DATA PROTECTION AGREEMENT

1. Scope, Order of Precedence, and Term

1.1. This Data Protection Agreement ("**DPA**") is between Liberty Iberoamerica, S.L.U. and its Affiliates (collectively, "**LLA**"), and the signatory to this DPA ("**Supplier**"). Supplier enters into this DPA on behalf of itself and its Affiliates.

1.2. This DPA is part of any and all agreements, purchase orders, statements of work and other contractual documents between LLA and Supplier (individually and collectively, the "**Agreement**"). LLA and Supplier are individually a "**party**" and, collectively, the "**parties**."

1.3. The effective date of the DPA is the date of the Agreement, or the date that LLA first begins using the Services, whichever is earlier.

1.4. This DPA applies only to the extent that Supplier is granted access to, receives, stores, or processes Personal Data in connection with the Services.

1.5. In the event of a conflict between this DPA and the Agreement, the DPA will control to the extent necessary to resolve the conflict. In the event the parties use an International Data Transfer Mechanism and there is a conflict between the obligations in that International Data Transfer Mechanism and this DPA, the International Data Transfer Mechanism will control.

2. Definitions

2.1. The following terms have the meanings set forth below. All capitalized terms not defined in this DPA will have the meanings set forth in the Agreement.

2.2. "**Consent**" means a Data Subject's freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her.

2.3. "**Controller**" means the entity that determines the purposes and means of the processing of Personal Data.

2.4. "**Data Exporter**" means the party that (1) has a corporate presence or other stable arrangement in a jurisdiction that requires an International Data Transfer Mechanism and (2) transfers Personal Data, or makes Personal Data available to, the Data Importer.

2.5. "**Data Importer**" means the party that is (1) located in a jurisdiction that is not the same as the Data Exporter's jurisdiction and (2) receives Personal Data from the Data Exporter or is able to access Personal Data made available by the Data Exporter.

2.6. "**Data Protection Legislation**" means all data protection and privacy laws relating to the processing of Personal Data and privacy including, where applicable, the legally binding guidance and codes of practice issued by Regulators.

2.7. "**Data Subject**" means an identified or identifiable natural person.

2.8. "**De-identified Data**" means a data set that does not contain any Personal Data. Aggregated data is De-identified Data. To "**De-identify**" means to create De-identified Data from Personal Data.

2.9. "**EEA**" means the European Economic Area.

2.10. "**International Data Transfer Mechanism**" means the special protections that some jurisdictions require the parties to adopt to make the transfer lawful, e.g., standard contractual clauses, binding

corporate rules, or statutory obligations that require the parties to adopt certain technical, organizational, or contractual measures. "**Transfer**," in the context of an International Data Transfer Mechanism, means to disclose or move Personal Data from a storage location in one jurisdiction to another, or to permit a party in one jurisdiction to access Personal Data that the other party stores in a jurisdiction that requires an International Data Transfer Mechanism.

2.11. "**Personal Data**" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a Data Subject. "Personal Data" includes equivalent terms in other Data Protection Legislation.

2.12. "**Personal Data Breach**" means a confirmed breach of security of the Services that caused an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, or an event that qualifies as a reportable data breach under applicable Data Protection Legislation.

2.13. "**process**" or "**processing**" means any operation or set of operations that a party performs on Personal Data, including collection, accessing, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

2.14. "**Processor**" means an entity that processes Personal Data on behalf of another entity.

2.15. "**Sensitive Data**" means the following types and categories of data: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data; biometric data; data concerning health, including protected health information governed by the Health Insurance Portability and Accountability Act; data concerning a natural person's sex life or sexual orientation; government identification numbers (e.g., SSNs, driver's license); payment card information; nonpublic personal information governed by the Gramm Leach Bliley Act, or analogous laws; an unencrypted identifier in combination with a password or other access code that would permit access to a Data Subject's account; and precise geolocation.

2.16. "**Services**" has the meaning given to it in the Agreement; otherwise, it means any services that Supplier provides to LLA under the Agreement.

2.17. "**Subprocessor**" means a Processor engaged by a party who is acting as a Processor.

3. Description of the Parties' Personal Data Processing Activities and Statuses of the Parties

3.1. Schedule 1 describes the purposes of the parties' processing, the types or categories of Personal Data involved in the processing, and the categories of Data Subjects affected by the processing.

3.2. Schedule 1 lists the parties' statuses under relevant Data Protection Legislation for each processing activity relevant to the Services.

4. International Data Transfer

4.1. The parties will comply with any International Data Transfer Mechanism that may be required by applicable Data Protection Legislation. The parties agree to abide by the transfer mechanisms in Schedule 1, which describe the International Data Transfer Mechanisms that the parties anticipate using at the outset of the Agreement.

4.2. If the International Data Transfer Mechanism on which the parties rely is invalidated or superseded, the parties will work together in good faith to find an alternative. If the parties are unable to find an

alternative within 60 days, or another period as agreed in writing, either of them may terminate the Agreement.

4.3. If either party reasonably determines that additional measures are necessary to ensure that the personal data they transfer meets the relevant standard of protection of applicable Data Protection Legislation, it will notify the other party and the parties will develop and implement appropriate supplementary measures.

5. Data Protection Generally

5.1. Compliance. The parties will comply with their respective obligations under Data Protection Legislation and their privacy notices.

5.2. Supplier's Lawful Basis of Processing of Personal Data. If Supplier collects Personal Data from Data Subjects directly in connection with the Services, Supplier represents and warrants that it has the Consent or other lawful basis necessary to collect such Personal Data. If a Data Subject revokes their Consent to Supplier's processing of their Personal Data, or otherwise exercises a right to opt out or object, then, consistent with its obligations under Data Protection Legislation, Supplier will be responsible for ceasing disclosure of that Data Subject's Personal Data to LLA (if that would be the result of the Data Subject's request).

5.3. Cooperation.

5.3.1. Data Subject Requests. Supplier will provide LLA with reasonable assistance to enable LLA to comply with its obligations to respond to Data Subjects' requests to exercise the rights to which those Data Subjects may be entitled under Data Protection Legislation.

5.3.2. Governmental and Investigatory Requests. If Supplier receives any type of request or inquiry from a governmental, legislative, judicial, law enforcement, or regulatory authority (e.g. the Federal Trade Commission, the Attorney General of a U.S. state, a European data protection authority or analogous authority), or faces an actual or potential claim, inquiry, or complaint in connection with the parties' processing of Personal Data (collectively, an "**Inquiry**"), Supplier with notify LLA without undue delay unless such notification is prohibited by applicable law. If requested by LLA, the Supplier will provide LLA with information relevant to the Inquiry to enable LLA to respond to the Inquiry.

5.3.3. Other Requirements of Data Protection Legislation. Upon request, Supplier will provide relevant information to LLA to fulfill LLA's obligations (if any) to conduct data protection impact assessments or prior consultations with data protection authorities.

5.4. Confidentiality. Supplier will ensure that its Personnel and Subcontractor Personnel are subject to an obligation to keep Personal Data confidential and have received training on data privacy and security that is commensurate with their responsibilities and the nature of the Personal Data.

5.5. De-identified, Anonymized, or Aggregated Data. The parties may create De-identified Data from Personal Data and process the De-identified Data for any purpose. If one party discloses De-identified Data to the other party, the recipient represents and warrants that it will not attempt to re-identify it.

5.6. Retention. As Controllers, the parties retain Personal Data for as long as they have a business purpose or for the longest time allowable by applicable law. As a Processor, Supplier retains Personal Data it collects or receives from LLA consistent with its obligations in the Agreement and this DPA.

6. Data Security

6.1. Security Controls. Supplier will abide by the security requirements of the Agreement and any other security controls to which the parties agree in writing. Notwithstanding anything to the contrary, Supplier will maintain a written information security policy that defines security controls that are based on Supplier's assessment of risk to Personal Data that Supplier processes and Supplier's information systems. When Supplier chooses security controls, it will consider the state of the art; cost of implementation; the nature, scope, context, and purposes of Personal Data processing; and the risk to Data Subjects of a security incident or Personal Data Breach affecting Personal Data.

7. Supplier's Obligations as a Processor or Subprocessor

7.1. Supplier will have the obligations set forth in this Section 7 if it processes the Personal Data of Data Subjects in its capacity as LLA's Processor; for clarity, these obligations do not apply to Supplier in its capacity as a Controller.

7.2. Scope of Processing.

7.2.1. Supplier will process Personal Data solely to provide Services to LLA and carry out its obligations under the Agreement and LLA's instructions, which include the Agreement and this DPA. Supplier will not process Personal Data for any other purpose, unless required by applicable law. Supplier will notify LLA if it believes that it cannot follow LLA's instructions or fulfil its obligations under the Agreement because of a legal obligation to which it is subject, unless Supplier is prohibited by law from making such notification.

7.2.2. Supplier is prohibited from: (a) accessing, retaining, using, or disclosing Personal Data for any purpose other than for the specific business purpose of performing LLA's documented instructions for the business purposes defined in this Agreement, including accessing, retaining, using, or disclosing the Personal Data for a commercial purpose other than performing LLA's instructions; or (b) accessing, retaining, using, or disclosing the Personal Data outside of the direct business relationship between the parties as defined in this Agreement. Supplier certifies that it understands these restrictions.

7.2.3. Regardless of the foregoing prohibitions, the parties agree that Supplier may, and LLA instructs Supplier to, process Personal Data for the following activities that are necessary to support the Services: detect data security incidents; protect against fraudulent or illegal activity; effectuate repairs; and maintain or improve the quality of the Services.

7.2.4. Processing any Personal Data outside the scope of the Agreement will require prior written agreement between Supplier and LLA by way of written amendment to the Agreement.

7.3. Data Subjects' Requests to Exercise Rights. Supplier will promptly inform LLA if Supplier receives a request from a Data Subject to exercise their rights with respect to their Personal Data under applicable Data Protection Legislation. LLA will be responsible for responding to such requests. Supplier will not respond to such Data Subjects except to acknowledge their requests unless the parties otherwise agree in writing. Supplier will provide LLA with commercially reasonable assistance, upon request, to help LLA to respond to a Data Subject's request.

7.4. Supplier's Subprocessors.

7.4.1. Existing Subprocessors. LLA agrees that Supplier may use the Subprocessors approved in writing by LLA's privacy and security teams.

7.4.2. Use of Subprocessors. LLA grants Supplier general authorization to engage Subprocessors if Supplier and those Subprocessors enter into an agreement that requires the Subprocessor to meet obligations that are no less protective than this DPA (including any applicable International Data Transfer Mechanism) and include at least the following elements: the Subprocessors are prohibited from (1) processing Personal Data for any purpose other than carrying out Supplier's obligations under this Agreement, (2) accessing, retaining, using, or disclosing Personal Data for any purpose other than for the specific business purpose of performing LLA's documented instructions for the business purposes defined in this Agreement, including accessing, retaining, using, or disclosing the Personal Data for a commercial purpose other than performing LLA's instructions; or (3) accessing, retaining, using, or disclosing the Personal Data outside of the direct business relationship between the parties as defined in this Agreement.

7.4.3. Notification of Additions or Changes to Subprocessors. Supplier will notify LLA of any additions to or replacements of its Subprocessors at privacy@lla.com and make that list available on LLA's request. Supplier will provide LLA with at least 30 days to object to the addition or replacement of Subprocessors in connection with Supplier's performance under the Agreement, calculated from the date Supplier provides notice to LLA. If LLA reasonably objects to the addition or replacement of Supplier's Subprocessor, Supplier will immediately cease using that Subprocessor in connection with Supplier's Services under the Agreement, and the parties will enter into good faith negotiations to resolve the matter. If the parties are unable to resolve the matter within 15 days of LLA's reasonable objection (which deadline the parties may extend by written agreement), LLA may terminate the Agreement and/or any statement of work, LLA purchase order or other written agreements. The parties agree that Supplier has sole discretion to determine whether LLA's objection is reasonable; however, the parties agree that LLA's objection is presumptively reasonable if the Subprocessor is a competitor of LLA and LLA has a reason to believe that competitor could obtain a competitive advantage from the Personal Data Supplier discloses to it, or LLA anticipates that Supplier's use of the Subprocessor would be contrary to law applicable to LLA.

7.4.4. Liability for Subprocessors. Supplier will be liable for the acts or omissions of its Subprocessors to the same extent as Supplier would be liable if performing the services of the Subprocessor directly under the DPA.

7.5. Personal Data Breach. Supplier will notify LLA within 48 hours after discovering a Personal Data Breach affecting Personal Data Supplier processes in connection with the Services. Upon request, Supplier will provide information to LLA about the Personal Data Breach to the extent necessary for LLA to fulfill any obligations it has to investigate or notify authorities, except that Supplier reserves the right to redact information that is confidential or competitively sensitive. Notifications will be delivered to privacy@lla.com. LLA agrees that email notification of a Personal Data Breach is sufficient. LLA agrees that it will notify Supplier if it changes its contact information. LLA agrees that Supplier may not notify LLA of security-related events that do not result in a Personal Data Breach.

7.6. Deletion and Return of Personal Data. At the earlier of the expiration or termination of the Agreement or written request by LLA to Supplier (which may occur via email to Supplier), Supplier will, without undue delay, (1) return all LLA Personal Data (including copies thereof) to LLA and (ii) destroy any copies it stored of LLA Personal Data, unless applicable law expressly requires otherwise or the parties otherwise expressly agree in writing. For any LLA Personal Data that Supplier retains after expiration or termination of this Agreement (for example, because Supplier is legally required to retain the

information), Supplier will continue to comply with the data security and privacy provisions of this DPA and Supplier will De-identify such Personal Data (if any) to the extent feasible.

7.7. Audits.

7.7.1. Scope. The terms of this Section 7.7 apply notwithstanding anything to the contrary. LLA agrees that Supplier's obligations under this Section 7.7 are limited to the Personal Data Supplier processes in connection with the Services.

7.7.2. Request. Upon written request that includes a statement of reasons for the request, Supplier will make available to LLA applicable documentation that is responsive to LLA's request, including third-party audit reports or certifications to the extent they are available. To the extent that such audit reports or certifications do not satisfy LLA's request, Supplier will provide LLA or LLA's designated third party (which LLA agrees may not be a competitor to Supplier) with the information and access to Supplier's facilities necessary to demonstrate compliance with Data Protection Legislation.

7.7.3. Access to Facilities. If LLA requires access to Supplier's facilities (the "**Inspection**"), LLA will provide Supplier with written notice at least 60 days in advance. Such written notice will specify the things, people, places, or documents to be made available. Such written notice, and anything produced in response to it (including any derivative work product such as notes of interviews), will be considered confidential information and will remain confidential information in perpetuity or the longest time allowable by applicable law after termination of the Agreement. Such materials and derivative work product produced in response to the Inspection will not be disclosed to anyone without the prior written permission of Supplier unless such disclosure is required by applicable law. If disclosure is required by applicable law, LLA will give Supplier prompt written notice of that requirement and an opportunity to obtain a protective order to prohibit or restrict such disclosure except to the extent such notice is prohibited by applicable law or order of a court or governmental agency. LLA agrees to negotiate in good faith with Supplier before seeking to exercise such audit or on-site inspection right more frequently than once per twelve (12) month period. LLA will make every effort to cooperate with Supplier to schedule the Inspection at a time that is convenient to Supplier. LLA agrees that if it uses a third party to conduct the Inspection, the third party will sign a non-disclosure agreement. LLA agrees that the Inspection will only concern Supplier's architecture, systems, policies, records of processing, data protection impact assessments, and procedures relevant to its obligations as set forth in the Agreement and the processing of Personal Data carried out by Supplier and the Services as provided to LLA. LLA agrees that Supplier will be allowed to protect or redact the names and identifying or proprietary information of other Supplier customers during the Inspection.

Schedule 1: Description of the Processing; Subprocessors; Jurisdiction-Specific Clauses

1. Description of the Processing

1.1. See Exhibit 1 (Description of the Processing).

2. Jurisdiction-specific Obligations and Information for International Transfers

2.1. Generally. The parties agree that, for any jurisdiction not listed below that requires an International Data Transfer Mechanism, they hereby enter into and agree to be bound by the EEA Standard Contractual Clauses (as specified in Section 2.2) for transfers of Personal Data from that jurisdiction unless (1) the parties otherwise agree in writing or (2) a jurisdiction promulgates its own International Data Transfer Mechanism, in which case the parties hereby agree to negotiate an update to this DPA to incorporate such International Data Transfer Mechanism. The parties agree to modify the EEA Standard Contractual Clauses as necessary to adapt them to the circumstances of the transfers (including by using the Data Exporter's location as the forum and jurisdiction); provided that they will not interpret the EEA Standard Contractual Clauses in a manner that materially reduces the protections the EEA Standard Contractual Clauses afford to Data Subjects.

2.2. European Economic Area.

2.2.1. "**EEA Standard Contractual Clauses**" means the European Union standard contractual clauses for international transfers from the European Economic Area to third countries, Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

2.2.2. For transfers from the EEA that are not subject to an adequacy decision or exception, the parties hereby incorporate the EEA Standard Contractual Clauses by reference and, by signing this DPA, also enter into and agree to be bound by the EEA Standard Contractual Clauses. The parties agree to select the following options made available by the EEA Standard Contractual Clauses.

- Clause 7: The parties do not incorporate the docking clause.
- Clause 9, Module 2(a): The parties select Option 2. The time period is 30 days.
- Clause 9, Module 3(a): The parties select Option 2. The time period is 30 days.
- Clause 11(a): The parties do not select the independent dispute resolution option.
- Clause 17: The parties select Option 1. The parties agree that the governing jurisdiction is Spain.
- Clause 18: The parties agree that the forum is Spain.
- Annex I(A): The data exporter is the Data Exporter (defined above) and the data importer is the Data Importer (defined above). The statuses of the parties as Controllers or Processors is described in Schedule 1.
- Annex I(B): The parties agree that Schedule 1 describes the transfer.

- Annex I(C): The competent supervisory authority is the Spanish data protection authority.
- Annex II: The parties agree that Section 6 of the DPA describes the technical and organizational measures applicable to the transfer.
- Annex III: The parties agree that Schedule 1 describes the relevant Subprocessors and their roles in processing Personal Data.

2.3. United Kingdom.

2.3.1. "**IDTA**" means the International Data Transfer Agreement issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as modified by the UK Information Commissioner's Office from time to time.

2.3.2. For transfers from the United Kingdom that are not subject to an adequacy decision or exception, the parties hereby incorporate the IDTA by reference and, by signing this DPA, also enter into and agree to be bound by the Mandatory Clauses of the IDTA.

2.3.3. Pursuant to Sections 5.2 and 5.3 of the IDTA, the parties agree that the following information is relevant to Tables 1 – 4 of the IDTA and that by changing the format and content of the Tables neither party intends to reduce the Appropriate Safeguards (as defined in the IDTA).

- Table 1: The parties' details, key contacts, Data Subject contacts, and signatures are in the signature block of the DPA.
- Table 2:
  - The UK country's law that governs the IDTA is: England and Wales.
  - The primary place for legal claims to be made by the parties is: England and Wales.
  - The statuses of the Data Exporter and Data Importer are described in Exhibit 1.
  - The UK GDPR may apply to the Data Importer's processing of Personal Data under the Agreement.
  - The relationship among the agreements setting forth data protection terms among the parties, including this Section, the DPA, and the Agreement, is described in Section 1 of the DPA.
  - The duration that the parties may process Personal Data is set forth in the DPA.
  - The IDTA is coterminous with the DPA. Neither party may terminate the IDTA before the DPA ends unless one of the parties breaches the IDTA or the parties agree in writing.
  - The Data Importer may transfer Personal Data to another organization or person (who is a different legal entity) if such transfer complies with the IDTA's applicable Mandatory Clauses.
  - The parties will review the Security Requirements listed in Table 4, and any supplementary measures they adopt, to this DPA each year.
- Table 3:

- The categories of Personal Data, Sensitive Data, Data Subjects, and purposes of processing are described in Exhibit 1. Such description may only be updated by written agreement of the parties.

- Table 4:
  - The security measures adopted by the parties are described in Section 6 of this DPA. Such security measures may only be updated by written agreement of the parties.

2.3.4. The parties agree to adopt the additional technical, organizational, and/or contractual protections that may be required by their transfer impact assessment pursuant to Section 4 of the DPA.

Exhibit 1: Description of the Processing

Processing Activity (nature and purpose of the processing; categories of Data Subjects)	Status of the Parties as Controllers or Processors	Categories of Personal Data Processed	Categories of Sensitive Data Processed	Frequency of Transfer	Applicable Standard Contractual Clauses Module
Supplier processes Personal Data to provide the Services, or in connection with the Services receives Personal Data from LLA, or collects Personal Data on LLA's behalf.	LLA is a Controller. Supplier is a Processor.	Any Personal Data LLA discloses to Supplier or that Supplier collects on LLA's behalf.	Any Sensitive Data LLA discloses to Supplier or that Supplier collects on LLA's behalf	Continuous	Module 2 Module 3, if LLA acts as a Processor to another Controller.
Supplier collects Personal Data of LLA's employees, Personnel, contractors, or agents to provide professional services in support of the Services.	LLA is a Controller. Supplier is a Controller.	Name, email address, other contact information, and end-user unique ID. For clarity, Supplier is a Processor with respect to any Personal Data that LLA provides about its customers or end-users.	Any Sensitive Data LLA discloses to Supplier or that Supplier collects on LLA's behalf	Continuous	Module 1
Supplier processes LLA Personnel's account data in support of its obligations under the Agreement.	LLA is a Controller. Supplier is a Controller.	Data that relates to the accounts that LLA's Personnel may create in connection with using the Services, including the names or contact information of individuals authorized by LLA to access LLA's account and billing information of individuals that LLA has associated with its account. Analytical, usage, telemetry, data, and logs that Supplier generates when LLA's Personnel use the Services. Data that Supplier may need to collect for the purpose of identity verification.	Any Sensitive Data LLA discloses to Supplier or that Supplier collects on LLA's behalf	Continuous	Module 1
The parties process Personal Data of their respective Personnel to, e.g., (a) administer and provide the Services; (b) manage invoices; (c) manage the Agreement and resolve any disputes relating to it; (d) respond and/or raise general queries; and (e) comply with their respective regulatory obligations.	LLA is a Controller. Supplier is a Controller.	Name, title, and contact information of the parties' Personnel.	Any Sensitive Data LLA discloses to Supplier or that Supplier collects on LLA's behalf	Continuous	Module 1