Last Update: 3 November 2025

Lattice: Data Processing Addendum

THIS DATA PROCESSING ADDENDUM ("DPA") forms part of and is incorporated into the Lattice Terms of Service or other written or electronic agreement governing Customer's use of the Service ("**Main Agreement**") between Customer and Lattice (each a "**party**" and together the "**parties**").

In the course of providing the Service to Customer, Lattice may process Customer Data (defined below) and the parties agree to comply with the following provisions with respect to any processing of Customer Data by Lattice as a processor or service provider to Customer.

1. **Definitions.** Capitalized terms used in this DPA shall have the meanings given to them in the Main Agreement unless otherwise defined herein. The following definitions are used in this DPA:

1.1. "**Affiliate**" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.

1.2. "**Authorized Affiliate**" means any Customer Affiliate permitted to use the Service pursuant to the Main Agreement but have not signed their own "Main Agreement" and are not a "Customer" as defined under the Main Agreement.

1.3. "**CCPA**" means Sections 1798.100 *et seq*. of the California Civil Code and any attendant regulations issued thereunder as may be amended from time to time, including but not limited to the California Privacy Rights Act of 2020 (the "**CPRA**") and its implementing regulations.

1.4. "**Customer Data**" means any Customer Content that is Personal Data and that Lattice processes on behalf of Customer in the course of providing the Service, as more particularly described in Schedule A of this DPA.

1.5. "**Control**" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests (as measured on a fully-diluted basis) then outstanding of the entity in question. The term "Controlled" will be construed accordingly.

1.6. "**Data Protection Laws**" means all data protection and privacy laws regulations applicable to a party and its processing of Personal Data under the Main Agreement, including, where applicable: (a) the GDPR, (b) all applicable implementations of the GDPR into national law, (c) in respect of the United Kingdom, the Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 ("**UK GDPR**"), (d) the Swiss Federal Data Protection Act ("**Swiss DPA**"), and (e) the CCPA; in each case, as may be amended, superseded or replaced.

1.7. "**Europe**" means for the purposes of this DPA the European Economic Area ("EEA"), United Kingdom and Switzerland.

1.8. "**GDPR**" means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation).

1.9. "**Personal Data**" means any information protected as "personal data", "personal information" or "personally identifiable information" under Data Protection Laws.

1.10. "**Restricted Transfer**" means: (i) where the GDPR applies, a transfer of Customer Data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission ("**EEA Restricted Transfer**"); (ii) where the UK GDPR applies, a transfer of Customer Data from the United Kingdom to any other country which is not subject based on adequacy

1.11 "**Standard Contractual Clauses**" means the standard contractual clauses between controllers and processors (Module 2) adopted by European Commission in its Implementing Decision (EU) 2021/91 of 4 June 2021 and currently located at: https://commission.europa.eu/system/files/2021-06/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf, as amended, superseded or replaced from time to time.

1.12 "**Security Incident**" means any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data, stored or otherwise processed by Lattice in connection with the provision of the Service. "Security Incident" shall not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful login attempts, pings, port scans, denial of services attacks, and other network attacks on firewalls or networked systems.

1.13 "**Subprocessor**" means any Processor having access to Customer Data and engaged by Lattice to assist in fulfilling its obligations with respect to providing the Service pursuant to the Main Agreement (excluding any employee, consultant or independent contractor of Lattice).

1.14 The terms "**controller**", "**data subject**", "**processor**", "**processing**", "**personal data**" and "**sensitive data**" shall have the meanings given to them in Data Protection Laws or if not defined therein, the GDPR, and the terms "**service provider**", "**business**", "**collects**" (and "**collected**" and "**collection**"), "**consumer**", "**business purpose**", "**sell**" (and "**selling**", "**sale**", and "**sold**"), "**share"** (and "**sharing**" and "**shared**"), and "**service provider**" have the meanings given to them in §1798.140 of the CCPA, as applicable.

1.15 "**UK Addendum**" means the International Data Transfer Addendum (version B1.0) to the EU Commission Standard Contractual Clauses issued by UK Information Commissioners Office under S.119(A) of the UK Data Protection Act 2018, as amended, superseded or replaced from time to time.

2. Roles and Scope of Processing

Data Processing Roles. Lattice shall process Customer Data for the Permitted Purpose as a processor on behalf of Customer as the controller. For the purposes of the CCPA (where applicable), Lattice shall process Customer Data as a service provider for the Customer as a business.

Compliance with Laws. Each party shall comply with its obligations under Data Protection Laws in respect of any Customer Data it processes under this DPA. For the avoidance of doubt, Lattice is not responsible for complying with Data Protection Laws uniquely applicable to Customer by virtue of its business or industry, such as those generally applicable to online service providers.

Processing Instructions. Lattice shall process Customer Data in accordance with Customer's documented lawful instructions, unless obligated to do otherwise by applicable law, in which case Lattice will notify Customer (unless that law prohibits Lattice from doing so on important grounds of public interest). For these purposes, Customer instructs Lattice to process Customer Data for the purposes described in Schedule A (the "**Permitted Purpose**", which, where CCPA applies, is a business purpose). The DPA and Main Agreement are Customer's complete and final instructions. Any additional or alternate instructions must be consistent with the terms of the DPA and the Agreement. Without prejudice to Section 2.4 (Customer Responsibilities), Lattice shall promptly notify Customer in writing, unless prohibited from doing so under Data Protection Laws, if it becomes aware or believes that any processing instructions from Customer violates Data Protection Laws (but without obligation to actively monitor Customer's compliance with Data

Protection Law) and in such event, Lattice shall not be obligated to undertake such processing until such time as the Customer has updated its processing instructions and Lattice has determined that the incidence of non-compliance has been resolved.

Customer Responsibilities. Customer shall, in its use of the Service and provision of instructions, process Customer Data in accordance with Data Protection Laws. Customer is solely responsible for: (i) the accuracy, quality, and legality of the Customer Data, (ii) the means by which Customer acquired such Customer Data; and (iii) the instructions it provides to Lattice regarding the processing of such Customer Data. Customer shall ensure (i) that it has provided notice and obtained (or will obtain) all consents and rights necessary for Lattice to process Customer Data pursuant to the Main Agreement and this DPA, (ii) its instructions are lawful and that the processing of Customer Data in accordance with such instructions will not violate applicable Data Protection Laws, and (iii) where the CCPA applies, that the Customer Data is provided to Lattice in order to perform the Service for a valid business purpose only.

3. Subprocessing

3.1 Authorized Subprocessors. Customer provides a general prior authorization for Lattice to engage Subprocessors and, where CCPA applies, other third party service providers (hereinafter referred to as Subprocessors) in order to provide the Service. The Subprocessors currently engaged by Lattice are listed at https://www.Lattice.com/privacy/subprocessors (or such other URL as may be updated from time to time) ("**Subprocessor Site**"). Lattice will remain responsible for any acts or omissions of any Subprocessor that causes Lattice to breach any of its obligations under this DPA.

3.2 Notification of New Subprocessors. Lattice will make available the Subprocessor Site and provide Customer with a mechanism to obtain notice, including the option to subscribe to notifications, of any updates to the Subprocessor Site. At least ten (10) days prior to authorizing any new Subprocessor to process Customer Data, Lattice will provide notice to Customer by updating the Subprocessor Site.

4. Security Measures and Security Incident Response

4.1 Security Measures. Lattice will implement and maintain appropriate and reasonable technical and organizational security measures designed to protect Customer Data from Security Incidents and to preserve the security and confidentiality of the Customer Data in accordance with the security measures described in Schedule B ("**Security Measures**"). Customer acknowledges that the Security Measures are subject to technical progress and development and that Lattice may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Service provided to Customer.

4.2 Personnel. Lattice restricts its personnel from processing Customer Data without authorization by Lattice as set forth in the Security Measures and shall ensure that any person who is authorized by Lattice to process Customer Data is under an appropriate obligation of confidentiality.

4.3 Customer Responsibilities. Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Service, including securing its account authentication credentials, protecting the security of Customer Data transmitted via the systems it administers and maintains (i.e. email encryption), and taking any appropriate steps to securely encrypt or back up any Customer Data uploaded to the Service.

4.4 Security Incident Response. Upon becoming aware of a Security Incident, Lattice will notify Customer without undue delay and, in any case within seventy-two (72) hours after becoming aware. Lattice will provide information relating to the Security Incident to Customer promptly as it becomes known or as is reasonably requested by Customer to fulfill Customer's obligations as controller. Lattice will also take appropriate and reasonable steps to contain, investigate, and mitigate any Security Incident.

5. **Audit and Records.**

5.1 Audit Rights. Lattice shall make available to Customer all information in Lattice's possession or control and provide all assistance in connection with audits of Lattice's premises, systems, and documentation as Customer may reasonably request to enable Customer to assess Lattice's compliance with this DPA. Customer acknowledges and agrees that it shall exercise its audit rights under this DPA (including this Section 5 and where applicable, the Standard Contractual Clauses) by instructing Lattice to comply with the audit measures described in the Security Measures and Section 5.2 below.

5.2 Audit Procedures. Where required under Data Protection Laws or where a data protection authority requires , Customer may, on giving at least thirty (30 days) prior written notice, request that Customer's personnel or a third party (at Customer's expense) conduct an audit of Lattice's facilities, equipment, documents and electronic data relating to the processing of Customer Data under the Main Agreement to the extent necessary to inspect and/or audit Lattice's compliance with this DPA, provided that: (i) Customer shall not exercise this right more than once per calendar year; (ii) such additional audit enquiries shall not unreasonably impact in an adverse manner Lattice's regular operations and do not prove to be incompatible with applicable Data Protection Laws or with the instructions of the relevant data protection authority; (iii) before the commencement of such additional audit, the parties shall mutually agree upon the scope, timing, and duration of the audit, and (iv) at all times during the scope of the audit, Customer and any appointed third party will comply with Lattice's policies, procedures, and reasonable instructions governing access to its systems and facilities, including limiting or prohibiting access to information that is confidential information. Without prejudice to the foregoing, Lattice will provide all assistance reasonably requested by Customer to accommodate Customer's request.

6. **Data Transfers**. Customer acknowledges and agrees that Lattice may transfer and process Customer Data to and in the United States and other locations in which Lattice, its Affiliates, or its Subprocessors maintain data processing operations as more particularly described in the Subprocessor Site (defined above). Lattice shall ensure that such transfers are made in compliance with Data Protection Laws and this DPA.

7. **Return or Deletion of Data.** Promptly upon Customer's request, or within one hundred eighty (180) days after the termination or expiration of the Main Agreement, Lattice shall delete or return Customer Data in its possession or control. This requirement shall not apply to the extent Lattice is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data Lattice shall securely isolate and protect from any further processing, except to the extent required by such laws.

8. **Cooperation**

8.1 Data Subject and Consumer Rights Requests. Lattice shall, taking into account the nature of the processing, reasonably assist Customer in responding to any requests from individuals or applicable data protection authorities relating to the processing of Customer Data for the Permitted Purposes.

a) In the event that any such request is made to Lattice directly, Lattice will not respond to such communication directly (except to direct the data subject to contact Customer) without Customer's prior authorization, unless legally compelled to do so. If Lattice is required to respond to such a request, Lattice will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

b) If Customer is unable to respond to the request with regard to personal data processed by Lattice in its capacity as either a processor or service provider to Customer (as applicable), upon Customer's reasonable request, and subject to any applicable restrictions or exemptions under applicable law, Lattice will use reasonable efforts to assist Customer in responding to verified individual requests received by Customer as it relates to the processing of personal data by Lattice as a processor or service provider to Customer.

8.2 Data Protection Impact Assessments (DPIAs). To the extent required under Data Protection Laws applicable to Europe, Lattice will provide requested information regarding the Service necessary to enable Customer to carry out data protection impact assessments and prior consultations with data protection authorities.

9. Europe

9.1 Scope. The terms in this Section 9 apply only if and to the extent Customer is established in Europe or the Customer Data is otherwise subject to Data Protection Laws applicable to Europe.

9.2 Subprocessor Obligations. Lattice will enter into a written agreement with each Subprocessor imposing data protection obligations no less protective of Customer Data as this DPA or the Data Protection Laws to the extent applicable to the nature of the services provided by such Subprocessor.

9.3 Subprocessor Objection Right. If Customer objects on reasonable grounds relating to data protection to Lattice's use of a new Subprocessor, then Customer shall promptly, and within ten (10) days following Lattice's notification pursuant to Section 3.2 (Notification of new Subprocessors) above, provide written notice of such objection to Lattice. In such event, the parties will discuss such concerns in good faith with a view to achieving resolution. If the parties cannot agree to a mutually acceptable resolution, Customer shall as its sole and exclusive remedy have the right to terminate the relevant affected portion(s) of the service without liability to either party (but without prejudice to any fees incurred by Customer prior to suspension or termination). Upon termination by Customer pursuant to this Section, Lattice shall refund Customer any prepaid fees for the terminated portion(s) of the Service that would have been provided after the effective date of the termination.

9.4 Transfer Mechanism. To the extent the transfer of Customer Data from Customer to Lattice is a Restricted Transfer and Data Protection Laws applicable to Europe require that appropriate safeguards are put in place, such transfer shall be governed by the Standard Contractual Clauses, which shall be incorporated by reference into and form an integral part of this DPA, as follows:

(a) In connection with an EEA Restricted Transfer: (i) Module Two (*controller to processor transfers*) shall apply and all other modules are deleted; (ii) in Clause 7, the optional docking clause will apply; (ii) in Clause 9 of Module Two, Option 2 will apply and the time period for prior notice of Sub-processor changes is identified in Section 3.2 of this DPA; (iii) in Clause 11, the optional language will not apply; (iv) in Clause 17, Option 1 will apply, and the Standard Contractual Clauses will be governed by Irish law; (v) in Clause 18(b), disputes shall be resolved before the courts of Ireland; (vi) Annex I shall be deemed completed with the information set out in Schedule A (Description of Processing/ Transfer) of this DPA; and (vii) Annex II shall be deemed completed with the information set out in Schedule B (Security Measures) (as applicable) of this DPA.

(b) In connection with a UK Restricted Transfer, the Standard Contractual Clauses shall apply in accordance with Section 9.4(a) above, but as modified and interpreted by the Part 2: Mandatory Clauses of the UK Addendum, which shall be incorporated into and form an integral part of this DPA. Any conflict between the terms of the Standard Contractual Clauses and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum. In addition, tables 1 to 3 in Part 1 of the UK Addendum shall be completed respectively with the information set out in Schedule A and Schedule B of this DPA and table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party".

(c) In connection with a Swiss Restricted Transfer, the Standard Contractual Clauses shall apply in accordance with Section 9.4(a) above, but with the following modifications: (i)

any references in the Standard Contractual Clauses to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA and the equivalent articles or sections therein; (ii) any references to "EU", "Union", "Member State" and "Member State law" shall be interpreted as references to Switzerland and Swiss law, as the case may be; (iii) any references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the relevant data protection authority and courts in Switzerland; and (iv) the Standard Contractual Clauses shall be governed by the laws of Switzerland and disputes shall be resolved before the competent Swiss courts.

(d) The rights and obligations afforded by Standard Contractual Clauses will be exercised in accordance with this DPA, unless stated otherwise. It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA) the Standard Contractual Clauses shall prevail to the extent of such conflict.

9.5 Data Transfer Arrangements. To the extent Lattice adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses adopted pursuant to Data Protection Laws) for the transfer of Personal Data ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism shall apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with Data Protection Laws applicable to Europe and extends to territories to which Personal Data is transferred).

9.6 Notification of Government Access Requests: For the purposes of Clause 15(1)(a) of Standard Contractual Clauses, Lattice shall notify Customer and not the data subject(s) in case of government access requests. Customer shall be solely responsible for promptly notifying the data subject, as necessary.

10. Authorized Affiliates

10.1 Affiliate Communications. Customer is responsible for coordinating all communications with Lattice on behalf of its Authorized Affiliates with regard to this DPA. Customer represents that it is authorized to issue instructions as well as make and receive any communications in relation to this DPA on behalf of its Authorized Affiliates.

10.2 Affiliate Enforcement. Authorized Affiliates may enforce the terms of this DPA directly against Lattice, subject to the following provisions:

(a) Customer will bring any legal action, suit, claim, or proceeding which the Affiliate would other have it if were a party to the Main Agreement (each an "Affiliate Claim") directly against Lattice on behalf of such Affiliate, except where Data Protection Laws to which the relevant Affiliate is subject require that the Affiliate bring or be a party to such Affiliate Claim; and

(b) for the purpose of any Affiliate Claim brought directly against Lattice by Customer on behalf of such Affiliate in accordance with this Section, any losses suffered by the relevant Affiliate may be deemed to be losses suffered by Customer.

11. Limitation of Liability

11.1 In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

11.2 Any claim or remedies Customer or its Affiliates may have against Lattice and its respective employees, agents, or Sub-processors arising under or in connection with this DPA including: (i) for breach of this DPA (including the Standard Contractual Clauses or the UK Addendum); (ii) as a result of fines (administrative, regulatory or otherwise)

imposed upon Customer; (iii) under Data Protection Laws, including but not limited to CCPA, GDPR, UK GDPR or Swiss DPA, including any claims relating to damages paid to a data subject, consumer, or other individual; and (iv) breach of its obligations under the Standard Contractual Clauses or UK Addendum, will, to the maximum extent permitted by law, be subject to any limitation and exclusion of liability provisions (including any agreed aggregate financial cap) that apply under the Main Agreement.

11.3 For the avoidance of doubt, Lattice and its Affiliates' total overall liability for all claims from Customer and its Affiliates arising out of or related to the Main Agreement and each DPA shall apply in the aggregate for all claims under the Main Agreement and this DPA together, including by Customer and its Affiliates.

12. CCPA

12.1 Scope. The terms in this Section 12 apply only if and to the extent the Customer Data is subject to Data Protection Laws applicable to the state of California.

12.2 For the purposes of the CCPA, Lattice is prohibited from:

(a) selling or sharing Customer Data;

(b) processing Customer Data for targeted and/or cross context behavioral advertising;

(c) retaining, using, or disclosing Customer Data for any purposes other than the specific purposes of performing the Service or as otherwise permitted under Main Agreement and this DPA;

(d) retaining using or disclosing Customer Data outside the direct business relationship between Lattice and Customer; or

(e) combining Customer Data with any other data if and to the extent doing so would be inconsistent with the Business Purpose or the limitations on service providers under the CCPA or other Data Protection Laws.

12.3 Lattice hereby certifies that it understands the restrictions set out in Section 12.1 and will comply with them, and that it will notify Customer if Lattice becomes unable to comply with the CCPA.

12.4 Notwithstanding the foregoing and anything to the contrary in the Main Agreement (including this DPA), Customer acknowledges that Lattice shall have a right to process Customer Data for the purposes of creating anonymized, aggregate and/or de-identified information for its own legitimate business purposes, including where Customer has requested a Lattice Service that includes the provision of benchmarking reports, compiling anonymized benchmarking reports and statistics.

12.5 Lattice maintains, and will continue to maintain during the term of the Main Agreement, tools and resources for consumers to exercise their rights under the CCPA. If Lattice, directly or indirectly, receives a request submitted by a consumer who is an employee of Customer to exercise a right it has under the CCPA in relation to that Consumer's Customer Data, Lattice will follow the procedures described in Section 8 of this DPA.

13. General

13.1 The parties agree that this DPA shall replace any existing DPA the parties have previously entered into in connection with the Service.

13.2 As between Customer and Lattice, this DPA is incorporated into and subject to the terms of the Main Agreement and shall be effective and remain in force for the term of the Main Agreement or the duration of the Service. In the event of any conflict between the terms of this DPA and the terms of the Main Agreement, the terms of this DPA shall prevail so far as the subject matter concerns the processing of Customer Data.

13.3 Except as described in Section 10 (Authorized Affiliates), in no event shall this DPA benefit or create any right or cause of action on behalf of a third party, but without prejudice to the

rights or remedies available to data subjects under Data Protection Laws or this DPA (including the Standard Contractual Clauses).

13.4 Each party acknowledges that the other party may disclose the Standard Contractual Clauses, this DPA, and any privacy related provisions in the Main Agreement to any regulator or supervisory authority upon request.

13.5 Notwithstanding anything to the contrary in the Main Agreement and without prejudice to Section 2.3, Lattice may periodically make modifications to this DPA as may be required to comply with Data Protection Laws.

13.6 Other than as required by applicable Data Protection Laws or the Standard Contractual Clauses, the dispute mechanisms, including those related to venue and jurisdiction, set forth in the Main Agreement govern any dispute pertaining to this DPA.

SCHEDULE A

Description of Processing/Transfer

Annex 1(A) List of Parties:

Data Exporter	**Data Importer**
Name: The party named as the 'Customer" in the Main Agreement.	**Name:** Degree, Inc. d/b/a Lattice ("Lattice")
Address: The address for the Customer associated with its Lattice account or as otherwise specified in the Order Form or Main Agreement. **Contact:** The contact details associated with the Customer's Lattice account or as otherwise specified in the Order Form or Main agreement. **Activities relevant to the transfer:** See Annex 1(B) below. **Signature and Date:** By using the Service to transfer Customer Data to Lattice located in a non-adequate country, the data exporter will be deemed to have signed this Annex 1.	**Address:** 360 Spear Street, Floor 4 San Francisco, CA 94105 **Contact:** privacy@lattice.com **Activities relevant to the transfer:** See Annex 1(B) below **Signature and Date:** By transferring Customer Data to non-adequate country on Customer's instructions, the data importer will be deemed to have signed this Annex 1.
Role: Controller	**Role:** Processor

Annex 1(B) Description of Transfer:

	Description
Categories of Data Subjects:	Depending on the nature of the Service, Personal Data transferred may concern the following categories of data subjects: ● Customer's current and former employees, agents, advisors, contractors and other personnel (who are natural persons) ("Customer Personnel') ● Users of the Service who are customer's current and former employees, agents, advisors, contractors and other personnel (who are natural persons) ("Users")
Categories of Personal Data:	**Customer Personnel:** The types of Personal Data processed by Lattice are determined and controlled by Customer in its sole discretion and may include, but are not limited to the following categories of Personal Data: ● general employee information including name, email, photograph or image, voice data (limited to use of certain Lattice AI Feature(s), phone number, job title, department, and direct manager; ● specific information related to an employee's professional goals, accomplishments, training and development, awards and performance, feedback, and reviews; and ● employee onboarding and exit survey responses, and associated sentiments and opinions. If Customer subscribes to Lattice's Compensation Service:

	• information relating to an employee's compensation and benefits. If Customer subscribes to Lattice's HRIS Service: • an employee's identifiers (including government identifiers such as driver's license number, citizenship or residency status including visa information, copies of right to work documentation, state, province, or national identification numbers, Social Security Number or other taxpayer/government identification number, National Insurance Number, and passport information), address, birth date, gender, marital status, dependents, emergency contact; information in connection with an employee's job (including, but not limited to, title, grade, location, reporting lines, team affiliation, hire date, working hours, contract details, compensation details, performance and evaluation data, discipline information, work history, benefits and insurance, training, time-off documentation, etc.), military/veteran status, termination date/reason, personal email, etc. If Customer subscribes to Lattice's Payroll Service: • an employee's pay group, wage (salary or hourly rate), bank account number, routing number, account type, etc. **Users:** Depending on the nature of the Services, the Personal Data may include: • Account log-in credentials such as email, username and password, and unique user or team ID; • Business contact information such as name, phone number, and email address; • Employment information, such as employer, job title, etc.
Special category data (if appropriate):	With the exception of Lattice's HRIS Service, Lattice does not intentionally collect or process special category data. However, Customer may submit special category data to the Service, the extent of which is determined and controlled by Customer in its sole discretion, and which may include but is not limited to the following categories of special category data: gender, race or ethnicity, health data, sexual orientation, trade union membership, and any other category of special category uploaded by (or on behalf of) Customer. If Customer subscribes to Lattice's HRIS Service, the types of special category data processed by Lattice are determined and controlled by Customer in its sole discretion and may include, but are not limited to the following categories of special category data: gender, race or ethnicity, sexual orientation, gender identity, trade union membership, health status, and disability information.

Frequency of the transfer (one-off or continuous):	Continuous basis depending on the nature of the Service.
Nature of processing:	The nature of the processing is the performance of the Service in accordance with the Main Agreement.
Purpose(s) of the data transfer and further processing:	Personal data may be processed for the following purposes: (i) to provide and improve the Service provided to Customer in accordance with the Main Agreement; (ii) processing initiated by Users in their use of the Service; (iii) to comply with other reasonable instructions provided by Customer (e.g. via email or support tickets) that are consistent with the terms of the Main Agreement and this DPA, and (iv) to comply with any legal obligation under applicable law, including Data Protection Law. Where data benchmarking is provided as part of the Service requested by Customer, Customer Data may also be aggregated with other customer's Customer Data for the purpose of overall trends, to compile anonymized benchmarking reports and statistics requested by Customer in connection with its use of the Service, in accordance with the Main Agreement. Where Customer chooses to use a Lattice AI product or feature, Customer authorizes, instructs, and warrants that it has obtained any necessary consents required for Lattice and its Subprocessors to process Customer Data for the purpose of providing Lattice AI Output and functionality, which includes investigating security incidents and fraudulent activity, detecting and preventing network exploits or abuse, and as necessary to comply with applicable law or regulation.
Retention period (or, if not possible to determine, the criteria used to determine that period):	The duration of the processing is the term of Main Agreement or any applicable Order Form plus the period from expiration of the Main Agreement or Order Form (as applicable) until the return or deletion of the personal data by Lattice in accordance with the DPA.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	As above.

Annex 1(C): Competent supervisory authority

The competent supervisory authority shall be determined in accordance with Clause 13 of 2021 Controller-to-Processor Clauses and the GDPR.

SCHEDULE B

Lattice Technical and Organizational Security Measures

Technical and organizational security measures to be implemented by Lattice (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons:

A. Annual Evidence of Compliance

1. Third Party Security Audit: Lattice is and shall continue to be annually audited against the SOC 2 Type II standard. The audit shall be completed by an independent third-party. Upon Customer's written request, Lattice will provide a summary copy (on a confidential basis) of the most recent resulting annual audit report, so that Customer can verify Lattice's compliance with the audit standards against which it has been assessed and this DPA. Although that report provides an independently audited confirmation of Lattice's security posture annually, the most common points of interest are further detailed below. Lattice shall provide Customer with this initial evidence of compliance within thirty (30) days of written request and annually upon written request.

2. Executive Summary of Web Application Penetration Test: Lattice shall continue to annually engage an independent, third-party to perform a web application penetration test. Upon Customer's written request, Lattice shall provide the executive summary of the report to Customer. Lattice shall address all medium, critical and severe vulnerabilities in the findings of the report within a reasonable, risk-based timeframe. Lattice shall provide Customer with this initial evidence of compliance within thirty (30) days of written request.

3. Security Awareness Training: Lattice shall provide annual Security Training to all personnel. "Security Training" shall address security topics to educate users about the importance of information security and safeguards against data loss, misuse or breach through physical, logical and social engineering mechanisms. Training materials should address industry standard topics which include, but are not limited to:

- The importance of information security and proper handling of personal information.
- Physical controls such as visitor protocols, safeguarding portable devices and proper data destruction.
- Logical controls related to strong password selection/best practices.
- How to recognize social engineering attacks such as phishing.

4. Vulnerability Scan: Lattice shall ensure that vulnerability scans are performed on servers continuously and network security scans are completed at a minimum biannually, in each case using an industry standard vulnerability scanning tool.

B. Security

1. Process-Level Requirements

   a. Lattice shall implement user termination controls that include access removal / disablement promptly upon termination of staff.

   b. Documented change control process will be used to record and approve all major releases in Lattice's environment.

   c. Lattice shall have and maintain a patch management process to implement patches in a reasonable, risk-based timeframe.

2. Network Requirements

   a. Lattice shall use firewall(s), Security Groups/VPCs, or similar technology to protect servers storing Customer Data.

3. Hosting Requirements

a. Where Lattice handles Customer Data, servers shall be protected from unauthorized access with appropriate physical security mechanisms including, but not limited to, badge access control, secure perimeter, and enforced user provisioning controls (i.e. appropriate authorization of new accounts, timely account terminations and frequent user account reviews). These physical security mechanisms are provided by data center partners such as, but not limited to, AWS, Salesforce and Google. All cloud-hosted systems shall be scanned, where applicable and where approved by the cloud service provider.

b. Cloud Environment Data Segregation: Lattice will virtually segregate all Customer Data in accordance with its established procedures. The Customer instance of Service may be on servers used by other non-Customer instances.

4. Application-Level Requirements

a. Lattice shall maintain documentation on overall application architecture, process flows, and security features for applications handling Customer Data.

b. Lattice shall employ secure programming techniques and protocols in the development of applications handling Customer Data.

c. Lattice shall employ industry standard scanning tools and/or code review practices, as applicable, to identify application vulnerabilities prior to release.

5. Data-Level Requirements

a. Encryption and hashing protocols used for Customer Data in transit and at rest shall support NIST approved encryption standards (e.g. SSH, TLS).

b. Lattice shall ensure laptop disk encryption.

c. Lattice shall ensure that access to information and application system functions is restricted to authorized personnel only.

d. Customer Data stored on archive or backup systems shall be stored at the same level of security or better than the data stored on operating systems.

6. End User Computing Level Requirements

a. Lattice shall employ an anti-virus solution with daily signature updates for end-user computing devices which connect to the Customer network or handle Customer Data.

b. Lattice will have a policy to prohibit the use of removable media for storing or carrying Customer Data. Removable media include flash drives, CDs, and DVDs.

7. Compliance Requirements

a. Lattice will, when and to the extent legally permissible, perform criminal background verification checks on all of its employees that provide Services to Customer prior to obtaining access to Customer Data. Such background checks shall be carried out in accordance with relevant laws, regulations, and ethics.

b. Lattice will maintain an Information Security Policy (ISP) that is reviewed and approved annually at the executive level.

8. Shared Responsibility: Lattice's Service requires a shared responsibility model. For example, Customer must maintain controls over Customer user accounts (such as disabling/removing access when a Customer employee is terminated, establishing password requirements for Customer users, etc.).

9. Specific Measures:

Measure	Description
Measures of pseudonymization and encryption of personal data	• Data at rest encrypted using AES-256 algorithm. • Employee laptops are encrypted using full disk AES-256 encryption. • HTTPS encryption on every web login interface, using industry standard algorithms and certificates. • Secure transmission of credentials using by default TLS 1.2. • Access to operational environments requires use of secure protocols such as HTTPS. • Data that resides in Amazon Web Services (AWS) is encrypted at rest as stated in AWS' documentation and whitepapers. In particular, AWS instances and volumes are encrypted using AES-256. Encryption keys via AWS Key Management Service (KMS) are IAM role protected, and protected by AWS-provided HSM certified under FIPS 140-2.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	• Lattice is and shall continue to be annually audited against the SOC 2 Type II standard. The audit shall be completed by an independent third-party. Upon Customer's written request, Lattice will provide a summary copy (on a confidential basis) of the most recent resulting annual audit report, so that Customer can verify Lattice's compliance with the audit standards against which it has been assessed and this DPA. Although that report provides an independently audited confirmation of Lattice's security posture annually, the most common points of interest are further detailed below. Lattice shall provide Customer with this initial evidence of compliance within thirty (30) days of written request and annually upon written request. • Lattice shall continue to annually engage an independent, third-party to perform a web application penetration test. Upon Customer's written request, Lattice shall provide the executive summary of the report to Customer. Lattice shall address all medium, critical and severe vulnerabilities in the findings of the report within a reasonable, risk-based timeframe. Lattice shall provide Customer with this initial evidence of compliance within thirty (30) days of written request.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	• Virtual Private Network (VPN) • Strong access controls based on the use of the 'Principle of Least Privilege'. • Differentiated rights system based on security groups and access control lists. • Employee is granted only the amount of access necessary to perform job functions. • Unique accounts and role-based access within operational and corporate environments. • Access to systems restricted by security groups and access-control lists.

	• Authorization requests are tracked, logged and audited on a regular basis. • Removal of access for employee upon termination or change of employment. • Enforcement of Multi-factor Authentication (MFA) for access to critical and production resources. • Strong and complex passwords required. Initial passwords must be changed after the first login. • Passwords are never stored in clear-text and are encrypted in transit and at rest. • Account provisioning and de-provisioning processes. • Segregation of responsibilities and duties to reduce opportunities for unauthorized or unintentional modification or misuse. • Confidentiality requirements imposed on employees. • Mandatory security training for employees, which covers data privacy and governance, data protection, confidentiality, social engineering, password policies, and overall security responsibilities inside and outside of Lattice. • Non-disclosure agreements with third parties. • Separation of networks based on trust levels.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	• Event reports are enabled and available to customers in their Lattice instance. These reports can be periodically downloaded. • User activity including logins, configuration changes, deletions and updates are written automatically to audit logs in operational systems. • Certain activities on Lattice systems are not available directly to customers such as timestamps, IPs, login/logouts, and errors. These logs are available only to authorized employees, stored off-system, and available for security investigations. • All logs can be accessed only by authorized Lattice employees and access controls are in place to prevent unauthorized access. • Write access to logging data is strictly prohibited. Logging facilities and log information are protected against tampering and unauthorized access through use of access controls and security measures. • Network segmentation and interconnections protected by firewalls. • Annual penetration testing for all components of the Lattice SaaS, including web and mobile applications. • Lattice has in place a public Vulnerability Disclosure Program and a private Bug Bounty program.

Measures for user identification and authorization	• Access to operational and production environments is protected by use of unique user accounts, strong passwords, use of Multi-Factor Authentication (MFA), role-based access, and least privilege principle. • Authorization requests and provisioning is logged, tracked and audited. • Customer-generated OAuth tokens are stored in an encrypted state. • Keys required for decryption of those secrets are stored in a secure, managed repository (such as AWS KMS) that employs industry-leading hardware security models that meet or exceed applicable regulatory and compliance obligations. • Access keys used by production Lattice applications (e.g., AWS Access Keys) are accessible only to authorized personnel. They are rotated (changed) as required (e.g., pursuant to a security advisory or personnel departure) and at least yearly. • User activity in operational environments including access, modification or deletion of data is being logged
Measures for the protection of data during transmission	• HTTPS encryption for data in transit (using TLS 1.2 or greater).
Measures for the protection of data during storage	• Lattice customer instances are logically separated and attempts to access data outside allowed domain boundaries are prevented and logged. Measures are in place to ensure executable uploads, code, or unauthorized actors are not permitted to access unauthorized data - including one customer accessing files of another customer. • Endpoint security software • System inputs recorded via log files • Access Control Lists (ACL) • Multi-factor Authentication (MFA)
Measures for ensuring physical security of locations at which personal data are processed	• Physical access to all restricted facilities is documented and managed. • All information resource facilities (e.g. network closets and storerooms) are physically protected in proportion to the criticality or importance of their function. • Access to information resource facilities is granted only to company personnel and contractors whose job responsibilities require access to those facilities. • The process for granting card and/or key access to information resource facilities includes the approval of the person responsible for physical facility management. • Everyone granted access rights to an information resource facility must sign the appropriate access and non-disclosure agreements. • Access cards and/or keys must not be shared or loaned to others. • Access cards and/or keys that are no longer required are returned to the person responsible for physical facility management. Cards must not be reallocated to another individual, bypassing the return process.

	• Lost or stolen access cards and/or keys must be reported to the person responsible for physical facility management as soon as practical. • Cards and/or keys must not have identifying information coded into them. • All information resource facilities that allow access to visitors will track visitor access with a sign-in log. • Card access records and visitor logs for information resource facilities are kept for routine review based upon the criticality of the information resources being protected. • The person responsible for information resource physical facility management removes the card and/or key access rights of individuals that change roles within the organization or are separated from their relationship with the organization. • Visitors in card access-controlled areas of information resource facilities must always be accompanied by authorized personnel. • The person responsible for physical facility management reviews access records and visitor logs for the facility on a periodic basis and investigate any unusual access. • The person responsible for physical facility management reviews card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access. • Signage for restricted access rooms and locations is practical, yet minimally discernible evidence of the importance of the location is displayed. • Only individuals authorized by asset owners are permitted to move assets off-site. Details of the individual's identity and role are documented and returned with the asset. • Equipment is protected to reduce the risks from environmental threats, hazards, and opportunities for unauthorized access.
Measures for ensuring events logging	• A central Security Information and Event Management (SIEM) system and other product tools monitor security or activities
Measures for ensuring system configuration, including default configuration	• Lattice has in place a Change Management Policy. • Lattice monitors changes to in-scope systems to ensure that changes follow the process and to mitigate the risk of un-detected changes to production. Changes are tracked in our change platform. • Access Control Policy and Procedures • Mobile device management
Measures for internal IT and IT security governance and management	• Lattice has in place a written information security policy, including supporting documentation. • The authority and responsibility for managing Lattice's information security program has been delegated to the Senior Director, Security, who is authorized by senior management to take actions necessary to establish, implement, and manage Lattice's information security program.

Measures for certification/assurance of processes and products	• Lattice has been audited by a third party and has achieved SOC 2 compliance, attesting to our commitment to controls that safeguard the confidentiality and privacy of information stored and processed in our service.
Measures for ensuring data minimization	• Detailed privacy assessments are performed related to implementation of new products/services and processing of personal data by third parties. • Data collection is limited to the purposes of processing (or the data that the customer chooses to provide). • Security measures are in place to provide only the minimum amount of access necessary to perform required functions. • Data retention time limits restricted and • An automatic deletion has been implemented to enforce data retention time limits (see below on Measures for ensuring limited data retention). • All deleted customer data follows a similar retention schedule of a recoverable delete between 0-90 days and a permanent delete within 91- 180 days. • Restrict access to personal data to the parties involved in the processing in accordance with the “need to know” principle and according to the function behind the creation of differentiated access profiles.
Measures for ensuring data quality	• Lattice has a process that allows individuals to exercise their privacy rights (including a right to amend and update information), as described in Lattice's Privacy Policy. • Applications are designed to reduce/prevent duplication. Many application level checks are in place to ensure data integrity. • QA team that helps to ensure these items are working as designed and implemented before reaching our production environment.
Measures for ensuring limited data retention	• After termination of all subscriptions associated with an environment, customer data submitted to the Services is retained in inactive status within the Services for 90 days, after which it is securely overwritten or deleted from production within 90 days (up to a max of 180 days) and from backups within 180 days. • All deleted customer data follows a similar retention schedule of a recoverable delete between 0-90 days and a permanent delete within 91- 180 days.
Measures for ensuring accountability	• Customer Privacy Assessments are required when introducing any new product/service that involves processing of personal data. • Data protection impact assessments are part of any new processing initiative.
Measures for allowing data portability and ensuring erasure	• Ability to export data to in common formats • Lattice has a process that allows individuals to exercise their privacy rights (e.g. right of erasure or right to data portability), as described in Lattice's Privacy Policy.