SIGNING INSTRUCTIONS FOR THIS DATA PROCESSING ADDENDUM:

The Data Processing Addendum ("**DPA**") on the following pages incorporates (where applicable) the EC Standard Contractual Clauses and UK Standard Contractual Clauses.

To complete and execute this DPA, please do the following:

1. Complete the form at https://ironcladapp.com/public-launch/6410a5a4e6f49e072d76c6d9 with the requested information. The DPA will be generated with your company's details filled in, and sent to your designated contact via DocuSign.

2. Review the DPA sent by DocuSign and sign as instructed.

DOES THE ADDENDUM APPLY TO MY ORGANISATION?

If the Customer signing is also party to an Agreement (both as defined in the DPA), then this DPA will constitute an addendum to and form part of that Agreement when signed by the parties. If the entity signing this DPA does not meet this criterion, then this DPA will not be valid or legally binding.

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 Figma's provision of the Figma Platform to the Customer (the "**Agreement**"), including the limitations of liability set forth in the Agreement, which shall apply in aggregate for all claims under the Agreement and this Addendum (including for Authorized Affiliates) and shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such Addendum. Each reference to the Addendum herein means this Addendum including its exhibits. Any capitalized term not defined herein shall have the meaning given to it 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.

1. Subject Matter, Duration & Customer Parties.

(a) Subject Matter. This Addendum reflects the parties' commitment to abide by Data Protection Laws when Processing Customer Personal Data pursuant to the Agreement. In providing the Figma Platform to the Customer pursuant to the terms of the Agreement, Figma may Process Personal Data on behalf of Customer and the parties agree to comply with the terms of this Addendum with respect to any such Personal Data.

(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.

(c) Customer Parties. The Customer is entering this Addendum on behalf of itself and to the extent required under applicable Data Protection Laws, in the name of or on behalf of its Authorized Affiliates.

2. Definitions.

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

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the Customer entity signing this Agreement, or with Figma, as the case may be. "**Control**," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Authorized Affiliate"** means any of Customer's Affiliate(s) which: (i) (a) is subject to the Data Protection Laws; and (b) is permitted to use the Figma Platform pursuant to the Agreement between Customer and Figma but has not signed its own Order Form with Figma and is not a "Customer" as defined under the Agreement; and (ii) if and to the extent Figma processes Personal Data for which such Affiliate(s) qualify as the Controller.

"**Customer Personal Data**" means Personal Data pertaining to logged-in Customer's Authorized Users of the Figma Platform Processed by Figma on behalf of Customer (of an Authorized Affiliate) under the Agreement.

"**Data Protection Laws**" means all 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**"), the California Privacy Rights Act ("**CPRA**"), the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, the Virginia Consumer Data Protection Act, and the EU General Data Protection Regulation 2016/679 ("**GDPR**") that are applicable to the Processing of Personal Data under the Agreement.

"**Figma Platform**" means the Figma offering identified in an Order, including any updates, enhancements, or improvements thereto, related mobile and desktop applications, and related Documentation, but, for the avoidance of doubt, excludes www.figma.com/community and all Non-Figma Resources. The Figma Platform does not include logged-out use of Figma.com websites.

"**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.

"**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of personal data to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; (ii) where the Swiss DPA applies, a transfer of personal data from Switzerland to any other country which has not been determined to have a legislation that guarantees an adequate level of data protection (binding adequacy decisions will be issued by the Federal Council after the coming into force of the revised Swiss DPA), and (iii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018;

"**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.

"**Standard Contractual Clauses**" means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 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 ("**EU SCCs**"); (ii) where the Swiss DPA applies, the EU SCCs with the Swiss amendments as required by the Federal Data Protection and Information Commissioner (FDPIC), and (iii) where the UK GDPR applies, standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR as amended or replaced from time to time ("**UK SCCs**").

"**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. When Processing Customer Personal Data in the provision of the Figma Platform to the Customer, the Customer will act as a "Business," or "Controller" and Figma will 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 Platform 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 Agreement is Customer's complete and final instructions to Figma in relation to Processing of Customer Personal Data. Processing outside the scope of this Agreement (if any) will require prior written agreement between Customer and Figma regarding additional instructions for Processing. 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 Platform.

(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) California Privacy Rights Act Terms. To the extent the CPRA applies to Figma's Processing of Customer Personal Data, this Section applies. Figma shall: (i) comply with its obligations under the CPRA; (ii) provide the same level of protection as required under the CPRA; (iii) notify Customer if it can no longer meet its obligations under the CPRA; (iv) not "sell" or "share" (as such terms are defined by the CPRA) Customer Personal Data; (v) not retain, use, or disclose Customer Personal Data for any purpose other than to provide the Figma Platform under the Agreement and any applicable ordering document between the parties; (vi) not retain, use, or disclose Customer Personal Data outside of the direct business relationship between Customer and Figma; and (vii) not combine Customer Personal Data with Personal Data that Figma (a) receives from, or on behalf of, another person or (b) collects from its own, independent consumer interaction, except, in either case, except as permitted under the CPRA. Customer may: (1) take reasonable and appropriate steps to help ensure that Figma processes Customer Personal Data in a manner consistent with Figma's CPRA obligations; and (b) upon notice, take reasonable and appropriate steps to stop and remediate unauthorized Processing of Customer Personal Data by Figma.

4. Information Security Program.

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 B.

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.

(b) Data Transfer Impact Assessment. Figma agrees to provide true, complete and accurate (to the best of its knowledge) responses in the Data Transfer Impact Assessment provided upon request.

(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, UK and Swiss Standard Contractual Clauses. The Parties acknowledge that the transfers of Customer Personal Data from Customer to Figma are Restricted Transfers and agree that such transfers shall be subject to the appropriate Standard Contractual Clauses as follows:

(a) In relation to Customer Personal Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

(i) Module Two will apply;

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 9, Option 2 will apply, and the time period for prior notice of subprocessor changes shall be as set out in Clause 3(e) of this Addendum;

(iv) in Clause 11, the optional language will not apply;

(v) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the law of the Republic of Ireland;

(vi) in Clause 18(b), disputes shall be resolved before the courts of the Republic of Ireland;

(vii) Annex I of the EU SCCs shall be deemed completed with the information set out in Exhibit A to this Addendum;

(viii) Annex II of the EU SCCs shall be deemed completed with the information set out in Exhibit B to this Addendum;

(b) in relation to Customer Personal Data that is protected by the UK GDPR, the UK SCCs will apply as follows:

(i) the EU SCCs, completed as set out above in clause 6(d)(a)(i) –(viii) of this Addendum shall apply to transfers of Customer Personal Data, subject to the provisions below of this sub-clause 6(d)(b) below;

(ii) The "UK Addendum to the EU Standard Contractual Clauses" issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018 ("UK Addendum") shall be deemed executed between Customer and Figma and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of Customer Personal Data;

(iii) the tables in Part 1 of the UK Addendum shall be deemed completed with the information set out in Exhibit D to this Addendum; and

(iv) the EU SCCs shall be deemed amended as specified by Part 2 of the UK Addendum in respect of the transfer of Customer Personal Data.

(c) In relation to Customer Personal Data that is protected by the Swiss DPA, the EU SCCs, Module Two, shall apply with the amendments listed in the following sub-clauses (i)-(vii). Insofar as the transfer is subject to both the Swiss DPA and the EU GDPR or UK GDPR, the amendments in sub-clauses (i)-(vii) shall only apply with respect to the Swiss DPA and shall not affect the application of the Clauses of the EU SCCs or UK SCCs for the purposes of the GDPR or UK GDPR.

(i) References to "Regulation (EU) 2016/679" or "that Regulation" are to be interpreted as references to the Swiss DPA to the extent applicable;

(ii) References to "Regulation (EU) 2018/1725" are removed;

(iii) References to "Union", "EU", and "EU Member State" shall be interpreted to mean Switzerland;

(iv) Clause 13 (a) and Part C of Annex I are not used; the competent supervisory authority is the FDPIC insofar as the transfers are governed by the Swiss Data Processing Addendum;

(v) Clause 17 is replaced to state that "These Clauses are governed by the laws of Switzerland insofar as the transfers are governed by the Swiss DPA";

(vi) Clause 18 is replaced to state:

"Any dispute arising from these Clauses relating to the Swiss DPA shall be resolved by the courts of Switzerland. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland in which they have their habitual residence. The parties agree to submit themselves to the jurisdiction of such courts".

(vii) As long as the Swiss DPA of 19 June 1992 is in force, the EU SCC shall also protect personal data of legal entities and legal entities shall receive the same protection under the EU SCC as natural persons.

(d) SCCs Prevail. In the event that any provision of this Addendum contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

(e) Onwards transfers. Figma shall not participate in (nor permit any subprocessor to participate in) any other Restricted Transfers of Customer Personal Data (whether as an exporter or an importer of Customer Personal Data) unless the Restricted Transfer is made in full compliance with Applicable Data Protection Laws.

(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 under Standard Contractual Clauses incorporated into 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.

(b) Audit Process. 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. When deciding on a review or audit, the Customer will take into account that Figma

holds SOC 2 type 2, ISO 27001 and ISO 27018 Certifications and can provide Customer with the relevant reports upon request.

8. Data Deletion.

At the expiry or termination of the Agreement, Figma will, as directed by Customer and 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 Platform 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 Platform 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 Platform.

(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.

10. Authorized Affiliates. The parties agree that, by executing the Addendum the Customer enters into the Addendum on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliate(s), thereby establishing a separate Addendum between Figma and each such Authorized Affiliate, subject to the provisions of the Agreement. Each Authorized Affiliate agrees to be bound by the obligations under this Addendum and, to the extent applicable, the Agreement. An Authorized Affiliate is not and does not become a party to the Agreement and is only a party to the Addendum. All access to and use of the Figma Platform by Authorized Affiliate(s) must comply with the terms and conditions of the Agreement and any violation thereof by an Authorized Affiliate shall be deemed a violation by Customer.

11. Exercise of Rights. Where an Authorized Affiliate becomes a party to the Addendum, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this Addendum, except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this Addendum against Figma directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this Addendum in a combined manner for all of its Authorized Affiliates together, instead of doing so separately for each Authorized Affiliate.

This Addendum is effective from the date on which it is signed by both parties (the "**Effective Date**").

Customer Name:	**Figma, Inc.**
Signature:	Signature:
Printed Name:	Printed Name:
Position:	Position:
Contact Details:	Contact Details: 760 Market Street, Floor 10, San Francisco, CA 94102, United States
Date:	Date:

Exhibit A

Data Processing Description

This Exhibit A forms part of the Agreement and describes the Processing that the processor will perform on behalf of the Controller.

A. LIST OF PARTIES

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

1.	Name:	See exporter name as set out in the Agreement.
	Address:	See address of the exporter as set out in the Agreement.
	Contact person's name, position and contact details:	As set out in the Agreement
	Activities relevant to the data transferred under these Clauses:	Processing of Customer Personal Data for the purpose of the Agreement.
	Signature and date:	See signatories to and date of the Addendum.
	Role (controller/processor):	Controller

Processor(s) / Data importer(s): *[Identity and contact details of the processor(s) /data importer(s), including any contact person with responsibility for data protection*]

1.	Name:	Figma, Inc.
	Address:	As set out in the Agreement
	Contact person's name, position and contact details:	As set out in the Agreement
	Activities relevant to the data transferred under these Clauses:	Processing of Customer Personal Data for the purpose of the Agreement.
	Signature and date:	See signatories to and date of the Addendum.
	Role (controller/processor):	Processor

B. DESCRIPTION OF TRANSFER

Customer Personal Data

Categories of data subjects whose personal data is transferred:	Customer's Authorized Users who access or use the Figma Platform through the Customer's account on behalf of the Customer.
Categories of personal data transferred:	Name, email address, job title, IP address, photograph (if uploaded by user for profile), and phone number if 2FA is enabled.
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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	Not to Figma's knowledge.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous by virtue of an Authorized User's use of the Figma Platform.
Nature of the processing:	The nature of the Processing of Customer Personal Data by Figma is the performance of the Figma Platform.
Purpose(s) of the data transfer and further processing:	The purpose of the Processing of Customer Personal Data by Figma is the performance of the Figma Platform pursuant to the Agreement.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	Figma will retain Customer Personal Data in accordance with the Agreement. Upon termination or expiry of the Agreement, Figma shall return or delete the Customer Personal Data in accordance with Clause 8 of the Addendum.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	Details of Subprocessors, including the subject matter, nature, and duration of processing, are available at: https://www.figma.com/sub-processors/

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 SCCs)	For Restricted Transfers from the EU: the Supervisory Authority of the Republic of Ireland. For Restricted Transfers from the UK: the Supervisory Authority of the UK For Restricted Transfers from Switzerland: the Supervisory Authority of Switzerland

Exhibit B

Technical and Organizational & Security Measures

Figma Security Standards

1. **Definitions.** For purposes of this Exhibit, the following terms apply. Any terms used in this Exhibit, but not defined herein below, will have the meaning given to them in the Addendum or the Agreement (as applicable):

   1.1. "**Agreement**" means the agreement between Figma and Customer governing Customer's use of the Figma Platform.

   1.2. "**Customer Data**" means Customer Materials and Customer Personal Data.

   1.3. "**Customer Materials**" means any application(s) and/or material(s) that are developed by Customer on the Figma Platform or uploaded to the Figma Platform by Customer.

   1.4. "**Systems**" means the applications, databases, infrastructure, and platforms under Figma's control that are utilized to Process Customer Data.

2. **Policies and Codes of Conduct**

   2.1. Figma maintains an Information Security Policy and reviews it at least annually, including after any major changes occur in applicable law or regulatory guidance or are otherwise made to the Systems.

   2.2. Figma maintains codes of conduct and other policies covering anti-bribery and corruption, whistleblowing and other ethics policies (such as anti-money laundering and anti-slavery) and communicates these policies to all relevant staff. Figma's codes of conduct are available upon request.

   2.3. Figma implements processes designed to ensure the ongoing compliance with these policies and to identify and enable Figma to take action against any areas of non-compliance. Failure to comply with policies are addressed through appropriate disciplinary actions.

3. **Information Security Program**

   3.1. Figma assigns responsibility for information security management to senior personnel.

   3.2. Figma implements technical and organizational measures designed to protect against unauthorized or unlawful processing of Customer Data and against accidental loss or destruction of, or damage to, Customer Data, including a written information security program, which includes policies, procedures, and technical and physical controls designed to ensure the security, availability, integrity and confidentiality of Customer Data.

4. **Background Checks and Confidentiality**

   4.1. Figma conducts pre-employment background screening on employees and contractors who will access Customer Data in the ordinary course of performing their job responsibilities, to the extent legally permissible and practicable in the applicable jurisdiction.

   4.2. Figma requires all Figma employees and Subprocessors to execute a confidentiality agreement as a condition of employment or engagement and to follow policies on the protection of Customer Data.

5. **Access Control**

5.1. Figma assigns unique User IDs to authorized individual users to access Systems. All access to Systems must be authorized and authenticated.

5.2. Figma access rights to Customer Data are based on the principle of least privilege and designed to ensure that persons entitled to use a System have access only to the Customer Data for which they have a business need.

5.3. Figma maintains an accurate and up to date list of all personnel who have access to Systems and has a process to promptly disable within one business day of transfer or termination access by any individual personnel.

5.4. Figma periodically reviews and revokes Systems access rights, as needed, and logs and monitors such access.

5.5. Non-privileged users are prohibited from executing privileged functions, including, but not limited to, disabling, circumventing, or altering implemented security safeguards/countermeasures.

5.6. Figma maintains a password management policy designed to ensure strong passwords consistent with industry standard practices and requires the use of multi-factor authentication to access Systems. Passwords are promptly changed if Figma becomes aware that an account has been compromised.

5.7. Figma implements controls designed to ensure that Systems access is subject to appropriate authentication and user access controls:

- User IDs are unique and authorized;
- User accounts are granted the minimum required privileges to enable a user to perform their designated function;
- Access to audit trails is restricted and logged;
- Default accounts are deleted or disabled where possible and suitably authorized and controlled where this is not possible;
- Privileged accounts (e.g., administrator, root) are only used when technically required under change control procedures and not for day-to-day system operation;
- Where privileged account access is used, this access is logged and reviewed and access can be attributed to a named individual.

6. **Logging, Audit, and Accountability**

6.1. Figma creates, protects, and retains Systems audit records to maintain integrity and enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate Systems activity.

6.2. Figma reviews and analyzes Systems audit records on a regular basis to detect significant unauthorized activity with respect to Systems. Actions of users can be uniquely traced to those users so they can be held accountable for their actions.

7. **System Change Control**

7.1. Figma establishes a configuration baseline for Systems using applicable information security standards, manufacturer recommendations, or industry standard practices. Monitoring is performed to validate that Systems are configured according to the established configuration baseline.

7.2. The introduction of new systems are controlled, documented, and enforced by the use of formal change control procedures including documentation, specifications, testing, quality control, recovery, and managed implementation.

7.3. Figma employs controls designed to secure source code, including version control, segregation of source code repositories, and least privilege access principles.

7.4. Figma follows a structured secure development methodology, adheres to secure coding standards, and undergoes security assessment activities (e.g., dynamic and static scans) to identify and remediate security vulnerabilities before being released to production.

7.5. Figma employs reasonable controls designed to remove or disable unnecessary ports and services from Systems in accordance with the vendors' recommendations and settings.

8. **Vulnerability Management**

8.1. Figma maintains up-to-date anti-malware software, has implemented a vulnerability management program with regular scanning for vulnerabilities, subscribes to a vulnerability notification service, has a method for prioritizing vulnerability remediation based on risk, and has established remediation timeframes based on risk rating.

8.2. Once a patch is released, and the associated security vulnerability has been reviewed and assessed for its applicability and importance, the patch is applied and verified in a timeframe which is commensurate with the risk posed to Systems.

8.3. Penetration testing and vulnerability scanning is conducted on the Systems at least annually. Any remediation items identified as a result of the assessment are resolved as soon as possible on a timetable commensurate with the risk. Upon request, Figma will provide summary details of the tests performed, findings, and whether the identified issues have been resolved.

8.4. Figma uses commercially reasonable efforts to regularly identify software vulnerabilities and, in the case of known software vulnerabilities, to provide relevant updates, upgrades, and bug fixes.

8.5. Figma deploys intrusion detection processes to monitor and respond to alerts which could indicate potential compromise of Customer Data.

8.6. Figma deploys a log management solution and retains logs produced by intrusion detection systems for a minimum period of one year.

9. **Capacity Planning**

9.1. Figma maintains a capacity management program that continuously and iteratively monitors, analyses, and evaluates the performance and capacity of the Systems.

10. **Physical and Environmental Security**

10.1. Figma implements physical access control measures at Figma facilities and data centers designed to prevent unauthorized access to Systems (e.g., access ID cards, card readers, front desk officers, alarm systems, video surveillance, and exterior security).

11. **Security Incidents**

11.1. Figma maintains an information security incident management program that addresses management of Security Incidents.

11.2. Figma maintains an incident response plan that specifies actions to be taken when it suspects or detects a Security Incident.

11.3. 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. 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.

11.4. Figma will take reasonable measures to mitigate the risks of further Security Incidents.

12. **Subprocessors**

12.1. Figma will conduct a risk-based review of all Subprocessors designed to ensure that they are taking appropriate technical and organizational measures.

12.2. Figma will enter into agreements with its Subprocessors that require such Subprocessors to secure and protect Customer Data by using at least the same degree of care outlined in this Standard.

13. **Data Encryption**

13.1. Figma encrypts Customer Data in Figma's possession or control so that it cannot be read, copied, changed, or deleted by unauthorized personnel while in transit and storage, including when saved on removable media.

13.2. Keys are protected from unauthorized use, disclosure, alteration, and destruction, and have a backup and recovery process.

13.3. If a private key is compromised, all associated certificates will be revoked.

14. **Data Retention.**

At the expiry or termination of the Agreement, Figma will, at Customer's option, delete or return all Customer 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 Data from any further Processing except to the extent required by applicable laws.

15. **Secure Disposal**

15.1. Figma implements controls designed to ensure the secure disposal of Customer Data in accordance with applicable law taking into account available technology so that Customer Data cannot be read or reconstructed.

15.2. Media will be securely erased electronically before disposal by overwriting or degaussing, or physically destroyed prior to disposal or reassignment to another system. Media cleansing/wipe products and processes prior to disposal comply with NIST SP 800-88 standard, "Guidelines for Media Sanitization" (or its successor) or equivalent industry standards.

16. **Risk Assessments**

16.1. Figma maintains a risk assessment program that includes regular risk assessments and controls for risk identification, analysis, monitoring, reporting, and corrective action.

16.2. At least annually, Figma will perform risk assessments (either internally or with contracted, independent resources) to identify risks to Customer Data, risks to Figma's business assets (e.g., technical infrastructure), threats against those elements (both internal and external), the likelihood of those threats occurring, and the impact upon the organization.

17. **Asset Management**

17.1. Figma will have an asset management program that classifies and controls hardware and software assets throughout their life cycle.

18. **Business Continuity and Disaster Recovery**

18.1. Figma will use industry standard practices for redundancy, robustness, and scalability designed to maintain the availability of the Figma Platform.

18.2. Figma implements and maintains contingency plans to address emergencies or other occurrences (for example, fire, vandalism, system failure, and natural disaster) that could damage or destroy Systems or Customer Data, including a data backup plan and a disaster recovery plan with at least annual testing of such plans. Figma may not modify such plans to provide materially less protection to the Customer without the Customer's prior written consent, which may not be unreasonably conditioned or withheld.

18.3. Backups are taken and recovery is tested on a regular basis.

19. **Security and Privacy Training**

19.1. Figma conducts mandatory training for Figma employees and relevant Subprocessors, at least annually, on ethics, privacy, and information security awareness. These trainings are reviewed for relevance and updated as needed, annually.

19.2. Teams associated with development efforts impacting Customer Data, undergo specific training focused on well-defined and secured coding practices.

20. **Security Control Testing**

At least annually, Figma will engage a qualified, independent external auditor to conduct periodic reviews of Figma's security practices against recognized audit standards, such as SOC 2 Type II and ISO 27001 certification audits (including surveillance and recertifications), as applicable. Upon request, Figma agrees to make such reports available to the Customer.

21. **Verification Rights.**

No more than once per calendar year, Figma will use commercially reasonable efforts to respond to appropriately scoped questionnaires from Customer that are designed to verify Figma's security practices. Questionnaire responses are provided for informational purposes only, and Figma may charge a reasonable fee for its costs in responding to such questionnaires.

22. **Data Protection Governance**

Figma assigns accountability for data protection to a designated individual or other body with appropriate seniority.

Exhibit C

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 this Addendum. 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 2022 – 30 June 2022

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

UK Addendum – Part 1: Tables

Table 1: Parties

Start date	The Effective Date			
The Parties	**Exporter (who sends the Restricted Transfer)**		**Importer (who receives the Restricted Transfer)**	
Parties' details	**Full legal name:**	The name of Customer as set out in the Agreement.	**Full legal name:**	Figma, Inc.
	Trading name (if different):		**Trading name (if different):**	
	Main address (if a company registered address):	The address of Customer set out in the Agreement.	**Main address (if a company registered address):**	As set forth in the Agreement
	Official registration number (if any) (company number or similar identifier):		**Official registration number (if any) (company number or similar identifier):**	5227257
Key Contact	As set forth in the Agreement		As set forth in the Agreement	
Signature	See execution block of this Addendum.		See execution block of this Addendum.	

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:					
Module	**Module in operation**	**Clause 7 (Docking clause)**	**Clause 11 (Option)**	**Clause 9a (Prior Authorization or General Authorization)**	**Clause 9(a) (Time period)**	**Is personal data received from the Importer combined with personal data collected by the Exporter?**
As set out in Clause 6(d)(a)(i)-(viii) of this Addendum.						NO

Table 3: Appendix Information

The Appendix Information shall be deemed completed as set out in Clause 6(d)(a)(i)-(viii) of this Addendum.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: The Importer