DATA PROCESSING ADDENDUM (GDPR and CCPA)

If required by Purchaser and expressly referenced in an Order Form executed between Devo and Purchaser, this data processing addendum (the "DPA") is expressly incorporated by reference into Devo Terms of Service between Devo and Purchaser (including any Exhibits and Schedules thereto, the "ToS"). Devo may be required to collect, process, store and transfer Personal Data (as defined below) that is subject to the GDPR and/or the CCPA (each as defined below), when providing Services to Purchaser under the ToS. The DPA governs Devo's collection, processing, storage and transfer of personal data, if any, under the ToS. Capitalized terms used in this DPA and not otherwise defined herein have the meaning as defined in the ToS. In the event of any conflict between this DPA and the ToS, the terms of this DPA shall govern and control.

1. Personal data types and processing purposes

1.1 The Purchaser and Devo acknowledge that for the purpose of applicable Privacy and Data Protection Requirements, the Purchaser is the data controller and Devo is the data processor.

1.2 The Purchaser retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Privacy and Data Protection Requirements, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to Devo.

1.3 Annex A describes the general Personal Data categories and Data Subject types Devo may process to fulfil the Business Purposes of the ToS.

2. Devo's obligations

2.1 Devo agrees that it will use Personal Data (i) for the following Purchaser business purposes, as to personal information: (a) Detecting or preventing security incidents or other illegal activity and (b) Performing services for or on behalf of Purchaser, such as customer service, order fulfillment, payment processing or analytic services (the "Purchaser Business Purposes"). Devo will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Purchaser's written instructions from Authorized Persons.

2.2 Devo will not process the Personal Data for any other purpose or in a way that does not comply with this DPA or the Privacy and Data Protection Requirements. Devo must promptly notify the Purchaser if, in its opinion, the Purchaser's instruction would not comply with the Privacy and Data Protection Requirements. Devo represents and warrants that it will not (i) sell the Personal Data, (ii) retain, use or disclose the Personal Data for any purpose other than for the Purchaser Business Purposes, including retaining, using, or disclosing the Personal Data for a commercial purpose other than providing the Services, or (iii) retain, use, or disclose the Personal Data outside of the business relationship between Purchaser and Devo.

2.3 Devo must promptly comply with any written Purchaser request or instruction from Authorized Persons requiring Devo to amend, transfer or delete the Personal Data, or to stop, mitigate or remedy any unauthorized processing.

2.4 Devo will maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless the Purchaser or this DPA specifically authorizes the disclosure, or as required by law. If a law requires Devo to process or disclose Personal Data, Devo must first inform the Purchaser of the legal requirement and give the Purchaser an opportunity to object or challenge the requirement, unless the law prohibits such notice.

2.5 Devo will reasonably assist the Purchaser with meeting the Purchaser's compliance obligations under the Privacy and Data Protection Requirements, taking into account the nature of Devo's processing and the information available to Devo.

2.6 Devo must promptly notify the Purchaser of any changes to Privacy and Data Protection Requirements that may adversely affect Devo's performance of the ToS.

2.7 The Purchaser acknowledges that Devo is under no duty to investigate the completeness, accuracy or sufficiency of any specific Purchaser instructions from Authorized Persons or the Personal Data other than as required under the Privacy and Data Protection Requirements.

3. Devo's employees

3.1 Devo will limit Personal Data access to:

(a) those employees who require Personal Data access to meet Devo's obligations under this Agreement; and

(b) the part or parts of the Personal Data that those employees strictly require for the performance of their duties.

3.2 Devo will ensure that all employees:

(a) are informed of the Personal Data's confidential nature and use restrictions;

(b) have undertaken training on the Privacy and Data Protection Requirements relating to handling Personal Data and how it applies to their particular duties; and

(c) are aware both of Devo's duties and their personal duties and obligations under the Privacy and Data Protection Requirements and this DPA.

3.3 Devo will take reasonable steps to ensure the reliability, integrity and trustworthiness of and conduct background checks consistent with applicable law on all of Devo's employees with access to the Personal Data.

4. Security

4.1 Devo must at all times implement appropriate technical and organizational measures designed to safeguard Personal Data against unauthorized or unlawful processing, access, copying, modification, storage, reproduction, display or distribution, and against accidental loss, destruction or damage including, but not limited to, the security measures set out in Annex C.

4.2 Devo must take reasonable precautions to preserve the integrity of any Personal Data it processes and to prevent any corruption or loss of the Personal Data, including but not limited to establishing effective back-up and data restoration procedures.

5. Devo's CCPA Certification

5.1 In accordance with Cal. Civ. Code 1798.100 through 1798.199, Devo understands the restrictions under the CCPA in place and agrees and warrants that it will comply with them.

5.2 It is understood and agreed that the CCPA remains subject to amendment and regulations that have not yet been promulgated, and that other states and the United States Congress are considering similar laws (all of the foregoing, "New Privacy Laws"). Devo agrees and warrants that it will implement such policies and commitments as Purchaser may reasonably request in connection with compliance with New Privacy Laws, including without limitation undertaking the commitments required of "service providers" or Devos exempt from the definition of "third party" under the CCPA (including, without limitation, providing CCPA-required commitments and certification), and undertaking reasonable commitments to otherwise address New Privacy Laws, with regard to which Purchaser and Devo agree and warrant that they will work together in good faith to agree upon and to amend this DPA accordingly before the applicable effective dates of the CCPA and applicable New Privacy Laws. If the parties cannot reach agreement on how to address CCPA and/or New Privacy Laws, Purchaser may terminate the Services Agreement, subject to a transition period designated by Purchaser during which Devo will continue to provide the Services and assist in transitioning the Services to a new provider, and Purchaser shall only be responsible for fees and costs on a pro rata basis through the post-transition termination date.

6. Security breach and personal data loss

6.1 Devo will promptly notify the Purchaser if any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable. Devo will restore such Personal Data at its own expense.

6.2 Either party will notify the other party if it becomes aware of:

(a) any unauthorized or unlawful processing of the Personal Data; or

(b) any Security Breach.

6.3 Immediately following any unauthorized or unlawful Personal Data processing or Security Breach, the parties will co-ordinate with each other to investigate the matter. Devo will reasonably co-operate with the Purchaser in the Purchaser's handling of the matter, including:

(a) assisting with any investigation;

(b) providing the Purchaser with physical access to any facilities and operations affected;

(c) facilitating interviews with Devo's employees, former employees and others involved in the matter; and

(d) making available all relevant records, logs, files, data reporting and other materials required to comply with all Privacy and Data Protection Requirements or as otherwise reasonably required by the Purchaser.

6.4 Devo will not inform any third party of any Security Breach without first obtaining the Purchaser's prior written consent, except when law or regulation requires it.

6.5 Devo agrees that the Purchaser has the sole right to determine:

(a) whether to provide notice of the Security Breach to any Data Subjects, regulators, law enforcement agencies or others, as required by law or regulation or in the Purchaser's discretion, including the contents and delivery method of the notice; and

(b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

6.6 Devo will cover all reasonable expenses associated with the performance of the obligations under clause 6.2 and clause 6.3, unless the matter arose from the Purchaser's specific instructions, negligence, wilful default or breach of this DPA, in which case the Purchaser will cover all reasonable expenses.

6.7 Devo will also reimburse the Purchaser for reasonable, documented, out-of-pocket expenses the Purchaser actually incurs and as necessary to respond to and mitigate damages caused by Devo's Security Breach.

7. Cross-border transfers of personal data

7.1 If the Privacy and Data Protection Requirements restrict cross-border Personal Data transfers, the Purchaser will only transfer that Personal Data to Devo under the following conditions:

(a) Devo, either through its location or participation in a valid cross-border transfer mechanism under the Privacy and Data Protection Requirements, may legally receive that Personal Data. Devo must identify in Annex A the location or mechanism that enables it to receive that Personal Data and must immediately inform the Purchaser of any change to that status;

(b) The Purchaser obtained valid Data Subject consent to the transfer under the Privacy and Data Protection Requirements; or

(c) The transfer otherwise complies with the Privacy and Data Protection Requirements for the reasons set forth in Annex A.

7.2 If any Personal Data transfer between Devo and the Purchaser requires execution of Standard Contractual Clauses and/or the UK Addendum in order to comply with the Privacy and Data Protection Requirements, the parties will complete all relevant details in, and execute, the Standard Contractual Clauses contained in Annex B and/or the UK Addendum contained in Annex C, and take all other actions required to legitimize the transfer, including, if necessary:

(a) co-operating to register the Standard Contractual Clauses with any supervisory authority in any member state of the European Economic Area; or

(b) procuring approval from any such supervisory authority; or

(c) providing additional information about the transfer to such supervisory authority.

8. Subcontractors

8.1 Devo may only authorize a third party (subcontractor) to process the Personal Data if:

(a) the Purchaser provides prior written consent;

(b) Devo enters into a written contract with the subcontractor that contains terms not less protective than those set out in this DPA and, upon the Purchaser's written request, provides the Purchaser with copies of such contracts;

(c) Devo maintains control over all Personal Data it entrusts to the subcontractor; and

(d) the subcontractor's contract terminates automatically on termination of this DPA for any reason.

8.2 Devo must list all approved subcontractors in Annex A.

8.3 Where the subcontractor fails to fulfil its obligations under such written agreement, Devo remains fully liable to the Purchaser for the subcontractor's performance of its agreement obligations.

8.4 Upon the Purchaser's written request and at Purchaser’s expense, Devo will audit a subcontractor's compliance with its obligations regarding the Purchaser's Personal Data and provide the Purchaser with the audit results.

8.5 The foregoing provisions shall not apply if and to the extent Devo subcontracts with Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure or other similarly reputable cloud hosting service provider (“CHP”). In such event, the standard terms and conditions of such cloud hosting service provider shall apply.

9. Complaints, data subject requests and third party rights

9.1 Devo must notify the Purchaser promptly if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Privacy and Data Protection Requirements, including a request from a Data Subject for access to their Personal Data

9.2 Devo will cooperate with and assist the Purchaser in responding to any complaint, notice, communication or Data Subject request.

9.3 Devo must not disclose the Personal Data to any Data Subject or to a third party other than at the Purchaser's request or instruction, as provided for in this DPA or as required by law.

10. Term and termination

10.1 This DPA will remain in full force and effect so long as (a) the ToS remains in effect, or (b) Devo retains any Personal Data related to the ToS in its possession or control (**Term**).

10.2 Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the ToS in order to protect Personal Data will remain in full force and effect.

10.3 In the event of Devo’s breach of this DPA, the parties will suspend the processing of Personal Data until, Devo has cured the breach, but no later than within 5 business days. In the event Devo is unable to cure the breach within 5 business days or in the event of a material breach, the Purchaser may terminate the part of the ToS authorizing the processing of Personal Data effective immediately upon written notice to Devo without further liability or obligation.

10.4 If a change in any Privacy and Data Protection Requirement prevents either party from fulfilling all or part of its ToS obligations, the parties will suspend the processing of Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data processing into compliance with the Privacy and Data Protection Requirement within 10 business days, they may terminate the ToS upon written notice to the other party.

11. Data return and destruction

11.1 At the Purchaser's request, Devo will give the Purchaser a copy of or access to all or part of the Purchaser's Personal Data in its possession or control in the format and on the media reasonably specified by the Purchaser.

11.2 On termination of the ToS for any reason or expiry of its term, Devo will securely destroy or, if directed in writing by the Purchaser, return and not retain, all or any Personal Data related to this agreement in its possession or control.

11.3 If any law, regulation, or government or regulatory body requires Devo to retain any documents or materials that Devo would otherwise be required to return or destroy, it will notify the Purchaser in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

11.4 Devo will certify in writing that it has destroyed the Personal Data after it completes the destruction.

12. Records

12.1 Devo will keep detailed, accurate and up-to-date records regarding any processing of Personal Data it carries out for the Purchaser, including but not limited to, the access, control and security of the Personal Data, approved subcontractors and affiliates, and the processing purposes (**Records**).

12.2 Devo will ensure that the Records are sufficient to enable the Purchaser to verify Devo's compliance with its obligations under this DPA.

12.3 The Purchaser and Devo must review the information listed in the Annexes to this DPA to confirm its current accuracy and update it when required to reflect current practices.

13. Audit

13.1 Devo will conduct at its own cost and expense, security and privacy assessments, and application penetration test reports performed by independent third parties and will maintain the following annual assessments for Devo's applications, services, and systems associated with accessing, processing, storage, communication and/or transmission of the Data and Sensitive Data: System and Organization Controls (SOC 2) Type II report including relevant principles (Security, Availability, Processing Integrity, Confidentiality and Privacy) providing coverage of the entire year; and at least annually, upon Purchaser's written request, Devo agrees to provide Purchaser with copies of all requested certificates, reports or packages in a timely manner. The Purchaser will treat such audit reports as Devo's confidential information under this Agreement.

13.3 Devo will promptly address any exceptions noted in the audit reports with the development and implementation of a corrective action plan by Devo's management.

14. Warranties

14.1 Devo warrants and represents that:

(a) its employees, subcontractors (except for CHP, with respect to whom the disclosure materials provided on the relevant CHP's website shall govern), agents and any other person or persons accessing Personal Data on its behalf have received the required training on the Privacy and Data Protection Requirements relating to the Personal Data; and

(b) it and anyone operating on its behalf will process the Personal Data in compliance with all applicable Privacy and Data Protection Requirements and other laws, enactments, regulations, orders, standards and other similar instruments; and

(c) it has no reason to believe that any Privacy and Data Protection Requirements prevent it from providing any of the ToS's contracted services; and

(d) considering the current technology environment and implementation costs, it will take appropriate technical and organizational measures to prevent the unauthorized or unlawful processing of Personal Data and the accidental loss or destruction of, or damage to, Personal Data, and ensure a level of security appropriate to:

(i) the harm that might result from such unauthorized or unlawful processing or accidental loss, destruction or damage; and

(ii) the nature of the Personal Data protected; and

(iii) comply with all applicable Privacy and Data Protection Requirement and its information and security policies, including the security measures required in clause 4.1.

14.2 The Purchaser warrants and represents that Devo's expected use of the Personal Data for the Business Purpose and as specifically instructed by the Purchaser will comply with all Privacy and Data Protection Requirements.

15. Notice

15.1 Any notice or other communication given to a party under or in connection with this DPA must be in writing and delivered to:

For the Purchaser: At the address provided on the signature page

For Devo: Devo Inc Spanish Branch, Legal Dept, 3-5 Calle Estebanez Calderon, 5th Floor, 28020 Madrid, Spain

15.2 Clause 14.1 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

16. Definitions and interpretation

The following definitions and rules of interpretation apply in this DPA.

16.1 Definitions:

Business Purpose: the services described in the ToS or any other purpose specifically identified in Annex A.

Data Subject: an individual who is the subject of Personal Data.

Personal Data: any information Devo processes for the Purchaser that (1) identifies or relates to an individual who can be identified directly or indirectly from that data alone or in combination with other information in Devo's possession or control or that Devo is likely to have access to, or (2) the relevant Privacy and Data Protection Requirements otherwise define as protected personal data.

Processing, processes and process: either any activity that involves the use of Personal Data or as the relevant Privacy and Data Protection Requirements may otherwise define processing, processes or process. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organizing, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring Personal Data to third parties.

Privacy and Data Protection Requirements: all applicable laws and regulations relating to the processing, protection or privacy of the Personal Data, including where applicable, the guidance and codes of practice issued by regulatory bodies in any relevant jurisdiction.

Security Breach: any act or omission that compromises the security, confidentiality or integrity of Personal Data or the physical, technical, administrative or organizational safeguards put in place to protect it. The loss of or unauthorized access, disclosure or acquisition of Personal Data is a Security Breach.

Standard Contractual Clauses (SCC): the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision (EU) 2021/914 of 4 June 2021, a completed copy of which comprises Annex B.

Standard Contractual Clauses (UK Addendum): The international data transfer addendum to the European Commission's standard contractual clauses for international data transfers adopted by the United Kingdom pursuant to the Data Protection Act of 2018 and other implementation of the GDPR, with an effective date of 21 March 2022, and issued by the UK Information Commissioner's Office under Section 119A of the Data Protection Act 2018 for the transfer of Personal Information/Data from the United Kingdom to controllers or processors established outside the UK, a completed version of which comprises Annex C.

16.2 This DPA is subject to the terms of the ToS and is incorporated into the ToS. Interpretations and defined terms set forth in the ToS apply to the interpretation of this DPA.

16.3 The Annexes form part of this DPA and will have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the Annexes.

16.4 A reference to writing or written includes faxes and email.

16.5 In the case of conflict or ambiguity between:

(a) any provision contained in the body of this DPA and any provision contained in the Annexes, the provision in the body of this DPA will prevail;

(b) the terms of any accompanying invoice or other documents annexed to this DPA and any provision contained in the Annexes, the provision contained in the Annexes will prevail;

(c) any of the provisions of this DPA and the provisions of the ToS, the provisions of this DPA will prevail; and

(d) any of the provisions of this agreement and any executed Standard Contractual Clauses or the UK Addendum, the provisions of the executed Standard Contractual Clauses or UK Addendum will prevail.

This agreement has been entered into on the date stated at the beginning of it.

Signed by	
for and on behalf of **Purchaser**	Name:
Purchaser Address:	Title:
	Date:
Signed by	
for and on behalf of **Devo**	Name:
	Title:
	Date:

ANNEX A Personal Data Processing Purposes and Details

A. LIST OF PARTIES

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officerand/or representative in the European Union]

1. Name: ……………………………………………………………………………………………

Address: …………………………………………………………………………………………

Contact person's name, position and contact details: ………………………………………………

Activities relevant to the data transferred under these Clauses: ……………………………………

Signature and date: ……………………………………………………………………………

Role (controller/processor): …………………………………………………………………

2. ……………………………………………………………………………………………

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for dataprotection]

1. Name: Devo Technology, Inc.

Address: 255 Main St., Suite 702, Cambridge, MA USA 02142

Contact person's name, position and contact details: ………………………………………………

Activities relevant to the data transferred under these Clauses: ……………………………………

Signature and date: ……………………………………………………………………………

Role (controller/processor): Processor

2. ……………………………………………………………………………………………

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Employees, customers, temporary workers, subcontractors, vendors, website users.

Categories of personal data transferred

User data (un)successful logins, timestamps, system usage data

Sensitive data 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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous

Nature of the processing

Querying and analysis of data, provide insights, alerts and reporting

Purpose(s) of the data transfer and further processing

Analysis for Security Incident and Event Management (SIEM), logging, data analytics

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

When no longer required to provide services and in accordance with applicable records retention rules

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

To cloud hosting providers for period specified above

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

. . . .

ANNEX B

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

(a) **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 withregard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] 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') transferringthe 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 anotherentity 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

(b) **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) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, 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 theydo 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 Regulation (EU) 2016/679.

Clause 3

(c) **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);

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC(OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legalact between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(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 Regulation (EU) 2016/679.

Clause 4

(d) **Interpretation**

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaningas in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU)2016/679.

Clause 5

(e) **Hierarchy**

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

Clause 6

(f) **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) forwhich they are transferred, are specified in Annex I.B.

Clause 7 – Optional

(g) **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 Clausesand 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 aParty.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

(h) **Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through theimplementation 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.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

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 ofthe 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 Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, itshall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personaldata 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 data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicableto 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 requiredunder 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 if it has reason to believe thatit is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

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 data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take dueaccount 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 forattributing the personal data to a specific data subject shall, where possible, remain under the exclusive controlof 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. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under anappropriate statutory obligation of confidentiality.

(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 breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the 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 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 shallcontain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, 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.

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 data may only be disclosed to a third party located outside the European Union[2] (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 of Regulation(EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 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 and at the data exporter's request, allow for and contribute to auditsof 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.

(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.

Clause 9

(i) **Use of sub-processors**

(a) SPECIFIC PRIOR AUTHORISATION 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 30 days prior to the engagement of the sub-processor, together with the information necessary to enablethe 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.

(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.[3] 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

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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 theright to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

(j) **Data subject rights**

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. 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

(k) **Redress**

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice oron its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[4] at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph(a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(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 informedabout 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 ofwork, 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 underthe conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(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 proceduralrights to seek remedies in accordance with applicable laws.

Clause 12

(l) **Liability**

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(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

[4] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

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 processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(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 theseClauses, 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) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of applicationof Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of applicationof Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, 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 authorityin any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respondto 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

(m) 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 oneof the objectives listed in Article 23(1) of Regulation (EU) 2016/679, 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 data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of 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;[5]

(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 with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree 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 the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, 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 inparagraph (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 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, insofar as it concerns the processingof personal data under these Clauses. If the contract 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 is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

(n) **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, witha 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

[5] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible onthe requests received (in particular, number of requests, type of 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 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 arequest, 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

(o) **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 whateverreason.

(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 is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, 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 regardingits obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non- compliance. Where the contract 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 pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the 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 deletionof the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(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) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 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 Regulation (EU) 2016/679.

Clause 17

(p) **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 Spain

Clause 18

(q) **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 Spain.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of theMember State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY
NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in thisregard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

_____

ANNEX I

Annex A to the Agreement shall also be deemed Annex I to these Standard Contractual Clauses

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONALMEASURES TO ENSURE THE SECURITY OF THE DATA

PLEASE SEE OUR SOC3 REPORT

ANNEX III

LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed in case of the specific authorisation of sub-processors (Clause9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. Name: Amazon Web Services

Address: 410 Terry Avenue North, Seattle, WA 98109-5210

Description of processing (including a clear delimitation of responsibilities in case several sub-processors areauthorised): Cloud hosting services

2. ....

ANNEX C

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

Part 1: Tables

Table 1: Parties

Start date	The Effective Date oft he ToS	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	As set forth in Annex A	As set forth in Annex A
Key Contact	As set forth in Annex A	As set forth in Annex A
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): Or X the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2	x	x	x	Prior	30 Days	
3						
4						

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As set forth in Annex A
Annex 1B: Description of Transfer: As set forth in Annex A
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set forth in Annex II of Annex B
Annex III: List of Sub processors (Modules 2 and 3 only): As set forth in Annex III of Annex B

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: X Importer X Exporter □ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.

Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

       "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

       "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d. Clause 8.7(i) of Module 1 is replaced with:

       "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

    e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

       "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to “Regulation (EU) 2016/679”, “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 (General Data Protection Regulation)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;

i. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;

j. Clause 13(a) and Part C of Annex I are not used;

k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;

l. In Clause 16(e), subsection (i) is replaced with:

> “the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;

m. Clause 17 is replaced with:

> “These Clauses are governed by the laws of England and Wales.”;

n. Clause 18 is replaced with:

> “Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a its direct costs of performing its obligations under the Addendum; and/or

    b its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.