RULES ON ORDER PROCESSING IN ACCORDANCE WITH ARTICLE 28 GDPR

1. General Provisions

1. This Rules determines undertakings in connection with data protection and rights and obligations of:

- Raiffeisenbank Austria d.d., when acting as data processor, according to contract or order of data controller;
- Legal and natural persons, when acting as data processor, pursuant to the order of Raiffeisenbank Austria d.d., during providing goods and/or services, process personal data.

2. In this Rules, the following terms will have the following meanings:

"Data Processor" means legal or natural person who processes personal data in the name of another person ("Data Controller") according to concluded contract.

„Data Controller" means legal or natural person which give order to the Data Processor for certain process of personal data.

"Personal Data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"GDPR" means Regulation (EU) 2016/679 of the European parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

"Data subject" means natural person whose personal data are subject of processing pursuant one or more grounds prescribed by GDPR. The Data subject could be a party to an agreement on services or who applied for services, his/her legal representative, attorney or custodian, as well as natural person who gave consent to Data Controller.

"Consent" means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

"Pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Pseudonymisation could be achieved either by deletion of personal data or permanent change of personal data.

3. The nature and the purpose of processing of personal data by the Data Processor for the Data Controller are stated in the particular contract.

4. 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 Data Controller 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.

5. The type of personal data used and the categories of data subjects are defined in the particular contract. If in the contract the type of personal data and categories of data subjects are not defined the Data processor undertakes to comply with this Rules in respect of all personal data which are made available during the term of the contract.

2. Technical and Organisational Measures

1. Before the commencement of processing, the Data Processor shall document the execution of the necessary technical and organisational measures, as set out in advance of the awarding of the contract according to Appendix 1, specifically with regard to the detailed execution of the order, and shall present these documented measures to the Data Controller for inspection. Insofar as the inspection/audit by the Data Controller shows the need for amendments, such amendments shall be implemented by mutual agreement. For the avoidance of doubt, the Bank shall not provide the Data Controller the internal documents which concerns security and/or are classified as strictly confidential.

2. The Data Processor 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 Data Processor to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

3. Data processing only on order of the Data Controller

1. The Data Processor 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 Data Controller including the powers granted in this contract, unless the Data Processor is required by law to process the personal data.

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

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

4. Quality assurance and other duties of the Data Processor

1. In addition to complying with the rules set out in the contract, the Data Processor shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, the Data Processor 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 Data Controller shall be informed immediately of any change of data protection officer or of his/her contact details. In case, the Data Processor does not have a data protection officer, the Data Processor will provide the Data Controller with a written explanation for that. If the Bank is the Data Processor the details of the data protection officer are available at www.rba.hr.
   (b) designation of a representative as laid down in Art 27 Paragraph 1 GDPR in the European Union, if the Data Processor 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 Data Processor 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 Data Processor.
   (d) implementation of and compliance with all technical and organisational measures necessary for the contract in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR.

(e) The Data Controller and the Data Processor shall cooperate, on request, with the supervisory authority in performance of its tasks.
(f) The Data Processor shall inform the Data Controller immediately of any inspections or measures by the supervisory authority, insofar as they relate to the agreement. This also applies if the Data Processor 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 the agreement.
(g) In case the Data Controller 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 contract data processing by the Data Processor, the Data Processor shall make every effort to support the Data Controller.
(h) documentation and proof of the technical and organisational measures by the Data Processor vis-a-vis the Data Controller as part of the Data Controller's supervisory powers referred to in item 6 of this Rules.
(i) The Data Processor 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 Data Processor does not have records of processing activities established, the Data Processor will provide the Data Controller with a written explanation for that.

5. Subcontracting

1. Subcontracting for the purpose of this regulation is to be understood as meaning services which the Data Processor 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 Data Processor 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 Data Controller's data, even in the case of outsourced ancillary services.

2. The Data Processor may commission Subcontractors (additional processors) only after prior explicit written or documented consent by the Data Controller. The Data Controller 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 Data Processor is subject due to under this contract. If the Subcontractor fails to fulfil its data protection obligations, the

Data Processor shall be liable vis-ŕ-vis the Data Controller for compliance with the obligations of the subcontractor.

3. The transfer of personal data from the Data Controller 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 Data Processor 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.

6. Supervisory powers of the Data Controller

1. The Data Controller has the right to carry out inspections and audits of the data processing systems of the Data Processor. The Data Controller may also authorise other persons to perform such inspection or audit. The Data Processor may object the selection of such authorised persons in case of reasonable grounds relating to the person of the selected authorised person. For the avoidance of doubt if the Bank is the Data Processor, the Data Controller shall have not right to carry out inspections of the Bank's systems if this could jeopardise the Bank's security.

2. In case of similar order processing activities for several Data Controllers, the Data Processor allows audits by auditors instructed by such Data Controllers jointly, or – by request or with the consent of the Data Controllers – 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 Data Controllers, their auditors, and upon request to the supervisory authorities competent for the Data Controllers.

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

4. Evidence of such measures, which concern not only the specific 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).

7. Assistance obligation of the Data Processor

1. The Data Processor shall assist the Data Controller 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 Data Controller.
   (c) The duty to assist the Data Controller with regard to the Data Controller's obligation to provide information to the data subject concerned, and to immediately provide the Data Controller with all relevant information in this regard.
   (d) Supporting the Data Controller with its data protection impact assessment.
   (e) Supporting the Data Controller with regard to prior consultation with the supervisory authority.

2. The Data Processor undertakes to assist the Data Controller with suitable technical and organisatorial measures, so that the Data Controller 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 Data Processor shall make available to the Data Controller all necessary information. If a relevant request is addressed to the Data Processor which shows that the applicant erroneously believes him to be the controller of the data processing operated by him, the Data Processor shall immediately forward the request to the Data Controller 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 Data Processor upon documented instruction of the Data Controller.

4. The Data Processor 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 Data Processor.

8. Authority of the Data Controller to issue instructions

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

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

9. Deletion and return of personal data

1. Copies or duplicates of the data shall never be created without the knowledge of the Data Controller, 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 Data Controller, at the latest upon termination of the service contract, the Data Processor shall hand over to the Data Controller 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 Data Processor shall – subject to the Data Controller'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 Data Processor processes data in a specific technical format he shall surrender the data either in that format or, at the Data Controller's request, in the format in which he received the data from the Data Controller or in any other common format after termination of the contract.

3. Documentation which is used to demonstrate orderly data processing in accordance with the contract shall be stored beyond the contract duration by the Data Processor in accordance with the respective retention periods. It may

hand such documentation over to the Data Controller at the end of the contract duration to relieve the Data Processor of this obligation.

10. Miscellaneous provisions

1. If the data of Data subjects kept by the Data Processor is jeopardised due to attachment or confiscation, insolvency proceedings or due to other events or measures of third parties, the Data Processor shall immediately notify the Data Controller thereof. The Data Processor shall immediately notify all institutions or persons competent or concerned that the Data Controller 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 Rules and all of its appendices, shall be made by the Bank. The Bank shall every modification of or amendments to this Rules made public at www.rba.hr.

3. The Data Processor undertakes to comply with the banking secrecy obligations under Article 157 of the Credit Institution Act in relation to all information of customers of the Data Controller, which are forwarded or become accessible or known to the Data Processor in the course of the order or the provision of the services. Further, the Data Processor 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 banking secrecy.

11. Entry into force

1. This Rules enter into force on 25 May 2018.

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 Data Controller 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 Data Controller (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 Control
- No data processing as per Article 28 GDPR without corresponding instructions from the Data Controller, 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.