GDPR AGREEMENT

Between

, hereinafter referred to as "**DATA CONTROLLER**" or "**USER**",

And

Editions Technique et Ferroviaires, Société par actions simplifiée incorporated under French law**,** headquartered at 16, rue Jean Rey, F-75015 Paris, SIRET (French business registration number) 47957875900017, represented by its chair Union Internationale des Chemins de fer, represented by Mr François Davenne, Director General "**DATA-PROCESSOR**" or "**UIC**",

hereinafter collectively referred to as the "**Parties**" or separately as a "**Party**".

Whereas:

- USER wishes to use eTCD services consisting in a modern, flexible for users and administrative staff, European-wide ticket control information system for the use of railway companies around the world with the aim to provide high quality ticket usage data concerning passenger services for users, namely the ticket control information systems, distribution systems, railway companies etc. whereby the UIC provides to USER eTCD services implementing the ticket data exchanges, including a central electronic ticketing control database for e-ticket control as defined in IRS 90918-4 ed 2024 (thereafter referred to as the "**Services**");
- UIC and USER have entered into an eTCD Agreement dated (hereinafter the "eTCD agreement") whereby the UIC provides to USER eTCD services implementing the ticket data exchanges, including a central electronic ticketing control database for e-ticket control as defined in IRS 90918-4 ed 2024;
- UIC is considered to be a DATA PROCESSOR as defined in article 4 (8) of the EU General Data Protection Regulation 2016/79 (hereinafter "GDPR") processing personal data, on behalf of the DATA CONTROLLER as defined in article 4 (7) of the GDPR, provided by the USER (e-ticket allocators);
- Parties wish by entering into this GDPR Agreement to comply amongst others with articles 28 of the GDPR. UIC declares that for the provision of services, UIC subcontracts the provision of IT services to a third Party which USER approves in compliance with article 28 (2) and (4) of the GDPR that refer to the case where a processor engages another party for carrying out processing activities;
- This GDPR Agreement is the Appendix 1 to the eTCD Agreement and entering into the GDPR Agreement constitutes an essential condition without which UIC would not enter into the said eTCD Agreement.

Parties have agreed the following:

1. Subject-matter of this GDPR Agreement

1.1 DATA CONTROLLER subcontracts certain services (as defined below) that may require the processing of personal data (subject to the duty to mitigate the transfer of personal data as provided under the GDPR) by the DATA PROCESSOR. For the avoidance of doubts, the DATA CONTROLLER shall be considered as being the DATA CONTROLLER only for the data it relates to and according to the purpose it defined and not for the data to which the DATA CONTROLLER and/or its stakeholders will not have access to.

1.2 This GDPR Agreement lays down the rights and obligations of the Parties in accordance with Article 3 and 28 of the GDPR.

1.3 The legal terms used in this GDPR Agreement shall have the meaning defined in Article 4 of the GDPR.

1.4 This GDPR Agreement consists of 18 Points and 3 Appendixes, which are deemed to be an inseparable part of this GDPR Agreement:

- Appendix 1: Dealing with data breaches.
- Appendix 2: Personal data processing and IT security.
- Appendix 3: Summary of eTCD GDPR processing.

2. Object and purpose of this GDPR Agreement

2.1 This GDPR Agreement applies to the processing of personal data in the context of the fulfilment of the Services.

3. INTENTIONALLY LEFT IN BLANK

4. Relationship between the Parties

4.1 In accordance with this GDPR Agreement, DATA CONTROLLER gives the DATA PROCESSOR instructions to process personal data that are necessary for the fulfilment of the Services.

4.2 With respect to the processing of personal data, UIC is considered to be the processor as defined in article 4 of the GDPR. USER is considered to be the DATA CONTROLLER as defined in article 4 of the GDPR and has and retains independent control of the purpose for which the personal data is processed and of the resources used to do so.

4.3 Prior to entering into this GDPR Agreement, the DATA PROCESSOR has ensured that DATA CONTROLLER is sufficiently informed about the Services provided by the DATA PROCESSOR and about the data processing and sub-processing to be carried out.

4.4 DATA CONTROLLER and the DATA PROCESSOR will give each other all the required information to ensure proper compliance with the relevant legislation and regulations regarding privacy.

5. Processing of personal data and related obligations of the DATA PROCESSOR

5.1 The processing of personal data as part of the performance of the Services shall comply with the applicable data protection laws and regulations, including the GDPR and any additional national legislation (if applicable). References made in this Agreement to the GDPR are to be understood as references to the applicable national legislation insofar as the data transfers are subject to it: Common requirements in terms of data processing are summarized under Appendix 3 of this GDPR Agreement.

5.2 The DATA PROCESSOR shall undertake not to use the personal data obtained from DATA CONTROLLER for other purposes or in any other way than that for which the data has been transmitted or disclosed. The DATA PROCESSOR is therefore not authorised to carry out any data processing operations other than those entrusted to it by DATA CONTROLLER. This obligation applies both during the term of this GDPR Agreement and after this GDPR Agreement has ended. By entering into this Agreement and notwithstanding the aforesaid, the DATA CONTROLLER expressly gives consent to DATA PROCESSOR using the data in anonym form for statistical purposes only during the performance of this GDPR Agreement.

5.3 The personal data categories as described in IRS 90918-4 will be used under the GDPR Agreement, subject always to the duty to mitigate the transfer of personal data to data that are strictly necessary to perform the Services.

5.4 The DATA PROCESSOR shall:

- create and maintain a record of its data processing activities in accordance with article 30 of the GDPR under this GDPR Agreement; if requested to do so, the DATA PROCESSOR shall, at the first time of asking, make the record available to DATA CONTROLLER, any auditor appointed by the latter, and/or the supervisory authority;
- promptly inform DATA CONTROLLER if it is not able to comply with DATA CONTROLLER's instructions with respect to the processing of the personal data or with any other obligation under this GDPR Agreement;
- inform DATA CONTROLLER immediately if it believes that any instructions from DATA CONTROLLER infringe the GDPR or other applicable data protection laws and regulations;
- deal promptly and properly with all reasonable inquiries from DATA CONTROLLER relating to the processing of personal data under this GDPR Agreement;
- make available to DATA CONTROLLER all information necessary to demonstrate compliance with the GDPR or other applicable data protection laws and regulations;
- not process the personal data for longer than the required retention period. DATA CONTROLLER will adequately inform the DATA PROCESSOR about the (legal) retention periods applicable to the processing of the personal data;
- submit its data processing facilities for audit or control of the data processing activities, in accordance with point 7.7 of this GDPR Agreement;
- promptly notify DATA CONTROLLER of:
  - any legally binding request for disclosure of the personal data by a data subject or by a judicial or regulatory authority (unless prohibited from doing so, for example by an obligation under criminal law to preserve the confidentiality of a judicial investigation), and to assist DATA CONTROLLER herewith,
  - any accidental or unauthorized access, and any unlawful processing more generally, and to assist DATA CONTROLLER herewith;

- not pass personal data on to third parties, unless this exchange takes place for the purpose of performing the Services or if it is necessary to meet a legal obligation imposed on the DATA PROCESSOR. The DATA PROCESSOR shall ensure that everyone involved in processing the personal data, including its employees, representatives and/or subcontractors, has entered into a confidentiality agreement or accepted a confidentiality clause. Should transfer to third parties be required by a legal obligation, the DATA PROCESSOR shall verify the basis for the request and the identity of the requesting party prior to transferring any personal data. In addition, if legally allowed to do so, the DATA PROCESSOR shall notify DATA CONTROLLER immediately of the transfer, if possible, prior to transferring the personal data;

- refrain from engaging any additional data sub-processor, other than those listed in point 10 of this contract, without the prior written consent of DATA CONTROLLER;

- the personal data subject to this GDPR Agreement shall not be transferred to any country outside the European Economic Area ("EEA") without prior written consent from DATA CONTROLLER. This could be the case when a railway undertaking outside the EEA would make use of the Services. If the Personal Data is transferred to a country outside the EEA, the Parties shall ensure that said personal data is adequately protected in line with the GDPR. Any transfer of personal data to a country outside the EEA shall be subject to an appropriate agreement between the DATA CONTROLLER and the railway undertaking, unless the country of destination to which the personal data is transferred is covered by an adequacy decision of the European Commission.

6. Confidentiality

6.1 Each Party to this GDPR Agreement acknowledges that during the performance of its obligations, a Party (the "receiving Party") may become privy to confidential information which is disclosed by the other Party (the "disclosing Party").

6.2 The receiving Party shall keep confidential all such confidential information as well as the Personal Data and shall not disclose it to any third party or use it for any other purposes than those of this GDPR Agreement.

6.3 Each Party agrees that before any of its employees, sub-processors or agents are given access to confidential information and/or Personal Data, each of them shall agree to be bound by a confidentiality agreement under comparable terms and conditions to those defined in this GDPR Agreement.

6.4 The DATA PROCESSOR shall ensure in each case that access is strictly limited to those individuals who need to know / access the personal data for the purposes of this Data Sub- Processing Contract.

6.5 If the receiving Party has a legal duty to disclose confidential information, e.g. by a court order, the receiving Party shall, to the extent possible, inform the disclosing Party of this fact without delay, thereby enabling the disclosing Party to seek an interlocutory injunction or other appropriate remedy.

7. Security and checks

7.1 The DATA PROCESSOR shall take appropriate technical and organisational measures to secure personal data against loss or against any form of unlawful data processing. These measures shall ensure an appropriate level of security, taking into account technical developments and implementation costs, and having regard to the risks associated with the processing of personal

data and the nature of the personal data to be protected, as described under Appendix 2 of this GDPR Agreement.

7.2 The measures referred to in point 7.1 shall include, at the very least:

- pseudonymisation and encryption of the personal data;
- measures enabling the availability of and access to the personal data to be restored in a timely manner in the event of a physical or technical incident;
- measures guaranteeing that only authorised employees have access to the personal data being processed under this GDPR Agreement;
- measures protecting the personal data, in particular against unintentional or unlawful destruction, unintentional loss or modification, or unauthorised or unlawful storage, processing, access or publication;
- measures whereby weak spots in the processing of personal data can be regularly identified in the systems used for providing services to DATA CONTROLLER;
- an appropriate information security policy for processing personal data.

7.3 The DATA PROCESSOR shall evaluate and strengthen, supplement or improve the information security measures it has taken, insofar as the requirements or technological or other developments give reason to do so.

7.4 The agreements between the Parties on the technical and organisational measures to be taken and the content and frequency of the reports to be supplied by the DATA PROCESSOR to DATA CONTROLLER on the security measures are : once at the beginning of the Services and every time a substantial change is made in the Services leading to a new major version of the IRS 90918-4.

7.5 The DATA PROCESSOR may use its adherence to an approved code of conduct or an approved certification mechanism to demonstrate its compliance with the technical and organisational measures required.

7.6 The DATA PROCESSOR shall enable DATA CONTROLLER to comply with its legal obligations to monitor compliance by the DATA PROCESSOR, in particular with the technical and organisational security measures, and with the obligations regarding data breaches as stated in Point 8.

7.7 DATA CONTROLLER may at any time audit (or commission an audit of) the technical and organisational security measures taken by the DATA PROCESSOR to ensure compliance with the GDPR, the applicable legislation and regulations, and this GDPR Agreement. This audit, the cost of which shall be borne by DATA CONTROLLER, shall be arranged in consultation with the DATA PROCESSOR, who shall be given reasonable notice thereof. The Parties may agree by mutual consent that the audit will be performed by a certified and independent auditor hired by the DATA PROCESSOR; this auditor shall issue a Third-Party Memorandum (TPM). DATA CONTROLLER shall be informed of the results of the audit. The costs of the audit shall be borne by the DATA PROCESSOR if and insofar as it has breached either the applicable legislation and regulations or this GDPR Agreement and shall be otherwise borne by the DATA CONTROLLER.

8. Data Breaches

8.1 The DATA PROCESSOR shall adopt an appropriate policy for handling data breaches as further

described under Appendix 1 of this GDPR Agreement.

8.2 If the DATA PROCESSOR becomes aware of a data breach, it shall notify DATA CONTROLLER as swiftly as possible, in accordance with the instructions in Appendix 1 to this GDPR Agreement. In the event of a data breach, the DATA PROCESSOR shall provide DATA CONTROLLER with all the relevant information about the data breach, including:

- the nature of the data breach,
- the categories and approximate number of data subjects concerned,
- the categories and approximate number of personal data records concerned,
- any further developments regarding the data breach,
- the likely consequences of the data breach,
- the measures taken by the DATA PROCESSOR to mitigate the impact of the data breach and prevent recurrence on its side.

8.3 If it transpires that the security breach is likely to have adverse effects on the privacy of the data subjects, the DATA PROCESSOR shall notify DATA CONTROLLER as swiftly as possible.

8.4 In the event of a data breach, the DATA PROCESSOR shall allow DATA CONTROLLER to take suitable follow-up steps in relation to the data breach; the DATA PROCESSOR shall use the existing processes that DATA CONTROLLER has set up for this purpose. The Parties undertake to take all reasonably required measures as quickly as possible in order to prevent or reduce (further) infringement or breaches concerning the processing of personal data and, in particular, (further) infringements or breaches of the GDPR or other data protection laws and regulations.

8.5 In the event of a data breach, DATA CONTROLLER will in turn notify the National Data Protection Authority of the data breach within 72 hours of DATA CONTROLLER being informed of it by the DATA PROCESSOR, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

9. Procedural rights of data subjects

9.1 DATA CONTROLLER shall comply with its duty to provide information on the purpose and means of processing and to grant access to the personal data to the owners of these personal data in compliance with the GDPR and with Appendix 3. Upon reasonable request by a DATA CONTROLLER, DATA PROCESSOR shall bring reasonable support to DATA CONTROLLER in order to allow the latter to comply with its obligations resulting from GDPR regulations.

9.2 In the unlikely event that DATA PROCESSOR receives complaints or requests from a data subject relating to the processing of the personal data shall be forwarded to DATA CONTROLLER by the DATA PROCESSOR without delay, since DATA CONTROLLER is responsible for handling such requests.

9.3 The DATA PROCESSOR shall, to the extent possible, cooperate fully with DATA CONTROLLER in order to meet the obligations pursuant to Articles 16 - 22 GDPR, in particular the rights of data subjects to request the inspection, correction, addition or deletion of personal data, and shall do so within the legally defined time limits. DATA CONTROLLER shall provide DATA PROCESSOR with instructions in this regard. The Parties shall consult in good faith on the reasonable distribution of any costs related to guaranteeing the procedural rights of data subjects.

10. Sub-Processors

10.1 For the provision of the eTCD service, the DATA PROCESSOR has GDPR-compliant sub-processor agreement with the following company:

- Hit Rail B.V., Stadsplateau 7, 3521 AZ Utrecht, Netherlands
- InQdo B.V. (subcontracted by Hitrail B.V.), Coltbaan 1-19, 3439 NG Nieuwegein, Netherlands

The DATA PROCESSOR may not commission an additional sub-processor (other than listed above) to process personal data without the explicit prior written permission of DATA CONTROLLER. DATA CONTROLLER shall not refuse such permission without reasonable grounds.

10.2 The DATA PROCESSOR shall contractually require each sub-processor to comply with at least the same obligations as those set out in this GDPR Agreement.

10.3 Irrespective of the permission given by DATA CONTROLLER, the DATA PROCESSOR shall remain liable for the actions of its sub-processors as designated in point 10.1.

10.4 In any event, the DATA PROCESSOR shall make contractually certain that no sub-processor processes personal data further than has been agreed as part of this Data Processing Contract.

11. Liability and Insurance

Article 8 of the ETCD agreement applies.

12. Provisions contrary to law and loopholes in the GDPR Agreement

12.1 Should any individual provision of this GDPR Agreement prove to be wholly or partly invalid or inoperable, this shall not affect the other provisions of the Data Sub- Processing Contract or the validity of the GDPR Agreement. In place of the invalid or inoperable provision, the Parties shall agree on a valid and operable provision which is as close as possible to the meaning and objective of the invalid provision.

12.2 If this GDPR Agreement proves to have loopholes, the Parties shall agree on provisions which correspond to the meaning and objectives of the GDPR Agreement and which would have been agreed had the loopholes been detected.

13. Languages

This GDPR Agreement is drawn up in the English language. This English version is authoritative. Translations may only be used internally by the Parties.

14. Amendment of the GDPR Agreement

14.1 Any amendments to this GDPR Agreement must be agreed in writing by both Parties.

14.2 Should a Party fail to exercise any of its rights under this GDPR Agreement, or should it fail to react in the event of a breach of obligations by the other Party, this shall not be interpreted as that Party waiving its right, nor shall it preclude any further exercise of any such rights in future. Any waiver of a right must be given expressly and in writing. If one Party has given an express written waiver of a right following a specific failure by a Party, this waiver cannot be invoked by the other Party in favour of a new failure, whether similar to the first or of any

other kind.

15. INTENTIONALLY LEFT IN BLANK

16. Duration and Termination

16.1 This GDPR Agreement is an accessory to the eTCD Agreement that is the principal, and Parties would not have entered into one of the agreements without entering into the other. As a consequence, Parties shall be entitled to terminate this GDPR Agreement under the same conditions than those applying to the eTCD Agreement. Both GDPR Agreement and eTCD Agreement shall expire under the same conditions and at the same time.

16.2 Termination of this GDPR Agreement shall not release the Parties from their obligations under this GDPR Agreement, which because of their nature are deemed to continue even after termination.

17. Return or deletion of Personal Data

17.1 The DATA PROCESSOR is obliged by DATA CONTROLLER to transfer the personal data processed on the instructions of DATA CONTROLLER within twenty one (21) days after the termination of GDPR Agreement to DATA CONTROLLER if DATA CONTROLLER requires such transfer before the end of the retention period, or within twenty one (21) days after the first instruction in writing by DATA CONTROLLER to do so, and to delete it from its systems and to destroy it or have it destroyed, unless the Personal Data has to be stored for a longer period, for example as a consequence of legal or other obligations, or on request by DATA CONTROLLER.

17.2 The DATA PROCESSOR shall confirm to DATA CONTROLLER (in writing or electronically) that the destruction of the processed Personal Data has taken place. DATA CONTROLLER may carry out a check that the destruction has taken place at its own expense.

17.3 The DATA PROCESSOR shall inform all sub-processors involved in the processing of personal data of the termination of the GDPR Agreement, and shall guarantee that all sub-processors destroy the personal data or have it destroyed.

17.4 The DATA CONTROLLERS are aware that they can consult data only relevant for their control purposes, according to the access rules set by the issuer of the ticket (“Allowed Access” field).

Tickets data are stored within eTCD until the occurrence of the following event, whichever comes first:

- Ticket expiry date; or
- 6 months after the date of travel of the ticket, subject to GDPR rule.

18. Jurisdiction and Applicable Law for Lawsuits between the Parties.

The Agreement is governed by French national law and the Parties submit to the exclusive jurisdiction of the relevant Court of Paris in relation to any disputes (contractual and/or non-contractual) concerning the Agreement

For the avoidance of doubts, it is hereby agreed between the Parties that this clause applies only

to the disputes between the DATA CONTRLLOER and the DATA PROCESSOR and shall not impact, modify or limit the entitlements and obligation of DATA CONTROLLER and of the data subjects under their national laws.

Date:

Signatures:

For the DATA CONTROLLER	For the DATA PROCESSOR