Instructions for executing this Data Processing Addendum:

This Data Processing Addendum ("**DPA**"), including the EC Controller – Processor Standard Contractual Clauses in Exhibit D (and UK Standard Contractual Clauses in Exhibit E) has been pre-approved and signed by Figma, Inc.

To complete and execute this DPA please do the following:

1. Complete the information in the Customer signature block on page 5 and countersign where directed.
2. Email the completed and fully signed document to: privacy@figma.com.

How this DPA applies:

- If the Customer signing this DPA is also party to an Agreement (as defined in the DPA) then this DPA is an addendum to and forms part of the Agreement.

- If the entity signing this DPA is not party to an Agreement with Figma and has not signed an Order Form with Figma, then this DPA is not valid and not legally binding. Figma recommends that the entity should request that the Customer entity that is party to the Agreement executes this DPA.

If you have any questions on the above, please email us at privacy@figma.com.

DATA PROCESSING ADDENDUM

This Data Processing Addendum, including its Exhibits, ("**Addendum**") supplements and is subject to the terms of the agreement between Figma and Customer governing Customer's use of the Figma Offering (the "**Agreement**"), including the limitations of liability set forth in the Agreement.

1. Subject Matter and Duration.

a) Subject Matter. This Addendum reflects the parties' commitment to abide by Data Protection Laws when Processing Customer Personal Data under the Agreement. All capitalized terms that are not expressly defined in this Addendum will have the meanings given to them in the Agreement. If and to the extent language in this Addendum or any of its Exhibits conflicts with the Agreement, this Addendum shall control.

b) Duration and Survival. This Addendum will become legally binding upon the date that the parties sign this Addendum. This Addendum will terminate automatically upon termination of the Agreement, or as earlier terminated pursuant to the terms of the Addendum.

2. Definitions.

For the purposes of this Addendum, the following terms and those defined within the body of this Addendum apply.

"**Customer Personal Data**" means Personal Data pertaining to Customer's Authorized Users of the Figma Offering Processed by Figma on behalf of Customer under the Agreement.

"**Data Protection Laws**" means all applicable data privacy, data protection, and cybersecurity laws, rules and regulations of the United States, the European Union, and the United Kingdom, to which the Customer Personal Data are subject. "Data Protection Laws" shall include, but not be limited to, the California Consumer Privacy Act of 2018 ("**CCPA**") and the EU General Data Protection Regulation 2016/679 ("**GDPR**").

"**Figma Offering**" means the Figma offering provided by Figma to Customer, as described in an ordering document between the parties.

"**Personal Data**" has the meaning assigned to the term "personal data" or "personal information" under applicable Data Protection Laws.

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

"**Security Incident(s)**" means the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data attributable to Figma.

"**Subprocessor(s)**" means Figma's authorized vendors and third-party service providers that Process Customer Personal Data.

3. Data Use and Processing.

a) Roles and Responsibilities. Customer may act as a "Business," or "Controller" and Figma may act as a "Service Provider," or "Processor" (as such terms are defined by Data Protection Laws). Customer shall ensure that it has lawfully collected and that it may lawfully provide Customer Personal Data to Figma for the purposes contemplated by the Agreement.

b) Documented Instructions. Figma shall Process Customer Personal Data only to provide the Figma Offering in accordance with the Agreement, this Addendum, any applicable ordering document between the parties, and any instructions agreed upon by the parties. The parties agree that this Addendum is Customer's complete and final instructions to Figma in relation to Processing of Customer Personal Data. Processing outside the scope of this Addendum (if any) will require prior written agreement between Customer and Figma regarding additional instructions for Processing, including agreement on any additional fees Customer will pay Figma for carrying out such instructions. Figma will, unless legally prohibited from doing so, inform Customer in writing if it reasonably believes that there is a conflict between Customer's instructions and applicable law or otherwise seeks to Process Customer Personal Data in a manner that is inconsistent with Customer's instructions.

c) Authorization to Use Subprocessors. To the extent necessary to fulfill Figma's contractual obligations under the Agreement, Customer hereby authorizes Figma to engage Subprocessors.

d) Figma and Subprocessor Compliance. Figma agrees to (i) enter into a written agreement with Subprocessors regarding such Subprocessors' Processing of Customer Personal Data that imposes on such Subprocessors data protection requirements

for Customer Personal Data that are consistent with this Addendum; and (ii) remain responsible to Customer for Figma's Subprocessors' failure to perform their obligations with respect to the Processing of Customer Personal Data.

e) Right to Object to Subprocessors. Prior to engaging any new Subprocessors that Process Customer Personal Data, Figma will notify Customer of these changes by posting its proposed new Subprocessors to the following website https://www.figma.com/sub-processors/. Figma will allow Customer ten calendar days to object after notice is given. It is Customer's responsibility to check this website regularly for updates. If Customer has legitimate objections to the appointment of any new Subprocessor that relates to Figma's compliance with this Addendum, Figma will make reasonable efforts to address Customer's objection. After this process, if a resolution has not been agreed to within five calendar days, Figma will proceed with engaging the Subprocessor. During the 30 days that follow any failure to reach such resolution, Customer may terminate the part of the service performed under the Agreement that cannot be performed by Figma without use of the objectionable Subprocessor by providing written notice to Figma.

f) Confidentiality. Any person authorized to Process Customer Personal Data must contractually agree to maintain the confidentiality of such information or be under an appropriate statutory obligation of confidentiality.

g) Personal Data Inquiries and Requests. Where required by Data Protection Laws, Figma agrees to provide reasonable assistance and comply with reasonable instructions from Customer related to any requests from individuals exercising their rights in Customer Personal Data granted to them under Data Protection Laws in cases where Customer cannot reasonably fulfill such requests independently by using the self-service functionality of the Figma Offering.

h) Data Protection Impact Assessment and Prior Consultation. Where required by Data Protection Laws, Figma agrees to provide reasonable assistance at Customer's expense to Customer where, in Customer's judgement, the type of Processing performed by Figma requires a data protection impact assessment and/or prior consultation with the relevant data protection authorities.

i) Demonstrable Compliance. Figma agrees to provide information reasonably necessary to demonstrate compliance with this Addendum upon Customer's reasonable request.

j) Sale of Customer Personal Data Prohibited. Figma shall not sell Customer Personal Data as the term "sell" is defined by the CCPA.

4. Information Security Program.

a) Security Measures. Figma shall implement and maintain commercially reasonable administrative, technical, and physical safeguards designed to protect Customer Personal Data in accordance with the Figma Security Standards attached hereto as **Exhibit A**.

5. Security Incidents.

a) Notice. Upon becoming aware of a Security Incident, Figma agrees to provide written notice without undue delay and within the time frame required under Data Protection Laws to Customer. A delay in giving such notice requested by law enforcement and/or in light of Figma's legitimate needs to investigate or remediate the matter before providing notice shall not constitute an undue delay. Where possible, such notice will include all available details required under Data Protection Laws for Customer to comply with its own notification obligations to regulatory authorities or individuals affected by the Security Incident. Figma's notification of or response to a Security Incident will not be construed as an acknowledgement by Figma of any fault or liability with respect to the Security Incident.

b) Remediation. Figma will take reasonable measures to mitigate the risks of further Security Incidents. Customer and Figma shall agree upon a remediation plan to address the Security Incident. Where the Security Incident is due to Figma's breach of this Addendum, Figma will reimburse Customer for its actual, out of pocket remediation costs and expenses incurred as a result of actions required to be taken under Data Protection Laws or agreed upon between the parties with respect to a Security Incident, including, where applicable, (i) the creation and transmission of legally required notices to affected individuals, (ii) call center support to respond to inquiries, and (iii) legally required credit monitoring services for affected individuals. Customer shall have sole discretion to control the timing, content and manner of any notices provided under this Remediation Section.

6. Cross-Border Transfers of Personal Data.

a) Cross-Border Transfers of Personal Data. Customer authorizes Figma and its Subprocessors to transfer Customer Personal Data across international borders, including from the European Economic Area, Switzerland, and/or the United Kingdom to the United States.

b) Data Transfer Impact Assessment Questionnaire. Figma agrees that it has provided true, complete, and accurate responses to the Data Transfer Impact Assessment Questionnaire attached hereto as **Exhibit B**.

c) Supplemental Measures. Figma agrees that it will comply with the obligations set forth in **Exhibit C** regarding supplemental measures for the transfer of Customer Personal Data originating in the European Economic Area, Switzerland,

and/or the United Kingdom to a country that has not been found to provide an adequate level of protection under applicable Data Protection Laws.

d) EEA and Swiss Standard Contractual Clauses. If Customer Personal Data originating in the European Economic Area and/or Switzerland is transferred by Customer to Figma in a country that has not been found to provide an adequate level of protection under applicable Data Protection Laws, the parties agree that the transfer shall be governed by the European Economic Area and Switzerland Standard Contractual Clauses ("**EEA and Swiss Standard Contractual Clauses**") attached hereto as **Exhibit D**. The parties agree that: (i) the certification of deletion required by Clause 8(a) and Clause 16(d) of the EEA and Swiss Standard Contractual Clauses will be provided upon Customer's written request; (ii) the measures Figma is required to take under Clause 8.6(c) of the EEA and Swiss Standard Contractual Clauses will only cover Figma's impacted systems; (iii) Figma may engage Subprocessors using European Commission Decision C(2010)593 Standard Contractual Clauses for Controllers to Processors or any other adequacy mechanism provided that such adequacy mechanism complies with applicable Data Protection Laws and such use of Subprocessors shall not be considered a breach of Clause 9 of the EEA and Swiss Standard Contractual Clauses; (iv) the termination right contemplated by Clause 14(f) and Clause 16(c) of the EEA and Swiss Standard Contractual Clauses will be limited to the termination of the EEA and Swiss Standard Contractual Clauses, in which case, the corresponding Processing of Customer Personal Data affected by such termination shall be discontinued unless otherwise agreed by the parties; (v) unless otherwise stated by Figma, Customer will be responsible for communicating with data subjects pursuant to Clause 15.1(a) of the EEA and Swiss Standard Contractual Clauses; (vi) the information required under Clause 15.1(c) will be provided upon Customer's written request; and (vii) notwithstanding anything to the contrary, Customer will reimburse Figma for all costs and expenses incurred by Figma in connection with the performance of Figma's obligations under Clause 15.1(b) and Clause 15.2 of the EEA and Swiss Standard Contractual Clauses without regard for any limitation of liability set forth in the Agreement. Each party's signature to this Addendum shall be considered a signature to the EEA and Swiss Standard Contractual Clauses to the extent that the EEA and Swiss Standard Contractual Clauses apply hereunder.

e) UK Standard Contractual Clauses. If Customer Personal Data originating in the United Kingdom is transferred by Customer to Figma in a country that has not been found to provide an adequate level of protection under applicable Data Protection Laws, the parties agree that the transfer shall be governed by the of the UK Standard Contractual Clauses attached hereto as **Exhibit E**. The parties agree that: (i) the audits described in Clause 5(f) and Clause 12(2) of the UK Standard Contractual Clauses shall be carried out in accordance with Section 7 of this Addendum; (ii) pursuant to Clause 5(h) and Clause 11 of the UK Standard Contractual Clauses, Figma may engage new Subprocessors in accordance with the Section 3(c) – 3(e) of the Addendum; (iii) the Subprocessor agreements referenced in Clause 5(j) and certification of deletion referenced in Clause 12(1) of the UK Standard Contractual Clauses will be provided upon Customer's written request; and (iv) any obligations Figma may have pursuant to Clause 5(j) will be satisfied by Figma providing Customer with a summary of the relevant Subprocessor agreement. Each party's signature to this Addendum shall be considered a signature to the UK Standard Contractual Clauses to the extent that the UK Standard Contractual Clauses apply hereunder.

f) Data Transfer Impact Assessment Outcome. Based on the information set forth in this Addendum, the parties agree that the transfer of Customer Personal Data originating in the European Economic Area, Switzerland, and/or the United Kingdom to a country that has not been found to provide an adequate level of protection under applicable Data Protection Laws is consistent with the obligations applicable to the parties in each of the respective sets of Standard Contractual Clauses attached to this Addendum.

7. Audits.

a) Customer Audit. Where Data Protection Laws afford Customer an audit right, Customer (or its appointed representative) may carry out an audit of Figma's facilities, policies, procedures, and records relevant to the Processing of Customer Personal Data. Any audit must be: (i) conducted during Figma's regular business hours; (ii) with 45 days' advance notice to Figma; (iii) carried out in a manner that prevents unnecessary disruption to Figma's operations; and (iv) subject to reasonable confidentiality procedures. In addition, any audit shall be limited to once per year, unless an audit is carried out at the direction of a government authority having proper jurisdiction. Customer shall be responsible for any costs arising from such audit.

8. Data Deletion.

a) Data Deletion. At the expiry or termination of the Agreement, Figma will, at Customer's option, delete or return all Customer Personal Data (excluding any back-up or archival copies which shall be deleted in accordance with Figma's data retention schedule), except where Figma is required to retain copies under applicable laws, in which case Figma will isolate and protect that Customer Personal Data from any further Processing except to the extent required by applicable laws.

9. Processing Details.

a) Subject Matter. The subject matter of the Processing is Figma's provision and maintenance of the Figma Offering for Customer.

b) Duration. The Processing will continue during the term of the Agreement, plus the period from expiration or termination until deletion of all Customer Personal Data by Figma in accordance with this Addendum.

c) Categories of Data Subjects. Customer's Authorized Users who access or use the Figma Offering through the Customer's account on behalf of Customer.

d) Nature and Purpose of the Processing. The purpose of the Processing of Customer Personal Data by Figma is the performance of the Figma Offering.

e) Types of Customer Personal Data. Name, email address, job title, IP address, photograph (if uploaded by user for profile), and phone number if 2FA is enabled.

CUSTOMER NAME:	**Figma, Inc.**
Signature: _____	Signature: DocuSigned by: Praveer Melwani E3153E7170EB4D5...
Printed Name: _____	Printed Name: Praveer Melwani
Position: _____	Position: VP, Business Operations & Finance
Contact Details: _____	Contact Details: privacy@figma.com
Date: _____	Date: 8/27/2021

Exhibit A to the Data Processing Addendum

Figma Security Standards

This Exhibit A forms part of the Addendum. All capitalized terms that are not expressly defined in this Exhibit A will have the meanings given to them in the Addendum or the Agreement.

1. **Information Security Program.** Figma will maintain a written information security program designed to (a) identify and help protect against reasonably foreseeable internal and external threats that could result in the unauthorized disclosure, misuse, alteration, or destruction of Customer Personal Data, and (b) minimize security risks, including through risk assessment and regular testing. The information security program will include the following measures:

a) **Administrative Safeguards:**

i) SOC 2 Type 2 certification during the Term;

ii) A written information security program that details administrative, technical, and physical safeguards;

iii) A dedicated, independent security team responsible for Figma's information security program;

iv) To the extent legally permissible and practicable in the applicable jurisdiction, pre-employment or pre-engagement screening on employees and contractors who have access to Customer Personal Data;

v) A requirement for all Figma employees and contractors to agree to a confidentiality agreement as a condition of employment or engagement and to follow policies on the protection of personal data, confidential information, and information security procedures;

vi) Mandatory training for Figma employees and contractors, at least annually, on privacy and information security awareness. These trainings are reviewed and updated annually; and

vii) A Code of Conduct and disciplinary process that is used when Figma employees or contractors violate Figma's security or privacy policies.

b) **Physical Safeguards:** Access ID cards, card readers, front desk officers, alarm systems, video surveillance, and exterior security for leased or owned offices and facilities.

c) **Technical Safeguards:**

i) Logical access to Figma systems and data that process Customer Personal Data are based on the principle of least privilege and designed to ensure that persons entitled to use such a data processing system have access only to the data to which they have a business need;

ii) Data handling control measures designed to ensure that the Customer Personal Data cannot be read, copied, modified, or removed without authorization during electronic transmission, transport, or storage on data media. In particular, Figma's information security program will be designed to encrypt Customer Personal Data in-transit and at rest as appropriate;

iii) Data entry control measures designed to ensure Figma can check and establish whether and by whom the Customer Personal Data have been input into data processing systems, modified, or removed;

iv) Subprocessor supervision measures designed to ensure that Customer Personal Data are processed strictly in accordance with the Agreement, including measures designed to ensure that:

(1) Customer Personal Data are protected from accidental destruction or loss, including data backup, retention and secure destruction policies; secure offsite storage of data sufficient for disaster recovery; uninterrupted power supply, and disaster recovery programs; and

(2) data collected for different purposes can be processed separately, including physical or adequate logical separation of Customer Personal Data.

d) **Continued Evaluation.** Figma will conduct periodic reviews of the security of the Figma Platform and the adequacy of its information security program as measured against industry security standards and its policies and procedures. Figma will regularly evaluate the security of the Figma Platform to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

Exhibit B to the Data Processing Addendum

Data Transfer Impact Assessment Questionnaire

This Exhibit B forms part of the Addendum. All capitalized terms that are not expressly defined in this Exhibit B will have the meanings given to them in the Addendum or the Agreement.

1. What countries will Customer Personal Data that is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom be stored in or accessed from? If this varies by region, please specify each country for each region.

    a. **Answer:** As set forth on https://www.figma.com/sub-processors/.

2. What are the categories of data subjects whose Customer Personal Data will be transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?

    a. **Answer:** Customer's Authorized Users.

3. What are the categories of Customer Personal Data transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?

    a. **Answer:** Customer Personal Data that is Processed in connection with the Agreement including name, email address, information related to an Authorized User's use of the Figma Offering.

4. Will any Customer 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 be transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom? If so, are there any 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?

    a. **Answer:** Not to Figma's knowledge.

5. What is the frequency of the transfer of Customer Personal Data outside of outside of the European Economic Area, Switzerland, and/or the United Kingdom? E.g., is Customer Personal Data transferred on a one-off or continuous basis?

    a. **Answer:** Customer Personal Data is transferred on a continuous basis by virtue of an Authorized User's use of the Figma Offering.

6. Broadly speaking, what are the services to be provided and the corresponding purposes for which Customer Personal Data is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?

    a. **Answer:** Figma provides a cloud based design platform.

7. What is the period for which the Customer Personal Data will be retained, or, if that is not possible, the criteria used to determine that period?

    a. **Answer:** Figma will retain Customer Personal Data in accordance with the Agreement.

8. What business sector is Figma involved in?

    a. **Answer:** digital design and project collaboration.

9. When Customer Personal Data is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom to Figma, how is it transmitted to Figma? Is the Customer Personal Data in plain text, pseudonymized, and/or encrypted?

    a. **Answer:** Figma encrypts Customer Personal Data as appropriate in transit and at rest.

10. Please list the Subprocessors that will have access to Customer Personal Data that is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom:

    a. **Answer:** As set forth on https://www.figma.com/sub-processors/.

11. Is Figma subject to any laws in a country outside of the European Economic Area, Switzerland, and/or the United Kingdom where Customer Personal Data is stored or accessed from that would interfere with Figma fulfilling its obligations under either of the attached set(s) of Standard Contractual Clauses? For example, FISA 702 or U.S. Executive Order 12333. If yes, please list these laws.

    a. **Answer:** As of the effective date of the Addendum, no court has found Figma to be eligible to receive process issued under the laws contemplated by Question 11, including FISA Section 702 and no such court action is pending.

12. Has Figma ever received a request from public authorities for information pursuant to the laws contemplated by Question 11 above (if any)? If yes, please explain.

    a. **Answer:** As of the effective date of the Addendum, Figma has not received any national security orders of the type described in Paragraphs 150-202 of the judgment in the CJEU Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, nor is Figma aware of any such orders in progress.

13. Has Figma ever received a request from public authorities for Personal Data of individuals located in European Economic Area, Switzerland, and/or the United Kingdom? If yes, please explain.

    a. **Answer:** No.

14. What safeguards will Figma apply during transmission and to the processing of Customer Personal Data in countries outside of the European Economic Area, Switzerland, and/or the United Kingdom that have not been found to provide an adequate level of protection under applicable Data Protection Laws?

    a. **Answer:** As set forth in Exhibit A and Exhibit C.

Exhibit C to the Data Processing Addendum

Supplemental Measures

This Exhibit C forms part of the Addendum and only applies to Figma's Processing of Customer Personal Data that is subject to Exhibit D or Exhibit E. All capitalized terms that are not expressly defined in this Exhibit C will have the meanings given to them in the Addendum or the Agreement.

PART 1:

Figma Principles Regarding Government and Other Third-Party Requests for Customer Personal Data

Figma is committed to providing users with control over their own data, to securing customer data against unauthorized access, and to protecting users' privacy. In accordance with this commitment Figma complies with the following principles in responding to third party requests, including requests by governmental entities, for Customer Personal Data:

1. Figma will retain and, as appropriate, consult with expert legal counsel regarding all third-party requests for customer data.

2. Figma seeks to refer each government request promptly to the relevant customer or user so that the customer or user can respond directly.

3. If the government declines to redirect its request to the relevant customer, Figma will provide the customer with prompt notice of the request unless it is legally prohibited from doing so.

4. If Figma is prohibited from providing prompt notice of a request to a customer, Figma provides such notice as soon as the prohibition expires or is no longer in effect.

5. Figma publishes and annually updates a Transparency Report that provides customers with information regarding the number and types of government requests for customer data it receives and how it responds to them.

6. Figma assesses the legality of all such requests and complies with requests only if and to the extent it assesses that they are valid, lawful and compulsory.

7. Figma will decline to comply with and undertake reasonable efforts to contest any request it determines is not absolutely required by applicable law, including any non-valid request under FISA 702 or U.S. Executive Order 12333.

PART 2:

Figma Transparency Report

Report Period: 1 July 2020 – 30 June 2021

Figma publishes this report on an annual basis to share information with its customers regarding the government information requests, if any, Figma has received for access to Customer Personal Data and how it has responded to them.

Government Information Requests:

- Figma received 0 government requests of the type described in Paragraphs 150-202 of the judgment in the CJEU Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, nor is Figma aware of any such orders in progress during the Report Period described above.

- During the Report Period no court has found Figma to be eligible to receive process issued under FISA Section 702 and no such court action is pending.

Customer Information Requests:

Not more than twice annually upon Customer's request and subject to reasonable confidentiality measures, Figma will, to the extent legally permitted and such information not already made available in its own transparency report, provide responses to Customer's transparency questionnaire indicating the types of binding legal demands for Customer Personal Data that Figma has received (if any).

Exhibit D to the Data Processing Addendum

This Exhibit D forms part of the Addendum.

EUROPEAN ECONOMIC AREA AND SWITZERLAND 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.

(e) To the extent applicable hereunder, these Clauses also apply mutatis mutandis to the Parties processing of personal data that is subject to the Swiss Federal Act on Data Protection. Where applicable, references to EU Member State law or EU supervisory authorities shall be modified to include the appropriate reference under Swiss law as it relates to transfers of personal data that are subject to the Swiss Federal Act on Data Protection.

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 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) 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 – Omitted

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 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, 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 (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.

(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 ten (10) 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. 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.

(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) Where the data exporter is established in an EU Member State, the following section applies: 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 application of 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 following section applies: 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 application of 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 following section applies: 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 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;

(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).

(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 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.

(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.).

(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.

(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 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 Netherlands.

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.

(b) The Parties agree that those shall be the courts of the Netherlands.

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

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

APPENDIX

ANNEX I

A. **LIST OF PARTIES**

MODULE TWO: Transfer controller to processor

Data exporter(s):

1. Name: Customer.

Address: As set forth in the Notices section of the Agreement.

Contact person's name, position and contact details: As set forth in the signature block of the Addendum

Activities relevant to the data transferred under these Clauses: As set forth in Exhibit B.

Role (controller/processor): Controller.

Data importer(s):

1. Name: Figma.

Address: As set forth in the Notices section of the Agreement.

Contact person's name, position and contact details: As set forth in the signature block of the Addendum.

Activities relevant to the data transferred under these Clauses: As set forth in Exhibit B.

Role (controller/processor): Processor.

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

As set forth in Exhibit B.

Categories of personal data transferred

As set forth in Exhibit B.

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.

As set forth in Exhibit B.

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

As set forth in Exhibit B.

Nature of the processing

As set forth in Exhibit B.

Purpose(s) of the data transfer and further processing

As set forth in Exhibit B.

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

As set forth in Exhibit B.

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

As set forth in Exhibit B.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

The supervisory authority mandated by Clause 13. If no supervisory authority is mandated by Clause 13, then the Irish Data Protection Commission (DPC), and if this is not possible, then as otherwise agreed by the parties consistent with the conditions set forth in Clause 13.

ANNEX II

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

MODULE TWO: Transfer controller to processor

Description of the technical and organisational measures implemented by the data importer(s) (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.

Data importer shall implement and maintain appropriate technical and organisational measures designed to protect personal data in accordance with the Addendum.

Pursuant to Clause 10(b), data importer will provide data exporter assistance with data subject requests in accordance with the Addendum.

Exhibit E to the Data Processing Addendum

This Exhibit E forms part of the Addendum.

UNITED KINGDOM – STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

Name of the data exporting organisation: Customer.

(the data **exporter**)

And

Name of the data importing organisation: Figma.

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'Commissioner'* shall have the same meaning as in the UK GDPR;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system covered by UK adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the UK;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing;

(g) *'UK GDPR'* means United Kingdom General Data Protection Regulation as supplemented by terms in the Data Protection Act 2018.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the Commissioner) and does not violate the applicable data protection law;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not covered by adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 Data Protection Act 2018;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the Commissioner;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the Commissioner;

   (b) to refer the dispute to the UK courts.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the Commissioner if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the Commissioner has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the country of the United Kingdom in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from (i) making changes permitted by Paragraph 7(3) & (4) of Schedule 21 Data Protection Act 2018; or (ii) adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the laws of the country of the UK where the exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the Commissioner.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the Commissioner, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed by the parties.

Data exporter
The data exporter is: Customer.

Data importer
The data importer is: Figma.

Data subjects
The personal data transferred concern the following categories of data subjects: As set forth in Exhibit B.

Categories of data
The personal data transferred concern the following categories of data: As set forth in Exhibit B.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data: As set forth in Exhibit B.

Processing operations
The personal data transferred will be subject to the following basic processing activities: As set forth in Exhibit B.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

Data importer shall implement and maintain appropriate technical and organisational measures designed to protect personal data in accordance with the Addendum.