EQUIPAT IP LLC

DATA PROCESSING AGREEMENT

This Data Processing Agreement (this "***DPA***") is incorporated into, and is subject to the terms and conditions of the Master Subscription Agreement and any applicable Order Form (collectively, the "***Agreement***") made by and between the customer that is a party to the Agreement (the "***Customer***") and Equipat IP LLC, a Georgia limited liability company (the "***Company***"), and reflects the Parties' agreement with regard to the Processing of Customer Personal Data (each as defined below). In the course of providing the Services to the Customer pursuant to the Agreement, the Company may Process Customer Personal Data on behalf of the Customer and the Parties agree to comply with the following provisions with respect to any Customer Personal Data. If there are any conflicting terms and conditions in this DPA and the Agreement, the terms herein shall supersede and replace those of the Agreement. Throughout this DPA, the Company and the Customer may be referred to herein, individually, as a "***Party***", or collectively, as the "***Parties***".

1. Definitions.

"***Affiliate***" means an entity that directly or indirectly controls, is controlled by or is under common control with an entity, where "***control***" means, for the purposes of this definition, an ownership, voting, or similar interest representing fifty percent (50.0%) or more of the total interests then outstanding of the entity in question.

"***Customer Personal Data***" means any Personal Data that the Company Processes on behalf of, and belonging to, the Customer in the Company's provision of the Services, as more particularly described in this DPA.

"***Data Breach***" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to Customer Personal Data. Data Breach shall *not* include *un*successful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"***Data Controller***" or "***Controller***" means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of Personal Data. For the purpose of this DPA, the Data Controller is the Customer and/or the other Data Controllers on whose behalf the Customer acts; *provided, however*, that the Parties understand, acknowledge and agree that, for purposes of applicable Data Protection Laws, the determination of who is the Data Controller, in any specific circumstance, may be a matter of law as applied to the specific facts and circumstances.

"***Data Processor***" or "***Processor***" means any natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of a Data Controller or on the instruction of another Processor acting on behalf of a Data Controller. For the purpose of this DPA, the Data Processor is the Company; *provided, however*, that the Parties understand, acknowledge and agree that, for purposes of any applicable Data Protection Laws, the determination of who is the Data Processor, in any specific circumstance, may be a matter of law as applied to the specific facts and circumstances.

"***Data Protection Laws***" means all applicable laws and regulations relating to the processing of Personal Data and privacy that may exist in the relevant jurisdictions, including, where applicable, EU Data Protection Laws and Non-EU Data Protection Laws.

"***Data Subject***" means an identified or identifiable natural person whom Personal Data relates.

"***EU Data Protection Laws***" means, (i) Regulation 2016/679 of the European Parliament and of the Council 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) (the "***GDPR***"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii).

"***Non-EU Data Protection Laws***" means all US State-specific data protection laws, including, but not limited to, the California Consumer Privacy Act, as amended by the California Privacy Rights Act, the Utah Consumer Privacy Act, the Colorado Privacy Act, the Connecticut Personal Data Privacy and Online Monitoring Act, and the Virginia Consumer Privacy Act (the "***US State-Specific Data Protection Laws***"); the Data Protection Act 2018 and the Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit) Regulations 2019 (the "***UK GDPR***"); the Swiss Federal Act on Data Protection (the "***FADP***"); and any other privacy laws or regulations applicable to the Processing of Customer Data under the Agreement.

"***Personal Data***" means any information relating to an identified or identifiable living individual, including information that can be linked, directly or indirectly, with a particular Data Subject and is protected as "personal data", "personal information", or "personally identifiable information", under Data Protection Laws.

"***Process***", "***Processing***" or "***Processed***" means any operation or set of operations which is performed upon Customer Personal Data whether or not by automated means, according to the definitions given to such terms in the GDPR and such applicable Non-EU Data Protection Laws.

"***Sensitive Data***" means any Personal Data that requires a heightened degree of protection by applicable law, including but not limited to, (a) social security number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) financial information or credit or debit card number (other than the truncated (last four digits) of a credit or debit card); (c) genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation; (e) trade union membership; or (f) information about a person's sexual life or sexual orientation.

"***Services***" means all services provided by the Company in accordance with the Agreement, including, but not limited to, as the case may be, access to the "Junior Platform" and such accompanying services and features provided via a Subscription.

"***Standard Contractual Clauses***" means the standard contractual clauses for the transfer of Personal Data to Data Processors established in third countries pursuant to Regulation (EU) 2016/679 of European Parliament and Council as set out in Annex D to this DPA.

"***Sub-processor***" means any sub-contractor engaged in the Processing of Customer Personal Data in connection with the provision of the Services.

"***Supervisory Authority***" means any regulatory, supervisory, governmental, or other competent authority with jurisdiction or oversight over compliance with the Data Protection Laws.

"***UK IDTA***" means the International Data Transfer Agreement UK Addendum to the EU Commission Standard Contractual Clauses issued by the United Kingdom Information Commissioner under 119A(1) Data Protection Act 2018.

2. Appointment and Data Processing.

2.1 Subject to the terms of the Agreement, the Customer is the Data Controller of Customer Personal Data or has been instructed by and obtained the authorization of the relevant Data Controller(s) to enter into this DPA in the name and on behalf of such Data Controller(s). The Customer is responsible for obtaining all of the necessary authorizations and approvals to enter, use, provide, store, and Process Customer Personal Data to enable the Company to provide the Services. The Customer, as the Data Controller, hereby appoints the Company as the Data Processor in respect of all Processing operations required to be carried out by the Company on Customer Personal Data in order to provide the Services in accordance with the terms of the Agreement.

2.2 The Company shall Process Customer Personal Data *only in accordance with the Customer's documented lawful instructions* as set forth in the Agreement and in this DPA, as necessary to comply with applicable law, or as otherwise agreed in writing. The Parties agree that the Agreement sets out the Customer's complete and final instructions to the Company in relation to the Processing of Customer Personal Data, and Processing outside the scope of these instructions (if any) shall require prior written agreement between the Parties.

2.3 The Customer will not provide (or cause to be provided) any Sensitive Data to the Company for Processing under the Agreement, and the Company will have no liability whatsoever for Sensitive Data, whether in connection with a Data Breach or otherwise. For the avoidance of doubt, this DPA will *not* apply to Sensitive Data.

2.4 The Customer represents and warrants that (a) it has complied, and will continue to comply, with all applicable laws, including Data Protection Laws, in respect of its Processing of Customer Personal Data and any Processing instructions it issues to the Company; and (b) it has provided, and will continue to provide, all notice and has obtained, and will continue to obtain, all consents and rights necessary under Data Protection Laws for the Company to Process Customer Personal Data for the purposes described in the Agreement. The Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired the Customer Personal Data.

2.5 The Customer will ensure that the Company's Processing of Customer Personal Data in accordance with the Customer's instructions will not cause the Company to violate any applicable law, regulation, or rule, including, without limitation, all Data Protection Laws. The Company shall immediately notify the Customer, where in its opinion an instruction of the Customer infringes any Data Protection Laws and request the Customer to withdraw, amend, or confirm the relevant instruction. Pending the decision on the withdrawal, amendment, or confirmation of the relevant instruction, the Company shall be entitled to suspend the implementation of the relevant instruction.

2.6 The subject matter, nature, purpose, and duration of the Processing of Customer Personal Data, as well as the types of Personal Data collected and categories of Data Subjects, are described in Annex B to this DPA.

2.7 The Company shall maintain complete, accurate, and up to date written records of all Processing activities carried out on behalf of the Customer containing information as required under any applicable Data Protection Laws.

2.8 The Company acknowledges that it has no right, title, or interest in the Customer Personal Data and may not sell, rent, or lease the Customer Personal Data to anyone.

3. **Sub-processors**.

3.1 The Company currently utilizes the Sub-processors set forth in Annex C of this DPA. The Customer acknowledges and agrees that the Company may engage third-party Sub-processors in connection with the provision of the Services, or to fulfil its contractual obligations under this DPA, or to provide certain services on its behalf, such as providing support services to the Company.

3.2 The Company shall notify the Customer (email is sufficient) if it adds or removes Sub-processors prior to any such changes. The Customer may object, in writing, to the Company's appointment of a new Sub-processor within fifteen (15) calendar days of such notice; *provided that* such objection is based on reasonable grounds relating to data protection. In such event, the Parties shall discuss such concerns in good faith with a view to achieving resolution. If this is not possible, the Customer may suspend or terminate the Agreement.

3.3 The Company has or will, as applicable, maintain a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Customer Personal Data to the extent applicable to the nature of the services provided by such Sub-processor. The Company will, exercising reasonable care, evaluate an organization's data protection practices before allowing the organization to act as a Sub-processor.

3.4 The Company shall be liable to the Customer for the acts and omissions of Sub-processors to the same extent that the Company would itself be liable under this DPA had it conducted such acts or omissions.

4. **Authorized Personnel**. The Company will ensure that its personnel engaged in the Processing of Customer Personal Data are informed of the confidential nature of Customer Personal Data, have received appropriate training on their responsibilities, and have executed written confidentiality agreements committing themselves to confidentiality. The Company will ensure that the Company's access to Customer Personal Data is limited to those personnel performing Services in accordance with the Agreement.

5. **Security Responsibilities**.

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Company will maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of Processing Customer Personal Data, including, but not limited to, the security measures set out in Annex A.

5.2 The Company will implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate: (a) the pseudonymization and encryption of Customer Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; (c) the ability to restore the availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident; and (d) a Process for regularly testing, assessing, and evaluating the effectiveness of security measures.

5.3 The Company maintains internal policies and procedures, and/or ensures that its Sub-processors do so, which are designed to:

(a) Secure any Customer Personal Data Processed by the Company against Data Breaches;

(b) Identify reasonably foreseeable and internal risks to security and unauthorized access to the Customer Personal Data Processed by the Company; and

(c) Minimize security risks, including through risk assessment and regular testing.

5.4 The Company will, and will use reasonable efforts to ensure that its Sub-processors, conduct periodic reviews of the security of their network and the adequacy of their information security program as measured against industry security standards and its policies and procedures.

5.5 The Company will, and will use reasonable efforts to ensure that its Sub-processors, periodically evaluate the security of their network and associated services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

5.6 The Customer acknowledges that such security measures implemented by the Company are subject to changes, from time to time, to reflect technological developments and industry practices; *provided, always*, that such changes do not result in any objective degradation to the security of Customer Personal Data, the manner in which the Services are provided, or which fall below the standard of any applicable law.

5.7 Notwithstanding the above, the Customer agrees that, except as provided by this DPA, the Customer is responsible for protecting the security of Customer Personal Data when in transit to the Company for the Company's provision of the Services.

6. **Data Breach Provisions**.

6.1 If the Company becomes aware of a Data Breach, the Company shall, promptly and without undue delay, (a) notify the Customer of the Data Breach; and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Data Breach.

6.2 In the event of a Data Breach, the Company shall provide Customer with all reasonable assistance in dealing with the Data Breach, in particular in relation to making any notification to a Supervisory Authority or any communication to Data Subjects. In order to provide such assistance, and taking into account the nature of the Services and the information available to the Company, the notification of the Data Breach shall include, at a minimum, the following: (a) a description of the nature of the Data Breach including the categories and approximate number of data records concerned; (b) the likely consequences of the Data Breach; and (c) the measures taken or to be taken by the Company to address the Data Breach, including measures to mitigate any possible adverse consequences. Where, and insofar as, it is not possible for the Company to provide such information at the time of the notice, then such notice shall nevertheless be made, in as complete a form as possible, and the remaining required information may be provided by the Company, in phases and as it shall become available, without undue delay.

7. **Deletion; Access and Export of Customer Personal Data**. Upon termination or expiration of the Agreement, the Company will, at the choice and written request of the Customer, return to Customer and/or securely destroy/delete all Customer Personal Data in its possession or control in accordance with the Agreement. Notwithstanding the foregoing, if this DPA is not subject to EU Data Protection Laws based on the Customer and/or the Customer Personal Data, then, upon termination or expiration of the Agreement, the Company will only be obligated to securely destroy/delete the Customer Personal Data in its possession or control, whereby if the Customer, instead, seeks the Company's return/export of the Customer Personal Data, the Company shall have the right to accept or decline such request as well as the right to require payment of a certain fee to comply with such request. However, the foregoing shall *not* apply (i) to the extent the Company is required by applicable law to retain some or all of the Customer Personal Data, or (ii) to Customer Personal Data the Company has archived on back-up systems whereby the Company shall securely isolate and protect such Customer Personal Data from any further Processing and delete in accordance with its deletion practices.

8. **Audits**.

8.1 At the Customer's written request, the Company will, not more than once annually, allow an audit to verify the Company's compliance with obligations under Data Protection Laws and this DPA, to be carried out either (a) by an independent third party audit firm bound by a duty of confidentiality selected by the Customer and approved by the Company (which approval will not unreasonably be withheld or delayed), or (b) by a Supervisory Authority. The Parties will agree on the scope of the audit prior to the audit being carried out. If the Customer requests that the Company incur out-of-pocket costs to assist the Customer in the audit, then the Company is entitled to a reasonable, pre-approved reimbursement for any costs of the audit incurred by the Company.

8.2 In addition to the foregoing, the Company shall respond to all reasonable requests for information made by the Customer to confirm the Company's compliance with this DPA, including responses to information security, due diligence, and audit questionnaires, by making additional information available regarding its information security program upon the Customer's written request to the Company, provided that the Customer shall not exercise this right more than once annually.

9. **Assistance on Data Protection Impact Assessment**. To the extent required under applicable Data Protection Laws, the Company will, at the Customer's expense and taking into account the nature of the Processing and the information available to the Company, provide all reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments or prior consultations with any Supervisory Authorities, as required by such Data Protection Laws.

10. **International Transfers**.

10.1 The Customer acknowledges that the Company may transfer and Process Customer Personal Data to and in the United States of America and anywhere else in the world where the Company or its Sub-processors maintain Processing operations. The Company shall, at all times, ensure that such transfers are made in compliance with the requirements of all applicable Data Protection Laws.

10.2 To the extent that the Company is a recipient of Customer Personal Data protected by EU Data Protection Laws ("***EU Data***"), the Company agrees to abide by and Process EU Data in compliance with the Standard Contractual Clauses in the form set out on Annex D. For the purposes of the descriptions in the Standard Contractual Clauses, the Company agrees that it is the "data importer" and the Customer is the "data exporter" (notwithstanding that the Customer may itself be an entity located outside of Europe). Further, if this Section 10.2 is applicable to the Parties hereto, the Parties entry into the Agreement shall affirmatively and legally bind the Parties to the Standard Contractual Clauses set forth on Annex D.

10.3 To the extent that the Company is a recipient of Customer Personal Data originating from Switzerland, the following additional requirements shall apply to the extent that the data transfers are exclusively subject to the FADP or are subject to both the FADP and the EU GDPR: (a) the term 'member state' must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 (c) of the Standard Contractual Clauses; (b) insofar as the data transfers underlying the

Standard Contractual Clauses are exclusively subject to the FADP, references to the EU GDPR are to be understood as references to the FADP; (c) insofar as the data transfers underlying the Standard Contractual Clauses are subject to both the FADP and the EU GDPR, the references to the EU GDPR are to be understood as references to the FADP insofar as the data transfers are subject to the FADP; and (d) until the revised Swiss Federal Act on Data Protection (rev. FADP) enters into force, the provisions of the Standard Contractual Clauses also protect the Customer Personal Data to the extent that these provisions are applicable to them under Swiss law.

10.4 To the extent that the Company is a recipient of Customer Data originating from the United Kingdom in a country that is not recognized as providing an adequate level of protection for Personal Data as described in the UK GDPR, the Parties agree that the Standard Contractual Clauses shall be read in accordance with, and deemed amended by, the provisions of Part 2 (Mandatory Clauses) of the UK IDTA (https://ico.org.uk/media/for-organisations/documents/4019483/international-data-transfer-addendum.pdf) , which is incorporated herein by reference as if fully set forth in this DPA. The parties confirm that the information required for the purposes of Part 1 (Tables) of the UK IDTA is set out in the Agreement. Each party's signature to this DPA will be considered a signature to the UK IDTA.

10.5 To the extent that the Company adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses) for the transfer of Customer Personal Data not described in this DPA ("***Alternative Transfer Mechanism***"), the Alternative Transfer Mechanism shall apply instead of the transfer mechanisms described in this DPA (but only to the extent such Alternative Transfer Mechanism is approved by the appropriate Supervisory Authority). In addition, if and to the extent that a court of competent jurisdiction or Supervisory Authority orders (for whatever reason) that the measures described in this DPA cannot be relied on to lawfully transfer EU Data (within the meaning of applicable Data Protection Laws), the Company may implement any additional measures or safeguards that may be reasonably required to enable the lawful transfer of Customer Personal Data.

11. Data Subject Requests and Other Communications.

11.1 The Company will, to the extent required by the Data Protection Laws, promptly notify the Customer upon receipt of a request by a Data Subject to exercise Data Subject rights under the applicable Data Protection Laws. The Company will advise the Data Subject to submit their request to the Customer and the Customer will be responsible for responding to such request.

11.2 The Company will, taking into account the nature of the Processing, assist the Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the Data Subject's rights under the Data Protection Laws. If requested by the Company, the Customer will provide such information to the Company as is reasonable and necessary for the Company to unambiguously identify the Data Subject requesting to exercise their Data Subject rights.

12. Permitted Disclosures of Customer Personal Data. The Company may disclose Customer Personal Data to the extent such data is required to be disclosed by law, by any government or Supervisory Authority, or by a valid and binding order of a law enforcement agency (such as a subpoena or court order), or other authority of competent jurisdiction. If any law enforcement agency government or Supervisory Authority sends the Company a demand for disclosure of Customer Personal Data, then the Company will attempt to redirect the law enforcement agency, government, or Supervisory Authority to request that data directly from the Customer and the Company is entitled to provide the Customer's basic contact information to such law enforcement agency, government, or Supervisory Authority. If compelled to disclose Customer Personal Data pursuant to this Section 12, the Company will give the

Customer reasonable notice of the demand to allow the Customer to seek a protective order or other appropriate remedy.

13. Liability; Limitations. Each Party's and all of its Affiliates' liability, taken together in the aggregate arising out of or related to this DPA (including the Standard Contractual Clauses), shall be subject to the exclusions and limitations of liability set forth in the Agreement, to the extent permitted by applicable Data Protection Laws. Any claims made against the Company under or in connection with this DPA (including, where applicable, the Standard Contractual Clauses) shall be brought solely by the Customer entity that is a party to the Agreement. In no event shall any Party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

14. Processing Personal Data Protected by a US State-Specific Data Protection Law.

(a) To the extent that the Company Processes Personal Data that is protected by a US State-Specific Data Protection Law, the terms in this Section 14 shall apply in addition to the terms in the remainder of the DPA. In the event of any conflict or ambiguity between the terms in this Section 14 and any other terms in this DPA, the terms in this Section 14 shall take precedence but only to the extent they apply to the Personal Data in question.

(b) The Company will not: (i) Sell (within the meaning of such applicable US State-Specific Data Protection Law) Personal Data; (ii) Process Personal Data for any purpose other than for the specific purposes set forth herein (for the avoidance of doubt, the Company will not Process Personal Data outside of the direct business relationship between the Customer and Company); or (iii) attempt to link, identify, or otherwise create a relationship between Customer Personal Data and non-Customer Personal Data or any other data without the express authorization of the Customer.

(c) The Parties acknowledge that Customer Personal Data that has been de-identified is not "personal information" (within the meaning of such applicable US State-Specific Data Protection Law). The Company may de-identify Customer Personal Data only if it: (i) has implemented technical safeguards that prohibit re-identification of the Data Subject to whom the information may pertain; (ii) has implemented business processes that specifically prohibit re-identification of the information; (iii) has implemented business processes to prevent inadvertent release of de-identified information; and (iv) makes no attempt to re-identify the information.

(d) The Company hereby certifies that it understands its restrictions and obligations set forth in this Section 14 and will comply with them.

15. Relationship with the Agreement. This DPA shall remain in effect for as long as the Company carries out Customer Personal Data Processing operations on behalf of the Customer or until termination of the Agreement (and all Customer Personal Data has been returned or deleted in accordance with Section 7 above). This DPA supersedes and replaces all prior representations, understandings, communications, and agreements by and between the Parties in relation to Customer Personal Data and the matters set forth in this DPA. In the event of any conflict or inconsistency between this DPA and the Agreement, the provisions of the following documents (in order of precedence) shall prevail: (a) the Standard Contractual Clauses; then (b) this DPA; and then (c) the Agreement. For matters not addressed under this DPA, the terms of the Agreement apply.

16. Annexes.

Annex A – "Information Protection and Security Standards".

Annex B – “Details of Data Processing”.

Annex C – “Sub-Processors List”.

Annex D – “Standard Contractual Clauses”.

ANNEX A

Information Protection and Security Standards

This document constitutes the Information Protection and Security Standard annex (the "***IPSS Annex***") of the Data Processing Agreement (the "***Agreement***"). The IPSS Annex is stated at a relatively high level and the Customer recognizes that the IPSS Annex may be revised by the Company from time to time. All terms used and not otherwise defined herein, shall have the meanings ascribed to them in the Agreement.

HUMAN RESOURCES SECURITY

The Company has implemented and maintains appropriate measures to ensure that Authorized Employees involved in the processing of the Customer Personal Data are authorized with a need to access the data, are bound by appropriate confidentiality obligations and have undergone appropriate training in the protection and handling of the Customer Personal Data.

The Company ensures that access to the Customer Personal Data is revoked immediately upon termination or when access is no longer required for personnel involved in the processing of the Customer Personal Data.

PHYSICAL SECURITY

Policies and procedures, and supporting business processes, are in place for maintaining a safe and secure working environment in the Company's offices and to control physical access, including access provisioning.

ACCESS CONTROL

The Company has implemented and maintains access control processes and mechanisms to prevent unauthorized access to Customer Personal Data and to limit access only to Authorized Employees with a business need to know.

The access to Customer Personal Data is achieved by means of authenticated individual accounts and is limited solely to Authorized Employees which need access to perform specific responsibilities or functions in the provision or support of the Services.

Accounts are disabled upon personnel termination or change of roles and responsibilities, and it is an established and maintained process to periodically review access controls.

ENCRYPTION

To the extent technically feasible, but in all situations where required by applicable law, the Company agrees to transmit Customer Personal Data in a commercially reasonable format using industry accepted encryption technology

BACKUP

Incremental backups of critical systems within the Company's Database Management System, are taken daily. Full backups of the Company's Database Management System are taken on regular basis, while active (point in time) logs ("***WAL***") are continuously captured to allow for recovery to any point in time. Backups are stored locally in different buildings inside the Company's headquarters, and mission critical backups are stored additionally on its cloud provider's storage.

DESKTOP AND LAPTOP SECURITY

The Company has implemented and maintains desktop and laptop system administration procedures that meet or exceed industry standards including automatic operating system patching and upgrading, anti-virus software and hard drive encryption.

NETWORK SECURITY

The Company has implemented and maintains technical measures designed to meet or exceed industry standards aimed to monitor, detect, and prevent malicious network activity on the network infrastructures under its control and management responsibility.

The Company ensures that firewalls, network routers, switches, load balancers, domain name servers, mail servers, and other network components of the network infrastructures under its control and management responsibility are configured and secured in accordance with commercially reasonable industry standards.

REMOTE ACCESS

The Company has implemented and maintains remote access policies and procedures that meet or exceed industry standards for the Company's personnel who require remote access to a network or system that protects, processes or stores Customer Personal Data.

DATA SEGMENTATION

The Company has implemented and maintains logical data segregation to ensure Customer Personal Data is not viewable by unauthorized users.

DATA DESTRUCTION

Data stored locally are destroyed in accordance with the Company's Data Retention Policy, and depending on the medium, such data is destroyed by physical damage of a disc or by using dedicated hardware to damage a disc. For data stored in the cloud, the Company relies on its cloud providers for data destruction and can only perform logical deletion on request.

AUDIT

At the Customer's request, but not more than once per calendar year, the Company may engage a competent third-party provider to perform a security audit in order to verify its compliance with this IPSS Annex.

[*End of Annex A*]

ANNEX B

DETAILS OF DATA PROCESSING

Subject Matter: The subject matter of the data Processing under this DPA is the Customer Personal Data.

Duration of Processing: The Company will process Customer Personal Data for the term of the Agreement plus the period until the Company deletes all Customer Personal Data processed on behalf of Customer in accordance with the Agreement.

Nature and Purpose of Processing: The Company will Process Customer Personal Data on behalf of Customer for the following purposes: (a) processing to perform the Services in accordance with the Agreement; and (b) to comply with any other reasonable instructions provided by the Customer that are consistent with the terms of the Agreement.

Categories of Data Subjects: The Personal Data transferred may include, but is not limited to, Personal Data relating to the Customer's customers, employees, contractors, and end users.

Types of Personal Data: The categories of Personal Data are determined by the Customer in its sole discretion and may include, but is not limited to, names, personal addresses, telephone numbers, emails, and IP addresses.

Sensitive Data Transferred: None.

Frequency of the Transfer: The frequency of the transfer will be on one-time or a continuous basis, as determined by Customer in its sole discretion and/or as provided for in the Agreement.

Transfers to Sub-processors: The subject matter and nature of the Processing by Sub-processors are as specified in Annex C of the DPA. The duration of the Processing carried out by the Sub-processors will be until thirty (30) days following the termination or expiration of the Agreement unless otherwise agreed.

Competent Supervisory Authority: Customer's competent Supervisory Authority will be determined in accordance with the applicable Data Protection Laws.

[*End of Annex B*]

ANNEX C

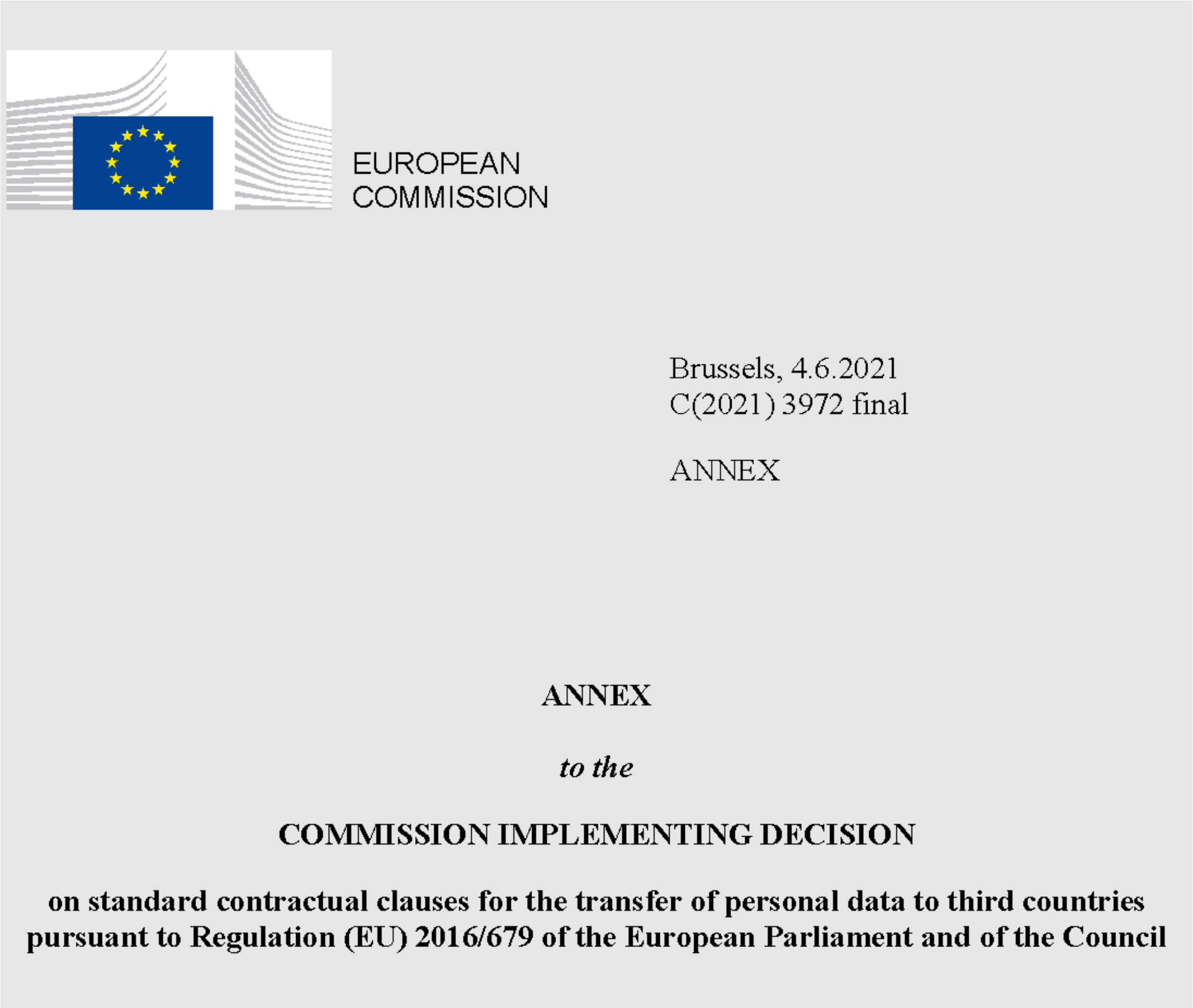
List of Sub-processors

Entity Name	Purpose of Processing	Processed Data	Location
OpenAI, LLC	Hosting of large language models	Customer Personal Data	United States
Amazon Web Services, Inc.	Servers, storage, and databases	Customer Personal Data	United States
Google LLC (GSuite)	Back-office operations	Customer Personal Data, specifically emails between Company and Customer	United States
Google LLC (Google Analytics)	Tracking users on marketing site	Customer Personal Data, specifically anonymized marketing website behavior	United States
Stripe, Inc.	Payment service provider	Customer Personal Data: Email, Name, and Billing information	United States

[*End of Annex C*]

ANNEX D

EU Standard Contractual Clauses



EUROPEAN
COMMISSION

Brussels, 4.6.2021
C(2021) 3972 final

ANNEX

ANNEX

to the

COMMISSION IMPLEMENTING DECISION

on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

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

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

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

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) 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 they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules Two and Three: Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

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

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

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 - Optional

Docking clause

Not used.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

MODULE TWO: Transfer controller to processor

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 of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the 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 personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

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 due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(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 shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall 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[1] (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 audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

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

[1] 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.

(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

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 15 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(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.[2] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(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.

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

(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

Redress

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

MODULE TWO: Transfer controller to processor

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

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

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

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

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) 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 procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

(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 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 these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

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

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

(a) 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.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) 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[3];

(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 in paragraph (a). For Module Three: The data exporter shall forward the notification to the controller.

(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

[3] 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.

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 (for Module Three: , if appropriate in consultation with the controller). 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 (for Module Three: the controller or) 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 processing of 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

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

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.

(For Module Three: The data exporter shall forward the notification to the controller.)

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

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the 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.). (For Module Three: The data exporter shall forward the information to the controller.)

(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 a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. (For Module Three: The data exporter shall make the assessment available to the controller.)

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract 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 regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority (for Module Three: and the controller) 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 deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the 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

Governing law

MODULE TWO: Transfer controller to processor

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 the Republic of Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(f) The Parties agree that those shall be the courts of the Republic of Ireland.

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

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

Appendix 1
to the Standard Contractual Clauses

A. LIST OF PARTIES

Data exporter(s):

Name: “Customer” as set forth in the Agreement.

Address: As set forth in the Agreement.

Contact person’s name, position and contact details: As set forth in the Agreement.

Activities relevant to the data transferred under these Clauses: The activities specified in Annex B of the DPA.

Signature: As set forth in the DPA.

Date: As set forth in the DPA.

Role (controller/processor): Controller.

Data importer(s):

Name: “Company” as set forth in the Agreement.

Address: As set forth in the Agreement.

Contact person’s name, position and contact details: As set forth in the Agreement.

Activities relevant to the data transferred under these Clauses: The activities specified in Annex B of the DPA.

Signature: As set forth in the DPA.

Date: As set forth in the DPA.

Role (controller/processor): Processor.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The categories of data subjects whose personal data is transferred are specified in Annex B of the DPA.

Categories of personal data transferred

The categories of personal data transferred are specified in Annex B of the DPA.

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.

No sensitive data will be transferred from the data exporter to the data importer.

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

The frequency of the transfer is specified in Annex B of the DPA.

Nature of the processing

The nature of the processing is specified in Annex B of the DPA.

Purpose(s) of the data transfer and further processing

The purposes of the data transfer and further processing are specified in Annex B of the DPA.

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

The period for which the personal data will be retained is specified in Annex B of the DPA.

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

The subject matter and nature of the processing by sub-processors are specified in Annex B of the DPA. The duration of the processing carried out by sub-processors is specified in Annex B of the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

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

The data exporter's competent supervisory authority is set forth in Annex B of the DPA.

Appendix 2
to the Standard Contractual Clauses

Description of the technical and organisational measures implemented by the data importer (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

The technical and organizational security measures implemented by the data importer are described in Section 5 and Annex A of the DPA.

[*End of Annex D*]