Data Processing Addendum

This Data Processing Addendum ("DPA") supplements the Terms of Service (the "Agreement") entered into by and between Railway Corporation ("Company" or "Railway") and the Customer entity that is a party to the Agreement ("Customer") (and, together, the "Parties"). This DPA incorporates the terms of the Agreement, and any capitalized terms that are used but not defined in this DPA shall have the meanings set forth in the Agreement.

In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms in the Standard Contractual Clauses; (2) the terms of this DPA; (3) the Agreement, and (4) Company's Privacy Policy. Any claims brought in connection with this DPA will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

1. Definitions

1.1 "Authorized Subprocessor" means a third-party entity engaged by Company to process Personal Data in order to provide the Services and that has been approved by Customer in accordance with Section 6.

1.2 "Company Account Data" means personal data that relates to Company's relationship with Customer, including the names or contact information of individuals authorized by Customer to access Customer's account and billing information of individuals that Customer has associated with its account. Company Account Data also includes any data Company may need to collect for the purpose of managing its relationship with Customer, identity verification, or as otherwise required by applicable laws and regulations.

1.3 "Company Usage Data" means Service usage data collected and processed by Company in connection with the provision of the Services, including without limitation data used to identify the source and destination of a communication, activity logs, and data used to optimize and maintain performance of the Services, and to investigate and prevent system abuse.

1.4 "Company's Privacy Policy" means the privacy policy set forth at https://railway.com/legal/privacy.

1.5 "Data Privacy Framework" means, as applicable, EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and/or the Swiss-U.S. Data Privacy Framework.

1.6 "Data Subject" means a natural person whose Personal Data is protected by Privacy Laws. For the avoidance of doubt, "Data Subject" includes the term "Consumer" under Privacy Laws.

1.7 "Data Subject Rights" means the rights recognized and granted to Data Subjects with respect to their Personal Data under Privacy Laws, including, when effective, the GDPR (as set forth in Articles 12 through 22 thereof) and the Data Privacy Framework.

1.8 "ex-EEA Transfer" means the transfer of Personal Data subject to the GDPR from the European Economic Area (the "EEA"), to a country where the transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the GDPR.

1.9 "ex-UK Transfer" means the transfer of Personal Data subject to Chapter V of the UK GDPR from outside the United Kingdom (the "UK") where such transfer is not governed by an adequacy decision made by the Secretary of State in accordance with the relevant provisions of the UK GDPR and the Data Protection Act 2018.

1.10 "Personal Data" means any information provided to Company by or on behalf of Customer in connection with the Services that relates to an identified or identifiable Data Subject and constitutes "personal data," "personal information," or equivalent term under Privacy Laws.

1.11 "Privacy Laws" means any applicable laws and regulations in any relevant jurisdiction relating to the processing of Personal Data including, each, to the extent applicable (i) the General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR") and the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "UK GDPR") (together, collectively, the "GDPR"), (ii) the Swiss Federal Act on Data Protection, (iii) the UK Data Protection Act 2018, (iv) the Privacy and Electronic Communications (EC Directive) Regulations 2003, and (v) U.S. state comprehensive privacy laws, such as the California Consumer Privacy Act, as amended by the California Privacy Rights Act of 2020 (the "CCPA"); in each case, as updated, amended or replaced from time to time. Each of the terms "affiliate," "business purpose," "Controller," "Personal Data Breach," "Processor," "process" or "processing," "sell," "share," or "Supervisory Authority," shall have the meaning set forth for that or any equivalent term under Privacy Laws. The terms "Controller" and "Processor" include "Business" and "Service Provider," respectively, each as defined in the CCPA.

1.12 "Standard Contractual Clauses" means, as applicable, (i) with respect to ex-EEA Transfers, the means standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for

transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time), as modified by Section 9 of this DPA. (the "EU SCCs") and, (ii) with respect to ex-UK Transfers, the EU SCCs amended by the UK Addendum (the "UK SCCs")

1.13 "UK Addendum" means the template International Data Transfer Addendum issued by the Information Commissioner and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022 (as may be amended from time to time), as completed by Exhibit D.

2. Role of the Parties; Description of Processing.

2.1 With respect to Personal Data, Customer is the Controller and Company is a Processor, or to the extent Customer is a Processor to a third-party Controller, except as expressly set forth in this DPA or the Agreement, Company is a subprocessor.

2.2 Company shall not process not process Personal Data (i) for purposes other than those set forth in the Agreement and/or Exhibit A, (ii) in a manner inconsistent with this DPA or any other documented instructions provided by Customer, including with regard to transfers of Personal Data to a third country or an international organization, unless required to do so by Supervisory Authority to which Company is subject; in such a case, Company shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest, or (iii) in violation of Privacy Laws. Customer hereby instructs Company to process Personal Data in accordance with the foregoing and as part of any processing initiated by Customer in its use of the Services. The subject matter, nature, purpose, and duration of this processing, as well as the types of Personal Data collected and categories of Data Subjects involved, are described in Exhibit A to this DPA.

3. Customer's Obligations. Customer shall, in its use of the Services, at all times process Personal Data, and provide instructions for the processing of Personal Data, in compliance with Privacy Laws. Customer shall ensure that the processing of Personal Data in accordance with Customer's instructions will not cause Company to be in breach of the Privacy Laws. Customer is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Company by or on behalf of Customer, (ii) the means by which Customer acquired any such Personal Data, and (iii) the instructions it provides to Company regarding the processing of such Personal Data. Customer shall not provide or make available to Company any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Services, and shall indemnify Company from all claims and losses in connection therewith. Company shall immediately notify Customer if an instruction, in Company's opinion, infringes Privacy Laws or instruction of a Supervisory Authority.

4. Use of Personal Data. Company shall not: (i) sell or share Personal Data; (ii) retain, use, or disclose Personal Data outside of Company's direct business relationship with Customer or for any purpose other for a business purpose under the CCPA on behalf of Customer or than as necessary to perform the Services for Customer pursuant to the Agreement, except as otherwise permitted in Agreement or by Privacy Laws; and (iii) combine Personal Data received from, or on behalf of, Customer with Personal Data that it receives from, or on behalf of, another party or person, except as necessary to provide the Services or as otherwise instructed by Customer.

5. Audit.

5.1 Company shall maintain records sufficient to demonstrate its compliance with its obligations under this DPA. Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Company shall, either (i) make available for Customer's review copies of certifications or reports demonstrating Company's compliance with prevailing data security standards applicable to the processing of Personal Data, or (ii) if the provision of reports or certifications pursuant to (i) is not reasonably sufficient under Privacy Laws, allow Customer's independent third party representative to conduct an audit or inspection of Company's data security infrastructure and procedures that is sufficient to demonstrate Company's compliance with its obligations under Privacy Laws, *provided that* (a) Customer provides reasonable prior written notice of any such request for an audit and such inspection shall not be unreasonably disruptive to Company's business; (b) such audit shall only be performed during business hours and occur no more than once per calendar year; and (c) such audit shall be restricted to data relevant to Customer. Customer shall be responsible for the costs of any such audits or inspections, including without limitation a reimbursement to Company for any time expended for on-site audits. If Customer and Company have entered into Standard Contractual Clauses as described in Section 9 (Transfers of Personal Data), the parties agree that the audits described in Clause 8.9 of the EU SCCs shall be carried out in accordance with this Section 5.1.

5.2 To the extent permitted under Privacy Laws, if Customer determines that Company is processing Personal Data in an unauthorized manner, Customer may, taking into account nature of Company's processing and the nature of the Personal Data processed by Company on behalf of Customer, and upon providing prior written notice, take commercially reasonable and appropriate steps to stop and remediate such unauthorized processing.

6. Authorized Subprocessors.

6.1 Customer acknowledges and agrees that Company may (1) engage its affiliates as well as the Authorized Subprocessors listed in Exhibit B to this DPA to access and process Personal Data in connection with the Services and (2) from time to time engage additional third parties for the purpose of providing the Services, including without limitation the processing of Personal Data pursuant to Section 6.2. By way of this DPA, Customer provides general written authorization to Company to engage subprocessors as necessary to perform the Services.

6.2 A list of Company's current Authorized Subprocessors (the "List") is available at trust.railway.com. Company may provide a mechanism to subscribe to notifications of new Authorized Subprocessors and Customer agrees to subscribe to such notifications where available. At least ten (10) days before enabling any third party other than existing Authorized Subprocessors to access or participate in the processing of Personal Data, Company will add such third party to the List and notify Customer via email. Customer may object to such an engagement by informing Company within ten (10) days of receipt of the aforementioned notice to Customer, provided such objection is in writing and based on reasonable grounds relating to data protection. Customer acknowledges that certain subprocessors are essential to providing the Services and that objecting to the use of a subprocessor may prevent Company from offering the Services to Customer. If Customer does not object to the engagement of a third party within ten (10) days of notice by Company, that third party will be deemed an Authorized Subprocessor.

6.3 If Customer reasonably objects to an engagement in accordance with Section 6.2, and Company cannot provide a commercially reasonable alternative within a reasonable period of time, Customer may discontinue the use of the affected Service by providing written notice to Company. Discontinuation shall not relieve Customer of any fees owed to Company under the Agreement.

6.4 Company will enter into a written agreement with the Authorized Subprocessor imposing on the Authorized Subprocessor data protection obligations comparable to those imposed on Company under this DPA with respect to the protection of Personal Data. In case an Authorized Subprocessor fails to fulfill its data protection obligations under such written agreement with Company, Company will remain liable to Customer for the performance of the Authorized Subprocessor's obligations under such agreement.

6.5 If Customer and Company have entered into Standard Contractual Clauses as described in Section 9 (Transfers of Personal Data), (i) the above authorizations will constitute Customer's prior written consent to the subcontracting by Company of the processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the parties agree that the copies of the agreements with Authorized Subprocessors that must be provided by Company to Customer pursuant to Clause 9(c) of the EU SCCs may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by Company beforehand, and that such copies will be provided by Company only upon request by Customer.

7. Confidentiality; Security of Personal Data.

7.1 Company shall ensure that any person it authorizes to process Personal Data has agreed to protect Personal Data in accordance with Company's confidentiality obligations in the Agreement. Customer agrees that Company may disclose Personal Data to its advisers, auditors or other third parties as reasonably required in connection with the performance of its obligations under this DPA, the Agreement, or the provision of Services to Customer.

7.2 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Company shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing Personal Data, as described in Exhibit C.

8. Personal Data Breach.

8.1 In the event of a Personal Data Breach, Company shall, without undue delay, inform Customer of the Personal Data Breach and take such steps as Company in its sole discretion deems necessary and reasonable to remediate such Personal Data Breach, to the extent that remediation is within Company's reasonable control.

8.2 In the event of a Personal Data Breach, Company shall, taking into account the nature of the processing and the information available to Company, provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under Privacy Laws with respect to notifying (i) the relevant Supervisory Authority or regulatory agency and (ii) Data Subjects affected by such Personal Data Breach without undue delay.

8.3 The obligations described in Sections 8.1 and 8.2 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Customer. Company's obligation to report or respond to a Personal Data Breach under Sections 8.1 and 8.2 will not be construed as an acknowledgement by Company of any fault or liability with respect to the Personal Data Breach.

9. Transfers of Personal Data.

9.1 The parties agree that Company may transfer Personal Data processed under this DPA outside the EEA, the UK, or Switzerland as necessary to provide the Services. Customer acknowledges that Company's primary processing operations take place in the United States and that the transfer of Personal Data to the United States is necessary for the provision of the Services to Customer. Without limiting the foregoing, Company may provide options for certain local data storage to Customer if Customer is receiving Paid Services pursuant to the Agreement. If Company transfers Personal Data protected under this DPA to a jurisdiction for which the European Commission has not issued an adequacy decision, Company will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Privacy Laws.

9.2 Ex-EEA Transfers. The Parties agree that ex-EEA Transfers shall either be made pursuant to (i) the Data Privacy Framework to the extent the recipient of the ex-EEA Transfer is certified accordingly, or (ii) the EU SCCs, which are deemed entered into (and incorporated into this DPA by this reference) and completed as follows:

9.2.1 Module One (Controller to Controller) of the EU SCCs applies when Company is processing Personal Data as a controller pursuant to Section 9 of this DPA.

9.2.2 Module Two (Controller to Processor) of the EU SCCs applies when Customer is a controller and Company is a processor of Personal Data in accordance with Section 2 of this DPA.

9.2.3 Module Three (Processor to Subprocessor) of the EU SCCs applies when Customer is a processor and Company is a subprocessor of Personal Data in accordance with Section 2 of this DPA.

9.3 For each module, where applicable the following applies:

9.3.1 The optional docking clause in Clause 7 does not apply.

9.3.2 In Clause 9, Option 1 (specific prior authorization) applies, and the minimum time period for prior notice of subprocessor changes shall be as set forth in Section 6.1 of this DPA.

9.3.3 In Clause 11, the optional language does not apply.

9.3.4 All square brackets in Clause 13 are hereby removed.

9.3.5 In Clause 17 (Option 1), the EU SCCs will be governed by the laws of the Republic of Ireland.

9.3.6 In Clause 18(b), disputes will be resolved before the courts of the Republic of Ireland.

9.3.7 Exhibit B to this DPA contains the information required in Annex I of the EU SCCs.

9.3.8 Exhibit C to this DPA contains the information required in Annex II of the EU SCCs,

9.3.9 By entering into this DPA, the Parties are deemed to have signed the EU SCCs incorporated herein, including their Annexes.

9.4 Ex-UK Transfers. The Parties agree that ex-UK Transfers shall either be made pursuant to (i) the Data Privacy Framework to the extent that recipient of the ex-UK Transfer is certified accordingly, or (ii) the UK SCCs, which are deemed entered into and incorporated into this DPA by reference. The UK Addendum (including the UK SCCs incorporated into it) (1) is governed by the laws of England and Wales and (2) any dispute arising from it shall be resolved by the courts of England and Wales.

9.5 Transfers from Switzerland. The Parties agree that transfers from Switzerland shall either be made pursuant to (i) the Data Privacy Framework to the extent that recipient of the transfer from Switzerland is certified accordingly, or (ii) the EU SCCs with the following modifications:

9.5.1 The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the EU SCCs shall be interpreted to include the Federal Act on Data Protection of 19 June 1992 (the "FADP," and as revised as of 25 September 2020, the "Revised FADP") with respect to data transfers subject to the FADP.

9.5.2 Clause 13 of the EU SCCs is modified to provide that the Federal Data Protection and Information Commissioner ("FDPIC") of Switzerland shall have authority over data transfers governed by the FADP and the appropriate EU Supervisory Authority shall have authority over data transfers governed by the GDPR. Subject to the foregoing, all other requirements of Clause 13 shall be observed.

9.5.3 The term "EU Member State" as utilized in the EU SCCs shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs.

9.6 Supplementary Measures. In respect of any transfer of Personal data made pursuant to the Standard Contractual Clauses, the following supplementary measures shall apply:

9.6.1 If, after the date of this DPA, Company receives any formal legal requests from any government intelligence or security service/agencies in the country to which the Personal Data is being exported, for access to (or for copies of) such Personal Data ("Government Agency Requests"), Company shall attempt to redirect the law enforcement or government agency to request that data directly from Customer. As part of this effort, Company may provide Customer's basic contact information to the government agency. If compelled to disclose Personal Data to a law enforcement or government agency, Company shall give Customer reasonable notice of the demand and cooperate to allow Customer to seek a protective order or other appropriate remedy unless Company is legally prohibited from doing so. Company shall not voluntarily disclose Personal Data to any law enforcement or government agency. Customer and Company shall (as soon as reasonably practicable) discuss and determine whether all or any transfers of Personal Data pursuant to this DPA should be suspended in the light of the such Government Agency Requests.

9.6.2 Customer and Company will confer as appropriate to consider whether: (i) the protection afforded by the laws of the country of Company to data subjects whose Personal Data is being transferred is sufficient to provide broadly equivalent protection to that afforded in the EEA or the UK, as applicable; (ii) additional measures are reasonably necessary for the transfer to comply with Privacy Laws; and (iii) it is still appropriate for Personal Data to be transferred to the relevant Company, taking into account all relevant information available, including guidance by the applicable Supervisory Authority, to the Parties.

9.6.3 If either (i) any of the means of legitimizing a transfer cease to be valid or (ii) any Supervisory Authority requires transfers of Personal Data pursuant to those means to be suspended, Customer and Company agree to amend the means of legitimizing transfers or alternative arrangements in respect of such transfers, as required by Privacy Laws. To the extent necessary to ensure the enforceability of the Standard Contractual Clauses, Customer and Company shall execute the Standard Contractual Clauses as a separate agreement.

10. Data Protection Assessments. Taking into account the nature of Company's processing and the information available to Company, Company shall reasonably cooperate with Customer to conduct any data protection or privacy impact assessments as required by Privacy Laws, including by providing Customer with information and documents necessary for such assessments that Customer cannot otherwise obtain without Company's assistance. Notwithstanding the foregoing, Customer and Company each remain responsible only for the measures respectively allocated to them under Privacy Laws pertaining to any such assessment.

11. Data Subject Request.

11.1 Company shall, to the extent permitted by Privacy Laws, notify Customer upon receipt of a request by a Data Subject to exercise Data Subject Rights under Privacy Laws with respect to his or her Personal Data (each a "Data Subject Request"). If Company receives a Data Subject Request in relation to Personal Data, Company will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Services. Customer is solely responsible for ensuring that Data Subject Requests communicated to Company, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each Data Subject.

11.2 Company shall, at the request of Customer, and taking into account the nature of the processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Customer in complying with Customer's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, *provided that* (i) Customer is itself unable to respond without Company's assistance and (ii) Company is able to do so in accordance with all applicable laws, rules, and regulations. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

12. Return or Destruction of Personal Data. Upon the termination or expiration of the Agreement, at Customer's choice, Company shall return or delete Personal Data, unless further storage of such Personal Data is required or authorized by applicable law. If return or destruction is impracticable or prohibited by law, rule or regulation, Company shall take measures to block such Personal Data from any further processing (except to the extent necessary for its continued hosting or processing required by law, rule or regulation) and shall continue to appropriately protect the Personal Data remaining in its possession, custody, or control. If Customer and Company have entered into Standard Contractual Clauses as described in Section 9 (Transfers of Personal Data), the parties agree that the certification of deletion of

Personal Data that is described in Clause 8.1(d) and Clause 8.5 of the EU SCCs (as applicable) shall be provided by Company to Customer only upon Customer's request.

13. Company's Role as a Controller. The parties acknowledge and agree that with respect to Company Account Data and Company Usage Data, Company is an independent controller, not a joint controller with Customer. Company will process Company Account Data and Company Usage Data as a controller (i) to manage the relationship with Customer; (ii) to carry out Company's core business operations, such as accounting, audits, tax preparation and filing and compliance purposes; (iii) to monitor, investigate, prevent and detect fraud, security incidents and other misuse of the Services, and to prevent harm to Customer; (iv) for identity verification purposes; (v) to comply with legal or regulatory obligations applicable to the processing and retention of Personal Data to which Company is subject; and (vi) as otherwise permitted under Privacy Laws and in accordance with this DPA and the Agreement. Company may also process Company Usage Data as a controller to provide, optimize, and maintain the Services, to the extent permitted by Privacy Laws. Any processing by Company as a controller shall be in accordance with Company's Privacy Policy.

14. Execution of this DPA. To complete this DPA, Customer must complete the information requested and submit the DocuSign form available here. This DPA will become legally binding upon Company's execution in the signature block below.

Customer: Nordic AI AS	**Railway Corporation**
Signature: Signed by: Stefan Kløvning E4DD0B5085A6413...	Signature: Signed by: Christian Ohrgaard 6A35A146AF1B48A...
Print Name: Stefan Kløvning	Print Name: Christian Ohrgaard
Title: Chief Operating Officer	Title: Head of Operations
Effective Date: 2026-04-22	

Exhibit A

Details of Processing

Nature and Purpose of Processing: Company will process Customer's Personal Data as necessary to provide the Services under the Agreement, for the purposes specified in the Agreement and this DPA, and in accordance with Customer's instructions as set forth in this DPA. The nature of processing includes, without limitation:

- Receiving data, including collection, accessing, retrieval, recording, and data entry
- Holding data, including storage, organization and structuring
- Using data, including analysis, consultation, testing
- Updating data, including correcting, adaptation, alteration, alignment and combination
- Protecting data, including restricting, encrypting, and security testing
- Sharing data, including disclosure, dissemination, allowing access or otherwise making available
- Returning data to the data exporter or data subject
- Erasing data, including destruction and deletion

Duration of Processing: Company will process Customer's Personal Data as long as required (i) to provide the Services to Customer under the Agreement; (ii) for Company's legitimate business needs; or (iii) by applicable law or regulation. Company Account Data and Company Usage Data will be processed and stored as set forth in Company's privacy policy.

Categories of Data Subjects: Customers and Customer employees

Categories of Personal Data: Company processes Personal Data contained in Company Account Data, Company Usage Data, and any Personal Data provided by Customer (including any Personal Data Customer collects from its end users and processes through its use of the Services) or collected by Company in order to provide the Services or as otherwise set forth in the Agreement or this DPA. Categories of Personal Data include profile or contact data, payment data (as described in the Company's privacy policy), commercial data, device/IP data, web analytics, and social network data.

Sensitive Data or Special Categories of Data: None

Exhibit B

The following includes the information required by Annex I and Annex III of the EU SCCs, and Table 1, Annex 1A, and Annex 1B of the UK Addendum.

1. **The Parties**

Data exporter(s):
Name: Nordic AI AS

Address: Sjolivegen 256, 2677 NEDRE HEIDAL, Norway

Contact information: stefan@nordicai.net

Activities relevant to the data transferred under these Clauses:

Signature and date: By entering into this DPA, Data Exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, as of the Effective Date of the Agreement.

Role (controller/processor): The Data Exporter's role is set forth in Section 2 of this Addendum.

Data importer(s):

Name: Railway Corporation

Address: 548 Market St PMB 68956, San Francisco, California 94104

Contact information: privacy@railway.com

Signature and date: By entering into this DPA, Data Importer is deemed to have signed these Standard Contractual Clauses incorporated herein, as of the Effective Date of the Agreement.

Role (controller/processor): The Data Importer's role is set forth in Section 2 of this Addendum.

2. **Description of the Transfer**

Data Subjects	As described in Exhibit A of the DPA
Categories of Personal Data	As described in Exhibit A of the DPA
Special Category Personal Data (if applicable)	As described in Exhibit A of the DPA
Nature of the Processing	As described in Exhibit A of the DPA
Purposes of Processing	As described in Exhibit A of the DPA
Duration of Processing and Retention (or the criteria to determine such period)	As described in Exhibit A of the DPA
Frequency of the transfer	As necessary to provide perform all obligations and rights with respect to Personal Data as provided in the Agreement or DPA
Recipients of Personal Data Transferred to the Data Importer	Company will maintain and provide a list of its sub-processors as set forth in Section 4 of this DPA

3. **Competent Supervisory Authority**: The Supervisory Authority shall be the Supervisory Authority of the Data Exporter, as determined in accordance with Clause 13 of the EU SCCs. The Supervisory Authority for the purposes of the UK Addendum shall be the UK Information Commissioner's Officer.
4. **List of Authorized Sub-**Processors: A list of the Company's Sub-Processors can be found at trust.railway.com/item/subprocessors.

Exhibit C

Description of the Technical and Organisational Security Measures implemented by the Data Importer

The following includes the information required by Annex II of the EU SCCs and Annex II of the UK Addendum.

Technical and Organizational Security Measure	**Details**
Measures of pseudonymisation and encryption of personal data	Customer data is stored in a multi-tenant application with logical isolation between customer environments. Sensitive authentication information is encrypted on logical database level, and the database is encrypted at rest.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Railway has policies, procedures, and controls in place to ensure confidentiality, integrity, and resilience of processing systems and services. This includes access controls, and the use of regular backups across multiple sites and regions. Railway will maintain and review these policies, procedures, and controls at least annually. Policies can be provided to Enterprise customers upon request.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	All customer data is backed up daily using backup tools that provide restoring capabilities in accordance with Railway's Backup Policy. Railway maintains an Incident Response Plan, a Business Continuity Plan, and a Disaster Recovery Plan. Backups and restore capabilities are tested on an ongoing basis.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Railway regularly monitors and tests controls to ensure they are operating as intended. Railway relies on Drata, Inc. for automated testing of controls and ensuring compliance with privacy and security frameworks and best practices. Railway's leadership monitors these controls regularly and is notified when control is at risk or about to expire, so that action can be taken.
Measures for user identification and authorization	Railway maintains a defined process used to allow access to the company's data and systems. Measures for access control include encrypted connection to production systems and networks, strong authentication mechanisms including 2FA, and mandated use of a password manager.
Measures for the protection of data during transmission	Railway uses secure communication protocols for data transmission, such as TLS/SSL. Data in transit is end-to-end encrypted using the WireGuard protocol.
Measures for the protection of data during storage	Databases are encrypted at rest, with access controls and monitoring in place to safeguard data at rest.
Measures for ensuring physical security of locations at which personal data are processed	Railway infrastructure is run on Google Cloud Platform, and physical access is restricted. Railway has processes and monitoring in place to secure any machine with access to customer data, including device monitoring, required encryption, operating system updates, and more.
Measures for ensuring events logging	Railway operates comprehensive event logging for all components of its platform. Anomalies are reviewed, and logs are inspected and analyzed in the event of an incident.
Measures for ensuring system configuration, including default configuration	Railway adopts secure default configurations for all platform components. Systems are regularly updated and patched to proactively address and mitigate vulnerabilities.
Measures for internal IT and IT security governance and management	Railway has defined a comprehensive Information Security Program, which includes policies, training and awareness, and plans.
Measures for ensuring data minimisation	Railway only collects and processes data that is necessary for the intended purpose as outlined in the "Our Commercial or Business Purposes for Collecting or Disclosing Personal Data" section of Railway's Privacy Policy.

	Railway has procedures in place to dispose of unnecessary data securely.
Measures for ensuring limited data retention	Railway purges or anonymizes customer data and customer content when a customer deletes their Railway account.
Measures for ensuring accountability	Railway employees are required to sign non-disclosure agreements before gaining access to Railway systems and are required to complete security awareness training on an annual basis. Railway conducts background checks on all new team members.
Measures for allowing data portability and ensuring erasure	Railway will support data portability and data erasure requests from customers. Railway has a process in place to provide a copy of all Personal Data stored by Railway for data portability requests. Similarly, Railway has a process in place to effectuate data erasure requests.
Technical and organizational measures of sub-processors	Railway ensures that sub-processors adhere to the same security standards as Railway. This includes entering into Data Processing Agreements with its Authorized Sub-Processors with data protection obligations substantially similar to those contained in this DPA.

Exhibit D

UK Addendum

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

Part 1: Tables

Table 1: Parties

Start Date	This UK Addendum shall have the same effective date as the DPA	
The Parties	Exporter	Importer
Parties' Details	Customer	Company
Key Contact	*See* Exhibit B of this DPA	*See* Exhibit B of this DPA

Table 2: Selected SCCs, Modules and Selected Clauses

EU SCCs	The Version of the Approved EU SCCs which this UK Addendum is appended to as defined in the DPA and completed by Section 6.2 and 6.3 of the DPA.

Table 3: Appendix Information

Annex 1A: List of Parties	As per Table 1 above
Annex 2B: Description of Transfer	*See* Exhibit B of this DPA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:	*See* Exhibit C of this DPA
Annex III: List of Sub-processors (Modules 2 and 3 only):	*See* Exhibit B of this DPA

Table 4: Ending this UK Addendum when the Approved UK Addendum Changes

Ending this UK Addendum when the Approved UK Addendum changes	☒ Importer ☒ Exporter ☐ Neither Party

Part 2: Mandatory Clauses

The Mandatory Clauses of the UK Addendum are incorporated herein by reference.