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 Wabtec 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 relevant Wabtec Affiliate responsible for the protection of any Wabtec Confidential Information, including Personal Data, 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, including for changes in laws or regulations which impact requirements. Shall the Contract Document be declared void or unenforceable, this Appendix shall remain enforceable by Wabtec and/or Wabtec Affiliates.

SECTION 1 – 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) **Adequacy Decision** means a European Commission, or any other official, decision determining that a transfer of Personal Data to a specific third country, territory or one or more specified sectors within that third country is secured by an adequate data protection regime in place. For illustration purposes and as of the effective date of this Appendix the following countries have received an Adequacy Decision from the European Union: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and United Kingdom (UK).

(ii) **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.

(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, California Consumer Privacy Act ("CCPA"), Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"), Brazil's General Law for the Protection of Personal Data ("LGDP"), China's Personal Information Protection Law ("PIPL"), South Africa's Protection of Personal Information Act ("POPIA"), and the European General Data Protection Regulation no. 2016/679 dated 27 April 2016 and its UK counter part (together, "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) **Data Controller or Controller** means the legal entity which determines the purposes and means of the Processing of Personal Data. A Controller is the entity which may, alone and without accountability, decides what happens to Personal Data (including with regard to its erasure). Should several legal entities Process the same set of Personal Data each for different Purposes on which they may independently and individually exercise control, each will be deemed a "Co-Controller". In most situations, the Wabtec entity employing an individual will be the Data Controller of such employee's Personal Data.

(v) **Data Processor or Processor** means a natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of the Data Controller. Examples include Wabtec

service providers, suppliers, and vendors.

(vi) **Data Transfer Mechanism** means a permitted mechanism, in compliance with data transfer requirements of applicable Data Protection Laws (e.g. Chapter V of the GDPR), to ensure valid and secure cross-border transfer of Personal Data. Depending on the jurisdictions involved and the nature of the Personal Data, the following may be appropriate Data Transfer Mechanisms: Adequacy Determination, contractual clauses, explicit consent of Data Subject, or authorization from a relevant Supervisory authority.

(vii) **Instructions** means Processor or Data Importer shall process shall Process Personal Data only on documented instructions from Controller or Data Exporter, respectively. The Controller or Data Exporter may give such instructions throughout the duration of the Contract Document, including as set forth in this Appendix, the Standard Contractual Clauses (in Section 4) and the Contract Document.

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

(ix) **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.

(x) **Wabtec Confidential Information** means 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, or Sensitive Personal Data.

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

(xii) **Personal Data** means any information related to an identified or identifiable natural person **("Data Subject")** that is Processed in connection with the Contract Document. Examples of Personal Data include identifiers (such as an identification number, location data, an online identifier, username, device ID, IP address, etc.) or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a natural person. Legal entities are Data Subjects where required by law (e.g. POPIA).

(xiii) **Personal Data Breach** means any actual or suspected 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, or any other Security Incident involving Personal Data.

(xiv) **Process(ing)** means any operation or set of operations which is performed on data (including Personal Data) or on sets of data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

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

(xvi) **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.

(xvii) **Sensitive Personal Data** means a category of Personal Data considered to be especially sensitive and, depending on applicable laws, includes medical records and other personal health information; personal bank account and payment card information and other financial account information; national identifiers; data relating to criminal convictions and offences; "Sensitive Data" as defined in Standard Contractual Clauses; and, **"Special Category of Personal Data**" such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life

or sexual orientation.

(xviii) **Standard Contractual Clauses** means the European Commission implementing decisions (EU) 2021/914 and 2021/915 of 4 June 2021 and deemed to form an integral part of the Contract Document as well as any other decision by a regulator allowing to recognize such decisions.

(xix) **Supervisory Authority** means the local entity or body regulating and enforcing compliance with specific privacy laws applicable to an individual country/nation/state (e.g. Commission nationale de l'informatique et des libertes (CNIL) in France; Information Commissioner's Office (ICO) in UK; California Attorney General for CCPA in California; or, Brazilian National Data Protection Authority (ANPD) in Brazil.

(xx) **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.

(xxi) **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.

SECTION 2 – INFORMATION SECURITY REQUIREMENTS.

This Section 2 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 2 and not defined in this Appendix shall have the meaning given to them in the Wabtec Third Party Security Requirements found at https://www.wabteccorp.com/supplier-resources.

Part A: Security Controls

1. Consistent with applicable laws and industry information security standards (including ISO 27001, 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, in no way less stringent that those detailed in Wabtec Third Party Security Requirements.
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, Security Incident or Personal Data Breach.
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 control 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 all data security requirements that Wabtec may provide. 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.
5. Supplier shall provide upon request by Wabtec all relevant documentation pertaining to such Safeguards and 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 in good faith without undue delay. Failure to respond within ten (10) days 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 upon – and in any event no later than twenty-four (24) hours after – 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 investigate and 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 or +1 (844) 422-0008.
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, at no additional costs, all 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 ten (10) business 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, or any third party appointed by it, bound by a duty of confidentiality 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. Nothing shall prevent or otherwise limit the possibility of any competent regulatory authority to

conduct or mandate either party to conduct a similar audit under the process, scope and timing set forth by such authority. Supplier agrees to cooperate in good faith with such mandate from such authority.

5. 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 at Supplier's cost.

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, and ensure that its personnel received sufficient training in data handling and are subject to all appropriate confidentiality undertakings. 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 3 – 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 or breach of any given Data Protection Laws. Where relevant, the Supplier shall compensate Wabtec for any conviction and legal expenses relating to such violation, including reasonable attorney's fees, pronounced against Wabtec in a judicial or administrative decision which has become enforceable. Supplier shall be liable for the damage caused by Processing where it has not complied with obligations of Data Protection Laws specifically directed to processors or where it has acted outside of or contrary to the Instructions.
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 compensation owed to Third Party for the provision of Services, in accordance with the Contract Document.
4. **Effective Date:** This Appendix shall come into force on the date of signature of the Contract Document or the first provision of the Wabtec Personal Data to Supplier, whichever the earlier. It shall be automatically terminated when the Contract Document terminates or expires for any reason, notwithstanding the survival of the relevant provision for as long as Wabtec Personal Data is retrained by Supplier.

SECTION 4 – PRIVACY & DATA PROTECTION

Introduction

Section 4 - Part A (below) governs, and forms an integral part of the Contract Document, whenever a Supplier Processes Personal Data in connection with the Contract Document as detailed in Annex I.B herein.

Section 4 - Part B replaces Section 4-Part A whenever: 1) the Processing of Personal Data involves **cross-border transfer** of Personal Data from a jurisdiction (e.g. EU, UK, Brazil, China, and South Africa) that requires a Data Transfer Mechanism to transfer Personal Data to other jurisdictions; and, 2) there is no Adequacy Decision by the exporting jurisdiction for the importing jurisdictions/entities. For Clarity, Section 4-Part B is not required if Personal Data is being transferred between entities within the EU/EEA and any third-country beneficiary of an Adequacy Decision by the European Commission.

It is intended that *Section 4 - Part A and Section 4 - Part B are mutually exclusive*. In the eventuality of a change of the Processing during performance of the Contract, the Parties agree to amend Annex I.B accordingly.

Regardless of the options applicable and detailed therein, the below (along with Sections 1, 2 and 3 above) shall be construed as additional commercial clauses completing the Standard Contractual Clauses.

1. **Compliance with Laws:** Supplier shall at all time comply with Data Protection Laws
2. **Roles & Responsibilities:** Under this Appendix, Supplier shall Process Wabtec Personal Data as Processor solely on behalf of and under the Instruction of Wabtec, and Wabtec shall be deemed to act as Controller. Should Supplier Process Wabtec Personal Data outside the scope of this Appendix and Contract Document, such as, without limitation, (i) for purposes of Processing other than those agreed in this Appendix or Contract Document, (ii) for any Processing operation outside of an Instruction, or (iii) for any Processing performed for a duration other than as specified in Section 4 of this Appendix, Supplier shall be considered as an independent Controller, implementing such Processing under its sole liability.
3. **Brexit consideration**: By executing the Contract Document including this Appendix, the Parties also agree to be bound by the UK Addendum to the SCC, as relevant to Section 4 - Part A and Section 4 - Part B below.

Part A - Standard Contractual Clauses on the basis of the EU Commission Implementing Decision (EU) 2021/915 of 4 June 2021

SECTION I

Clause 1 - Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the "**Clauses**") is to ensure compliance with Article 28(3) and (4) of 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 ("**GDPR**") and other applicable Data Protection Laws.

(b) Controllers and Processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) GDPR and similar provisions in other applicable Data Protection Laws.

(c) These Clauses apply to the processing of Personal Data as specified in Annex I.B.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which Controller is subject by virtue of GDPR.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of GDPR.

Clause 2 - Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.
(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3 - Interpretation

(a) Where these Clauses use the terms defined in GDPR, those terms shall have the same meaning as in that Regulation.
(b) These Clauses shall be read and interpreted in the light of the provisions of GDPR.
(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in GDPR or in a way that prejudices the fundamental rights or freedoms of the Data Subjects.

Clause 4 - Hierarchy

In the event of a contradiction between these Clauses and the provisions of the Contract Document or related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 - Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a Controller or a Processor by completing the Annexes and signing Annex I.
(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a Controller or a Processor, in accordance with its designation in Annex I.
(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II
OBLIGATIONS OF THE PARTIES

Clause 6 - Description of processing(s)

The details of the Processing operations, in particular the categories of Personal Data and the purposes of Processing for which the Personal Data is Processed on behalf of Controller, are specified in Annex I.B.

Clause 7 - Obligations of the Parties

7.1. Instructions

(a) Processor shall Process Personal Data only on documented written instructions from Controller, including as set forth in these Clauses and the Contract Document ("**Instructions**"), unless required to do so by Union or Member State law to which Processor is subject. In this case, Processor shall inform Controller of that legal requirement before Processing, unless the law prohibits this on important grounds of public interest. Subsequent Instructions may also be given by Controller throughout the duration of the Processing of Personal Data. These Instructions shall always be documented.
(b) Processor shall immediately inform Controller if, in Processor's opinion, Instructions given by Controller infringe GDPR or the applicable Union or Member State data protection provisions prior

to implementing such Instructions. Processor shall not be liable for not carrying out any allegedly infringing Instruction whose status duly notified to Controller until the status of such Instruction has been resolved by the Parties.

7.2. Purpose limitation

Processor shall process the Personal Data only for the specific purpose(s) of the Processing, as set out in Annex I.B, unless it receives further Instructions from Controller.

7.3. Duration of the Processing of Personal Data

Processing by Processor shall only take place for the duration specified in Annex I.B or for the duration of the Contract Document or these Clauses, whichever the earlier.

7.4. Security of processing

(a) Processor shall at least implement the technical and organisational measures specified in Annex II to ensure the security of the Personal Data. This includes protecting the Personal Data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data ("**Personal Data Breach**"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the Data Subjects.

(b) Processor shall grant access to the Personal Data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the Contract Document or these Clauses. Processor shall ensure that persons authorised to process the Personal Data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and have received sufficient training on data protection compliance.

7.5. Sensitive data

If the Processing involves Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("**Sensitive Data**"), Processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) Processor shall deal promptly and adequately with inquiries from Controller about the Processing of Personal Data in accordance with these Clauses at no additional costs.

(c) Processor shall make available to Controller, at no additional costs, all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from GDPR. At Controller's request, Processor shall also permit and contribute to audits of the Processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, Controller may take into account relevant certifications held by Processor.

(d) Controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of Processor and shall, where appropriate, be carried out with reasonable notice. In that regard, should Controller decide to inspect, or have inspected by an, independent auditor, Processor's operations and equipment, Controller shall inform Processor with a fifteen (15) business days written notice. Such inspection shall not interfere with the ordinary business activity carried out by Processor during its working hours and shall not adversely impact the normal course of Processor's business. Audit shall be limited to one per contractual year, unless mandated subsequent to a Personal Data Breach. In such case, all audit costs shall be borne by Processor. Nothing in the foregoing shall be construed

as limiting the possibility for a Supervisory Authority to conduct or mandate either Party to conduct any audit; in such case, each Party shall bear its own costs.

(e) Should the audit show a breach to these Clauses, this Appendix or the Data Protection Laws, especially but not limited to security or confidentiality requirements, Controller may require Processor to immediately remedy to this breach. Nothing shall prevent, or otherwise limit the possibility by, any Supervisory Authority to conduct, or mandate either party to conduct, a similar audit under the process, scope and timing set forth by such authority. Supplier agrees to cooperate in good faith with such Supervisory Authority.

(f) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) Processor shall not subcontract any of its Processing operations performed on behalf of Controller in accordance with these Clauses to a sub-processor, without Controller's prior specific written authorisation. Processor shall submit the request for specific authorisation at least fifteen (15) days prior to the engagement of the sub-processor in question, together with the information necessary to enable Controller to decide on the authorisation. Silence of Controller shall not be construed as implicit approval of the sub-contractor considered. The list of sub-processors authorised by Controller can be found in Annex IV. The Parties shall keep Annex IV up to date.

(b) Where Processor engages a sub-processor for carrying out specific processing activities (on behalf of Controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on Processor in accordance with these Clauses. Processor shall ensure that the sub-processor complies with the obligations to which Processor is subject pursuant to these Clauses and to GDPR.

(c) At Controller's request, Processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to Controller. To the extent necessary to protect business secret or other confidential information, including Personal Data, Processor may redact the text of the agreement prior to sharing the copy.

(d) Processor shall remain fully responsible to Controller for the performance of the sub-processor's obligations in accordance with its contract with Processor. Processor shall notify Controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) Processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event Processor has factually disappeared, ceased to exist in law or has become insolvent - Controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the Personal Data in accordance with Clause 10.(d) below.

7.8. International transfers

(a)) Any transfer of Personal Data to a third country or an international organisation by Processor shall be done only on the basis of documented instructions from Controller or in order to fulfil a specific requirement under Union or Member State law to which Processor is subject and shall take place in compliance with Chapter V GDPR. In such case, the Parties agree to reconvene and execute any additional contractual documentation as may be required to make such international transfer of Personal Data compliant with GDPR, including Section 4 - Part B herein.

(b) Controller agrees that where Processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of Controller) and those Processing activities involve a transfer of Personal Data within the meaning of Chapter V GDPR, Processor and the sub-processor can ensure compliance with Chapter V GDPR by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) GDPR, provided the conditions for the use of those standard contractual clauses are met. Nothing in the foregoing shall be construed as implicitly authorizing Processor to engage and sub-processor without the prior written approval of Controller.

Clause 8 - Assistance to Controller

(a) Processor shall promptly, and in any event no later than twenty-four (24) hours from receipt, notify Controller of any request it has received from the Data Subject, any legally binding request for disclosure of and/or request for access to Controller 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; or any legally binding request, order or inspection activity by a Supervisory Authority or other competent authority relating to Personal Data or privacy protection. It shall not respond to the request itself, unless authorised to do so by Controller, except in order to notify the Data Subject that the request has been duly transferred, upon such transfer. Processor shall not respond independently to any such questions and/or requests, unless otherwise expressly agreed in writing by Controller in such case, Processor undertakes to comply with the processes and conditions set out by Controller to this effect.

(b) At no additional costs provided that Controller does not have direct access to the Personal Data in order to address such request, Processor shall assist Controller in fulfilling its obligations to respond to Data Subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), Processor shall comply with Controller's instructions

(c) In addition to Processor's obligation to assist Controller pursuant to Clause 8(b), and at no additional costs provided that Controller does not have direct access to the Personal Data and/or required information in order to address such undertaking, Processor shall furthermore assist Controller in ensuring compliance with the following obligations, taking into account the nature of the Processing and the information available to Processor:

1. the obligation to carry out an assessment of the impact of the envisaged Processing operations on the protection of Personal Data (a "**Data Protection Impact Assessment**") where a type of Processing is likely to result in a high risk to the rights and freedoms of natural persons;
2. the obligation to consult the competent Supervisory Authority/ies prior to Processing where a Data Protection Impact Assessment indicates that the Processing would result in a high risk in the absence of measures taken by Controller to mitigate the risk;
3. the obligation to ensure that Personal Data is accurate and up to date, by informing Controller without delay if Processor becomes aware that the Personal Data it is Processing is inaccurate or has become outdated;
4. the obligations in Article 32 GDPR.

(d) The Parties shall set out in Annex II the appropriate technical and organisational measures by which Processor is required to assist Controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9 - Notification of Personal Data Breach

In the event of a Personal Data Breach, Processor shall cooperate with and assist Controller for Controller to comply with its obligations under Articles 33 and 34 of the GDPR, where applicable, taking into account the nature of Processing and the information available to Processor. Processor shall promptly following discovery or notice of such Personal Data Breach, at its own costs and expenses, take (i) corrective action to mitigate any risks or damages involved with such Personal Data Breach and to protect Controller Personal Data from any further use and/or access, (ii) investigate, evidence and document such Personal Data Breach, 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 Personal Data Breach, and the direct and indirect consequences of this Personal Data Breach, and provide Controller with such evidence and documents, and (iii) any other actions that may be required by applicable Data Protection Laws as a result of such Personal Data Breach, subject to Controller's prior written approval.

9.1 Personal Data Breach concerning Personal Data Processed by Controller

In the event of a Personal Data Breach concerning Personal Data Processed by Controller, Processor shall assist Controller:

(a) in notifying the Personal Data Breach to the competent Supervisory Authority/ies, without undue delay after Controller has become aware of it unless the Personal Data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

(b) in obtaining the following information which, pursuant to Article 33(3) GDPR, shall be stated in Controller's notification, and must at least include:

1. the nature of the Personal Data including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
2. the likely consequences of the Personal Data Breach;
3. the measures taken or proposed to be taken by Controller to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 GDPR, with the obligation to communicate without undue delay the Personal Data Breach to the Data Subject, when the Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons.

(d) In any case, Processor shall notify without undue delay Controller of all suspected or actual Personal Data Breach it encounters.

9.2 Personal Data Breach concerning Personal Data Processed by Processor

In the event of a Personal Data Breach concerning Personal Data Processed by Processor, Processor shall notify Controller without undue delay and in any event no later than twenty-four (24) hours after Processor having become aware of the Personal Data Breach. Such notification shall contain, at least:

(a) a description of the nature of the Personal Data Breach (including, where possible, the categories and approximate number of Data Subjects and data records concerned);

(b) the details of a contact point where more information concerning the Personal Data Breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the Personal Data Breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex II all other elements to be provided by Processor when assisting Controller in the compliance with Controller's obligations under Articles 33 and 34 GDPR.

SECTION III
FINAL PROVISIONS

Clause 10 - Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of GDPR, in the event that Processor is in breach of its obligations under these Clauses, Controller may instruct Processor to suspend the Processing of Personal Data until the latter complies with these Clauses or the Contract Document is terminated. Processor shall promptly inform Controller in case it is unable to comply with these Clauses, for whatever reason.

(b) Controller shall be entitled to terminate the Contract Document insofar as it concerns Processing of Personal Data in accordance with these Clauses if:

1. the Processing of Personal Data by Processor has been suspended by Controller pursuant to Clause 10.(a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
2. Processor is in substantial or persistent breach of these Clauses or its obligations under GDPR;
3. Processor fails to comply with a binding decision of a competent court or the competent Supervisory Authority/ies regarding its obligations pursuant to these Clauses or to GDPR.

(c) Processor shall be entitled to terminate the Contract Document insofar as it concerns Processing of Personal Data under these Clauses where, after having informed Controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), Controller insists on compliance with the instructions.

(d) Following termination of the Contract Document, Processor shall, at the choice of Controller, delete all Personal Data Processed on behalf of Controller and certify to Controller that it has done so, or, return all the Personal Data to Controller and delete existing copies unless Union or Member State law requires storage of the Personal Data in accordance with the process detailed below. Until the Personal Data is deleted or returned, Processor shall continue to ensure compliance with these Clauses.

(e) Upon expiration or termination for whatever reason of these Clauses or the Contract Document:

1. Processor shall inquire from Controller about Controller's intention with regard to the Personal Data at least fifteen (15) days prior to the effective termination of these Clauses or the Contract Document. Further to this inquiry, where Controller inform Processor of its intention to retrieve Personal data, Processor shall retrieve all Personal Data and make them available to Controller under a commonly used electronic format within fifteen (15) days from effective termination or expiration.
2. Further to such provision, or if Controller has not instructed Processor for the retrieval of Personal Data prior to the effective expiration or termination of these Clauses or the Contract Document, Processor shall delete all Personal Data on its systems (without prejudice to any backup archives) unless otherwise instructed by Controller prior to the effective date of termination. Processor shall cooperate reasonably and in a timely manner with the efforts by Controller, or any other party acting on Controller's behalf, to provide for an orderly transition of the Processing to Controller or another service provider. The costs attached to such request are included in the financial conditions set forth in the Contract Document.
3. Notwithstanding anything to the contrary, Processor may retain one copy of the Personal Data only for as long as there exists a legal requirement to do but in compliance with applicable Data Protection Laws and subject to the provision of these Clauses.

Clauses 11 - California Consumer Protection Act

(a) Processor is a service provider.

(b) Controller discloses Personal Data to Processor solely for Processor to perform the Services.

(c) Processor is prohibited from: (i) selling the Personal Data; (ii) retaining, using, or disclosing the Personal Data for any purpose other than for the specific purpose of performing the Services, including retaining, using, or disclosing the Personal Data for a commercial purpose other than providing the Services; and (iii) retaining, using, or disclosing the Personal Data outside of the direct business relationship between Processor and Controller.

(d) Processor understands the restrictions set forth in this Appendix and represents, warrants, and certifies that it does and will comply with the same.

Part B - Standard Contractual Clauses on the basis of the EU Commission Implementing Decision (EU) 2021/914 of 4 June 2021

Section I

Clause 1 **- Purpose and scope**

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (hereinafter, "**GDPR**") and similar provisions of other applicable Data Protection Laws for the transfer of Personal Data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "**Entity/ies**") transferring the Personal Data, as listed in Annex I.A. (hereinafter each "**Data Exporter**"), and

(ii) the Entity/ies in a third country receiving the Personal Data from the Data Exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "**Data Importer**")

have agreed to these standard contractual clauses (hereinafter, "**Clauses**").

(c) These Clauses apply with respect to the transfer of Personal Data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2 **- Effect and invariability of the Clauses**

(a) These Clauses set out appropriate safeguards, including enforceable Data Subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) GDPR (and similar provisions in other applicable Data Protection laws) and, with respect to Personal Data transfers from Data Controllers to Data Processors and/or Data Processors to Data Processors, standard contractual clauses pursuant to Article 28(7) GDPR (and similar provisions of other applicable Data Protection Laws), provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of Data Subjects.

(b) These Clauses are without prejudice to obligations to which the Data Exporter is subject by virtue of GDPR.

Clause 3 **- Third-party beneficiaries**

(a) Data Subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the Data Exporter and/or Data Importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii) Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);
(iii) Clause 9 - Clause 9(a), (c), (d) and (e);
(iv) Clause 12 - Clause 12(a), (d) and (f); ;
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18 - Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of Data Subjects under GDPR.

Clause 4 **- Interpretation**

(a) Where these Clauses use terms that are defined in GDPR, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of GDPR.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in GDPR.

***Clause 5* - Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

***Clause 6* - Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of Personal Data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

***Clause 7* – Docking clause**

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a Data Exporter or as a Data Importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a Data Exporter or Data Importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

Section II
OBLIGATIONS OF THE PARTIES

***Clause 8* - Data protection safeguards**

The Data Exporter warrants that it has used reasonable efforts to determine that the Data Importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 **Instructions**

(a) The Data Importer shall Process the Personal Data only on documented instructions from the Data Exporter. The Data Exporter may give such instructions throughout the duration of the Contract Document, including as set forth in these Clauses and the Contract Document ("**Instructions**".)

(b) The Data Importer shall immediately inform the Data Exporter if it is unable to follow those Instructions, prior to implementing such Instructions. Data Importer shall not be liable for not carrying out any allegedly infringing Instruction whose status duly notified to Data Exporter until the status of such Instruction has been resolved by the Parties.

8.2 **Purpose limitation**

The Data Importer shall Process the Personal Data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the Data Exporter.

8.3 **Transparency**

On request, the Data Exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the Data Subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and Personal Data, the Data Exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the Data Subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the Data Subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the Data Exporter under Article 13 and Article 14 GDPR.

8.4 **Accuracy**

If the Data Importer becomes aware that the Personal Data it has received is inaccurate, or has become outdated, it shall inform the Data Exporter without undue delay. In this case, the Data Importer shall cooperate with the Data Exporter to erase or rectify the Personal Data.

8.5 **Duration of Processing and erasure or return of Personal Data**

Processing by the Data Importer shall only take place for the duration specified in Annex I.B or for the duration of the Contract Document or these Clauses, whichever the earlier. After the end of the provision of the Processing services, the Data Importer shall, at the choice of the Data Exporter, delete all Personal Data Processed on behalf of the Data Exporter and certify to the Data Exporter that it has done so, or return to the Data Exporter all Personal Data Processed on its behalf and delete existing copies. Until the Personal Data is deleted or returned, the Data Importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the Data Importer that prohibit return or deletion of the Personal Data, the Data Importer warrants that it will continue to ensure compliance with these Clauses and will only Process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the Data Importer under Clause 14(e) to notify the Data Exporter throughout the duration of the Contract Document if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

Upon expiration or termination for whatever reason of these Clauses or the Contract Document:

1. Data Importer shall inquire from Data Exporter about Data Exporter's intention with regard to the Personal Data at least fifteen (15) days prior to the effective termination of these Clauses or the Contract Document. Further to this inquiry, where Data Exporter inform Data Importer of its intention to retrieve Personal Data, Processor shall retrieve all Personal Data and make them available to Data Exporter under a commonly used electronic format within fifteen (15) days from effective termination or expiration.
2. Further to such provision, or if Data Exporter has not instructed Data Importer for the retrieval of Personal Data prior to the effective expiration or termination of these Clauses or the Contract Document, Data Importer shall delete all Personal Data on its systems (without prejudice to any backup archives) unless otherwise instructed by Data Exporter prior to the effective date of termination. Data Importer shall cooperate reasonably and in a timely manner with the efforts by Data Exporter, or any other party acting on Data Exporter's behalf, to provide for an orderly transition of the Processing to Data Exporter or another service provider. The costs attached to such request are included in the financial conditions set forth in the Contract Document.
3. Notwithstanding anything to the contrary, Data Importer may retain one copy of the Personal Data only for as long as there exists a legal requirement to do but in compliance with applicable data protection laws and subject to the provision of these Clauses.

8.6 **Security of Processing**

(a) The Data Importer and, during transmission, also the Data Exporter shall implement appropriate technical and organisational measures to ensure the security of the Personal Data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that Personal Data (hereinafter "**Personal Data Breach**"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of Processing and the risks involved in the Processing for the Data Subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of Processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the Personal Data to a specific Data Subject shall, where possible, remain under the exclusive control of the Data Exporter. In complying with its obligations under this paragraph, the

Data Importer shall at least implement the technical and organisational measures specified in Annex II. The Data Importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The Data Importer shall grant access to the Personal Data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the Contract Document. It shall ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and have received sufficient training on data protection compliance.

(c) In the event of a Personal Data Breach concerning Personal Data Processed by the Data Importer under these Clauses, the Data Importer shall take appropriate measures to address the Personal Data Breach, including measures to mitigate its adverse effects. The Data Importer shall also notify the Data Exporter without undue delay, and in any case within [twenty-four (24) hours, after having become aware of the Personal Data Breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the Personal Data Breach (including, where possible, categories and approximate number of Data Subjects and Personal Data records concerned), its likely consequences and the measures taken or proposed to address the Personal Data Breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The Data Importer shall, at its sole costs, cooperate with and assist the Data Exporter to enable the Data Exporter to comply with its obligations under GDPR, in particular to notify the competent Supervisory Authority and the affected Data Subjects, taking into account the nature of Processing and the information available to the Data Importer.

(e) Data Importer shall promptly following discovery or notice of such Personal Data Breach, at its own costs and expenses, take (i) corrective action to mitigate any risks or damages involved with such Personal Data Breach and to protect Data Exporter Personal Data from any further use and/or access, (ii) investigate, evidence and document such Personal Data Breach, 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 Personal Data Breach, and the direct and indirect consequences of this Personal Data Breach, and provide Data Exporter with such evidence and documents, and (iii) any other actions that may be required by applicable Data Protection Laws as a result of such Personal Data Breach, subject to Data Exporter's prior written approval.

(f) In any case, the Data Importer shall notify without undue delay the Data Exporter of all suspected or actual Personal Data Breach it encounters.

8.7 **Sensitive Data**

Where the transfer involves Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "**Sensitive Data**"), the Data Importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 **Onward Transfers**

The Data Importer shall only disclose the Personal Data to a third party on documented instructions from the Data Exporter. In addition, the Personal Data may only be disclosed to a third party located outside the European Union (in the same country as the Data Importer or in another third country, hereinafter "**Onward Transfer**") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the Onward Transfer is to a country benefitting from an adequacy decision pursuant to Article 45 GDPR that covers the Onward Transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Article 46 or Article 47 GDPR with respect to the Processing in question;

(iii) the Onward Transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the Onward Transfer is necessary in order to protect the vital interests of the Data Subject or of another natural person.

Any Onward Transfer is subject to compliance by the Data Importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 **Documentation and compliance**

(a) The Data Importer shall promptly and adequately deal with enquiries from the Data Exporter that relate to the Processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the Data Importer shall keep appropriate documentation on the Processing activities carried out on behalf of the Data Exporter.

(c) The Data Importer shall make available to the Data Exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses, at no additional costs, and at the Data Exporter's request, allow for and contribute to audits of the Processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the Data Exporter may take into account relevant certifications held by the Data Importer.

(d) The Data Exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the Data Importer and shall, where appropriate, be carried out with reasonable notice as follows:

(i) Where required by applicable law, or where mandated by a competent Supervisory Authority, Data Exporter may, upon ten (10) calendar days' prior written notice, at its own expense, perform or have a third party audit professional perform, an audit of Data Importer's compliance with applicable data protection laws and these Clauses.

(ii) Before the commencement of any such additional audit inquiries, both Parties shall mutually agree upon the scope, timing and duration of the audit.

(iii) Data Exporter shall promptly notify Data Importer with information regarding any non-compliance discovered during the course of such audit inquiries. Data Exporter agrees to provide Data Importer with a draft of the audit report for review.

(iv) During such audit, Data Importer shall provide all reasonable cooperation and assistance to the auditors and/or Data Exporter. Where such audit inquiry is subsequent to a Personal Data Breach incumbent upon Data Importer, all audit costs shall be borne by Data Importer, without prejudice to any damages which may be further sought by Data Exporter.

(v) Such inspection shall not interfere with the ordinary business activity carried out by Processor during its working hours and shall not adversely impact the normal course of Processor's business. Audit shall be limited to one per contractual year, unless mandated subsequent to a Personal Data Breach. In such case, all audit costs shall be borne by Processor. Nothing in the foregoing shall be construed as limiting the possibility for a Supervisory Authority to conduct or mandate either Party to conduct any audit; in such case, each Party shall bear its own costs.

(vi) Should the audit show a breach to these Clauses, this Appendix or the Data Protection Laws, especially but not limited to security or confidentiality requirements, Controller may require Processor to immediately remedy to this breach. Nothing shall prevent, or otherwise limit the possibility by, any Supervisory Authority to conduct, or mandate either party to conduct, a similar audit under the process, scope and timing set forth by such authority. Supplier agrees to cooperate in good faith with such Supervisory Authority.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent Supervisory Authority on request.

(f) At no additional costs provided that Data Exporter does not have direct access to the Personal Data and/or required information in order to address such undertaking, Data Importer shall furthermore assist Data Exporter in ensuring compliance with the following obligations, taking into account the nature of the Processing and the information available to Data Importer:

(i) the obligation to carry out an assessment of the impact of the envisaged Processing operations on the protection of Personal Data (a "Data Protection Impact Assessment") where a type of Processing is likely to result in a high risk to the rights and freedoms of natural persons;

(ii) the obligation to consult the competent Supervisory Authority/ies prior to Processing where a Data Protection Impact Assessment indicates that the Processing would result in a high risk in the absence of measures taken by Data Exporter to mitigate the risk;

(iii) the obligation to ensure that Personal Data is accurate and up to date, by informing Data Exporter without delay if Data Importer becomes aware that the Personal Data it is Processing is inaccurate or has become outdated;

(iv) the obligations in Article 32 GDPR.

***Clause 9* - Use of sub-Processors**

(a) The Data Importer shall not sub-contract any of its Processing activities performed on behalf of the Data Exporter under these Clauses to a sub-Processor without the Data Exporter's prior specific written authorisation. The Data Importer shall submit the request for specific authorisation at least [Specify time period] prior to the engagement of the sub-Processor, together with the information necessary to enable the Data Exporter to decide on the authorisation. The list of sub-Processors already authorised by the Data Exporter can be found in Annex III. The Parties shall keep Annex III up to date. Silence of Data Exporter shall not be construed as implicit approval of the sub-contractor considered

(b) Where the Data Importer engages a sub-Processor to carry out specific Processing activities (on behalf of the Data Exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the Data Importer under these Clauses, including in terms of third-party beneficiary rights for Data Subjects. The Parties agree that, by complying with this Clause, the Data Importer fulfils its obligations under Clause 8.8. The Data Importer shall ensure that the sub-Processor complies with the obligations to which the Data Importer is subject pursuant to these Clauses.

(c) The Data Importer shall provide, at the Data Exporter's request, a copy of such a sub-Processor agreement and any subsequent amendments to the Data Exporter. To the extent necessary to protect business secrets or other confidential information, including Personal Data, the Data Importer may redact the text of the agreement prior to sharing a copy.

(d) The Data Importer shall remain fully responsible to the Data Exporter for the performance of the sub-Processor's obligations under its contract with the Data Importer. The Data Importer shall notify the Data Exporter of any failure by the sub-Processor to fulfil its obligations under that contract.

(e) The Data Importer shall agree a third-party beneficiary clause with the sub-Processor whereby - in the event the Data Importer has factually disappeared, ceased to exist in law or has become insolvent - the Data Exporter shall have the right to terminate the sub-Processor contract and to instruct the sub-Processor to erase or return the Personal Data.

***Clause 10* - Data Subject rights**

(a) The Data Importer shall promptly, and in any event no later than twenty-four (24) hours from receipt, notify the Data Exporter of any request it has received from a Data Subject, any legally binding request for disclosure of and/or request for access to Controller 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; or any legally binding request, order or inspection activity by a Supervisory Authority or other competent authority relating to Personal Data or privacy protection. It shall not respond to that request itself unless it has been authorised to do so by the Data Exporter or to confirm that such request has been duly forwarded to Data Exporter upon doing so. Data Importer shall not respond independently to any such questions and/or requests, unless otherwise expressly agreed in writing by Data Exporter in such case, Data Importer undertakes to comply with the processes and conditions set out by Data Exporter to this effect. .

(b) The Data Importer shall assist, at no additional cost, the Data Exporter in fulfilling its obligations to respond to Data Subjects' requests for the exercise of their rights under GDPR. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the Processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the Data Importer shall comply with the instructions from the Data Exporter.

Clause 11 - Redress

(a) The Data Importer shall inform Data Subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a Data Subject.

(b) In case of a dispute between a Data Subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the Data Subject invokes a third-party beneficiary right pursuant to Clause 3, the Data Importer shall accept the decision of the Data Subject to:

  (i) lodge a complaint with the Supervisory Authority in the Member State of his/her habitual residence or place of work, or the competent Supervisory Authority pursuant to Clause 13;

  (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the Data Subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) GDPR.

(e) The Data Importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The Data Importer agrees that the choice made by the Data Subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 - Liability

(a) Each Party shall be liable to the other Party/ies for any damages it, its staff or its authorized sub-Processors, causes the other Party/ies by any breach of these Clauses and/or any data protection laws, including, but not limited to, loss of profits, reputation, image or business opportunity, and reasonable attorney's fees and subject to potential limitation of liability agreed between the Parties.

(b) The Data Importer shall be liable to the Data Subject, and the Data Subject shall be entitled to receive compensation, for any material or non-material damages the Data Importer or its sub-Processor causes the Data Subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the Data Exporter shall be liable to the Data Subject, and the Data Subject shall be entitled to receive compensation, for any material or non-material damages the Data Exporter or the Data Importer (or its sub-Processor) causes the Data Subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the Data Exporter and, where the Data Exporter is a Data Processor acting on behalf of a Data Controller, to the liability of the controller under GDPR.

(d) The Parties agree that if the Data Exporter is held liable under paragraph (c) for damages caused by the Data Importer (or its sub-Processor), it shall be entitled to claim back from the Data Importer that part of the compensation corresponding to the Data Importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the Data Subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the Data Subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The Data Importer may not invoke the conduct of a sub-Processor to avoid its own liability.

***Clause 13* - Supervision**

(a) The Supervisory Authority with responsibility for ensuring compliance by the Data Exporter with GDPR as regards the Personal Data transfer, as indicated in Annex I.C, shall act as competent Supervisory Authority.

(b) The Data Importer agrees to submit itself to the jurisdiction of and cooperate with the competent Supervisory Authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the Data Importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the Supervisory Authority, including remedial and compensatory measures. It shall provide the Supervisory Authority with written confirmation that the necessary actions have been taken.

Section III
LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

***Clause 14* - Local laws and practices affecting compliance with the Clauses**

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the Processing of the Personal Data by the Data Importer, including any requirements to disclose Personal Data or measures authorising access by public authorities, prevent the Data Importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

  (i) the specific circumstances of the transfer, including the length of the Processing chain, the number of actors involved and the transmission channels used; intended Onward Transfers; the type of recipient; the purpose of Processing; the categories and format of the transferred Personal Data; the economic sector in which the transfer occurs; the storage location of the Personal Data transferred;

  (ii) the laws and practices of the third country of destination– including those requiring the disclosure of Personal Data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

  (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the Processing of the Personal Data in the country of destination.

(c) The Data Importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the Data Exporter with relevant information and agrees that it will continue to cooperate, at no additional costs, with the Data Exporter in ensuring compliance with these Clauses.

(d) The Parties agree, at no additional costs, to document the assessment under paragraph (b) and make it available to the competent Supervisory Authority on request.

(e) The Data Importer agrees to notify, at no additional costs, the Data Exporter promptly if, after having agreed to these Clauses and for the duration of the Contract Document, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the Data Exporter otherwise has reason to believe that the Data Importer can no longer fulfil its obligations under these Clauses, the Data Exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the Data Exporter and/or Data Importer to address the situation. The Data Exporter shall suspend the Personal Data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent Supervisory Authority to do so. In this case, the Data Exporter shall be entitled to terminate the Contract Document, insofar as it concerns the Processing of Personal Data under these Clauses. If the Contract Document involves more than two Parties, the Data Exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the Contract Document is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 - Obligations of the Data Importer in case of access by public authorities

15.1 Notification

(a) The Data Importer agrees to notify the Data Exporter and, where possible, the Data Subject promptly (if necessary with the help of the Data Exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of Personal Data transferred pursuant to these Clauses; such notification shall include information about the Personal Data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to Personal Data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the Data Importer is prohibited from notifying the Data Exporter and/or the Data Subject under the laws of the country of destination, the Data Importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The Data Importer agrees to document its best efforts in order to be able to demonstrate them on request of the Data Exporter.

(c) Where permissible under the laws of the country of destination, the Data Importer agrees to provide the Data Exporter, at regular intervals for the duration of the Contract Document, with as much relevant information as possible on the requests received (in particular, number of requests, type of Personal Data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The Data Importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the Contract Document and make it available to the competent Supervisory Authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the Data Importer pursuant to Clause 14(e) and Clause 16 to inform the Data Exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The Data Importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the

request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The Data Importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the Data Importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the Personal Data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the Data Importer under Clause 14(e).

(b) The Data Importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the Data Exporter. It shall also make it available to the competent Supervisory Authority on request.

(c) The Data Importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

Section IV
FINAL PROVISIONS

Clause 16 - Non-compliance with the Clauses and termination

(a) The Data Importer shall promptly inform the Data Exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the Data Importer is in breach of these Clauses or unable to comply with these Clauses, the Data Exporter shall suspend the transfer of Personal Data to the Data Importer until compliance is again ensured or the Contract Document is terminated. This is without prejudice to Clause 14(f).

(c) The Data Exporter shall be entitled to terminate the Contract Document, insofar as it concerns the Processing of Personal Data under these Clauses, where:

(i) the Data Exporter has suspended the transfer of Personal Data to the Data Importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the Data Importer is in substantial or persistent breach of these Clauses; or

(iii) the Data Importer fails to comply with a binding decision of a competent court or Supervisory Authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent Supervisory Authority of such non-compliance. Where the Contract Document involves more than two Parties, the Data Exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal Data that has been transferred prior to the termination of the Contract Document pursuant to paragraph (c) shall at the choice of the Data Exporter immediately be returned to the Data Exporter or deleted in its entirety, in accordance with the Process detailed below. The same shall apply to any copies of the Personal Data. The Data Importer shall certify the deletion of the Personal Data to the Data Exporter. Until the Personal Data is deleted or returned, the Data Importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the Data Importer that prohibit the return or deletion of the transferred Personal Data, the Data Importer warrants that it will continue to ensure compliance with these Clauses and will only Process the Personal Data to the extent and for as long as required under that local law.

Upon expiration or termination for whatever reason of these Clauses or the Contract Document:

1. The Data Importer shall inquire from the Data Exporter about the Data Exporter's intention with regard to the Personal Data at least fifteen (15) days prior to the effective termination of these Clauses or the Contract Document. Further to this inquiry, where the Data Exporter inform the Data Importer of its intention to retrieve Personal Data, the Data Importer shall retrieve all Personal Data and make them available to the Data Exporter under a commonly used electronic format within fifteen (15) days from effective termination or expiration.

2. Further to such provision, or if the Data Exporter has not instructed the Data Importer for the retrieval of Personal Data prior to the effective expiration or termination of these Clauses or the Contract Document, the Data Importer shall delete all Personal Data on its systems (without prejudice to any backup archives) unless otherwise instructed by the Data Exporter prior to the effective date of termination.
3. Notwithstanding anything to the contrary, the Data Importer may retain one copy of the Personal Data only for as long as there exists a legal requirement to do but in compliance with applicable data protection laws and subject to the provision of these Clauses.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) GDPR that covers the transfer of Personal Data to which these Clauses apply; or (ii) GDPR becomes part of the legal framework of the country to which the Personal Data is transferred. This is without prejudice to other obligations applying to the Processing in question under GDPR.

Clause 17 - Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of France.

Clause 18 - Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
(b) The Parties agree that those shall be the courts of Paris, France. All disputes arising out of, or relating to, these Clauses shall be subject to the exclusive jurisdiction of the International Chamber of the Paris Court of First Instance (Tribunal de commerce de Paris), and all appeals from any decision of such court shall be subject to the exclusive jurisdiction of the International Chamber of the Paris Court of Appeals. The Parties hereby unconditionally agree on the protocols which set out the terms pursuant to which the cases will be examined and adjudicated before these chambers.
(c) A Data Subject may also bring legal proceedings against the Data Exporter and/or Data Importer before the courts of the Member State in which he/she has his/her habitual residence.
(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Such choices of governing law and forum and jurisdiction shall only be relevant as between the Parties for the sole purpose of this Section 4 - Part B.

ANNEX I.A
List of parties

Controller(s):
[Identity and contact details of the Controller(s), and, where applicable, of the Controller's data protection officer]

Controller:

- Name: …
- Address: …
- Contact person's name, position and contact details: …
- Signature and accession date: …

Processor(s):
[Identity and contact details of the Processor(s) and, where applicable, of the Processor's data protection officer]

Processor:

- Name: …
- Address: …
- Contact person's name, position and contact details: …
- Signature and accession date: …

ANNEX I.B
Description of the processing

The Contract Document relates to:

☐ **Processing under Section 4 Part A only (no transfer)**
☐ **Processing and transferring under Section 4 Part B (transfer)**

- **Categories of data subjects whose Personal Data is processed/transferred**

  …

- **Categories of Personal Data processed/transferred**

  …

- **Sensitive data processed/transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for Onward Transfers or additional security measures.**

  …

- **The frequency of the transfer (e.g. whether the Personal Data is transferred on a one-off or continuous basis) (Section 4 - Part B only)**

  …

- **Nature of the processing (Section 4 - Part A only)**

  …

- **Purpose(s) for which the Personal Data is processed/transferred on behalf of the Controller**

  …

- **Duration of the processing (Section 4 - Part A only)**

  …

- **For Processing by/transfers to (sub-) Processors, also specify subject matter, nature, and duration of the processing**

  …

- **The period for which the Personal Data will be retained or, if that is not possible, the criteria used to determine that period (Section 4 - Part B only)**

  …

ANNEX I.C
Competent Supervisory Authority
As per Clause 13 - Section 4 - Part B

Commission Nationale de l'Informatique et des Libertés
3 Place de Fontenoy
TSA 80715
75334 PARIS CEDEX 07
FRANCE

ANNEX II

Technical and organizational measures measures to ensure the security of the data

EXPLANATORY NOTE:

The technical and organizational measures need to be described concretely and not in a generic manner.

Description of the technical and organizational security measures implemented by the Processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons. Examples of possible measures:

For transfers to (sub-) Processors, also describe the specific technical and organizational measures to be taken by the (sub-) Processor to be able to provide assistance to the Controller

Description of the specific technical and organizational measures to be taken by the Processor to be able to provide assistance to the Controller.

- Measures of pseudonymization and encryption of personal data
- Measures for ensuring ongoing confidentiality, integrity, availability and resilience of Processing systems and services
- 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
- Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing
- Measures for user identification and authorization
- Measures for the protection of data during transmission
- Measures for the protection of data during storage
- Measures for ensuring physical security of locations at which Personal Data are processed
- Measures for ensuring events logging
- Measures for ensuring system configuration, including default configuration
- Measures for internal IT and IT security governance and management
- Measures for certification/assurance of processes and products
- Measures for ensuring data minimization
- Measures for ensuring data quality
- Measures for ensuring limited data retention
- Measures for ensuring accountability
- Measures for allowing data portability and ensuring erasure]

ANNEX IV
List of sub-Processors

EXPLANATORY NOTE:
This Annex needs to be completed in case of specific authorization of sub-Processors (Clause 7.7(a), Option 1).

The Controller has authorized the use of the following sub-Processors:

Sub-Processor no.1

- Name: …
- Address: …
- Contact person's name, position, and contact details: …
- Description of the Processing (including a clear delimitation of responsibilities in case several sub-Processors are authorized): …

Sub-Processor no.2

…