WABTEC PRIVACY AND DATA PROTECTION APPENDIX

This Appendix applies in the circumstances set out below. In the event of inconsistency or conflict between this Appendix and the Contract Document with respect to a subject covered by this Appendix, the provision requiring the higher level of protection for any Personal Data or other Wabtec information governed by this Appendix shall prevail. The requirements in this Appendix are in addition to any confidentiality obligations between Wabtec and the Supplier under the Contract Document. Wabtec or the applicable Wabtec Affiliate responsible for the protection of any of the Personal Data or other Wabtec information governed by this Appendix may enforce the terms of this Appendix. This Appendix is also applicable when a Supplier affiliate is providing Products, services and/or deliverables under the Contract Document directly, in its own name, in which event Supplier's agreement to the terms of this Appendix is also given on behalf of such Supplier affiliate; and Supplier warrants that it has the power and authority to do so. As used herein, "Supplier" shall mean Supplier and Supplier Affiliate, collectively. Wabtec reserves the right to update Appendix from time to time.

SECTION I – DEFINITIONS

The following definitions and rules of interpretation apply in this Appendix. Any words following the terms "including," "include," "e.g.,", "for example" or any similar expression are for illustration purposes only.

(i) ***Contract Document*** means the relevant agreement, contract, statement of work, task order, purchase order or other document governing the provision of Products, services and/or deliverables by Supplier to Wabtec.

(ii) ***Controlled Data*** is technical or government information with distribution and/or handling requirements proscribed by law, including, but not limited to, controlled unclassified information and license required export-controlled data, which is provided by Wabtec to the Supplier in connection with performance of the Contract Document.

(iii) ***Data Protection Laws*** means rules and regulations applicable with respect to the Processing of Wabtec Personal Data under a Contract Document, including, but not limited to, the European General Data Protection Regulation no. 2016/679 dated 27 April 2016 ("GDPR"), as amended and supplemented, as the case may be, by the relevant EU Member States laws and regulations in which Wabtec directly or indirectly operates, and the Directive no 2002/58 or any other text that may replace it and/or as amended and supplemented, as the case may be, by the relevant EU Member States laws and regulations in which Wabtec directly or indirectly operates.

(iv) ***EU Law*** means the laws of the European Union or of any member state of the European Union and/or the European Economic Area.

(v) ***Wabtec means*** the Westinghouse Air Brake Technologies Corporation or a Wabtec Affiliate party to the Contract Document with Supplier.

(vi) ***Wabtec Affiliate*** means any entity that is directly or indirectly in control of, controlled by, or under common control with Wabtec, whether now existing, or subsequently created or acquired during the term of the Contract Document.

(vii) ***Wabtec Confidential Information*** is information created, collected, or modified by Wabtec that would pose a risk of causing harm to Wabtec if disclosed or used improperly, and is provided to the Supplier under the Contract Document. Wabtec Confidential Information includes, but is not limited to, information pertaining to business operations and strategies, trade secrets, Personal Data, Controlled Data, or Sensitive Personal Data.

(viii) ***Wabtec Information System(s)*** means any systems and/or computers managed by Wabtec, which includes laptops and network devices.

(ix) ***Mobile Devices*** means tablets, smartphones and similar devices running mobile operating systems. Laptops are not considered Mobile Devices.

(x) ***Personal Data*** means any information related to an identified or identifiable natural person (Data Subject), as defined under applicable law, that is Processed in connection with the Contract Document. Legal entities are Data Subjects where required by law.

(xi) ***Personal Data Breach*** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed

(xii) ***Process(ing)*** means to perform any operation or set of operations upon Wabtec Confidential Information, whether by automatic means, including, but not limited to, collecting, recording, organizing, storing, adapting or altering, retrieving, accessing, consulting, using, disclosing by transmission, disseminating, or otherwise making available, aligning or combining, blocking, erasing or destroying.

(xiii) ***Product(s)*** mean any goods, systems, components products, software and deliverables supplied under the Contract Document.

(xiv) ***Security Incident*** means any event in which Wabtec Confidential Information is or is suspected to have been lost, stolen, improperly altered, improperly disclosed, improperly destroyed, used for a purpose not permitted under the Contract Document or this Appendix, or accessed by any person other than Supplier Personnel pursuant to the Contract Document or this Appendix.

(xv) ***Sensitive Personal Data*** is a category of Personal Data considered to be especially sensitive and includes medical records and other personal health information, including protected health information (PHI), as defined in and subject to the U.S. Health Insurance and Portability Act of 1996; personal bank account and payment card information and other financial account information; customer bank account and payment card information; national identifiers; and special categories of data under applicable law (such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data, home life and sexual orientation).

(xvi) ***Supplier or Third Party is*** the entity providing goods, services and/or deliverables to Wabtec pursuant to the Contract Document. It also refers to Wabtec joint ventures.

(xvii) ***Third Party Information System(s)*** means any Third-Party system(s) and/or computer(s) used to Process, Store, Transmit and/or Access Wabtec Confidential Information pursuant to the Contract Document, which includes laptops and network devices.

(xviii) ***Supplier Personnel*** means all persons or entities providing services and/or deliverables under the Contract Document, including Supplier's employees, permitted affiliates and third parties (for example, suppliers, contractors, subcontractors, and agents), as well as anyone directly or indirectly employed, engaged or retained by any of them.

(xix) ***Trusted Third Party Network Connection*** is a physically isolated segment of a third party's network connected to Wabtec internal network in a manner identical to a standard Wabtec office.

SECTION II – INFORMATION SECURITY REQUIREMENTS. This Section II applies whenever a Supplier or Supplier Personnel Processes Wabtec Confidential Information, has access to a Wabtec Information System in connection with the Contract Document, or provides certain services or Products to Wabtec. Capitalized terms used in this Section II and not defined in this Appendix shall have the meaning given to them in the Wabtec Third Party Security Requirements referenced herein.

Part A: Security Controls

1. Consistent with applicable laws and industry information security standards (including ISO 27002, FedRAMP, PCI-DSS and NIST Cybersecurity Framework), Supplier shall implement appropriate physical, technical and organizational measures ("Safeguards") to protect the confidentiality, integrity and availability of Products, services, or information systems.
2. Supplier shall implement Safeguards to protect Wabtec Confidential Information, including

Personal Data, against accidental loss, alteration, unauthorized disclosure, unauthorized destruction or access, in particular where the processing involves the transmission of Wabtec Confidential Information over a network, and against all forms of unauthorized or unlawful processing.

3. The Safeguards shall ensure a level of security appropriate to the risk, including *inter alia,* as appropriate: (i) the pseudonymization and encryption of Wabtec Confidential Information, (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, (iii) the ability to restore the availability and access to Wabtec Confidential Information in a timely manner in the event of a physical or technical incident, and (iv) a process for regularly testing, assessing and evaluating the effectiveness of physical, technical and organizational measures in place for ensuring the security of any processing for the purpose of providing the services, Products or other deliverables under the Contract Document.
4. Supplier shall in any event comply with any data security requirements that Wabtec may provide, from time to time. Where a Supplier a) Processes Wabtec Confidential Information, b) has access to Wabtec Information System, c) develops software for Wabtec, d) provides data center services to Wabtec, e) provides to Wabtec a Product, hardware or component that includes binary code, f) supports a critical business function as defined by Wabtec and/or g) provides to Wabtec Services with high availability requirements, the Supplier shall implement the applicable security controls reflected in Wabtec Third Party Security Requirement (attached herein as Exhibit A to Appendix)
5. Supplier may be subject to additional requests from Wabtec for Supplier to confirm its implementation of certain security controls. These requests may include surveys, certifications and attestations such as SOC1 or SOC2 Type II. Supplier agrees to respond to such requests without undue delay. Failure to respond to Wabtec's request for these additional confirmation of security controls is a breach of Supplier's security obligations under this Appendix.

Part B: Security Incidents

1. Supplier shall notify Wabtec without delay – and in any event no later than twenty-four (24) hours after – upon becoming aware of any Security Incident.
2. Supplier shall, in a timely manner, document and provide Wabtec with all data and details relating to such Security Incident and provide any necessary assistance to enable Wabtec to remedy any such Security Incident and provide Wabtec with all required assistance to provide notification of any such Security Incident to any regulatory authorities and/or Data Subjects impacted by such Security Incident.
3. In particular, and without prejudice to any other right or remedy available to Wabtec, Supplier shall promptly, following discovery or notice of a Security Incident, at its own costs and expenses, take (i) corrective action to mitigate any risks or damages involved with such Security Incident and to protect Wabtec Confidential Information from any further use and/or access, (ii) steps to document such Security Incident, in particular its context, date of occurrence, type, extent and data involved, as well as any elements pertaining to the diagnosis of the origin or the occurrence of such Security Incident, and the direct and indirect consequences of this Security Incident, and provide Wabtec with such evidence and documents, and (iii) any other actions that may be required by applicable Data Protection Laws as a result of such Security Incident, subject to Wabtec's prior written approval.
4. Supplier shall report Security Incident to security@wabtec.com.
5. Unless prohibited by law, Supplier shall provide Wabtec reasonable notice of, and the opportunity to comment on and approve, the content of any notice related to a Security Incident prior to publication or communication to any third party ("Security Notice"), except Wabtec shall not have the right to reject content in a Security Notice that must be included to comply with applicable law, including Data Protection Laws.
6. Should Wabtec elect to send a Security Notice regarding a Security Incident, Supplier shall provide reasonable and timely information relating to the content and distribution of that Security Notice as permitted by applicable law or regulation pursuant to the Security Notice.
7. Other than approved Security Notices, or to law enforcement or as otherwise required by law,

Supplier may not make any public statements concerning Wabtec's involvement with a Security Incident to any third-party without explicit written authorization of Wabtec's Legal Department.

Part C: Wabtec Audit Rights

1. Wabtec reserves the right to conduct an audit, upon 30 days advance notice, of Supplier's compliance with the requirements in this Appendix and applicable laws, including but not limited to: (i) review of the Supplier's applicable policies, processes, and procedures, (ii) review of the results of Supplier's most recent vulnerability assessment and accompanying remediation plans, and (iii) on-site assessments during regular business hours of Supplier's physical security arrangements and Supplier Information Systems. Wabtec reserves the right to conduct a vulnerability assessment of Supplier's systems and applications related to the services and Product if Supplier's vulnerability assessments do not meet or exceed Wabtec application security requirements. This right shall survive termination or expiration of the Contract Document so long as Supplier Processes Wabtec Confidential Information.
2. Further, Wabtec, any third party appointed by it, bound by a duty of confidentiality, or a competent regulatory authority, shall be entitled to conduct an audit of Suppliers (and/or any of its subcontractors) facilities data processing facilities and activities to ensure compliance with this Appendix and applicable laws.
3. Such audits shall be performed during normal business hours and in a way that does not interfere with normal business activities of Supplier and, where relevant, Supplier's subcontractors.
4. Should the audit show a breach of this Appendix or Data Protection Laws, especially but not limited to security or confidentiality requirements, Wabtec may require Supplier to immediately remedy this breach.

Part D: Additional Regulatory Requirements

If Supplier Processes Wabtec Confidential Information that is subject to additional regulatory requirements, or in a manner subject to additional regulatory requirements, Supplier agrees to cooperate with Wabtec for Wabtec's compliance with such requirements. Such cooperation may include, without limitation, execution of additional agreements required by applicable law (e.g., EU Standard Contractual Clauses, U.S. Protected Health Information Agreement), compliance with additional security requirements, completion of regulatory filings applicable to Supplier, and participation in regulatory audits.

Part E: Supplier Personnel

Supplier is responsible for compliance with this Appendix by all Supplier Personnel. Prior to providing access to any Wabtec Confidential Information to any Supplier Personnel, Supplier must obligate them to comply with applicable requirements of the Contract Document and this Appendix. Supplier shall take reasonable steps to ensure continuing compliance by such Supplier Personnel. Supplier may not appoint any third party engaged in providing services and/or deliverables under the Contract Document without the prior written consent of Wabtec. Where such consent has been given, any change of such third party requires Wabtec's prior written approval.

SECTION III – PRIVACY & DATA PROTECTION

Part A. Privacy & Data Protection - General Provisions. ***This Part A applies whenever a Supplier and/or its Supplier Personnel Process Personal Data in connection with the Contract Document.***

1. **Processing**. Supplier shall, and shall ensure that all of its Supplier Personnel shall:
   (a) at all-time comply with applicable laws, including Data Protection Laws;
   (b) only Process Personal Data on, and in compliance with, Wabtec's written instructions in a

Contract Document and as issued from time to time;

(c) Process all Personal Data fairly and lawfully and in accordance with all laws applicable to Supplier's activities concerning Personal Data governed by this Appendix;

(d) only collect Personal Data directly where Wabtec has provided prior written approval for such direct collection (including where expressly provided in the Contract Document), and, where such direct collection has been approved by Wabtec, comply with Data Protection Laws, including provisions concerning notice, consent, access and correction/deletion; any notices to be provided and any consent language to be used when collecting such information directly from a Data Subject are subject to Wabtec's prior and written approval;

(e) keep and maintain adequate and complete documentation and records of Supplier's Processing or use of Wabtec Personal Data, in accordance with Data Protection Laws;

(f) perform, without limitation, any formality, request for authorization, approval, and data protection impact assessment, as may be prescribed by Data Protection Laws; and

(g) undertakes to comply with the principles of "privacy by design" and "privacy by default", as provided for in the Data Protection Laws.

2. **International Transfers & Hosting Locations**.

(a) Supplier must receive approval from Wabtec prior to (i) moving Personal Data from the hosting jurisdictions identified in the Contract Document to a different hosting jurisdiction; or (ii) provisioning remote access to such Personal Data from any location other than such hosting jurisdictions identified in the Contract Document; where Wabtec approves, such approval may be conditioned on execution of additional agreements to facilitate compliance with applicable law.

(b) Supplier acknowledges that some Data Protection Laws may require additional measures be taken to secure transfers of Personal Data outside the country or region they originate from. In such a case, Supplier shall assist and, where relevant, Wabtec affiliates, in implementing these additional measures and, for instance, enter into separate Personal Data transfer agreements, where and as mandated under Data Protection Laws.

3. **Inquiries**. Supplier shall notify Wabtec without delay upon – and in any event no later than twenty-four (24) hours after – becoming aware of (i) any legally binding request for disclosure of and/or request for access to Wabtec Personal Data by a law enforcement authority unless otherwise prohibited under applicable law, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation; (ii) any legally binding request, order or inspection activity by a regulatory authority or other competent authority relating to Personal Data or privacy protection; or (iii) any request or question received from Data Subjects in relation to their Wabtec Personal Data, such as requests for access, rectification, portability or deletion of their Wabtec Personal Data. Except in order to confirm that such request is properly directed to Wabtec, Supplier shall not respond independently to any such questions and/or requests, unless otherwise expressly agreed in writing by Wabtec in such case, Supplier undertakes to comply with the processes and conditions set out by Wabtec to this effect.

4. **Confidentiality & Information Security**. Supplier shall comply with Section II above if Supplier processes Personal Data in connection with the Contract Document. Supplier shall limit disclosure of or access to Personal Data to its Supplier Personnel who have legitimate business need-to-know relating to this Contract Document, and who have received proper training and instruction as to the requirements of the Contract Document (such as confidentiality requirements) and this Appendix.

5. **Return of Personal Data and Termination**. Supplier shall, within fifteen (15) days of termination of the Contract Document, or if requested during the term of the Contract Document, cease all Processing of Personal Data and return to Wabtec all copies of Personal Data. In lieu of returning copies, Wabtec may, at its sole discretion, require Supplier to destroy all copies of Personal Data, using agreed upon methods to ensure such Personal Data is not recoverable, and certify to such destruction. Supplier may continue to retain Personal Data beyond the period prescribed in this section above where required by law, or in accordance with the Contract

Document and/or applicable regulatory or industry standards, provided that (i) Supplier notifies Wabtec prior to the Contract Document's termination or expiration of the obligation, including the specific reasons for such retention; (ii) Supplier has a documented retention period and secure deletion procedure for such copies, with back-up copies retained only to the end of their legally required retention period; (iii) following such period, all copies and back-up copies are deleted in such a manner that they are not recoverable; (iv) Supplier performs no Processing of Personal Data other than that necessitated by retaining or deleting the relevant copies; and (v) Supplier continues to comply with all the requirements of this Appendix in relation to any such retained Personal Data until the same is securely deleted. Termination or expiration of the Contract Document for any reason shall not relieve the Supplier from obligations to continue to protect Personal Data in accordance with the terms of the Contract Document and this Appendix.

6. **Supplier Personal Data.** Wabtec may require Supplier to provide certain Personal Data such as the name, address, telephone number, and e-mail address of Supplier's representatives to facilitate the performance of the Contract Document, and Wabtec and its contractors may store such data in databases located and accessible globally by their personnel and use it for necessary purposes in connection with the performance of the Contract Document, including but not limited to Supplier payment administration. Wabtec agrees to use reasonable technical and organizational measures to ensure that such information is processed in conformity with applicable data protection laws. Supplier may obtain a copy of the Supplier personal information by written request or submit updates and corrections by written notice to Wabtec.

Part B - European Privacy & Data Protection. This Part B applies whenever Processing of Personal Data by Supplier and/or Supplier Personnel in connection with the Contract Document falls within the scope of any EU Law or the laws of the United Kingdom. In addition to the other sections of this Appendix, to comply with the requirements of applicable EU law, Supplier agrees to the following (which shall prevail in the event of conflict with the other provisions of this Appendix):

1. Supplier shall assist Wabtec in the fulfilment of Wabtec's obligations under applicable EU law and Data Protection Laws including:
   (a) preparation of Privacy Impact Assessments (where required);
   (b) response to Data Subject access requests; and
   (c) any required breach notification to Data Protection Authorities and Data Subjects.
2. Supplier shall notify Wabtec without undue delay after becoming aware of any Security Incident involving the Processing of Personal Data that falls within the scope of this Part B.
3. Supplier shall assist Wabtec in obtaining approval for Processing from Data Protection Authorities where required.
4. Supplier shall, at Wabtec's election, either return or destroy Personal Data at the termination of the Contract Document (except as required by EU or Member State law).
5. Upon request, Supplier shall provide Wabtec with all information necessary to demonstrate Supplier's compliance with applicable EU law.
6. Supplier shall refrain from transferring any Wabtec Personal Data to a country which would not be deemed as offering an adequate level of protection by the European Commission, without relying, for the entire duration of the Agreement, on (i) an agreement strictly based on the European Commission Decision of 5 February 2010, as provided in Exhibit B of Appendix hereto, including any European Commission Decision updating or replacing the aforementioned Decision, entered into with Wabtec and/or Wabtec affiliates or, if agreed by Wabtec, (ii) an alternate mechanism in accordance with the applicable legislation of the European Union. In the event that any transfer mechanism under Data Protection Laws of the European Union is determined by the European Court of Justice or another organism of the European Union not to be adequate, Supplier shall, as soon as possible, adopt and implement an appropriate alternative transfer mechanism. In the event that Supplier fails to adopt an alternative transfer mechanism within one (1) month of the invalidation decision by the European Union organism, notwithstanding anything to the contrary in the Agreement, Wabtec may terminate the Agreement, at no cost, as of right and without prejudice to Wabtec's other rights and remedies.

7. Where both Wabtec and all Supplier Processing of Personal Data are located within the EU, EEA and/or United Kingdom, or Supplier Processing occurs outside the EU, EEA and/or United Kingdom and related international transfers are subject to a transfer mechanism other than EU Standard Contractual Clauses (e.g. adequacy, Supplier BCR-Processor or EU/Swiss- US Privacy Shield), the categories of Data Subjects' Personal Data Processed and the types of such Personal Data Processed may concern the following:

Categories of Data Subjects

Employees; trainees; applicants; contract and temporary workers; directors and others whose personal information is shared with Wabtec in the context of an employment relationship; suppliers; distributors and agents; customers; prospects; and clients.

Examples of Types of Personal Data

Identification data (name, surname, address, email address, date and other identifying information); professional identification data (CV, professional status, education, awards, job description, hierarchical positioning, performance levels);financial and economic information (bank details, salary); system log data; geolocation data; identifiers such as any unique personal identifier or IP address; other personal data that may be contained in business related communications and interactions, internal systems and log data; and sensitive personal data including information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life, health or medical records and criminal records.

SECTION IV – MISCELLANEOUS

1. **Limitation of Liability.** Notwithstanding anything to the contrary in this Appendix, the liability of Supplier for any breach of this Appendix shall not be subject to the limitations of liability provisions included in the Contract Document, if any.
2. **Indemnification**: Supplier shall indemnify and hold Wabtec harmless against every claim, litigation, compensation or sanction, of any nature (civil, administrative or criminal), which would arise from the violation by the Supplier of the commitments contained in this Appendix. Where relevant, the Supplier shall compensate Wabtec for any conviction and legal expenses, including reasonable attorney's fees, pronounced against Wabtec in a judicial or administrative decision which has become enforceable.
3. **Compensation**: The Parties acknowledge and agree that the activities performed by Supplier under this Appendix do not involve any right to specific compensation other than that compensation owed to Third Party for the provision of Services in accordance with the Agreement.