AGREEMENT ON

PLANNING, SCHEDULING, REPORTING AND RISK MANAGEMENT SOFTWARE SUPPLY, IMPLEMENTATION AND MAINTENANCE

Between

RB Rail AS

and

PRM YAZILIM DANISMANLIK TIC LTD, STI

Agreement registration number **1.19/LV-7**

CEF[1] Agreement No. INEA/CEF/TRAN/M2016/1360716 **C01C**

Procurement procedure identification No **RBR 2019/5**

Riga

Dated **4 February** 202**0**

RB Rail AS, registration No 40103845025, registered address: Krišjāņa Valdemāra iela 8 - 7, Riga, LV-1010, Latvia, represented by Chairman of the Management Board **Agnis Driksna** and Management Board Member **Ignas Degutis** acting on the basis of the Regulations on Representation Rights dated 25 May 2018 (the **Customer**),

and

PRM YAZILIM DANISMANLIK TIC LTD, STI, registration No. 510317, registered address: Kucukbakkalkoy Mah. Ayse Hatun Cesme Sok. 5/8 Atasehir Istanbul Turkey, represented by General Manager **Nihat YILDIRIM** (the **Supplier**),

jointly also referred as the Parties (the **Parties**), hereby enter into the following Agreement on the Planning, Scheduling, Reporting and Risk management software supply, implementation and maintenance (the **Agreement**) as the result of competitive procedure with negotiation No. RBR 2019/5:

1. SUBJECT MATTER OF THE AGREEMENT

1.1. The Supplier undertakes to supply Oracle Primavera P6 Cloud and Oracle Primavera Cloud (formerly Prime) software (the **Software**) to the Customer on an "end user" basis under the terms of the licence issued by the Supplier to the Customer (Annex 2). To dispel any doubts the Parties agree that the terms of the licence issued by the Supplier to the Customer (Annex 2) shall be directly applied only in cases specifically stipulated in this Agreement and in cases where Annex 2 contains more detailed provisions on specific matters provided that such specific provisions conform with the general spirit and meaning of the Agreement. In case of any discrepancies or conflicting provisions between the Agreement and Annex 2, the provisions of the Agreement shall be applied at all times.

1.2. The Supplier will provide the Software installation and configuration of the Software, as well as the installation and configuration of the cloud solution as specified in Annex 6 of the Agreement on the devices required by the Customer and provide unlimited cloud storage accessible for the Customer within the deadlines set out in this Agreement and meeting the technical requirements set out in the Technical Proposal (Annex 6).

1.3. The Supplier undertakes to provide a constantly available (24 hours a day / 7 days a week) support service to the Customer by e-mail, phone and online during the period of the Agreement, in accordance with Tenderer's standard conditions provided in Technical proposal (Annex 6).

1.4. The Supplier will provide training to the Customer's employees in accordance with the deadlines and requirements of the Agreement and Annex 6 and will provide training materials in the amount and form set out in Annex 6.

1.5. The above-mentioned Software and storage installation, configuration, support, and training, as well as provision of training materials in the context of this Agreement together are called the Products (the **Products**).

1.6. When fulfilling the obligations under this Agreement, the Supplier undertakes to deliver the Products in a workmanlike and professional manner.

1.7. The Customer will pay the Supplier the fees within the deadlines and in the amount set in this Agreement.

2. SUBCONTRACTING

2.1.   The Supplier has the right to hire a sub-contractor (the **Sub-Contractor**) for the delivery of the Products required by this Agreement subject to the conditions described below in this section.

2.2.   The Supplier undertakes to reflect the same terms and conditions as in this Agreement into the sub-contract agreement with the Sub-Contractor.

2.3.   The Supplier and the Sub-Contractor must be entities which process data solely in the countries of the European Union and which are compliant with the requirements of the GDPR[2] and the Information Security Directive[3] and the applicable national legal acts in the field of personal data protection and information security.

2.4.   Appointment or replacement of each Sub-Contractor and any agreement made in that respect between the Supplier and a Sub-Contractor is subject to the Customer's prior written approval.

2.5.   The Supplier remains liable for the performance of this Agreement and has an obligation to ensure that any Sub-Contractor adheres to the applicable provisions of this Agreement.

2.6.   The Sub-Contractor must be able to meet the same data processing and information security requirements as the Supplier.

2.7.   If the Supplier wants to replace the Sub-Contractor, the Supplier submits a prior written application to the Customer. The application must be accompanied by information and documents proving that the proposed Sub-Contractor meets the requirements of the Agreement.

2.8.   The Customer refuses sub-contracting of such company, if the potential Sub-Contractor does not meet the requirements of the Agreement or its staff does not meet the same professional qualification and experience as the staff evaluated in the selection procedure in order to determine the most economically advantageous tender.

2.9.   The Customer refuses sub-contracting of the company, if the initial indication of the proposed Sub-Contractor in the offer would have influenced the selection of the tender in accordance with the tender evaluation criteria specified in the procurement documents.

3. REPLACEMENT

3.1.   The Sub-Contractor and the Project Manager indicated in the Supplier's offer may only be replaced by prior approval of the Customer.

3.2.   The Customer will adopt a decision to allow or refuse replacement of the Project Manager or Sub-Contractor as soon as possible, but not later than within five working days after receiving all the information and documents necessary for making the decision.

---

[2] 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

[3] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

3.3. The Customer refuses to replace the Sub-Contractor if:

3.3.1. the proposed Sub-Contractor does not meet qualification criteria set out in the procurement procedure;

3.3.2. the existing Sub-Contractor has the qualities, which the Supplier has relied on in order to prove its own conformity with the requirements of the Agreement and the procurement procedure documents, and the proposed Sub-Contractor does not have at least the same qualification as the previous Sub-Contractor, or if the proposed Sub-Contractor meets the exclusion criteria set out in the procurement procedure;

3.3.3. the proposed Sub-Contractor whose value of work is at least 10% of the total value of the Agreement meets the exclusion criteria set out in the procurement procedure;

3.3.4. the change of the Sub-Contractor would affect the selection of the tender in accordance with the tender evaluation criteria specified in the procurement procedure.

3.4. The proposed Project Manager must meet the same qualification criteria as the Project Manager indicated in the Supplier's offer.

3.5. The Customer refuses the replacement of the Project Manager, if the new Project Manager does not meet criteria set out in the procurement procedure or he/she does not meet at least the same criteria which were evaluated when choosing the most economically advantageous offer.

3.6. The Project Manager indicated in the offer may be replaced. Sections 3.4 and 3.5 remain applicable to such replacement.

Security Clearance Requirements

3.7. The Supplier shall not involve employee and/or staff, including but not limited to key personnel, consultants and sub – consultants (if any) who have a criminal record, in the implementation of the Agreement.

3.8. The Supplier shall submit to the Customer the name, surname, personal code (identification number), professional title (job position) of every person that will implement the Agreement at least ten (10) working days prior involvement of this person in the implementation of the Agreement. The Supplier shall provide a brief (concise) description of duties towards the implementation of the Agreement of the persons and if requested by the Customer.

3.9. The Customer has a right to demand dismissal of such a natural person non-compliant with the security clearance requirements stipulated in this Section at the Customer's sole discretion on the basis of the Customer's written request for dismissal. Parties agree that such Customer's decision is incontestable.

3.10. The Supplier shall immediately undertake all the necessary actions and measures to ensure that any risk of involvement of such a natural person in the implementation of the Agreement is promptly and duly eliminated.

3.11. The Supplier is obliged:

3.11.1. to prevent involvement of such a natural person in the implementation of the Agreement, and

3.11.2.   to immediately replace the dismissed person according to Article 62 of the Public Procurement Law of the Republic of Latvia and the Agreement, and

3.11.3.   to comply with the Customer's written instructions pursuant to this Section and not to challenge these instructions, and

3.11.4.   to inform the Customer about dismissal or replacement proceedings pursuant to Sub-Section 3.12.

3.12.   In any occasion the Supplier shall immediately notify the Customer in writing about any situation that emerged before and during the implementation of the Agreement, as a result of which there could appear or appears a risk of involving such a natural person in the implementation of the Agreement, and about the immediate replacement of non-compliant or dismissed natural person involved in the implementation of the Agreement.

3.13.   In case if the immediate dismissal or replacement of the dismissed natural person non-compliant with the security clearance requirements stipulated in this Section results in the unreasonable increase of the costs towards the Supplier, the Supplier shall immediately inform the Customer about this fact in written and the Parties shall agree upon the conditions of the provision of the Services.

3.14.   The Supplier's non-compliance with the security clearance requirements stipulated in this Clause, the Customer's instructions towards the Supplier regarding these security clearance requirements or other provisions of this Clause constitutes a material breach (breach of a material term or condition) of the Agreement.

4.   PRODUCTS

4.1.   The Supplier provides software supply and implementation (including training services) within two (2) months from the date of the mutual signing of the Agreement.

4.2.   The Supplier ensures unlimited storage space (the **storage space**) for the Customer's data throughout the duration of the Agreement, unless the Customer uses its rights of Partial Termination as described in Section 15.3.

4.3.   The Supplier provides system and service support of the Software and cloud solution in accordance with the Supplier's standard conditions provided in Technical proposal (Annex 6).

5.   DELIVERY AND ACCEPTANCE

5.1.   The Parties agree that the acceptance of Products will be confirmed by a mutual signing of the delivery-acceptance deed.

5.2.   The Customer will sign the delivery-acceptance deed only if the Products delivered by the Supplier comply with Technical specification (Annex 1) and Technical proposal (Annex 6) and the Customer does not have objections against the quality of the delivered Products.

5.3.   Any objections and/or claims with respect to the Software will be limited by the terms of the Oracle Cloud Services Agreement (Annex 2); whereas any objections and/or claims concerning the deliverables of the Products will be handled as follows:

5.3.1.   when complete, the Supplier shall submit final deliverables and a copy of a "Deliverable Acceptance Deed" to the Customer's identified person(s), who will conduct a review to determine the deliverables' conformance with the Technical specifications (Annex 1) and

the Supplier's proposal (Annex 6). Upon completion of this review the Customer will complete the Deliverable Acceptance Deed indicating acceptance or rejection and return it to the Supplier;

5.3.2.   if a deliverable is neither accepted nor rejected within ten (10) business days, the deliverable will be deemed to have been accepted by the Customer without change or comment. The Customer may also request an extension to the ten (10) day acceptance period, which will not be unreasonably withheld by the Supplier unless it affects the schedule defined in the Technical proposal (Annex 6), which could then trigger a change request that may impact the project timeline, resources and/or cost;

5.3.3.   if the Customer rejects a deliverable, the Customer will provide Supplier with a written description of why the deliverable was rejected on the Deliverable Acceptance Deed. If the identified deliverable discrepancies are mutually agreed to be within the Technical specifications (Annex 1), the Technical proposal (Annex 6) or other documentation approved by Parties, the Supplier shall rework the deliverable at its sole cost as necessary to achieve its conformance with the Technical specification (Annex 1) and Technical proposal (Annex 6). If the discrepancies are mutually agreed to be outside the specifications, the Customer shall either accept the deliverable as-is or request a change order. If the Parties cannot come to an agreement regarding the discrepancies, the issue shall be elevated to respective management teams to discuss the deliverable and project specifications in detail.

6.   PAYMENTS

6.1.   The Customer undertakes to pay for the delivered Products to the Supplier's bank account indicated in this Agreement within 60 days after the mutual signing of the Delivery-Acceptance Deed and receipt of the respective invoice, with the exception of a yearly license fees provided in Section 6.2.2 and 6.2.3. below for the use of the Software and the storage space and additional licences, which the Customer pays yearly, within 30 days after receipt of the respective invoice.

6.2.   The Customer undertakes to make the following payments to the Supplier:

6.2.1.	A single payment for the software supply and implementation (including installation / configuration of the Software / configuration of the online databases and solutions, the provision of the unlimited storage space.	EUR 93 000,00
6.2.2.	A yearly license fee for the use of the Software and the storage space, which includes maintenance and support of the Software.	Fees specified in Section 8.1
6.2.3.	A yearly license fee for any additional licenses if such are requested by the Customer.	Fees specified in Section 8.2
6.2.4.	A training fee, including the fee for provision of training materials and the User Manual and Administrator Manual as described in the Annex 6.	EUR 28 000,00

6.3.   When extending the license for the next one-year period, the Supplier issues an invoice 30 days in advance before the start of the next licensing period.

6.4. All payments are indicated including all and any taxes (except VAT), if such are payable according to the applicable law.

6.5. All the invoices have to be issued electronically and sent to the Customer's e-mail address: invoices@railbaltica.org.

6.6. The Parties agree that in accordance with the Law on Accounting and Value Added Tax Law of the Republic of Latvia the invoices may be issued without the requisite "*signature*".

7. RESIDENCE CERTIFICATE

7.1. The Supplier represents and warrants to the Customer, as of the effective date of this Agreement, that its income from this Agreement will not derive through permanent establishment or fixed base maintained by the Supplier in the Republic of Latvia.

7.2. The Supplier agrees to submit to the Customer 4 (four) copies of Residence Certificate– Application for Reduction of or Exemption from Latvian anticipatory taxes withheld at source from payments (management and consultancy fees, leasing fees and certain other types of income), paid to residents of the Republic of Turkey (the **Residence Certificate**) confirmed by Competent Authority of the Republic of Turkey and the Latvian State Revenue Service.

7.3. The Residence Certificate must be submitted to the Customer prior the Customer is due to make a payment of the fee or other payments to the Supplier. Otherwise the Customer withholds withholding tax at the rate of 20% from the payments made to the Supplier.

7.4. The Customer will make relevant deductions from the payments due to the Supplier if the Supplier does not comply with this provision.

8. LICENSE FEE

8.1. The Customer undertakes to pay a standard yearly license fee for the use of Software and the storage space as set in the Supplier's Financial proposal (Annex 7) "Licence fee (including support services)".

8.2. The Customer reserves the right to request the inclusion of the additional Software accounts during the term of the Agreement subject to additional costs. The Customer undertakes to pay no more as standard yearly license fee according to Clause 8.1 of the Agreement.

9. TRANSFER OF RIGHTS

9.1. The Supplier conducts the transfer of the administration rights of the Software to the Customer to the extent indicated in Annex 6, including the rights to change the configuration of the Software and the content of the data within 30 days from the moment of the mutual signing of the Agreement.

9.2. Following completion of the deployment and configuration phase of the project and upon final acceptance of the delivered solution, the Supplier shall ensure the rights to change the configuration of the storage space by the employees of the Customer's IT Department within 30 days from the installation of the storage space; for this purpose the employees of the Customer shall have access rights to configure the Software as described in the Technical Specification (Annex 1).

9.3. In order to ensure its business continuity, the Customer is allowed to make a back-up copy of all data stored in the Software and store it on its own devices.

9.4. In the event of termination of the Agreement, the Customer has the right to immediately extract its data from the Software and from the cloud storage and obtain the audit history trail from the Software. This applies to the respective extent in case of the Partial Termination (Section 15.3). The Supplier will not prevent or disturb the Customer in any way within the process of the extraction of data, and the Supplier must ensure the possibility of the extraction of the data in an unencrypted, compatible and interoperable manner.

9.5. If liquidation, bankruptcy, insolvency or legal protection proceedings have been initiated against the Supplier or the Supplier itself has filed for liquidation, bankruptcy, insolvency or legal protection proceedings, or the Products cease to exist, the Supplier must immediately notify the Customer and must ensure the extraction of data and audit history trail as set out in Section 9.4.

10. SIGNIFICANT CHANGES

10.1. If the Products cease to exist within the period of the Agreement, the Supplier will pay to the Customer the contractual penalty in amount of EUR 20 000 (twenty thousand euros).

10.2. If major interface and/or functionality changes of the Software are made by the Supplier, the Customer has the following rights:

10.2.1. the Supplier has to provide training materials on new functionality of the Products without additional cost;

10.2.2. to obtain without additional cost the latest version of the Products for all the Customer's users licensed by the Supplier;

10.2.3. if after a significant change the Products do not meet the Customer's needs specified in the Agreement, the Customer has rights to terminate the Agreement without a prior notice.

11. TRAINING

11.1. The Supplier undertakes to provide on-site training in Riga for administrator level employees (superusers) and for regular user-level trainings.

11.2. In addition to the training a training material for the end-users, the User Manual and the Administrator Manual must be provided not later than 5 (five) business days prior to the on-site training day agreed by the Parties.

11.3. The Customer reserves the right to record the video training and use it solely only for license users training on non-commercial basis.

12. TECHNICAL SUPPORT

12.1. The Supplier will provide 24-hour technical support seven (7) days a week (including weekends and any public holidays) via phone, chat, email and knowledgebase, provided that after the normal business hours at the Customer's regional support location, the Customer may be required to contact another regional support centre. Support contact details are: [CONFIDENTIAL]

13. INTELLECTUAL PROPERTY

13.1. The Customer has rights to use the Software provided by the Supplier in accordance with the End-User License Agreement(s) (Annex 2).

13.2. The Customer will prevent any infringement of the Supplier's intellectual property rights in the Software and will promptly report to the Supplier any such infringement that comes to its attention. In particular, the Customer:

13.2.1. will ensure that each user, before starting to use the Software, is made aware that it is proprietary to the Supplier and that it can only be used in accordance with this Agreement;

13.2.2. has right to permit the third parties, with which the Customer have concluded the cooperation agreement on implementation of the Global Project (including but not limited to national implementing bodies of Rail Baltica Global Project: "Rail Baltic Estonia" OÜ, Sabiedriba ar ierobezotu atbildibu "EIROPAS DZELZCEĻA LĪNIJAS", UAB "Rail Baltica statyba", AB "Lietuvos geležinkeliai", AB "Lietuvos geležinkelių infrastruktūra" , beneficiaries of the Rail Baltica Global Project: Ministry of Transport and Communications of the Republic of Lithuania, Ministry of Transport of the Republic of Latvia, Ministry of Economic Affairs and Communications of the Republic of Estonia and designers of detail technical designs of the railway line for the Rail Baltica Global Project), to have access to the Software without the prior written consent of the Supplier;

13.3. The Supplier ensures that the intellectual property rights to the Software are duly owned (or licensed, or assigned, or held on any other valid legal basis) by the Supplier, and the use of the Software by the Customer in the way described in this Agreement will not harm any third party intellectual property rights.

13.4. The Supplier defends, holds harmless and indemnifies the Customer from all third party claims and related costs (including without limitation reasonable attorneys' fees and costs) resulting from any claims or potentially unlawful use of third party intellectual property, which is the result of misleading or incomplete information provided by the Supplier, or which are in any way connected with the actions or omissions of the Supplier unless conditions included in End-User Licence Agreement (Annex 2) does not provide stricter requirements.

14. RESPONSIBILITY

14.1. For violation of any material terms or deadlines provided in the Agreement, the violation of which was not due wholly or partially to the Customer's action or inaction, the Supplier pays a contractual penalty to the Customer in the amount of EUR 5 000 on case by case basis. The cumulative amount of any and all penalties payable by the Supplier to the Customer under this Agreement shall not exceed 10% (ten percent) of the total project fee stipulated in the Agreement.

14.2. The payment of the contractual penalty does not release the Supplier from the performance of the contractual obligations.

15. DURATION AND TERMINATION

15.1. This Agreement enters into force on the day of its signing by both Parties and remains in force until 31 December 2026.

15.2. Parties may terminate this Agreement by submitting a written notice to the other Party: The Customer – at least 3 months in advance, the Supplier – at least 6 months in advance.

15.3. The Customer may choose not to use data storage of the Supplier, by submitting a written notice to the Supplier at least 3 months in advance (the **Partial Termination**). The Partial Termination does not affect the license fee for the use of Software.

15.4. Any Party may terminate this Agreement by submitting a written notice to the other Party at least 30 days in advance:

    15.4.1. if the other Party commits a material breach of any of the terms of this Agreement and that breach (if capable of remedy) is not remedied within 30 days of notice being given by the suffering Party requiring the remedy;

    15.4.2. if liquidation, bankruptcy, insolvency or legal protection proceedings have been initiated against the other Party or if the other Party itself has filed for liquidation, bankruptcy, insolvency or legal protection proceedings.

15.5. The Customer may terminate this Agreement with immediate effect by submitting a relevant written notice to the Supplier:

    15.5.1. if the Supplier or the Sub-Contractor fails to meet any requirements set out for the data processing within the European Union, in the Agreement, or in any applicable law;

    15.5.2. if by the third party's decision the Connecting Europe Facility (CEF) co-financing of the Agreement becomes unavailable to the Customer fully or partly;

    15.5.3. if international or national sanctions, or substantial sanctions by a Member State of the European Union or the North Atlantic Treaty Organization affecting the financial and capital market interests have been imposed on the Supplier;

    15.5.4. in the cases specifically indicated in Section 64 of the Public Procurement Law of the Republic of Latvia.

15.6. In the case of unilateral termination or Partial Termination from the Customer's side, the Customer will pay the Supplier the fees in respect of the Products provided under this Agreement up to the date of the notification on the termination of this Agreement, and the Customer is not obliged to pay contractual or any other penalty, damages or compensation to the Supplier.

15.7. The Supplier must ensure that in case if international or national sanctions or substantial sanctions by a Member State of the European Union or the North Atlantic Treaty Organization affecting the financial and capital market interests are applied on the Sub-Contractor, the agreement between the Supplier and the Sub-contractor must be terminated with the immediate effect.

15.8. Within 45 days after the termination of the Agreement, the Customer will pay the Supplier for all Products provided by the Supplier up to the date of termination, provided that there are no obstacles to the access and transfer of data as described in Section 15.9 and 15.10 below.

15.9. Following the termination or the Partial Termination of this Agreement due to any reason and upon a written request by Customer, the Supplier must immediately return the Customer's data in one of the ways agreed by the Parties:

15.9.1. The Supplier ensures the transfer of data sets from its Software, cloud storage, and any Sub-Contractors storage to the Customer within 6 months after the termination of the Agreement; for the avoidance of doubt, the data must be transferred as soon as practically possible, but in any event not later than within 6 months after the termination;

15.9.2. If any of the Parties submits a notification to terminate the Agreement with a 3-6 months prior termination notice, the hand-over of the datasets has to be conducted on the date of the termination of the Agreement.

15.10. The Supplier ensures the data extraction and transfer from the Software and cloud storage, as well as assistance to the Customer, as far as necessary to ensure safe, efficient and interoperable data transfer from the Software to the Customer without any additional cost.

16. AMENDMENTS

16.1. Any amendments to the Agreement may be made in compliance with Section 61 of the Public Procurement Law including but not limited to the Customer right to extend duration of the Agreement due to extending of the duration of the Global project until the end of the Global project.

16.2. The Customer may request to increase the number of users to whom the Software is licensed as specified in Section 8.2. and Annex 1 of the Agreement "Technical specification" Section 4 "Invitation to submit final proposal".

16.3. Any technical solutions proposed by the Customer in the Annexes to the Agreement must not be changed without a direct documented consent of the Customer.

16.4. Any amendments and changes to the Agreement are valid only if they are in writing and signed by the Parties.

16.5. The correspondence between the Parties prior to the concluding the Agreement (Annex 5) is an integral and inseparable part of the Agreement.

17. PERSONAL DATA PROTECTION

17.1. The Supplier processes personal data on behalf of the Customer in accordance with the Agreement.

17.2. The Customer is the data controller, and the Supplier is the data processor, therefore the parties sign a Personal Data Processing Agreement as attached in Annex 3 of the Agreement on the day of the signing of this Agreement. The Supplier is obliged to follow data processing rules specified in Annex 3 of the Agreement.

18. CONFIDENTIALITY

18.1. The Supplier is prohibited to disclose to a third party any information related to this Agreement, its performance (*inter alia* disputes and their settlement), or any other information relating to the business or other activities of the Customer, and any information on the intellectual property, which has come to the knowledge of the Supplier or which it has otherwise obtained (*inter alia* from customers or cooperation partners) in the course of negotiation or performing of this Agreement (even accidentally), unless the information:

18.1.1. was publicly known at the time of its disclosure or was already known to the Supplier before such information was provided by the Customer; or

18.1.2. subsequently has lawfully become into the possession of the Supplier from a third party.

18.2. The provisions of this section remain in force during the validity of the Agreement and for an unlimited period after the expiry of the Agreement.

18.3. If the Supplier violates the confidentiality obligation, the Supplier pays to the Customer a contractual penalty in the amount of 50 000 EUR (fifty thousand euros) for each breach.

19. VISIBILITY REQUIREMENTS

19.1. During performance of the Agreement, the Supplier undertakes to comply with all of the following requirements:

19.1.1. any report, brochure, document or information related to the activities conducted by the Supplier or any other person on behalf of the Supplier, or which the Supplier makes publicly available will include each of the following:

(a) a funding statement which indicates that the Agreement is financed from CEF funds substantially in the following form: "Co-financed by the Connecting Europe Facility of the European Union";

(b) with respect to printed materials, a disclaimer releasing the European Union from liability with respect to any contents of any distributed materials substantially in the form as follows: "The sole responsibility of this publication lies with the author. The European Union is not responsible for any use that may be made of the information contained therein". The disclaimer in all official languages of the European Union can be viewed on the website https://ec.europa.eu/inea/connecting-europe-facility/cef-energy/beneficiaries-info-point/publicity-guidelines-logos; and

(c) the flag of the Council of Europe and the European Union.

19.2. the requirements set forth in Section 19.1.1(a) and 19.1.1(c) of this Agreement can be complied with by means of utilizing the following logo:

19.3. in the event the Supplier decides to utilize the above logo, the Supplier will ensure that the individual elements forming part of the logo are not separated (the logo will not be utilized as a single unit) and sufficient free space is ensured around the logo; and

19.4. in order to comply with the latest applicable visibility requirements established by the European Union, the Supplier must regularly monitor changes to visibility requirements; as of the Effective Date, the visibility requirements are available for review on the webpage https://ec.europa.eu/inea/connecting-europe-facility/cef-energy/beneficiaries-info-point/publicity-guidelines-logos.

20. FORCE MAJEURE

20.1. If an extraordinary situation arises that is beyond the control of the Parties and which could not be reasonably predicted by the relevant Party, which makes the fulfilment of the obligations pursuant to the Agreement absolutely impossible, this situation is deemed to be *force majeure*, such as war, strike, earthquake, flood, lockout, embargo, governmental acts or orders or restrictions, or any other reason where failure to perform is beyond the reasonable control and is not caused by the negligence or intentional conduct or misconduct of the nonperforming Party.

20.2. In case of force majeure the affected Party must notify the other Party without any undue delay and provide proof of the event occurred.

20.3. The affected Party's obligations will be suspended as long as the extraordinary force majeure situation lasts. The other Party's counter-performances will be suspended during the same period of time.

21. WARRANTIES AND DISCLAIMERS

21.1. The Supplier warrants that the Products will be provided in conformity with industry standards and the Technical Proposal (Annex 6).

21.2. The Supplier declares that Products complies with Customer's requirements set in Technical specification (Annex 1) and Supplier's Technical proposal (Annex 6).

21.3. The Products must be complete and fit for immediate use for the intended purpose.

22. SEVERABILITY

22.1. If any provision of this Agreement is found to be illegal, invalid or unenforceable under applicable law effective during the term of this Agreement, the remaining provisions of this Agreement will nevertheless remain binding. The Parties will negotiate in a good faith to replace the invalid provision with a provision with the economic effect as close as possible to that of the illegal, invalid or unenforceable provisions.

22.2. None of the contracting Parties may transfer its rights and obligations to a third party without a prior written approval of the other Party, with the exception of the cloud storage provider approved by the Customer in advance.

22.3. The Agreement is drawn up on 106 (one hundred and six) pages in 2 copies, one for each Party. Both copies have equal legal force.

23. GOVERNING LAW AND DISPUTE RESOLUTION

23.1. This Agreement (including it's Annexes) is governed by the laws of the Republic of Latvia.

23.2. Any dispute, controversy or claim arising out of or in connection with this Agreement (including it's Annexes), or the breach, termination or invalidity thereof, will be settled by courts of the Republic of Latvia.

24. NOTICES

24.1. All notices and communications under this Agreement must be addressed as set out below:

24.2.   If to the Customer: Contact person: Aigars Smuškovs; Address: Krišjāņa Valdemāra iela 8 - 7, Riga, LV 1010, Latvia; Phone No.:+37122002233; E-mail: aigars.smuskovs@railbaltica.org.

24.3.   If to the Supplier: Contact person: Nihat YILDIRIM; Address: Kucukbakkalkoy Mah. Ayse Hatun Cesme Sok. 5/8 Atasehir Istanbul Turkey; Phone No.: +90(533)2834969; E-mail: nihat@prmyazilim.com.

25.   ANNEXES

25.1.   Annex 1 – Planning, Scheduling, Reporting and Risk management software supply, implementation and maintenance Technical Specification.

25.2.   Annex 2 – Oracle Cloud Services agreement.

25.3.   Annex 3 – Personal data processing agreement.

25.4.   Annex 4 – Correspondence.

25.5.   Annex 5 – Supplier's Declaration.

25.6.   Annex 6 – Technical proposal.

25.7.   Annex 7 – Financial proposal.

26.   PAYMENT DETAILS

26.1.   The Customer: RB Rail AS
Bank: Luminor Bank AS
Account No.: LV73NDEA0000084270995
VAT No.: LV40103845025

26.2.   [CONFIDENTIAL]

27.   SIGNATURES

On behalf the Customer   On behalf of the Supplier

_____   _____

Chairman of the Management Board   General Manager
Agnis Driksna   Nihat YILDIRIM

_____

Management Board Member
Ignas Degutis

1. TECHNICAL TERMS AND ABBREVIATIONS

Programme: in building design and construction the Programme typically describes the sequence in which specific project tasks must be carried out in the way that a project (or part of a project) can be completed on time. The Programme will often identify: dates and durations allocated to specific tasks; a critical path (the sequence of critical tasks upon which the overall duration of the programme is dependent); tasks which can only be carried out after other tasks have been completed; tasks which can be carried out simultaneously; 'float' within the tasks that are not on the critical path (that is, delays that can be incurred without affecting the critical path); the need for specific resources such as plant, services or materials and their lead time, etc..

Critical Path Method (CPM): The critical path is the one that requires the longest period of time to progress from start to completion and indicates the minimum timeframe necessary to complete the whole project. The critical path method, or critical path analysis (CPA), is an algorithm for scheduling a set of project activities.

Activity: operation or process consuming time and possibly other resources. It is a measurable element of the total project programme (time, implementation cost, ect.).

Schedule: In project management, a schedule (also known as work schedule or project schedule) is a chart which includes activity lists, project deliverables, milestones and their start and finish dates. Duration of deliverables are often estimated by considering the quantities, resource availability, activity relationships, constraints and requirements. Gantt Chart, Critical Path Method, PERT Method, Critical Chain Method are some of the methods used to create schedules.

Baseline schedule: baseline schedule is also known as schedule baseline or target schedule. It is an approved copy of project schedule that can be used to analyse the project performance and report the schedule variances.

Work Breakdown Structure (WBS): tool used for project management which divides the project into manageable and minor components. The project deliverables are divided into smaller work packages as hierarchical groups. Working with smaller work packages provides many benefits while creating and reporting a project schedule

Organizational Breakdown Structure (OBS): tool to create a thorough picture of the project organization for the purposes of establishing a relationship between and among the various project related work packages as well as between those work packages and the project's pre-defined performing organizational units.

Earned value management (EVM): also known as Earned value analysis (EVA) is a technique used to assess project progress by comparing the amount and cost of work that was planned to have been done by a particular stage with the amount that has actually been done and what it has actually cost.

2. TECHNICAL SPECIFICATIONS – MANDATORY

2.1 Systems Functional Requirements – Planning and Scheduling

- An integrated solution - scheduling, cost control, risk analysis, change control, reporting - in one system and web or cloud-based;
- Critical Path Method analysis;
- Storage and comparison of multiple baselines;
- Rapid what-if analysis of multiple schedule scenarios, and on-screen comparison of these scenarios with each other and with the project baseline; Ability to open multiple projects / schedules together in the same window;
- Capacity to manage unlimited number of activities and large volumes of data;
- Resource levelling and optimisation; facility to optimise resource usage by suggesting alternative schedule dates considering resource limits and availability;
- Multiple calendars and work patterns;
- Support for multiple schedules e.g. work in progress schedule, baseline schedules, variations schedules, etc.;
- Full project history maintained;
- Multi-user access to same projects and working in parallel;
- External links in between activities from different projects / schedule must be allowed;
- Capability to combine separately maintained schedules into an overall master schedule for analysis and reporting;
- Management of common resources across multiple projects;
- Facility to define hierarchical and/or non-hierarchical Work/Organizational Breakdown Structures to be assigned to activities for summarizing, sorting and filtering of data on screens and reports;
- Progress options shall include Retained Logic and Progress Override.

2.2 Systems Functional Requirements – Risk Management / Risk Analysis tool

- An integrated solution to identify, assess and analyse risks alongside a project implementation timeline (master schedule/program);
- Integrated risk register including a risk card to be used to assign individual risks to risks owners in order to plan and follow up on specific mitigation measures;
- quantitative and qualitative risk analysis before and after application of mitigation measures;
- Integrated cost risk analysis;
- Integrated schedule (time) risk analysis;
- Combined cost and schedule risk analysis reporting;
- Real-time visualization of the impact of identified risks on the project schedule;
- Prioritisation of risks depending on the likely adverse impact on costs or schedule;
- Capability to combine separately maintained schedules into an overall master schedule for analysis and reporting;
- Provide a means to visualise the P50, P80 and P90 outcomes;
- Risk calendars (e.g. for weather or other limitation modelling);
- Risk correlation.

2.3 Systems Functional Requirements – Reporting and Progressing

Remote Reporting
- Facility to summarise and filter reports based on user-defined WBS and OBS codes, and permissions;
- Detail of different reports options must be provided (e.g. Resources and Cost S-Curves and Histograms, Progress Reports. For Risk reports e.g.: Tornado charts, Risk Distribution S-curves);
- All report data and information can be downloaded or exported to Microsoft Excel as either a native Excel worksheet or a comma-separated value text file, according to user selection

Earned Value Reports
- Reports of cost and schedule efficiencies based on earned value and expenditure to identify:
    - SPI - Schedule Performance Index;
    - Cost Performance Index;
    - ETC - Estimate to Completion (hours and costs).

2.4 Systems Functional Requirements – Change Management

- Integrated Change Order / Variations Orders Register to facilitate
    - Maintenance of history of all scope changes.

2.5 Systems Functional Requirements – Interface

Network Editor Interface
- Planning, Scheduling, Reporting and Risk Management tool fully integrated, intuitive and easy to use;
- Different types of interfaces:
    - Cloud-based and Online (Web-browser) based UI;
    - Customized Dashboards for project follow up.
- Allow for review and editing of:
    - All activity date and time related information (durations, targets starts and finishes etc.);
    - Logic constraints;
    - Resource requirements and availabilities.
- Real-time network analysis to show impact of changes on the project schedule;
- Filtering of activities by any combination of activity fields;
- Creation of user-defined fields;
- Creation of Activity Notebooks;
- Multiple setting options for activity types (e.g. fixed duration, fixed units or fixed duration and units, etc.);
- Ability to add steps on activities, to facilitate progress tracking and update;
- Open multiple projects / schedules in parallel and in the same window.

Information logging
- The solution shall have information log and information tracking;
- The history log shall be clearly readable and understandable using standard tools and shall display a clear path of actions which can be associated with a particular user;
- The log shall not be editable.

As-built information
- The solution shall support the administration of the as-built data

2.6 Systems Functional Requirements – Scalability

Scalability
- The system solution shall be scalable so that it can be used to manage information on multiple projects at any time

User set up
- The system solution shall provide for the provision to allow simple set up users and assign them to their respective companies, departments or teams, and assign them the access rights to the project and asset workspaces as required;
- The solution shall allow users from RB Rail AS or any appointed partner organization.

2.7 Data Storage, Access and Security

Security and storage
- The software solution shall provide for security measures within the architecture of the system to ensure adequate control of access to data according to user role, preventing access to data by unauthorised users

Data Storage Location
- Data is to be stored within the European Union or European Economic Area. Exact data centres and physical locations needs to be stated;
- Fully adhere to the General Data Protection Regulation (GDPR);
- The file store shall be presented as a fully configurable secure electronic document management system, capable of receiving and storing native and open format file, and other format files.

Backup and retrieval
- The software solution shall make provisions for the backup and retrieval of data in the event of an outreach, incident or perceived information loss;
- Target restore times (means time to restore date in case of accidental loss etc.) should be specified in a service level agreement
- The extracted data cannot be encrypted and must be accessible by any system or solution;
- Moving Data out of the system, must be possible without any additional effort or cost.

Access rights
- The software solution shall be capable of using and distributing individually granted access rights based on project role and responsibilities and file status;
- Software can be run accessing data stored on cloud servers located within the European Union or European Economic Area via an internet connection and should not require any other additional downloads or plugins;
- RB Rail AS shall have the full administration rights over the users/accounts and their access rights to the software solution;
- The solution shall provide a secure accessibility via mobile application (for iOS and Android phones and tablets);
- Access to the system shall be secure and available for authorized users 24hrs a day, 365 days a year.

Information assurance
- The software solution shall include for functionality to enable a suitable level of information assurance in order to mitigate mistakes and errors and provide assurance the supplied information is suitable and reliable for its intended purpose. Features to include:

- Automated and manual checking;
- Report and compare functionality to highlight incomplete information.
- One single point of contact for support.

2.8 Systems Non-Functional Requirements

Implementation support
- Implementation support, including creating first schedules, activity codes, wbs structures, etc, full support to be provided where required on site.
- The Tenderer shall provide the contracting authority with a:
  o Project Manager focusing on software implementation and delivery, including but not limited with setting up the system itself, providing training for all superusers, together with superusers prefill the system with information e.g. schedules etc. (2 months);
  o Planning Engineer/Planner for onsite support, in depth user training and support to ensure quality of schedules prepared etc. (6 months).
- Exact implementation schedule (number of hours, number of meetings required based on previous experience) to be recommended by Tenderer.

Training (minimum requirements)
- During first two months an on-site training to be provided in Riga:
  o for administrator level employees (superusers);
  o for regular user-level trainings.
- Exact training schedule (number of hours, number of users per training and number of meetings/training sessions required based on previous experience) to be recommended by Tenderer;
- In addition to the training a training material for the end-users, the User Manual and the Administrator Manual must be provided not later than 5 (five) business days prior to the on-site training day agreed by the Parties.
- Details of training schedules and costs must be described in Technical proposal.

Licenses
- Provision of 24-hour technical support seven (7) days a week (including weekends and any public holidays) via phone, provided that after the normal business hours at RB Rail AS regional support location, RB Rail AS may be required to contact another regional support centre.
- Expected amount of licences[4]:

Year	Administrator/ Full account licences	User's account licences
2019	15-30	20-40
2020	25-50	25-50
2021	25-50	35-100
2022	30-55	45-110
2023	40-60	45-140
2024	40-60	45-140
2025	30-50	45-100
2026	30-50	45-100

[4] The amount of licences is indicative and is not binding to the Contracting authority. Amount of licences during the contract period will be bought according to current needs of the Contracting authority.

User Support & Maintenance
- Details of arrangements for user support, including availability of support personnel and maximum response time to be discussed and agreed during negotiations and fixed as part of SLA (Service Level Agreement);
- Guarantee of timely release of software versions, bug fixes;
- Details of maintenance costs.

2.9 Schedule and Deadlines

- Deployment, implementation, configuration of the software and training of all the administrator level employees – 2 months from commencement date of contract after completion of which (or in parallel) additional trainings for the rest of the users could be planned. Detailed implementation schedule and proposed training plan explanation to be submitted by the Tenderer in Technical proposal.
- Maintenance and full Support through the overall project life-cycle.

3.   TECHNICAL SPECIFICATIONS - OPTIONAL

3.1 Systems Functional Requirements – Planning and Scheduling

- Validate schedule integrity with access to a full report of each project / schedule (i.e. 14 points DCMA Assessment, Schedule log, etc.).

3.2 Systems Functional Requirements – Risk Management / Risk Analysis tool

- Risk status/change notification;
- Risk escalation feature (e.g. high level risks get automatically escalated to next reporting level);
- Support cost risk analysis before a time schedule is completed.

3.3 Systems Functional Requirements – Reporting and Progressing

Remote Reporting
- Generation of reporting functionality is embedded in the cloud-based / web-based application:
  - The Reporting interface can be configurable at system and user level and present users with a summary of notifications and common functions;
  - The Reporting interface shall alert users of any updates or changes to information and a summary of incoming and outgoing tasks.
- Batch reporting: Reports can be produced in batches and Batches can be scheduled, including scheduled data export (e.g. to CSV file for automatically loading into other system).

Remote recording of progress and expenditure
- Web-based recording of progress and expenditure:
  - The Progress interface shall be configurable at system and user level and present users with a summary of notifications and common functions;

- The Progress interface shall alert users of any updates or changes to information and a summary of incoming and outgoing tasks.
- Facility to define hierarchical and/or non-hierarchical Work/Organizational Breakdown Structures to be assigned to activities for summarizing, sorting and filtering of data on screens and reports.

Earned Value Reports
- EVM trend analysis.

External Reporting Systems
- Possibility of integration with external reporting tools, such as Microsoft Power BI or Tableau or similar.

3.4 Systems Functional Requirements – Change Management

- Integrated Change Order / Variations Orders Register to facilitate:
  - Recording of scope changes at resource level;
  - Identify pending and approved changes to cost and schedule;
  - Reporting of impacts of changes to the overall schedule of costs and plans.

3.5 Systems Functional Requirements – Interface

Network Editor Interface
- Different types of interfaces:
  - Desktop Version (on top of the online);
  - No need for other software to be installed to enable the system to run (i.e. Citrix, Java, etc).

Information logging
- History of all actions within the solutions shall be stored in history log.

As-built information
- The solution shall support the up-load and amend the as-build data.

3.6 Data Storage, Access and Security

Security and storage
- Security minded principles and relevant security measures shall be applied to enable the software solution to aid effective collaboration while being mindful of increased risks of security breaches through widening access to RB Rail AS asset information associated with cloud and web-based solutions. Data storage, access and security measures must comply with current cybersecurity best practice.

Access rights
- Secure access to the system shall be ensured by using 2-factor authentication, if required.

Interoperability
- System shall support interoperability with other software vendors such as the Common Data Environment (to support 4D - construction sequencing or scheduling and 5D – cost workflows for BIM solutions) using native (built-in) functionality or via an application programming interface. Any such API should be part of the solution provided (with no additional licensing requirements or restrictions), documented in full and subject to a change control process which is in turn part of the Service Level Agreement. RB Rail AS BIM

Manual can be found here: http://www.railbaltica.org/wp-content/uploads/2019/04/RBR-DOC-BIM-BMA-0001_BIMManual-2.pdf.

4. Invitation to submit final proposals

[CONFIDENTIAL]

ANNEX 2 – ORACLE CLOUD SERVICES AGREEMENT

[Please see as a separate file]

ANNEX 3 – PERSONAL DATA PROCESSING AGREEMENT

Riga   4 February, 2020

RB Rail AS, registration No. 40103845025, registered address: Krišjāņa Valdemāra iela 8 - 7, Rīga, LV-1010, represented by Management Board Chairman Agnis Driksna and Management Board Member Ignas Degutis (**Customer**), and

PRM YAZILIM DANISMANLIK TIC LTD, STI, registration No. 510317, registered address: Kucukbakkalkoy Mah. Ayse Hatun Cesme Sok. 5/8 Atasehir Istanbul Turkey, represented by General Manager Nihat YILDIRIM (the **Supplier**) hereby undertake to meet the following requirements of the personal data protection:

1.   INTRODUCTION

1.1.   This Annex concerning the processing of personal data (the **Annex**) is an inseparable part of the Agreement on Planning, Scheduling, Reporting and Risk management software supply, implementation and maintenance (the **Agreement**), signed between the Supplier and the Customer.

1.2.   The purpose of this Annex is to agree on the privacy and data security of Customer's personal data in the software provided by the Supplier.

1.3.   The Annex is applicable when the Supplier processes personal data on behalf of the Customer based on the Agreement.

1.4.   This Annex forms an agreement on the processing on personal data in accordance with the EU General Data Protection Regulation (2016/679) (**GDPR**).

1.5.   In the event of any discrepancy between the provisions of the Agreement and this Annex, the provisions of this Annex shall prevail.

2.   DEFINITIONS

For the purposes of this Annex and in accordance with the GDPR, the following refers to:

2.1.   **"controller"** - the Customer, which determines the purpose and means of the processing of personal data.

2.2.   **"processor"** - the Supplier, which based on the Agreement, processes personal data on behalf of the controller.

2.3.   **"processing"** - 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.

2.4.   **"personal data"** - any information relating to an identified or identifiable natural person (**data subject**) that Supplier is processing on behalf of the Customer. 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.

2.5. **"personal data breach"** - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3. THE DUTIES OF THE SUPPLIER AND THE CUSTOMER

3.1. Based on the Agreement, the Supplier processes the Customer's personal data on behalf of the Customer based on the Agreement. Personal data may be for example the data identifying the employees, customers or other natural persons.

3.2. As the controller, the Customer is responsible for ensuring that it has the necessary rights to process personal data. The Customer is responsible for informing the data subjects of the processing of information concerning them. The Customer is responsible for the accuracy of the personal data provided to the Supplier.

3.3. The Customer has the right and obligation to determine the purpose and means of the processing of personal data. The subject-matter, nature and purposes of the processing are further defined in the Annex.

3.4. The Supplier has the right to process customer data only in accordance with the Agreement, this Annex and the written guidance of the Customer and only insofar as it is necessary to deliver the Products. The Supplier informs the Customer in case any non-compliance with the EU or competent jurisdiction's privacy legislation or regulation is detected under the guidance, except prohibitions by law, and in such case the Supplier may immediately refuse from and stop applying the Customer's guidance.

3.5. The Supplier maintains a description of the Software or other regulatory description of the processing operations performed by the Software. The Supplier has the right to collect anonymous and statistic data about the use of the Software under the Agreement, provided that the data does not identify the Customer or the data subject and is used for analysing and developing the Supplier's services.

4. DELETION OF/RETURNING THE PERSONAL DATA

4.1. At the expiry of the Agreement, the Supplier returns all the personal data to the Customer in accordance with the provisions of the Agreement, unless the applicable law requires the retention of the personal data.

5. SUBCONTRACTOR

5.1. The Supplier may use subcontractors for processing of the personal data. The Supplier is responsible for its subcontractor's actions as for its own and Supplier must sign similar written agreements with its subcontractors about the processing of personal data in cloud storage. If requested, the Supplier must in advance inform the Customer of the subcontractors it intends to use in the processing of personal data under the Agreement. The Customer has the right to deny the use of new subcontractors on reasonable grounds.

6. THE SUPPLIER'S OBLIGATION TO ASSIST

6.1. The Supplier must immediately forward all requests to inspect, rectify, erase, ban the processing of personal data or other requests received from the data subjects, to the

Customer. It is the Customer's duty to respond such requests. Considering the nature of the processing, the Supplier helps the Customer with appropriate technical and organisational measures, in order for the Customer to fulfil its duty to respond to the data subject's requests.

6.2. Considering the nature of the processing and the available data, the Supplier must assist the Customer in ensuring that the Customer complies with its obligations in accordance with the GDPR. Such obligations may concern data security, notifications of data security incidents, data protection impact assessment and prior consultations. The Supplier must assist the Customer only to the extent that the privacy legislation sets requirements for the processor of personal data.

6.3. The Supplier directs all inquiries from the supervisory authorities directly to the Customer if it is not prohibited by applicable law because the Supplier has no authority to represent the Customer or act on behalf of the Customer in the Customer Supervisory Authority.

7. DATA PROCESSING SPECIFICATION

7.1. Nature and purpose of service: Planning, Scheduling, Reporting and Risk management software supply, implementation and maintenance.

7.2. Categories of persons on which the processing operations apply: Representatives, employees and partners of the Customer, stakeholders of the Rail Baltica Global Project.

7.3. Categories of collected personal data:

7.3.1. First Name (required);

7.3.2. Last Name(required);

7.3.3. Email(required);

7.3.4. Office Postal Code (required);

7.3.5. Office City (required);

7.3.6. Office Country (required);

7.3.7. User photo;

7.3.8. User Title;

7.3.9. Phone Number;

7.3.10. Mobile Number.

7.4. Purpose of data processing: participation of employees of the Customer and its cooperation partners (any stakeholders of Rail Baltica Global Project under agreement) in architecture or engineering project management.

8. PROCESSING OUTSIDE OF EU / EEA

8.1. The Supplier and its subcontractors do not process outside the EU / EEA.

9. AUDITS

9.1. The Customer or a third-party auditor (not being a competitor of the Supplier) on behalf of the Customer may inspect the operations under this Annex.

9.2. The Parties agree on the date of the audit and other details no later than 14 working day before the audit. The audit must be carried out in a way that does not interfere with the Supplier's or its subcontractor's commitments with third Parties. The representative of the Customer and the auditor must sign confidentiality agreements.

9.3. Each Party must cover its own costs caused by the audit.

10. DATA SECURITY

10.1. The Supplier implements appropriate technical and organizational measures to protect the personal data, considering the risks that are presented by the personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. The technical options and the costs of the options in relation to the special risks connected with the processing of and sensitive nature of the personal data, of which the Customer has informed or in writing brought out, must be taken into account when organizing the security measures.

10.2. The Customer must ensure that the Supplier is informed of all matters regarding the personal data provided by the Customer, such as risk assessments and processing of special categories of persons, which may affect the technical and organizational measures in accordance with this Annex. The Supplier ensures that the personnel of the Supplier or its subcontractors, that take part in the processing of personal data, maintains appropriate confidentiality.

11. NOTIFICATION OF PERSONAL DATA BREACH

11.1. The Supplier notifies the Customer of all personal data breaches without undue delay after the Supplier having become aware of or its subcontractor having become aware of the personal data breach, but not later than within 24 hours from the moment when the Supplier or the Sub-Contractor became aware of the breach.

11.2. If requested by the Customer, the Supplier must without undue delay provide the Customer with all appropriate information of the personal data breach. To the extent that this information is held by the Supplier, the notification must describe at least:

11.2.1. the personal data breach that has taken place,

11.2.2. as far as possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned,

11.2.3. description of the likely consequences of the personal data breach, and

11.2.4. description of the remedial actions that the Supplier has taken or must take to prevent future personal data breach and, if necessary, also measures to mitigate its possible adverse effects.

11.3. The Supplier must without delay document the results of the investigation and the actions taken for the Customer.

11.4.   The Customer is responsible for necessary notifications to the supervisory authorities.

12.   OTHER PROVISIONS

12.1.   Customer shall be liable for the damage caused by processing which infringes the GDPR. Supplier shall be liable for the damage caused by processing only where it has not complied with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the Customer.

12.2.   Each Party is obliged to pay the part of the imposed damages and administrative fines that reflects its liability for the damage according to the supervisory authority or court decision. In other respects, the Parties' liability is determined in accordance with the Agreement.

12.3.   The Supplier informs the Customer in writing of all changes that may affect its ability or prospects to comply with this Annex and the written guidance of the Customer. The Parties will agree of all additions and changes to this Annex in writing.

12.4.   This Annex enters into force when signed by both Parties. The Annex remains in force for as long as the Agreement remains in force or the Parties have obligations towards each other based on the Agreement.

12.5.   The obligations, which due to their nature are intended to remain in force regardless of the expiry of this Annex remains in force after the expiry of this Annex.

12.6.   This Annex expires with respect to Agreement, when the processing of personal data under the Agreement and this Annex has ended.

13.   SIGNATURES

On behalf the Customer   On behalf of the Supplier

_____

Chairman of the Management Board   General Manager

Agnis Driksna   Nihat YILDIRIM

_____

Management Board Member

Ignas Degutis

ANNEX 4 – CORRESPONDENCE

Customer:

RB Rail AS, registered address: Kr.Valdemāra street 8-7, Riga, LV-1010, Latvia.

Supplier:

PRM YAZILIM DANISMANLIK TIC LTD, STI, registered address: Kucukbakkalkoy Mah. Ayse Hatun Cesme Sok. 5/8 Atasehir Istanbul Turkey.

ANNEX 5 – SUPPLIER'S DECLARATION

DECLARATION OF SUPPLIER

I, the undersigned duly authorised representative, on behalf of PRM YAZILIM DANISMANLIK TIC LTD, STI undertake:

1. To respect the freely-exercised right of workers, without distinction, to organize, further and defend their interests and to bargain collectively, as well as to protect those workers from any action or other form of discrimination related to the exercise of their right to organize, to carry out trade union activities and to bargain collectively;

2. Not to use forced or compulsory labour in all its forms, including but not limited to not employ people against their own free will, nor to require people to lodge 'deposits' or identity papers upon commencing employment;

3. Not to employ: (a) children below 15 years of age or, if higher than that age, the minimum age of employment permitted by the law of the country or countries where the performance, in whole or in part, of a contract takes place, or the age of the end of compulsory schooling in that country or countries, whichever is higher; and (b) persons under the age of 18 for work that, by its nature or the circumstances in which it is carried out, is likely to harm the health, safety or morals of such persons;

4. To ensure equality of opportunity and treatment in respect of employment and occupation without discrimination on grounds of race, colour, sex, religion, political opinion, national extraction or social origin and such other ground as may be recognized under the national law of the country or countries where the performance, in whole or in part, of a contract takes place;

5. To ensure the payment of wages in legal fashion, at regular intervals no longer than one month, in full and directly to the workers concerned; to keep an appropriate record of such payments. Deductions from wages will be conducted only under conditions and to the extent prescribed by the applicable law, regulations or collective Contract, and the workers concerned shall be informed of such deductions at the time of each payment. The wages, hours of work and other conditions of work shall be not less favourable than the best conditions prevailing locally (i.e., as contained in: (i) collective Contracts covering a substantial proportion of employers and workers; (ii) arbitration awards; or (iii) applicable laws or regulations), for work of the same character performed in the trade or industry concerned in the area where work is carried out;

6. To ensure, so far as is reasonably practicable, that: (a) the workplaces, machinery, equipment and processes under their control are safe and without risk to health; (b) the chemical, physical and biological substances and agents under their control are without risk to health when the appropriate measures of protection are taken; and (c) where necessary, adequate protective clothing and protective equipment are provided to prevent, so far as is reasonably practicable, risk of accidents or of adverse effects to health;

7. To support and respect the protection of internationally proclaimed human rights and not to become complicit in human rights abuses;

8. To create and maintain an environment that treats all employees with dignity and respect and will not use any threats of violence, sexual exploitation or abuse, verbal or psychological harassment or abuse. No harsh or inhumane treatment coercion or corporal punishment of any kind is tolerated, nor is there to be the threat of any such treatment;

9. To have an effective environmental policy and to comply with existing legislation and regulations regarding the protection of the environment; wherever possible support a precautionary approach to environmental matters, undertake initiatives to promote greater environmental responsibility and encourage the diffusion of environmentally friendly technologies implementing sound life-cycle practices;

10. To identify and manage chemical and other materials posing a hazard if released to the environment to ensure their safe handling, movement, storage, recycling or reuse and disposal;

11. To monitor, control and treat as required prior to discharge or disposal wastewater and solid waste generated from operations, industrial processes and sanitation facilities;

12. To characterize, monitor, control and treat as required prior to discharge or disposal air emissions of volatile organic chemicals, aerosols, corrosives, particulates, ozone depleting chemicals and combustion by-products generated from operations;

13. To reduce or eliminate at the source or by practices, such as modifying production, maintenance and facility processes, materials substitution, conservation, recycling and re-using materials, waste of all types, including water and energy;

14. To adhere to the highest standards of moral and ethical conduct, to respect local laws and not engage in any form of corrupt practices, including but not limited to extortion, fraud, or bribery;

15. To disclose (a) any situation that may appear as a conflict of interest, such as but not limited to: where a Supplier or an undertaking related to the Supplier has advised a Beneficiary or Implementing Body or has otherwise been involved in the preparation of the procurement procedure; and (b) if any Beneficiaries' or Implementing Bodies' official, professional under contract with Beneficiary or Implementing Body or sub-contractor may have a direct or indirect interest of any kind in the Supplier's business or any kind of economic ties with the Supplier;

16. Not to offer any benefit such as free goods or services, employment or sales opportunity to a Beneficiary's and Implementing Body's staff member in order to facilitate the Suppliers' business with Beneficiaries or Implementing Bodies;

17. Within a period set in the applicable national legislation following separation from service or award of a contract, as the case may be, to refrain from offering employment to any Beneficiaries' and Implementing Bodies' staff in service and former Beneficiaries' and Implementing Bodies' staff members who participated in the procurement process and to whom a legal restriction to receive material benefits from or be employed by a Supplier which participated in a procurement procedure or restrictions with similar effect applies;

18. To promote the adoption of the principles set forth in this Supplier's Declaration by my potential business partners and promote the implementation of the principles set forth in this document towards own Suppliers;

19. Not procure goods, works and services from other Suppliers:

a. Who, or its member of the Management Board or the Supervisory Board or procurator of such Supplier, or a person having the right to represent such Supplier in activities related to a subsidiary, has been found guilty in any of the following criminal offences by a such punishment prescription of prosecutor or a judgement of a court that has entered into effect and is non-disputable and not subject to appeal:

i. bribetaking, bribery, bribe misappropriation, intermediation in bribery, taking of prohibited benefit or commercial bribing;

ii. fraud, misappropriation or laundering;

iii. evading payment of taxes and payments equivalent thereto,

iv. terrorism, financing of terrorism, invitation to terrorism, terrorism threats or recruiting and training of a person for performance of terror acts;

b. who, by such a decision of a competent authority or a judgment of a court which has entered into effect and has become non-disputable and not subject to appeal, has been found guilty of an infringement of employment rights which means:

i. employment of such one or more citizens or nationals of countries, which are not citizens or nationals of the European Union Member States, if they reside in the territory of the European Union Member States illegally;

ii. employment of one person without entering into a written employment contract, not submitting an informative declaration regarding employees in respect of such person within a time period laid down in the laws and regulations, which is to be submitted regarding persons who commence work;

c. who, by such a decision of a competent authority or a judgment of a court which has entered into effect and has become non-disputable and not subject to appeal, has been found guilty of

infringement of competition rights manifested as a vertical Contract aimed at restricting the opportunity of a purchaser to determine the resale price, or horizontal cartel Contract, except for the case when the relevant authority, upon determining infringement of competition rights, has released the candidate or tenderer from a fine or reduced fine within the framework of the co-operation leniency programme;

d. whose insolvency proceedings have been announced (except the case where a bailout or similar set of measures is applied within insolvency proceedings oriented towards prevention of possible bankruptcy and restoration of solvency of the debtor, in which case I shall evaluate the possibility of such Supplier to participate in the tender), economic activity of such Supplier has been suspended or discontinued, proceedings regarding bankruptcy of such Supplier have been initiated or such Supplier will be liquidated;

e. who has tax debts in the country where the procurement is organised or a country where such Supplier is registered or permanently residing, including debts of State social insurance contributions, in total exceeding an amount which is common threshold in public procurements in the respective country.

_____ Nihat YILDIRIM, General Manager, 04.02.2020.

ANNEX 6 – TECHNICAL PROPOSAL

[CONFIDENTIAL]

ANNEX 7 – FINANCIAL PROPOSAL

[CONFIDENTIAL]