JACQUARD

DATA PROCESSING ADDENDUM

Last revised 7 October 2025

Should Jacquard or any Jacquard Personnel have access to or Process any Personal Information of Client, Jacquard shall comply with this Data Processing Addendum (the "**DPA**").

1. **Definitions**. The following capitalized terms have the meanings provided below and, where applicable, will be interpreted based on the definitions given to them in the Privacy Laws:

a. "**Cardholder Data**" means, with respect to a payment card or other payment technology: (i) the account holder's name, PAN or account number, service code, card validation code/value, PIN or PIN block, valid to/from dates and/or magnetic stripe data and
(ii) information relating to a payment transaction that can be associated with a specific account.

b. "**CCPA**" means the California Consumer Privacy Act, as amended from time to time.

c. "**CPA**" means the Colorado Privacy Act.

d. "**CTDPA**" means the Connecticut Personal Data Privacy and Online Monitoring Act.

e. "**CPRA**" means the California Privacy Rights Act, as amended from time to time.

f. "**Client Data**" means any information provided by Client or collected for Client, in any form, format or media (including paper, electronic and other records) that Jacquard Processes in connection with the performance of Services and that includes any Personal Information or Cardholder Data.

g. "**Client Systems**" means all technology solutions and equipment, all associated or interconnected network equipment, routers, embedded software, and communication lines, and all components of any information system or equipment owned or operated by, or operated on behalf of, Client.

h. "**Data Subject**" means an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

i. "**Data Subject Request**" means any request by a Data Subject (or by another person acting on behalf of a Data Subject) to exercise a right under any Privacy Law, or any other complaint or inquiry or similar communication about the Processing of

the individual's Personal Information.

j. "**EEA**" means the European Economic Area.

k. **"EEA Personal Data"** means personal data (as defined in the GDPR) subject to the laws of the EEA, Switzerland and (post-Brexit) the United Kingdom.

l. "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and any national data protection laws implementing that Regulation, as amended from time to time.

m. "**GLBA**" means the U.S. Gramm-Leach-Bliley Act, as amended from time to time.

n. "**HIPAA**" means the U.S. Heath Information Portability and Accountability Act, as amended from time to time.

o. "**Personal Data**" means any information relating to a Data Subject.

p. "**Personal Information**," or "**PI**," means all data (regardless of format) that (i) identifies or can be used to identify, contact or locate a natural person, or (ii) pertains in any way to an identified natural person.

q. "**Personnel**" means a Party's employees, contingent workers, agents, consultants and individual contractors.

r. "**PIPEDA**" means the Canadian Personal Information Protection and Electronic Documents Act, as amended from time to time.

s. "**Privacy Law(s)**" means any applicable law, regulation, rule or other mandatory legal obligation which regulates the Processing of Personal Information or that otherwise relates to data protection, data security or security breach notification obligations for Personal Information, including (by way of example only) the GDPR, UK GDPR, CPA, CTDPA, CCPA, CPRA, UCPA, VCDPA, PIPEDA, GLBA, and the U.K. Data Protection Act 2018.

t. "**Processing**" means any operation or set of operations that is performed upon Personal Information or on sets of Personal Information, whether or not by automated means, such as collection, recording, structuring, storage, alteration, accessing, consultation, use, copying, disclosure, combination, de-identification, redaction, erasure or destruction. ("Process" and "Processed" are construed accordingly.)

u. "**Security Breach**" means a "personal data breach" (as defined in the GDPR), a "breach of the security of a system" or similar term (as defined in any other applicable Privacy Law) or any other event that compromises the security, confidentiality or integrity of any Client Data. Security Breach includes, for example, incidents that involve unauthorized, unlawful, or accidental use, disclosure, loss, alteration, destruction of, or access to any Client Data.

v. "**Subprocessor**" means a third party, including an affiliate of Jacquard, that Processes Client Data in the course of providing services to Client or that has access (even inadvertent access) to any Client Data.

w. "**Transfer**" means to disclose or otherwise make any Client Data available to a third party (including to any affiliate or Subprocessor), either by physical movement of the Client Data to such third party or by enabling remote access to the Client Data by other means.

x. "**UCPA**" means the Utah Consumer Privacy Act.

y. "**UK GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th 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 or "GDPR") as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019.

z. "**VCDPA**" means the Virginia Consumer Data Protection Act.

2. **General.**

a. Jacquard and its subsidiaries have taken commercially reasonable actions to comply with, and are in material compliance with, the Privacy Laws. To ensure compliance with the Privacy Laws, Jacquard has in place, complies with, and take takes appropriate steps reasonably designed to ensure compliance in all material respects with their policies and procedures relating to data privacy and security and the collection, storage, use, processing, disclosure, handling, and analysis of Personal Data and Confidential Data. Jacquard makes all disclosures to users or customers required by applicable laws and regulatory rules or requirements, and none of such disclosures have, to the knowledge of Jacquard, been inaccurate or in violation of any applicable laws and regulatory rules or requirements in any material respect.

b. Jacquard further certifies that neither it nor any subsidiary:

i. has received notice of any actual or potential liability under or relating to, or actual or potential violation of, any of the Privacy Laws, and has no knowledge of any event or condition that would reasonably be reasonably expected to result in any such notice;

ii. is currently conducting or paying for, in whole or in part, any investigation, remediation, or other corrective action pursuant to any Privacy Law; or

iii. is a party to any order, decree, or agreement that imposes any obligation or liability under any Privacy Law.

3. **Processing of Client Data**. Jacquard will Process Client Data only as necessary to perform the Services, in accordance with Client's written instructions or

as needed to comply with law. Annex 1 contains a general description of the Processing activities and Services, including contact information for those Jacquard personnel who have primary responsibility for privacy and data security. Jacquard will update Annex 1 and provide the updated version to Client as needed to inform Client of any changes, including any changes to the privacy & security contacts, and Subprocessors.

4. **Compliance**. Each Party must use reasonable efforts to stay informed of the legal and regulatory requirements for its Processing of Personal Information. If Jacquard Processes Client's Personal Information, Jacquard will comply with those obligations applicable to it as a "Data Processor" and Client will comply with those obligations applicable to it as a "Data Controller" (as defined in the GDPR and similar Privacy Laws). Jacquard will promptly notify Client if, in its opinion, any instructions given by Client for Processing violate any law or regulation. Jacquard will also promptly notify Client of any circumstances that may prevent it or any Subprocessor from complying with its obligations under any applicable Privacy Law or these Terms.

5. **Specific Compliance Requirements**. To the extent applicable:

a. The Parties agree that Client Data shall not include "protected health information" as defined in HIPAA ("**PHI**"). If however the Client Data at any time includes such information, Client shall notify Jacquard of such inclusion and provide Jacquard with an opportunity to object to such inclusion. Should the Client Data include PHI, Jacquard and Client agree that the Client's Business Associate Agreement Terms are incorporated herein as required by HIPAA.

b. If the Client Data includes EEA Personal Data, Jacquard and Client will ensure adequate protection for the EEA Personal Data. The Parties will ensure adequate protection for any Transfers of EEA Personal Data using the mechanism indicated on Annex 1. In the event that EEA authorities or courts determine that the Transfer mechanism selected is no longer an appropriate basis for Transfers, Jacquard and Client will promptly take all steps reasonably necessary to demonstrate adequate protection for the EEA Personal Data using another approved mechanism.

c. If the Services involve the collection of Personal Information directly from individuals, Jacquard will provide the individuals with a clear and conspicuous privacy notice, which notice will either be (i) Client's privacy notice, or (ii) Jacquard's privacy notice, provided that such notice must address any legal requirements for such notices in the jurisdictions where it is given, be translated into the languages regularly used in connection with Jacquard's interaction with the individuals, and indicate that Jacquard is Processing the data as a processor on behalf of its clients.

6. **Jacquard Personnel**. Jacquard will limit access to the Client Data to its Personnel that reasonably need to access Client Data to perform the Services. Prior to allowing Personnel to Process Client Data, Jacquard will (i) conduct an appropriate background investigation of the individual as permitted by law (and receive an acceptable response), (ii) require the individual to execute an enforceable

confidentiality agreement, and (iii) provide the individual with appropriate privacy and security training. Jacquard will also use commercially-reasonable efforts to monitor its Personnel for compliance with these Terms and apply appropriate disciplinary measures for individuals that fail to comply.

7. **Data Security**. Jacquard maintains a comprehensive, written information security program that can be found at https://jacquard.com/legal/information-security-addendum/.

8. **Transfers of Client Data**. Jacquard will not Transfer any Client Data across any national borders or permit remote access to Client Data without the prior written consent of Client. Approved Transfers will be described in the Agreement and/or on Annex 1 below. Jacquard will notify Client thirty (30) days prior to any proposed new Transfer. Client will evaluate the proposed new Transfer and notify Jacquard of any objections or additional legal requirements. Jacquard will not undertake such Transfers until such objections or requirements have been addressed to Client's reasonable satisfaction.

9. **Subprocessors.**

a. Jacquard represents that it:

i. Conducts adequate due diligence on any Subprocessor to ensure that it is capable of providing the level of protection for Client Data as is required by these Terms;

ii. Provides that the Subprocessor's right to Process Client Data can be terminated by Jacquard immediately on expiry or termination of the Agreement for whatever reason; and

iii. Remains primarily liable to Client for the acts, errors and omissions of the Subprocessor, as if they were Jacquard's own acts, errors and omissions.

b. A list of all Subprocessors (the "Subprocessor List") as at the date of the Agreement is set out in Annex 2 below, and Client shall notify Jacquard in writing within 30 days of any objection. Upon written request, Jacquard will provide Client with a then-current copy of the Subprocessor List.

10. **Third Party Requests for Client Data**. If Jacquard receives any subpoena, order, demand, warrant, or any other document requesting or purporting to compel the production of Client Data (a "**Third Party Request**"), Jacquard will (unless prohibited by law) immediately notify Client. If the Third Party Request is not legally valid and binding, Jacquard will not respond to it. If a Third Party Request is legally valid and binding, Jacquard will use good faith efforts to provide Client at least twenty-four (24) hours' notice prior to the required disclosure, so that Client may exercise any rights as it may have under applicable law to prevent or limit such disclosure. Notwithstanding the foregoing, Jacquard will exercise commercially reasonable efforts

to prevent and limit any such disclosure and to otherwise preserve the confidentiality of Client Data. Jacquard will also cooperate with Client with respect to any action taken with respect to such Third Party Request, including to obtain (at Client's sole expense) an appropriate protective order or other reliable assurance that confidential treatment will be accorded to Client Data. In all cases, Jacquard will provide a copy to Client of all Client Data and any relevant information that it does so disclose unless prohibited by applicable law.

11. **Data Subject Requests**. Jacquard will immediately notify Client of any Data Subject Requests by sending an email to the Client's contact name on file in the most recent Service Order. Unless otherwise agreed (such as for handling of requests contemplated by the Agreement), Client will handle Data Subject Requests, and Jacquard will not disclose any Client Data in response to any such requests, except to the extent Jacquard is required to do so under applicable law. Jacquard will reasonably assist Client with Data Subject Requests as may be required to comply with applicable Privacy Laws. Should Jacquard be legally obligated to respond to a Data Subject Request, it will also provide a copy to Client of all Client Data and any relevant information that it discloses.

12. **Data Protection Impact Assessments and Prior Consultation with Regulator**. As may be required by Privacy Laws, Jacquard will reasonably assist Client (at Client's sole expense) with any Data Protection Impact Assessments ("**DPIA**"s) and prior consultations with regulators, in each case solely in relation to Processing of Client Data by Jacquard.

13. **Return, Deletion and Retention.**

a. When Jacquard ceases to perform Services for Client (and at any other time, upon Client's written request), Jacquard will, and will cause its Representatives to, immediately cease use of the Client Confidential Information. Upon written request, Jacquard will also either (i) return the Client Data (and all media containing copies of the Client Data), or (ii) securely purge, delete and destroy the Client Data in accordance with applicable law. Electronic media containing Client Data will be disposed of in a manner that renders the Client Data unrecoverable. Upon written request, Jacquard will provide Client with certification of compliance with this provision. If Jacquard is required by applicable law to retain any Client Data containing Personal Information, Jacquard warrants that it will (i) ensure the continued confidentiality and security of the Client Data, (ii) securely delete or destroy the Client Data when the legal retention period has expired, and (iii) not actively Process the Client Data other than as needed for to comply with law.

b. Notwithstanding the foregoing, Jacquard will be permitted to retain: (i) Client Confidential Information for a longer period if such retention is strictly necessary to meet Jacquard's legal compliance obligations, (ii) Client Confidential Information in backup media, and (iii) De-Identified Data (as described in Section 10(f) of the Master Subscription Agreement). Retention of Client Confidential Information pursuant to (i)

and (ii) shall be pursuant to Jacquard's fully implemented and documented records management program, provided that such retention shall not be indefinite and shall not exceed industry standards. In addition, Client Confidential Information so retained shall not be used for any other purpose and such Client Confidential Information shall be otherwise maintained in accordance with this Addendum.

14. **Accountability and Audits**. Upon request, Jacquard will provide Client with information reasonably needed to demonstrate compliance with the obligations in these Terms. Jacquard will also cooperate with any supervisory authority audit or investigation regarding its (or its Subprocessors) Processing of Client Data. In the event that such an audit or investigation reveals material gaps or weaknesses in Jacquard's security program that affects Jacquard's provision of Services to Client, Jacquard agrees to work with Client, in good faith and at Jacquard's expense, to resolve the issues. Client will be entitled to suspend Jacquard's Processing of Client Data until such issues are resolved.

15. **Conflicts and Consideration**. The terms of this DPA shall supersede any conflicting provision of the Agreement related to the Processing of Client Data. Jacquard agrees that the consideration provided by the Agreement is also sufficient consideration for its agreement to these Terms.

16. **Term and Survival**. The obligations of Jacquard under this DPA will continue for so long as Jacquard Processes Client Data, even if all other agreements between Jacquard and Client have expired or have been terminated.

JACQUARD

Annex 1: General Description of Processing

1) Description:

Employee information will be used to set up an account and log in to the Jacquard platform, a SaaS platform which uses AI to optimize brand content.

If the Services involve the collection of Personal Information directly from Client's customers, Jacquard will amend this Annex 1 to reflect the specific items processed by Jacquard.

2) Physical Location(s) of the Personal Information:

Amazon Web Servers ("AWS") Ireland ("eu-west-1" server).

3) Jacquard Privacy and Security Contacts:

Data Privacy Contact: General Counsel, Peter Patterson, peter.patterson@jacquard.com

Data Security Contact: VP, Engineering, Russell Peto, russell.peto@jacquard.com

Data Protection Officer: President & CTO, Jasper Pye, jasper@jacquard.com

4) Categories of Personal Data (GDPR) / Personal Information (CCPA):

For Client's employees who use the Services:
first name, last name, company, job title and business email address.

5) Categories of Sensitive Information (select all that apply):

☐ Government-issued identification numbers

☐ Online account access information, including usernames, passwords, and password recovery information

☐ Cardholder Data, PANs or other financial account numbers

☐ Health data, health insurance data, genetic information and biometric information

☐ Consumer reporting data, including employment background screening reports

☐ Data related to criminal convictions or offenses or allegations of crimes

☐ Special categories of data that reveal race or ethnicity, political opinions, religious or philosophical beliefs, trade union membership, health, or sex life or sexual orientation

☐ Other:_____

☒ None of the above

6) Categories of Data Subjects (select all that apply):

☒ Client employees, contractors
☐ Consumers, website visitors
☐ Client commercial customers
☐ Merchants
☐ Suppliers
☐ Cardholders
☐ Job applicants
☐ Professionals, trade show attendees,
☐ Prospective customers
☐ Other

7) Mechanism of Transfers of EEA Personal Data:

If EEA Personal Data is transferred, Jacquard will enter into an International Data Transfer Agreement ("IDTA") and an International Data Transfer Agreement Addendum ("ITDA Addendum") to the European Commission's standard contractual clauses for international data transfers (the "IDTA Addendum"), as issued by the UK Information Commissioner's Office under Section 119A of the Data Protection Act 2018 and having force and effect as of 21 March 2022. For purposes of the ITDA and the ITDA Addendum, Client (or the applicable Client affiliate, or a corporate customer) will act as the "data exporter" and Jacquard (or its approved Subprocessor, as applicable) will act as the "data importer."

8) Retention of Client Personal Information (select one):

Upon termination of the Agreement, unless otherwise requested by Client, Client Data will be retained for the following durations and purposes:

Document Type	**Maximum Retention Period**	**Data Retention Purpose**
Records relating to a contract or agreement with a client, customer or supplier ('counterparty')	One year from counterparty's last indication of interest in reactivating services, unless data deletion is sooner requested (which all clients have the right to do at any time).	In order to support future services reactivation by a client.
Tax records (employee and business applicable tax records)	Eight years from the end of the tax year to which the records relate.	In order to comply with applicable tax regulations.
Records relating to employees (excluding tax, pensions and health and safety)	Ten years following end of employment.	In order to comply with applicable employment regulations.

Health and Safety records	Ten years.	In order to comply with applicable health and safety regulations.
Employee pension records	Seven years from the end of employment in the case of personal pension records, eighty years from the end of employee's employment in the case of occupational pension records.	In order to comply with applicable employee pension regulations.
Marketing or business development records	Three years following last contact from subject, unless data deletion is requested (which all marketing contacts have the right to do at any time).	In order to fulfill the purpose of maintaining contact with potential customers of our services.
Access logs (platform & infrastructure, production)	Six years.	In order to comply with audit and compliance purposes.
Platform logs (production & preproduction)	Two years.	In order to facilitate business operations.
Production Client data	One month after the cessation of the business relationship with client.	In order to support future services reactivation by a client.
De-Identified Data (i.e. De-identified Language Performance data)	Six years, unless data deletion is sooner requested (which all clients have the right to do at any time).	In order to improve system performance.

These are the maximum retention periods and there may be circumstances in which the records are kept for a shorter period.

For any category of document not specifically defined above and unless otherwise specified by applicable law, the maximum retention period for any document will be deemed to be seven (7) years from the date of creation of the document.

JACQUARD

Annex 2: Subprocessor List

Subprocessor Legal Name and Company Number (if applicable)	Registered Address	Description of the Services and/or Purposes for the Subprocessing	Categories of PI	Location of the Processing	Transfer Mechanism (if EEA Data)
Amazon Web Services, Inc.	410 Terry Avenue North, Seattle, WA 98109-5210, U.S.A.	Cloud Infrastructure Hosting	n/a	EU-west-1 (Dublin)	See Section 7 of Annex 1.
Snowflake Inc.	Suite 3A, 106 East Babcock Street, Bozeman, Montana 59715, U.S.A.	Database as a service	All categories in Annex 1 pt 4	EU	See Section 7 of Annex 1.
MongoDB, Inc.	229 W. 43rd Street, 5th Floor, New York, New York 10036 U.S.A.	Database as a service	All categories in Annex 1 pt 4	EU	See Section 7 of Annex 1.
Anthropic PBC	548 Market Street, PMB 90375, San Francisco, CA 94104, U.S.A.	Language generation and processing	All categories in Annex 1 pt 4	EU	See Section 7 of Annex 1.
OpenAI, Inc.	1455 3rd St., San Francisco, CA 94158, U.S.A.	Language generation and processing	All categories in Annex 1 pt 4	EU	See Section 7 of Annex 1.