the concerned Party to contract termination with immediate effect. However, prior to any extraordinary termination, such must be threatened in writing and opportunity must be given to the other Party to cure such violation within a reasonable time period.

5.3 The commencement date of maintenance shall be set forth in the Individual Agreement.

6 Maintenance (Individual Software)

6.1 If all or any of the Services provided for in Section 2 are agreed in an Individual Agreement in connection with Individual Software, the applicable provisions of Sections 2, 3 and 5 above shall also apply to these services, respectively, unless agreed otherwise in the respective Individual Agreement.

6.2 The fees for the maintenance of Individual Software shall be agreed in the respective Individual Agreement.

7. Additional Definitions

Update: A new program version of the Standard Software including the remedy of defects as well as minor modifications and enhancements of Standard Software.

Upgrade: A new program version of the Standard Software including substantial modifications and enhancements of the Standard Software, which are generally made available to the customers.

F I N A N C I A L S E R V I C E S

Supplemental Agreement

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 Raiffeisen Group Members ("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.

2) 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 Customer's "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.

3) Locations

The Service Provider shall provide the Services to the Customer and its Affiliates 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.

4) 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.

5) 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.

6) 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.

7) 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.

8) 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.

9) 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.

10) 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.

11) 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).

12) 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 4

RAIFFEISEN
CODE OF CONDUCT for SUPPLIERS

(RI-C version 2.0_Oct24 - hereinafter referred to as "CoC")

INTRODUCTION

Based on our core values addressing business ethics, social and environmental commitments, we require our Suppliers to adhere to the hereafter listed principles (as defined below) which will apply to any contract entered between us and Suppliers (the "Contract"). The CoC shall apply to all Suppliers that deliver goods, services or licenses to or on behalf of any Raiffeisen business units and subsidiaries. The Supplier shall do its utmost to implement these principles throughout its whole supply chain This CoC is not intended to replace the laws and regulations in force in any country where Raiffeisen operates. It seeks to respect these laws and regulations and ensures that they are faithfully and effectively applied. The Supplier shall interact honestly, transparently and with mutual appreciation with Raiffeisen and its representatives.

THE PRINCIPLES

1. Economic Sanctions and Embargoes

In addition to the following provisions as detailed in sections 1 to 7 below, the Supplier shall check potentially applicable economic sanctions and embargoes [especially, but not limited to the laws and regulations of the European Union and any European Authority (e.g. European Banking Authority, European Central Bank, Single Resolution Board)] and avoid anything in relation to the business relationship with us which might finally result in a breach of sanctions or embargoes by us.

2. Underlying Principles

The Supplier shall respect international climate targets as defined in the UN Climate Change Conference in Paris (COP21), internationally proclaimed human rights and shall avoid being complicit in human rights abuses of any kind. The Supplier shall adhere to the UN Guiding Principles on Business and Human Rights, the generally recognized standards drawn up by the International Labor Organization (ILO) and moreover the rules on the prohibition of forced labour. The personal dignity, privacy and rights of each individual shall be respected.

3. Social Responsibility Practices

3.1 Freedom of Association and Right to Collective Bargaining

The Supplier shall seek to implement internationally recognized standards without violating national legislation. It shall ensure that its employees and representatives including temporary (agency) workers may openly express themselves in their company concerning matters related to their working conditions.

3.2 Child Labour

Child labour as defined by ILO-IPEC and Article 32 of the United Nations Convention on the Rights of the Child (UNCRC) is strictly prohibited. If any child is found working in violation of the above expressed

principles at the premises of the Supplier, the Supplier shall immediately take steps to redress the situation in accordance with the best interests of the child.

3.3. Modern Slavery and Human Trafficking
The Supplier shall not tolerate forced labour in particular abstaining from any forms of modern slavery and human trafficking.

3.4 Diversity and non-discrimination
The Supplier shall prohibit and combat any discrimination based on factors such as gender, race, color, ethnic origin, social/economic class, sexual orientation or gender identity, language, religion or belief, political opinion, nationality, place of birth, migration, health condition, disability or age. The Supplier shall promote diversity, equality of opportunity, and equitable treatment in employment and occupation. All employees must be treated with respect, and the use of corporal punishment, mental or physical coercion, any form of abuse or harassment is strictly prohibited.

3.5 Remuneration
The Supplier shall provide remuneration according to national legal standard on minimum wage and avoid any wage deductions as disciplinary measure. Where no national legal standards exist, the remuneration shall be sufficient to meet basic needs (ILO C131 – Minimum Wage Fixing Convention).

3.6 Working Hours
Working hours, including overtime, shall comply with applicable local laws. Where no national legal standards exist, ILO standards shall apply.

3.7 Occupational Health and Safety
The Supplier shall provide its workers with a safe and healthy workplace and should implement effective programs to – where necessary – improve the working environment. The Supplier shall do its utmost to control hazards and take necessary precautionary measures against accidents and occupational diseases. The Supplier is encouraged to implement a Health & Safety Management System based on international standards such as OHSAS 18001 or similar.

3.8 Affected Communities
The Supplier shall take into consideration its impacts on the groups potentially affected by its operations (affected communities and if applicable, indigenous peoples) in relation to their rights to adequate housing, adequate food, land-related and security-related impacts, freedom of expression as well as freedom of assembly.

4. Environmental Responsibility Practices

4.1 Environmental Protection
The Supplier shall act in accordance with relevant local and internationally recognized environmental standards and applicable local laws, whereby the highest standard shall be applied especially including ROHS (Restriction of Hazardous Substances) and WEEE (Waste from Electrical and Electronic Equipment). The Supplier shall minimize its environmental impact and should implement measures contributing to the protection of the environment.

RBI expects the Supplier to follow the rules of circular economy during the whole product life cycle: conception, development, production, transport, use and disposal and/or recycling. The Supplier shall minimize or strive to avoid hazardous air emissions, energy consumption and CO2 emissions. In particular, the Supplier shall develop products and services that feature low energy consumption and CO2 emission reduction during the whole life cycle.

4.2 Waste- and Resource-Management

The Supplier shall limit the use of materials and resources when sourcing or producing goods in order to minimize its environmental impact. The Supplier is encouraged to track the source of conflict minerals, to promote transparency along its own supply chain and to put in place measures for this purpose. The use of rare resources shall be limited or avoided where possible. The waste produced by all its activities shall be identified, monitored and managed. The Supplier shall strive to reduce the waste. Waste treatment shall be in accordance with applicable environmental laws.

5. Business Integrity

5.1 Anti-Corruption and Financial Crime Principles

The Supplier shall refrain from any form of corruption or financial crime actions that could potentially be construed as such. The Supplier shall be aware of any applicable laws (especially, but not limited to the US Foreign Corrupt Practices Act, the UK Bribery Act) and avoid anything in relation to the business relationship with Raiffeisen which might finally result in a breach of law by Raiffeisen.

Any potential or existing conflict of interest (e.g. close relationship, supplementary job) between supplier/ supplier employees and Raiffeisen must be disclosed immediately to us via the established communication channels.

The Supplier may not offer, promise or grant illegal benefits to national or international public officials or decision-makers operating in the private sector including but not limited to bank representatives in order to achieve a preferential treatment or favorable decision; same applies when dealing with donations, gifts or invitations to business meals and events.

The Supplier may not allow itself to be promised or offered advantages and shall not accept the same if this may or shall create the appearance to the party bestowing the advantages that it can thus be influenced in business decisions. Likewise, the Supplier may not request advantages.

In order to ensure compliance with the Code for the duration of the Contract, Supplier shall provide on demand and at all time to us all elements requested to establish such compliance, and shall inform us, without delay, when it knows or has reason to know, of any failure to comply with the Rules by itself or any Third Party, as well as the corrective measures adopted to ensure compliance with the Rules.

A material non-compliance with the Rules may trigger a termination right of the Contract in accordance with its provisions.

5.2 Free Competition Principle

The Supplier shall respect the rules of free and fair competition in all business relation, in particular not act against any competition and/or antitrust law. The Supplier does not take part in any collusive

conduct, does not exchange or disclose any information with any third party related to any planned, running or pending procurement of Raiffeisen.

5.3 Sponsorship Principle
All sponsoring measures by the Supplier must be in accordance with applicable local (national) legislation.

5.4 Political Contributions Principle
The Supplier shall only donate money or grant any monetary benefits to any political party within regulation by local (national) law and in compliance with the local (national) law.

5.5 Anti Money Laundering and Counter Terrorist-Financing Principle
Raiffeisen is committed to fully comply with all applicable EU directives and local (national) legislation. We reject doing business in a way that assists or facilitates tax evasion by our Suppliers or other third parties. We consider our Suppliers as an important pillar in our money laundering prevention and counter terrorist-financing efforts and expect as such that the Supplier shall take all measures to prevent money laundering and terrorist financing within its sphere of influence. For Suppliers that are legally obligated to implement such policies and procedures, the Supplier shall do so in full and adhere to such laws as amended from time to time.

5.6 Intellectual Property, Data Security and Data Protection
The Supplier shall comply with the Non-Disclosure Agreement (or similar) concluded with us and adhere to all applicable intellectual property and data protection laws and all specific data protection and security requirements agreed to in the Contract.

6. Sub-contracting

Supplier shall with best effort try to bind its contractors and/or subcontractors (hereinafter referred to as “Subcontractors”) to the Principles of this CoC insofar as they are involved in substantial provisioning deliverables under the Contract. The Supplier shall with best efforts refrain from unreasonable usage of subcontractors or any third parties for services under the Contract to evade applicable legal requirements and any of the standards set in the CoC.

The Supplier shall ensure that its suppliers undertake to:
- Promote and ensure compliance with the principles of this CoC by their suppliers and subcontractors
- Implement a monitoring system enabling them to prevent and deal with any risk having an environmental and/or social impact across the whole supply chain.

7. Compliance, Monitoring and Audits

It is recommended, that the Supplier appoints a responsible person with the necessary mandate and resources to implement and follow up provisions of this CoC (including, e.g. ensuring that its employees understand and comply with these standards and monitoring its operation regularly to ensure compliance with the Code.)

We might audit the Supplier’s and in some cases subcontractors’ compliance with the CoC and the information given by the Supplier. If the Supplier or subcontractors are in breach of the CoC, we will initiate a dialogue and is entitled to require an implementation plan for improvements that will bring the Supplier and/or subcontractor back into full compliance with the CoC.

A material non-compliance with the principles of the Code by the Supplier triggers a termination right of the Contract in accordance with its provisions, initiated by direct contractual Party of the Supplier.

The Supplier is solely responsible for any expenses incurred for complying with the CoC. The Supplier should proactively report to us as the direct contractual Party of the Supplier any deviation from the Code.

Supplier is entitled to use the Whistleblower-Hotline from Raiffeisen Informatik GmbH & Co KG https://raiffeiseninformatik.integrityline.com or email to compliance@ri-c.at.

ANNEX 5

Security Requirements for Suppliers

RI-C version v1.5

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:
    a. Contact information of SUPPLIER incident responsible
    b. What occurred
    c. How occurred
    d. Why occurred
    e. Components/assets affected
    f. CUSTOMER services/data affected
    g. Date and time the incident occurred
    h. Date and time the incident was discovered
    i. Business impact/effect for CUSTOMER services/data
    j. Incident resolution
    k. Action taken to resolve incident
    l. Action planned to resolve incident
(3) use reasonable efforts to avoid and detect such incidents in future;
(4) regularly update the CUSTOMER of the measures the SUPPLIER is taking or intends to take; and
(5) 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:

AGREEMENT ON ORDER PROCESSING IN ACCORDANCE WITH ARTICLE 28 GDPR

entered into by and between

Raiffeisen Informatik Consulting GmbH

Lilienbrunngasse 7-9

A-1020 Vienna

(hereinafter referred to as "**Client**")

and

.....

.....

(hereinafter referred to as the "**Processor**" or the "**Supplier**")

as follows:

1. Subject matter and duration of the Order or Contract

The subject matter and duration (term) of the Order or Contract are defined in Appendix 2.

2. Specification of the Order or Contract details

(1) The nature and the purpose of processing of personal data by the Supplier for the Client are stated in Appendix 2.

The undertaking of the contractually agreed processing of data shall be carried out exclusively within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA). Each and every transfer of data to a state which is not a Member State of either the EU or the EEA requires the prior agreement of the Client and shall only occur if the specific conditions of Article 44 *et seq.* GDPR have been fulfilled and if an adequate level of protection has been established by means of an adequacy decision by the Commission (Art 45 GDPR) or by means of binding corporate rules (Art 46 Paragraph 2 Point b in conjunction with Art 47 GDPR), standard data protection clauses (Art 46 Paragraph 2 Point c and d GDPR), approved codes of conduct (Art 46 Paragraph 2 Point e in conjunction with Art 40 GDPR), an approved certification mechanism (Art 46 Paragraph 2 Point f in conjunction with Art 42 GDPR), other measures like contract clauses approved by the data protection authority (Art 46 Paragraph 2 Point a, Paragraph 3 Point a and b GDPR) or derogations for specific situations as defined in Art 49 Paragraph 1 GDPR.

(2) The type of personal data used and the categories of data subjects are defined in Appendix 2.

3. Technical and Organisational Measures

(1) Before the commencement of processing, the Supplier shall document the execution of the necessary technical and organisational measures, as set out in advance of the awarding of the Order or Contract according to Appendix 1, specifically with regard to the detailed execution of the order, and shall present these documented measures to the Client for inspection. Insofar as the inspection/audit by the Client shows the need for amendments, such amendments shall be implemented by mutual agreement.

(2) The Supplier shall establish the security in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and

resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR must be taken into account (details in Appendix 1).

(3) The technical and organisational measures are subject to technical progress and further development. In this respect, it is permissible for the Supplier to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

4. Data processing only on order of the Client

(1) The Supplier and any person acting under its authority who has access to personal data, shall not process the personal data without documented orders or instructions from the Client including the powers granted in this contract, unless the Supplier is required by law to process the personal data .

(2) The Supplier may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Client, but only on documented instructions from the Client. Insofar as a data subject contacts the Supplier directly concerning a rectification, erasure, or restriction of processing, the Supplier will immediately forward the data subject's request to the Client.

(3) In case the Supplier is ordered by a competent authority to disclose personal data of the Client, the Supplier must immediately inform the Client thereof, as far as this legally permissible, and refer the authority to the Client. Further, any processing of the data by the Supplier for its own purposes requires a written instruction by the Client.

5. Quality assurance and other duties of the Supplier

In addition to complying with the rules set out in this Order or Contract, the Supplier shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, the Supplier ensures, in particular, compliance with the following requirements:

(a) written appointment of a data protection officer, who performs his/her duties in compliance with Articles 38 and 39 GDPR. His/her contact details are stated in Appendix 2. The Client shall be informed immediately of any change of data protection officer or of his/her contact details. In case, the Supplier does not have a data protection officer, the Supplier will provide the Client with a written explanation for that.

(b) designation of a representative as laid down in Art 27 Paragraph 1 GDPR in the European Union, if the Supplier is established outside the European Union.

(c) confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR. The Supplier entrusts only such employees with the data processing who have been bound to confidentiality or who are subject to an appropriate statutory obligation of confidentiality. In particular, the obligation of confidentiality of the person in charge of data processing shall continue after they stop working for and leave the Supplier.
(d) implementation of and compliance with all technical and organisational measures necessary for this Order or Contract in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR (details in Appendix 1).
(e) The Client and the Supplier shall cooperate, on request, with the supervisory authority in performance of its tasks.
(f) The Supplier shall inform the Client immediately of any inspections or measures by the supervisory authority, insofar as they relate to this Order or Contract. This also applies if the Supplier is under investigation by a competent authority in connection with an administrative offence procedure or a criminal procedure regarding the processing of personal data in connection with under this Order or Contract.
(g) In case the Client is subject to an inspection by the supervisory authority, an administrative offence procedure, a criminal procedure, a liability claim by a data subject or by a third party or any other claim in connection with the Order or Contract data processing by the Supplier, the Supplier shall make every effort to support the Client.
(h) documentation and proof of the technical and organisational measures by the Supplier vis-a-vis the Client as part of the Client's supervisory powers referred to in item 7 of this contract.
(i) The Supplier is advised that it has to establish records of processing activities as laid down in Art 30 GDPR for order processing under this Agreement. In case, the Supplier does not have records of processing activities established, the Supplier will provide the Client with a written explanation for that.

6. Subcontracting

(1) Subcontracting for the purpose of this regulation is to be understood as meaning services which the Supplier does not render itself but for which it instructs another processor ("Subcontractor") and which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The Supplier shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Client's data, even in the case of outsourced ancillary services.

(2) The Supplier may commission Subcontractors (additional processors) only after prior explicit written or documented consent by the Client in compliance with Appendix 2 (7). The Client shall be notified of an intended instruction of a Sub-processor in due time. It must be ensured that the Sub-processor will assume the same obligations as those to which the Supplier is subject due to under this contract. If the Subcontractor fails to fulfil its data protection obligations, the Supplier shall be liable vis-à-vis the Client for compliance with the obligations of the subcontractor.

(3) The transfer of personal data from the Client to the Subcontractor and the Subcontractor's commencement of the data processing shall only be undertaken after compliance with all requirements for the subcontracting has been achieved.

(4) If the subcontractor provides the agreed service outside the EU/EEA, the Supplier shall ensure compliance with EU Data Protection Regulations by appropriate measures. The same applies if service providers are to be used within the meaning of Paragraph 1 Sentence 2.

7. Supervisory powers of the Client

(1) The Client has the right to carry out inspections and audits of the data processing systems of the Supplier. The Client may also authorise other persons to perform such inspection or audit. The Supplier may object the selection of such authorised persons in case of reasonable grounds relating to the person of the selected authorised person.

In case of similar order processing activities for several Clients, the Supplier allows audits by auditors instructed by such Clients jointly, or – by request or with the consent of the Clients – instructs suitable audits (e.g. by internal auditors, external auditors, IT security auditors, data protection auditors, quality auditors) and provides the audit reports to the Clients, their auditors, and upon request to the supervisory authorities competent for the Clients.

(2) The Supplier shall ensure that the Client is able to verify compliance with the obligations of the Supplier in accordance with Article 28 GDPR and this contract. The Supplier undertakes to provide the Client with all information necessary for verification of the Supplier's compliance with its obligations, in particular the taking of the technical and organisatorial measures.

(3) Evidence of such measures, which concern not only the specific Order or Contract, may be provided by

- Compliance with approved Codes of Conduct pursuant to Article 40 GDPR;
- Certification according to an approved certification procedure in accordance with Article 42 GDPR; or

- current auditor's certificates or reports provided by independent bodies (auditor, IT security auditors, data privacy auditor, quality auditor).

8. Assistance obligation of the Supplier

(1) The Supplier shall assist the Client in complying with the obligations concerning the security of personal data, reporting requirements for data protection infringements, data protection impact assessments and prior consultations, referred to in Art. 32 to 36 of the GDPR. These include:

(a) Ensuring an appropriate level of protection through technical and organizational measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.
(b) The obligation to immediately report a personal data breach to the Client
(c) The duty to assist the Client with regard to the Client's obligation to provide information to the data subject concerned, and to immediately provide the Client with all relevant information in this regard.
(d) Supporting the Client with its data protection impact assessment
(e) Supporting the Client with regard to prior consultation with the supervisory authority

(2) The Supplier undertakes to assist the Client with suitable technical and organisatorial measures, so that the Client is able to observe the rights of the data subjects as laid down in Chapter III GDPR (information, access, rectification and erasure, data portability, objection and automated individual decision-making) within the statutory periods at any time, and for that purpose the Supplier shall make available to the Client all necessary information. If a relevant request is addressed to the Supplier which shows that the applicant erroneously believes him to be the controller of the data processing operated by him, the Supplier shall immediately forward the request to the Client and notify the applicant thereof.

(3) Unless agreed otherwise, data deletion concept, right to be forgotten, rectification, data portability and right of access must be ensured by the Supplier upon documented instruction of the Client.

(4) The Supplier may claim reasonable compensation for support services which are neither included in the description of the services nor attributable to failures on the part of the Supplier.

9. Authority of the Client to issue instructions

(1) The Client shall immediately confirm oral instructions in writing (e-mail sufficient).

(2) The Supplier shall inform the Client immediately if it considers that an instruction violates data protection provisions. The Supplier shall then be entitled to suspend the execution of the relevant instructions until the Client confirms or changes them.

10. Deletion and return of personal data

(1) Copies or duplicates of the data shall never be created without the knowledge of the Client, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory retention requirements.

(2) After conclusion of the contracted work, or earlier upon request by the Client, at the latest upon termination of the service agreement, the Supplier shall hand over to the Client all documents that have come into its possession, all processing and utilization results, and all data sets related to the order contract without keeping any copies, notwithstanding legal requirements to the contrary; alternatively, the Supplier shall – subject to the Client's prior consent – delete or otherwise destroy all respective documents, processing and utilization results and data sets in a data-protection compliant manner and in such a way that the destruction or deletion can be verified and cannot be reversed. The same applies to any and all connected test, waste, redundant and discarded material. A proof of the successful destruction or deletion shall be provided on request. If the Supplier processes data in a specific technical format he shall surrender the data either in that format or, at the Client's request, in the format in which he received the data from the Client or in any other common format after termination of this Agreement.

(3) Documentation which is used to demonstrate orderly data processing in accordance with the Order or Contract shall be stored beyond the contract duration by the Supplier in accordance with the respective retention periods. It may hand such documentation over to the Client at the end of the contract duration to relieve the Supplier of this contractual obligation.

11. Miscellaneous provisions

(1) If the data of data subjects kept by the Supplier is jeopardised due to attachment or confiscation, insolvency proceedings or due to other events or measures of third parties, the Supplier shall immediately notify the Client thereof. The Supplier shall immediately notify all institutions or persons competent or concerned that the Client as the Controller as defined in the General Data Protection Regulation holds the exclusive sovereignty over and exclusive title to the data.

(2) Modifications of or amendments to this agreement and all of its appendices, shall require a written agreement, which may also be made electronically (in particular by e-mail with copies of the signed amendment agreement) and an express reference to the fact that it is a modification of or amendment to this agreement. This shall equally apply to a waiver of this requirement of written form.

(3) The Supplier undertakes to comply with the banking secrecy obligations under section 38 of the Austrian Banking Act in relation to all information of customers of the Client, which are forwarded or become accessible or known to the Supplier in the course of the order or the provision of the services. Further, the Supplier undertakes to obligate all employees and other persons authorised with the order or provision of the services to banking secrecy and to ensure that they comply with the bankingy secrecy.

(4) This agreement is entered into in relation to a service agreement according to Appendix 2, to regulate the data protection aspects of the services by Supplier in compliance with GDPR. Accordingly, in the case of contradictions, the provisions of this agreement and its appendices shall prevail over the regulations of the service agreement.

(5) If any parts of this agreement or of its appendices are ineffective, effectiveness of the residual Agreement and its Appendixes shall not be affected.

(4) This agreement is subject to Austrian law. Any disputes over, out of or in connetcion with this agreement shall be settled by the courts having jurisdiction over Vienna's First District and the subject matter (non-exclusive place of jurisdiction).

.....	.....
Place, Date	Supplier
.....	.....
Place, Date	Client

Appendix 1
Technical and Organisational Measures

1. Confidentiality (Article 32 Paragraph 1 Point b GDPR)

- **Physical Access Control**
  Protection against unauthorised access to data processing facilities, e.g.: magnetic or chip cards, keys, electronic door openers, security staff, porter, alarm systems, video/CCTV Systems;
- **Electronic Access Control**
  Protection against unauthorised use of the data processing and data storage systems, e.g.: (secure) passwords (including a relevant policy), automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media;
- **Internal Access Control**
  No unauthorised reading, copying, changing or deleting of data within the system, e.g.: standard authorisation profiles on a need-to-know basis, standard procedure for granting authorisations, keeping access logs, periodical review of the authorisations granted, including but not limited to administrative user accounts;
- **Separation Control**
  Separated processing of data, which is collected for different purposes, e.g. multiple client support, sandboxing;
- **Pseudonymisation** (Article 32 Paragraph 1 Point a GDPR; Article 25 Paragraph 1 GDPR)
  If necessary or expedient for the relevant data processing activities, the primary identification features of the personal data are removed from the relevant data processing application, so that the data cannot be associated with a specific data subject without the assistance of additional information, provided that this additional information is stored separately, and is subject to appropriate technical and organisational measures.
- **Data classification scheme**
  Compliance with data classification scheme of the Client (e.g. secret/confidential/in-house/public);
- **Technical Erasure Concept Controls**
  For data as well as meta-data like logfiles etc.;

2. 2. Integrity (Article 32 Paragraph 1 Point b GDPR)

- **Data Transfer Control**
  No unauthorised reading, copying, changing or deleting of data in the course of electronic transfer or transport, e.g.: encryption, virtual private networks (VPN), electronic signature;
- **Data Entry Control**
  Verification, whether and by whom personal data is entered into a data processing system, or is changed or deleted, e.g.: logging, document management;

3. Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)

- **Availability Control**

  Prevention of accidental or wilful destruction or loss, e.g.: backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS, diesel generator set), anti-virus program, firewall, reporting procedures and emergency plans; security checks at infrastructure and application level, multi-stage backup concept including encrypted outsourcing of backups to a backup data centre, standard processes for cases where staff changes or leaves the undertaking
- **Rapid Recovery** (Article 32 Paragraph 1 Point c GDPR);

4. Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)

- Data protection management, including regular staff training;
- Incident response processes;
- Data protection by design and default (Article 25 Paragraph 2 GDPR);
- Order or Contract Contro l

  No data processing as per Article 28 GDPR without corresponding instructions from the Client, e.g.: clear and unambiguous contractual arrangements, formalised Order Management, strict controls on the selection of the service provider, duty of pre-evaluation, supervisory follow-up checks.

Appendix 2
Individual agreement

(1) Data protection officer and representative pursuant to Article 27 GDPR

The Supplier's designated data protection officer is:

Name:	……
Organisational unit:	……
Address:	……
Phone:	……
E-mail:	……

(2)

Provided the Supplier is established outside the European Union, it designates the following representative in the European Union as defined in Art 27 Paragraph 1 GDPR:

Name:	……
Organisational unit:	……
Address:	……
Phone:	……
E-mail:	……

(3) The Supplier shall immediately inform the Client of any change of the data protection officer or of the representative according to Art 27 Paragraph 1 GDPR.

(2) Subject matter

This agreement is entered into in relation to the service agreement between the Client and the Supplier of [.....], to regulate the data protection aspects of the services.

☐ For the subject matter of the order, reference is made to [item [...]] of the service agreement.

☐ The subject matter of the order shall be the carrying out of the following tasks by the Supplier (definition of tasks): [……]

(3) Term

☐ The term of this agreement corresponds to the term of the service agreement and accordingly ends together with that.

☐ This Agreement shall be concluded for an indefinite period of time and can be terminated by either party by giving three months' notice to the end of a calendar quarter.

The option to terminate the Agreement for important reasons and with immediate effect shall remain unaffected.

(4) Nature and purpose of the envisaged processing of data

☐ The nature and purpose of the processing of personal data by the Supplier for the Client is specifically described in [item [...]] of the service agreement, to which reference is made.

☐ The nature and purpose of processing personal data by the Supplier for the Client shall be ……

(5) Type of data

☐ The types and categories of data which are the subject matter of the data processing, are specifically described in [item [...]] of the service agreement, to which reference is made.

☐ The following types and categories of data (list/description of data categories) shall be the subject matter of the processing of personal data:

.....
.....
.....
.....
.....

6) Data subject categories

☐ The categories of data subjects which concerned by the data processing, are specifically described in [item [...]] of the service agreement, to which reference is made.

☐ The categories of data subjects which concerned by the data processing, are:

.....

.....
.....
.....

(7) Subcontracting

☐ Outsourcing of activities to subcontractors shall be not permissible.

☐ Outsourcing of activities to subcontractors shall be permissible provided that:
- the Supplier notifies the Client of such outsourcing to (a) subcontractor(s) reasonably in advance (at least 4 weeks) in writing; and
- the Client does not object to the planned outsourcing vis-à-vis the Supplier until the date at which the data is transmitted; and
- it is based on a contractual agreement as laid down in Art 28 Paragraph 2-4 GDPR.

The current subcontractor may be changed if:
- the Supplier notifies the Client of such outsourcing to (a) subcontractor(s) reasonably in advance (at least 4 weeks) in writing; and
- the Client does not object to the planned outsourcing vis-à-vis the Supplier until the date at which the data is transmitted; and
- it is based on a contractual agreement as laid down in Art 28 Paragraph 2-4 GDPR.

Any other outsourcing by the subcontractor shall require the (principal) Client's express approval.

All contractual regulations in the chain of contracts shall also be imposed on the subcontractor.

.....	.....
Place, Date	Supplier
.....	.....
Place, Date	Client