

Data Processing Agreement

This Data Processing Agreement (“**DPA**”) forms part of and supplements the existing customer agreement (“**Agreement**”) between Palatial Platforms Inc. (“**Palatial**”), and the counterparty to the Agreement (“**Customer**”). If any conflict arises between this DPA and the Agreement with respect to the Processing of Personal Data, the terms of this DPA prevail; in all other respects, the Agreement controls. Capitalized terms used in this DPA that are not otherwise defined will have the meanings given to them under the Agreement or, if not defined in the Agreement, under applicable Data Protection Laws.

This DPA does not require signature. By entering into the Agreement, Customer accepts this DPA and is deemed to have executed it, together with the SCCs and the UK Addendum to the extent they apply, and the Annexes to this DPA are deemed to populate the corresponding annexes and tables of those instruments.

Customer and Palatial agree as follows:

1. Definitions

For purposes of this DPA:

- 1.1 “**Affiliate**” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “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.
- 1.2 “**Data Protection Laws**” means all applicable laws, regulations, and other legal or self-regulatory requirements in any jurisdiction relating to privacy, data protection, data security, breach notification, or the Processing of Personal Data, including without limitation, to the extent applicable, the following: the General Data Protection Regulation, Regulation (EU) 2016/679 (“**GDPR**”) (including, for purposes of this DPA, the United Kingdom Data Protection Act of 2018 and as amended by the Data Protection, Privacy and Electronic Communications Act (Amendments etc.) (EU Exit) Regulations 2019); the Swiss Federal Act on Data Protection (“**FADP**”); and the following (collectively, the “**U.S. Privacy Laws**”): the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.* (“**CCPA**”), including its regulations and the amendments made by the California Privacy Rights Act of 2020 (“**CPRA**”), the Virginia Consumer Data Protection Act, the Colorado Privacy Act and related regulations (“**CPA**”), the Utah Consumer Privacy Act, and the Connecticut Act Concerning Personal Data Privacy and Online Monitoring. If a Party’s activities involving Personal Data are not within the scope of a given Data Protection Law, that law is not applicable for purposes of this DPA.
- 1.3 “**Personal Data**” includes “personal data,” “personal information,” “personally identifiable information,” and analogous terms, as defined by Data Protection Laws, that Palatial Processes in relation to the Agreement.
- 1.4 “**Process**” and its cognates “**Processing**,” “**Processed**,” etc. mean any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring,

storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

- 1.5 “**SCCs**” means Module 2 (Transfer: Controller to Processor) of the standard contractual clauses set out in the European Commission Implementing Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries according to GDPR.
- 1.6 “**Security Breach**” means any confirmed unlawful acquisition, destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.
- 1.7 “**Services**” means the services that Palatial performs on behalf of Customer pursuant to the Agreement.
- 1.8 “**Sub-processor**” means any third party or Palatial Affiliate that Palatial engages to Process Personal Data.
- 1.9 “**UK Addendum**” means the United Kingdom International Data Transfer Addendum to the SCCs issued by the United Kingdom’s Information Commissioner’s Office.
- 1.10 The terms “**Business**,” “**Consumer**,” “**Controller**,” “**Data Subject**,” “**Processor**,” and “**Service Provider**” are defined as in Data Protection Laws. “Controller” is deemed to also refer to “Business,” and “Processor” is deemed to also refer to “Service Provider.” “Data Subject” is deemed to include “Consumer.”

2. Roles of the Parties; Scope and Purposes of Processing

- 2.1 Unless otherwise specified, this DPA applies to all Personal Data that Palatial Processes in relation to the Agreement.
- 2.2 Palatial Processes Personal Data on Customer’s behalf in the course of providing the Services. With respect to that Processing, Customer is the Controller and Palatial is its Processor; to the extent Customer is itself a Processor of that Personal Data, Palatial is its Sub-processor. Except where this DPA provides otherwise, references in this DPA to Personal Data mean Personal Data that Palatial Processes in that capacity.
- 2.3 “**Account Personal Data**” means Personal Data that Palatial Processes to establish and administer the customer relationship itself, including the names and business contact details of Customer’s administrators, users, and billing contacts, authentication credentials and API keys, and records of platform activity to the extent they identify an individual. Palatial is an independent Controller of Account Personal Data and Processes it to provision and secure the Services, to meter and invoice usage, to provide support, and to comply with its own legal obligations, in each case in accordance with its privacy policy. Customer does not instruct Palatial with respect to Account Personal Data, and Palatial’s obligations as a Processor under this DPA do not apply to it.
- 2.4 The Services are not designed to Process Personal Data, and Customer will not submit Personal Data to the Services except where it is incidental to material whose purpose is technical, such as an individual appearing in a reference image or authorship information embedded in an engineering file. Customer will not submit special

PALATIAL

categories of personal data within the meaning of Article 9 of the GDPR, personal data relating to criminal convictions or offences, government identifiers, payment card or financial account numbers, or protected health information, and Palatial has no obligation to Process any such data. This restriction limits what Customer may submit. It does not limit Palatial's obligations under this DPA, which apply to all Personal Data that Palatial in fact Processes on Customer's behalf.

2.5 Palatial will Process Personal Data solely: (1) to fulfill its obligations to Customer under the Agreement, including this DPA; (2) on Customer's behalf; and (3) in compliance with Data Protection Laws. Palatial will:

- 2.5.1 not retain, use, or disclose Personal Data outside of the direct business relationship between Customer and Palatial;
- 2.5.2 not "sell" any Personal Data, as such term is defined in U.S. Privacy Laws (regardless of whether any such laws apply);
- 2.5.3 not "share" any Personal Data, as such term is defined in the CCPA (regardless of whether the CCPA applies);
- 2.5.4 comply with any applicable restrictions under Data Protection Laws on combining Personal Data with personal data that Palatial receives from, or on behalf of, another person or persons, or that Palatial collects from any interaction between it and any individual;
- 2.5.5 not attempt to re-identify any pseudonymized or otherwise de-identified Personal Data received from Customer without Customer's express written permission;
- 2.5.6 not otherwise engage in any Processing of Personal Data that is prohibited or not permitted by Processors or Service Providers under Data Protection Laws; and
- 2.5.7 use commercially reasonable efforts to provide the level of protection for the Personal Data subject to the CPRA as is required under the CPRA.

3. No Model Training

- 3.1 Palatial will not use Personal Data to train, fine-tune, or otherwise develop machine learning models, and will not disclose Personal Data to any third-party model or inference provider for that purpose.
- 3.2 Palatial's use of data that is not Personal Data, including for model training, asset generation, and platform improvement, is governed by the Agreement. This DPA neither expands nor limits those rights.

4. Personal Data Processing Requirements

Palatial will:

- 4.1 Ensure that the persons it authorizes to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

PALATIAL

- 4.2 Assist Customer in the fulfillment of Customer's obligations to respond to verifiable requests by Data Subjects (or their lawful representatives) for exercising their rights under Data Protection Laws (such as rights to access or delete Personal Data).
- 4.3 Promptly notify Customer of any Data Subject requests to exercise their rights under Data Protection Laws with regard to the Personal Data or any government request for access to or information about Customer's Processing of Personal Data on Customer's behalf (collectively, "**Personal Data Request**"), unless prohibited by applicable law from making such notification. Unless otherwise required by applicable law, if Palatial receives a Personal Data Request, Palatial will await written instructions from Customer on how, if at all, to assist in responding. Palatial will provide Customer with reasonable cooperation and assistance in relation to any Personal Data Request.
- 4.4 Solely to the extent that such Processing activities are within Palatial's control and directly relate to the Services, Palatial will provide reasonable assistance to and cooperation with Customer for Customer's (i) performance of a data protection impact assessment of Processing or proposed Processing of Personal Data, when required by Data Protection Laws; and/or (ii) consultation with regulatory authorities in relation to the Processing or proposed Processing of Personal Data, including complying with any applicable obligation upon Palatial to consult with a regulatory authority in relation to Palatial's Processing or proposed Processing of Personal Data.

5. Data Security

- 5.1 Palatial will implement appropriate administrative, technical, physical, and organizational measures to protect Personal Data, as set forth in Annex II. In the event of any conflict between the body of this DPA and the Annexes, the body of this DPA will prevail.

6. Security Breach

- 6.1 Palatial will notify Customer of any Security Breach promptly, and in any event within 72 hours after becoming aware of such Security Breach. Palatial will comply with the Security Breach-related obligations directly applicable to it under Data Protection Laws. Palatial will also assist Customer in Customer's compliance with its Security Breach-related obligations, including by:
 - 6.1.1 At Palatial's own expense, taking steps to mitigate the effects of the Security Breach and reduce the risk to Data Subjects whose Personal Data was involved; and
 - 6.1.2 Providing Customer with the following information, to the extent known:
 - (a) The nature of the Security Breach, including, where possible, how the Security Breach occurred, the categories and approximate number of Data Subjects concerned, and the categories and approximate number of Personal Data records concerned;
 - (b) The likely consequences of the Security Breach; and

- (c) Measures taken or proposed to be taken by Palatial to address the Security Breach, including, where appropriate, measures to mitigate its possible adverse effects.

7. Sub-Processors

- 7.1 Customer acknowledges and agrees that Palatial may use Sub-processors to Process Personal Data in accordance with the provisions within this DPA and Data Protection Laws. Where Palatial sub-contracts any of its rights or obligations concerning Personal Data to a Sub-processor, Palatial will: (i) take steps to select and retain Sub-processors that are capable of maintaining appropriate privacy and security measures to protect Personal Data consistent with Data Protection Laws; and (ii) enter into a written agreement with each Sub-processor requiring it to comply with obligations that are, in all material respects, no less protective of Personal Data than those imposed on Palatial under this DPA.
- 7.2 Palatial will maintain an up-to-date list of its Sub-processors. The initial list is provided in Annex III of this DPA, and Customer consents to Palatial's use of the Sub-processors on this list. To the extent required by applicable Data Protection Laws, Palatial will provide Customer notice of any new Sub-processor in a reasonable manner, which may include notice via Palatial's website. Palatial will allow Customer 30 days from the day Palatial gives such notice to object to the appointment. If Customer has legitimate objections to the appointment of a new Sub-processor, Palatial will work with Customer in good faith to resolve the grounds for the objection.
- 7.3 Palatial uses third-party model and inference providers to generate assets from the materials Customer submits to the Services. Those providers do not receive Personal Data and are not Sub-processors for purposes of this DPA. If Palatial engages a model or inference provider in a manner that would involve the Processing of Personal Data, Palatial will add that provider to Annex III and the notice and objection process in this section will apply to it.

8. Data Transfers

- 8.1 Palatial Processes and stores Personal Data in the United States. Where Palatial is certified under the EU-U.S. Data Privacy Framework, including the UK Extension and the Swiss-U.S. Data Privacy Framework (together, the "**DPF**"), transfers of Personal Data from the European Economic Area, the United Kingdom, and Switzerland are made in reliance on that certification, and Palatial will Process that Personal Data in accordance with the DPF Principles. If Palatial is not certified under the DPF, or if the DPF ceases to provide a valid transfer mechanism for a territory, the SCCs and the UK Addendum apply as set out in this section.
- 8.2 In the event that Palatial Processes Personal Data transferred from the European Union, the European Economic Area and/or its member states, and/or Switzerland (collectively, "**EEA**") and/or the United Kingdom to countries that do not ensure an adequate level of data protection within the meaning of the Data Protection Laws and Regulations of the foregoing territories, the SCCs provisions set forth in this Data Transfers section will apply.

PALATIAL

- 8.3 The SCCs apply to a transfer of Personal Data under this DPA from the EEA between Customer and Palatial. Customer agrees the SCCs are completed and supplemented as follows:
- 8.3.1 Customer is the data exporter and Palatial is the data importer;
 - 8.3.2 The optional docking clause under Clause 7 of the SCCs will not apply;
 - 8.3.3 option 2 under Clause 9 of the SCCs applies and Customer generally authorizes Palatial to engage Sub-processors according to the Sub-processors section of this DPA;
 - 8.3.4 the optional redress language under Clause 11(a) of the SCCs will not apply;
 - 8.3.5 the governing law under Clause 17 of the SCCs will be the law of Ireland;
 - 8.3.6 the choice of forum and jurisdiction under Clause 18 of the SCCs will be the courts of Ireland;
 - 8.3.7 Annexes I, II and III of the SCCs are deemed to be populated with the information set out in Annexes I, II and III of this DPA; and
 - 8.3.8 Annex IV of this DPA supplements the SCCs with additional clauses as described in it.
- 8.4 The UK Addendum applies to a transfer of Personal Data under this DPA from the United Kingdom between Customer and Palatial, Customer agrees the UK Addendum is completed and supplemented as follows:
- 8.4.1 Customer is the data exporter and Palatial is the data importer;
 - 8.4.2 Table 1 of the UK Addendum is deemed to be populated with the information set out in Annex I of this DPA;
 - 8.4.3 for the purposes of Table 2 of the UK Addendum, the version of the Approved EU SCCs (including the appendix information, modules and selected clauses) appended to the UK Addendum is the SCCs;
 - 8.4.4 the optional docking clause under Clause 7 of the SCCs will not apply;
 - 8.4.5 option 2 under Clause 9 of the SCCs applies and Customer generally authorizes Palatial to engage Sub-processors according to the Sub-processors section of this DPA;
 - 8.4.6 the optional redress language under Clause 11(a) of the SCCs will not apply;
 - 8.4.7 Annex IV of this DPA supplements the SCCs with additional clauses as described in it;
 - 8.4.8 Table 3 of the UK Addendum is deemed to be populated with the information set out in Annexes I, II and III of this DPA;
 - 8.4.9 The “importer” and “exporter” option applies for the purposes of Table 4 of the UK Addendum;

PALATIAL

8.4.10 under Part 2, the mandatory clauses of the UK Addendum will apply; and

8.4.11 by using the Services to transfer Personal Data to Palatial, Customer will be deemed to have signed the UK Addendum.

8.5 The terms applicable to the transfer of Personal Data under this DPA from any other country or region are listed in Annex IV of this DPA and are incorporated into this DPA.

9. Audits

9.1 Palatial will provide Customer with the information reasonably necessary to demonstrate Palatial's compliance with this DPA, through the process described in this section. Customer may conduct an audit to confirm Palatial's compliance with this DPA by submitting a data protection questionnaire of reasonable length not more than once annually. Palatial will promptly complete and return such questionnaire to Customer. To the extent Customer is able to demonstrate that Palatial's questionnaire responses do not provide sufficient information to demonstrate compliance with this DPA, Customer may conduct follow-up interviews with Palatial's personnel at times mutually agreed by the parties, subject to the confidentiality obligations in the Agreement, and at Customer's reasonable expense.

10. Return or Destruction of Personal Data

10.1 Except to the extent required otherwise by Data Protection Laws, Palatial will, at the choice of Customer, return to Customer and/or securely destroy all Personal Data upon (a) written request of Customer or (b) termination of the Agreement. Except to the extent prohibited by Data Protection Laws, Palatial will inform Customer if it is not able to return or delete Personal Data.

11. Survival

11.1 The provisions of this DPA survive the termination or expiration of the Agreement for so long as Palatial or its Sub-processors Process Personal Data.

ANNEX I

Approved Data Transfer Mechanism: Description of Processing and Transfer

A. LIST OF PARTIES

MODULE TWO: Transfer Controller to Processor

Data exporter(s):

- *Name:* Customer, as identified in the Agreement.
- *Address:* As provided in the Agreement.
- *Contact person's name, position, and contact details:* As provided in the Agreement.
- *Activities relevant to the data transferred under these Clauses:* The data exporter receives the data importer's Services pursuant to their underlying Agreement.
- *Signature and date:* The Parties agree that execution of the Agreement shall constitute execution of these SCCs by both parties.
- *Role:* Controller and/or Processor

Data importer(s):

- *Name:* Palatial, as identified in the Agreement.
- *Address:* As provided in the Agreement.
- *Contact person's name, position, and contact details:* As provided in the Agreement.
- *Activities relevant to the data transferred under these Clauses:* The data importer provides Services to the data exporter pursuant to their underlying Agreement.
- *Signature and date:* The Parties agree that execution of the Agreement shall constitute execution of these SCCs by both parties.
- *Role:* Processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer Controller to Processor

- *Categories of data subjects whose personal data is transferred:* Individuals whose Personal Data is incidentally contained in the materials Customer submits to the Services, such as individuals appearing in a reference image or identified in authorship or device information embedded in an engineering file.
- *Categories of personal data transferred:* Personal Data incidentally contained in the materials Customer submits to the Services, which may include images or likenesses of individuals and names, contact details, or authorship information embedded as file metadata. The Services are not designed to Process Personal Data, and Customer is instructed not to submit it.

PALATIAL

- *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:* None. Customer is prohibited from submitting special categories of personal data to the Services under the Roles of the Parties section of this DPA.
- *The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):* Continuous for the duration of the Agreement, to the extent the materials Customer submits contain Personal Data.
- *Nature of the processing:* Data importer's Processing activities shall be limited to those discussed in the Agreement and the DPA.
- *Purpose(s) of the data transfer and further processing:* The purpose of the transfer to and further Processing of Personal Data by Palatial is for Palatial to provide the Services to Customer.
- *The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:* Personal Data will be retained for the period of time necessary for Palatial to provide the Services to Customer under the Agreement and/or in accordance with applicable legal requirements.
- *For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:* Same as above to the extent that Personal Data is provided to Sub-processors for purposes of providing the Services.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer Controller to Processor

To the extent legally permitted, the competent supervisory authority is the supervisory authority of the EEA Member State in which Customer is established or, where Customer is not established in the EEA, the supervisory authority of the Member State in which Customer's representative under Article 27 of the GDPR is established.

ANNEX II

Technical and Organisational Measures to Ensure the Security of the Data

MODULE TWO: Transfer Controller to Processor

1. Scope

- 1.1 Permitted Purpose. Palatial may collect, use, store and retain only the Personal Data that is authorized under the Agreement, and then may only collect, use, store and retain that Personal Data solely as necessary for Palatial to perform the Services in accordance with the Agreement (“**Permitted Purpose**”).
- 1.2 Security Program. This Annex II sets out Palatial’s information security program (the “**Security Program**”), which Palatial will maintain and comply with in all material respects. The Security Program applies to Palatial’s performance under the Agreement and all access, collection, use, storage, transmission, disclosure, destruction or deletion of, and security incidents regarding all Personal Data. The Security Program does not limit other obligations of Palatial, including under the Agreement or any laws that apply to Palatial, Palatial’s performance under the Agreement, the Personal Data or the Permitted Purpose.

2. Requirements

- 2.1 Written Security Policy. Palatial will implement and enforce a written information and network security policy applicable to its employees, subcontractors, agents, and suppliers that supports the requirements of this Security Program.
- 2.2 Safeguards. Palatial will, consistent with current industry standards, maintain physical, administrative and technical safeguards and other security measures to maintain the security and confidentiality of Personal Data accessed, collected, used, stored or transmitted by Palatial. Those safeguards and measures will also protect that Personal Data from known or reasonably anticipated threats or hazards to its security and integrity, accidental loss, alteration, disclosure and all other unlawful forms of processing. Palatial will comply with the following requirements without limiting the preceding sentences:
 - 2.2.1 Firewall. Palatial will install and maintain a working network firewall or equivalent designed to protect Personal Data accessible via the Internet. The firewall will provide both ingress and egress filtering, and have a default policy of blocking network traffic.
 - 2.2.2 Updates. Palatial will use commercially reasonable efforts to keep its systems and software current with upgrades, updates, bug fixes, new versions and other modifications reasonably necessary to maintain the security of Personal Data, in accordance with Palatial’s patch management practices.
 - 2.2.3 Anti-virus. Palatial will at all times use industry standard anti-virus software on endpoints and scanning technologies for the production environment, and regularly updated signature files, designed to detect, prevent and remove

PALATIAL

viruses, spyware and malicious code on operating systems, software and other systems hosting, storing, processing, or that have access to Personal Data. Palatial will mitigate threats from all viruses, spyware, and other malicious code that are or should reasonably have been detected.

- 2.3 Testing. Palatial will regularly test its security systems and processes to confirm they meet the requirements of this Security Program.
- 2.4 Access Controls. Palatial will restrict access to Personal Data to only those people with a “need-to-know” for a Permitted Purpose.
- 2.5 Encryption. Palatial will encrypt Personal Data in transit over public networks and at rest, including on portable media and portable devices, using industry standard algorithms and methods.
- 2.6 Data Location. Palatial stores and Processes Personal Data in data centers located in the United States. Palatial will not change the region in which Personal Data is stored without giving Customer notice in the manner described in the Sub-Processors section of this DPA.
- 2.7 Data Retention and Destruction.
 - 2.7.1 Retention. Palatial will retain Personal Data only for the purpose of, and as long as is necessary for, the Permitted Purpose.
 - 2.7.2 Return or Deletion. Palatial will promptly, and in any event within 72 hours after Customer’s request, return to Customer and permanently and securely delete all Personal Data upon and in accordance with Customer’s notice requiring return and/or deletion. Also, Palatial will permanently and securely delete all live (online or network accessible) instances of the Personal Data within 30 days after the earlier of completion of the Permitted Purpose or termination or expiration of the Agreement.
- 2.8 Disaster Recovery / Business Continuity. Palatial will implement appropriate disaster recovery and business continuity plans designed to maintain the availability, security, integrity, and (where necessary) restoration of Personal Data on the occurrence of a business interruption event. Palatial will provide a summary of its disaster recovery and business continuity plans to Customer upon request.
- 2.9 Security Incidents. Palatial will inform Customer of any Security Breach within the period, and in the manner, set forth in the Security Breach section of this DPA. Palatial will remedy each Security Breach in a timely manner and provide Customer written details regarding Palatial’s internal investigation regarding each Security Breach.

ANNEX III**List of Sub-Processors**

Entity Name	Subprocessing Activities
CoreWeave (United States)	Hosting, compute, and storage for the Services
Modal (United States)	Hosting, compute, and storage for the Services
Nebius (United States)	Hosting, compute, and storage for the Services
RunPod (United States)	Hosting, compute, and storage for the Services
Cloudflare (United States)	Content delivery, network security, and cloud infrastructure for the Services
Stripe (United States)	Billing and payment processing
Twilio SendGrid (United States)	Account, billing, and service notifications
PostHog (United States)	Usage analytics for the Services
Slack (United States)	Customer support and account communications

Palatial's third-party model and inference providers are not listed here because they do not receive Personal Data. See the Sub-Processors section of this DPA.

ANNEX IV

Supplemental Clauses

SWITZERLAND

The SCCs and as adapted and supplemented as set forth in this section will only apply to a transfer of Personal Data Processed under this DPA from Switzerland to Palatial. Customer agrees that:

1. Any reference to “Member State” will not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland);
2. Any references to “personal data” extend to personal data of legal entities if and to the extent such personal data pertaining to legal entities is within the scope of the FADP; and
3. To the extent the transfer of Personal Data is governed by the FADP, the Swiss Federal Data Protection and Information Commissioner will act as the competent supervisory authority. To the extent the transfer of Personal Data is governed by the GDPR, the supervisory authority determined in Annex I(C) will act as the competent supervisory authority. Any references to the “competent supervisory authority” will be interpreted accordingly.