Last Updated:
February 1, 2021

Lattice: Data Processing Addendum

THIS DATA PROCESSING ADDENDUM, including the Model Clauses and its Annexes ("DPA") forms part of and is subject to the terms and conditions of the Lattice Terms of Service or other written or electronic agreement ("**Main Agreement**") between Customer and Lattice. Each of Customer and Lattice may be referred to herein as a "**party**" and together as the "**parties**."

In the course of providing the Service to Customer under the Main Agreement, Lattice may process Customer Personal Data (defined below) on behalf of Customer and the parties agree to comply with the following provisions with respect to any processing of Customer Personal Data by Lattice. This DPA shall not replace any comparable or additional rights relating to processing of Customer Personal Data contained in the Main Agreement (including any existing data processing addendum to the Main Agreement).

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:

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

   (b) "**Business Purpose**" has the meaning attributed to in Section 1798.140(d) of the CCPA.

   (c) "**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.

   (d) "**Customer Personal Data**" means any Customer Content that: (i) relates to an identified or identifiable natural person; or (ii) that is otherwise protected as "personal data" or "personal information" (as such terms are defined in applicable Data Protection Laws), that Lattice processes on behalf of Customer in the course of providing the Service.

   (e) "**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.

   (f) "**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, GDPR (or in respect of the United Kingdom, any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data protection and privacy as a consequence of the United Kingdom leaving the European Union), implementations of the GDPR into national law, and the CCPA; in each case, as may be amended, superseded or replaced.

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

   (h) "**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).

   (i) "**Model Clauses**" means the Standard Contractual Clauses (Processors) (2010/87/EU): Commission decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593) in the form attached at Annex 3

of this DPA (as amended, replaced or superseded from time to time in accordance with this DPA).

(j) "**Security Incident**" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal 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 Personal Data, including unsuccessful login attempts, pings, port scans, denial of services attacks, and other network attacks on firewalls or networked systems.

(k) "**Subprocessor**" means any Processor having access to Customer Personal Data and engaged by Lattice to assist in fulfilling its obligations with respect to providing the Service pursuant to the Main Agreement or this DPA. Subprocessors may include third parties or Lattice Affiliates but shall exclude any employee, consultant or independent contractor of Lattice provided such individual is performing services in a capacity equivalent to those performed by employees.

(l) "**controller**", "**processor**", "**processing**" and "**personal data**" shall have the meanings given to them in Data Protection Laws or if not defined therein, the GDPR.

2. Roles and Scope of Processing

2.1 Processing Description. The type of personal data processed pursuant to this DPA and the subject matter, duration, nature and purpose of the processing, and the categories of data subjects, are as described in Annex 1 of this DPA.

2.2 Data Processing Roles. In respect of the parties' rights and obligations under this DPA regarding the Customer Personal Data, the parties acknowledge and agree that Customer is the controller (where applicable Data Protection Laws recognizes such concept) and, with respect to the CCPA, a "business" as defined therein, and Lattice is the processor (where applicable Data Protection Laws recognizes such concept) and, with respect to the CCPA, a "service provider" as defined therein.

2.3 Compliance with Laws. Lattice shall process Customer Personal Data in accordance with this DPA and Data Protection Laws applicable to its role 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.

2.4 Processing Instructions. Lattice shall process Customer Personal Data in accordance with Customer's written lawful instructions and only for the following purposes: (i) processing to provide the Service in accordance with the Main Agreement; (ii) processing to perform any steps necessary for the performance of the Main Agreement; (iii) processing initiated by Authorized Users in their use of the Service; and (iv) processing 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 (individually and collectively, the "**Permitted Purpose**"). The parties agree that the Main Agreement (including this DPA) sets out Customer's complete and final instructions to Lattice in relation to the processing of Customer Personal Data and processing outside the scope of these instructions (if any) shall require prior written agreement between Customer and Lattice.

2.5 Customer Responsibilities. Customer, as a controller or as a business, is responsible for: (i) the accuracy, quality, and legality of the Customer Personal Data, (ii) the means by which Customer acquired such Customer Personal Data; and (iii) the instructions it provides to Lattice regarding the processing of such Customer Personal 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 Personal Data pursuant to the Main Agreement and this DPA, (ii) its instructions are lawful and that the processing of Customer Personal Data in accordance with such instructions will not violate applicable Data Protection Laws, and (iii) where the CCPA applies, that the Customer Personal Data is provided to Lattice in order to perform the Service for a valid "Business Purpose" (as defined in CCPA) only.

3. Subprocessing

3.1 Authorized Subprocessors. Customer agrees to and hereby provides a general prior authorization for Lattice to engage Subprocessors. The Subprocessors currently engaged by Lattice are listed at https://www.Lattice.com/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 cause Lattice to breach any of its obligations under this DPA or the Data Protection Laws.

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

4. Security Measures and Security Incident Response

4.1 Security Measures. Lattice has implemented and will maintain appropriate technical, and organizational security measures intended to protect Customer Personal Data from Security Incidents and to preserve the security and confidentiality of the Customer Personal Data in accordance with the security measures described in Annex 2 ("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 Personal 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 Personal 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 Personal 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 Personal 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 fulfil 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 Model 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 any applicable Data Protection Laws or where a data protection authority requires under applicable Data Protection Laws, 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 Personal 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; and (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 Personal 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 Law 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 Personal 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 Personal Data, or to Customer Personal Data it has archived on back-up systems, which Customer Personal 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 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 Personal Data under the Main Agreement. 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.

8.2 Requests by Law Enforcement. As a matter of general practice, Lattice does not voluntarily provide government agencies or authorities (including law enforcement) with access to Customer Personal Data. If a government agency or authority (including law enforcement) sends Lattice a compulsory demand for Customer Personal Data (for example, through a subpoena, court order, search warrant, or other valid legal process), Lattice will: (i) inform the government agency that Lattice is a processor or service provider (as applicable of the Customer Personal Data) and (ii) attempt to redirect the law enforcement agency to request that Customer Personal Data directly from Customer. As part of this effort, Lattice may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Personal Data to a law enforcement agency, Lattice will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Lattice is legally prohibited from doing so or it has a reasonable and good-faith belief that urgent access is

necessary to prevent an imminent risk of serious harm to any individual, public safety, or Lattice's property, product, or services. Lattice shall not provide access to the Customer Personal Data until the earlier of: (a) Customer provides authorization to Lattice; (b) Lattice is informed or affirmatively learns that a protective order or other appropriate remedy is being sought or has been issued; or (c) thirty (30) days have elapsed since notice of the compulsory request to Customer and Customer has not responded.

8.3 Data Protection Impact Assessments (DPIAs). To the extent required under Data Protection Laws applicable to the EEA, 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 the EEA or the Customer Personal Data is otherwise subject to Data Protection Laws applicable to the EEA.

9.2 Processing Instructions. Without prejudice to Section 2.4 (Customer Responsibilities), Lattice shall 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 applicable Data Protection Laws.

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

9.4 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 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 were provided after the effective date of the termination.

9.5 Transfer Mechanism. To the extent that Lattice is a recipient of and processes any Customer Personal Data that originated from the EEA in a country that does not provide an adequate level of protection under applicable Data Protection Laws, the parties agree that Lattice shall abide by and process such Customer Personal Data in compliance with the Model Clauses, which are incorporated into and form an integral part of this DPA. For the purposes of the Model Clauses, the parties agree that: (i) Lattice is a "data importer" and Customer is the "data exporter" (notwithstanding that Customer may be an entity located outside the EEA); and (ii) it is not the intention of either party to contradict or restrict any of the provisions set forth in the Model Clauses and, accordingly, if and to the extent the Model Clauses conflict with any provision of the Main Agreement (including this DPA) the Model Clauses shall prevail to the extent of such conflict.

9.6 Alternative Data Transfer Arrangements. To the extent Lattice adopts an alternative data export mechanism (including any new version of or successor to the Model Clauses adopted pursuant to Data Protection Laws) for the transfer of personal data ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism shall automatically 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 the EEA and extends to territories to which Customer Personal Data is transferred).

9.7 UK Data Transfers. For the avoidance of doubt, when the European Union law ceases to apply to the UK upon the UK's withdrawal from the European Union and until such time as UK is deemed to provide adequate protection for personal data (within the meaning of applicable UK Data Protection Laws) then to the extent Lattice processes (or causes to be processed) any Customer Personal Data protected by Data Protection Laws applicable to European Economic Area and Switzerland in the United Kingdom, Lattice shall process such Customer Personal Data in compliance with the Model Clauses or any applicable Alternative Transfer Mechanism implemented in accordance with Sections 9.5 and Section 9.6 above.

10. Controller Affiliates

10.1 Affiliate Communications. Customer is responsible for coordinating all communications with Lattice on behalf of its 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 Affiliates.

10.2 Affiliate Enforcement. Customer 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 Subprocessors arising under or in connection with this DPA including: (i) for breach of this DPA; (ii) as a result of fines (administrative, regulatory or otherwise) imposed upon Customer; (iii) under GDPR (or UK GDPR), including any claims relating to damages paid to a data subject; and (iv) breach of its obligations under the Model Clauses, will 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. RESTRICTIONS

12.1 Lattice is prohibited from:

(a) selling Customer Personal Data;

(b) retaining, using, or disclosing Customer Personal Data for any purposes other than the specific purposes of performing the Service or as otherwise permitted under Main Agreement and this DPA, including retaining, using, or disclosing Customer Personal Data for a commercial purpose other than providing the Service; or

(c) retaining using or disclosing Customer Personal Data outside the direct business relationship between Lattice and Customer.

12.2 Lattice hereby certifies that it understands the restrictions set out in Section 12.1 and will comply with them.

13. General

13.1 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 Personal Data.

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

13.3 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.

13.4 This DPA does not confer any third-party beneficiary rights, it is intended for the benefit of the parties hereto, respective permitted successors and assigns only, and is not for the benefit of, nor may any provision hereof be enforced by, any other person.

13.5 Other than as required by the Model Clauses, the dispute mechanisms, including those related to venue and jurisdiction, set forth in the Main Agreement govern any dispute pertaining to this DPA.

Annex 1: Data Processing Details

Data Importer

Degree Inc., d/b/a Lattice is a provider of enterprise software as a service platform to conduct employee performance reviews and performance management, enable employee goal setting, and encourage peer-to-peer feedback between employees.

Data Exporter

A customer of Lattice's enterprise software as a service platform and related applications.

Data Subjects

The personal data transferred concern the following categories of data subjects:

Current and former employees and other workers of Customer

Categories of data

The personal data transferred concern the following categories of data:

Customer may submit personal 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 data required for people performance management: general employee information including name, email, phone number, job title, department, and direct manager as well as specific information related to the employees' professional goals, accomplishments, training and development, awards and performance.

Special categories of data (if appropriate)

The personal data transferred concern the following categories of special categories of data:

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 data which may be required for people performance management: 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.

Nature and purposes of processing

Lattice will only process personal data for the Permitted Purposes (as defined in the DPA).

Subject matter and duration of processing

The subject matter of the processing is the performance of the Service. 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.

Processing operations

The personal data transferred will be subject to the following basic processing activities:

The personal data transferred will be subject to the following basic processing activities: collection, recording, organization, structuring, storage, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data. All such activities are related to the performance of the Service as described in the Main Agreement, and as further instructed by Customer in its use of the Service.

Annex 2: Security Measures

Technical and organizational security measures to be implemented by Lattice:

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 Personal Data.

3. Hosting Requirements

a. Where Lattice handles Customer Personal 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 Personal 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 Personal Data.

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

b. Lattice will have a policy to prohibit the use of removable media for storing or carrying Customer Personal 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 Personal 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.).

Annex 3: Standard Contractual Clauses (Processors)

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to processor transfers)

Data Transfer Agreement

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Degree, Inc d/b/a/ Lattice (hereinafter the "**data importer**")

and

Customer (hereinafter the "**data exporter**")
each a "**party**"; together "**the parties**",

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

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

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

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

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

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

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

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

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

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

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

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

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

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

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

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

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

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

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

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

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

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

  (ii) any accidental or unauthorised access, and

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

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

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

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2

which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

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

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

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

Clause 6

Liability

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

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

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

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

Clause 7

Mediation and jurisdiction

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

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

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

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

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at

least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses.

The details of the transfer are specified in Annex 1 of the DPA.

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) are set forth in Annex 2 of the DPA.

Appendix 3 to the Standard Contractual Clauses

The parties acknowledge that Clause 10 of the Clause permits them to include additional business-related terms provided they do not contradict with the Clauses. Accordingly, this Appendix sets out the parties' interpretation of their respective obligations under specific Clauses identified below. Where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Clauses.

Where a party complies with the commercial interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Clauses. However, it is not the intention of either party that the commercial clauses below will have the effect of contradicting the Clauses.

Clauses 4(h) and 8: Disclosure of these Clauses

1. Data exporter agrees that these Clauses constitute data importer's Confidential Information (as that term is defined in the Main Agreement) and may not be disclosed by data exporter to any third party without data importer's prior written consent unless permitted pursuant to the Main Agreement. This shall not prevent disclosure of these Clauses to a data subject pursuant to Clause 4(h) or a supervisory authority pursuant to Clause 8.

Clause 5(a): Suspension of data transfers and termination

1. The parties acknowledge that data importer may process the personal data only on behalf of the

data exporter and in compliance with its instructions as set out in the DPA and that pursuant to the DPA, these instructions shall be the data exporter's complete and final instructions.

2. The parties acknowledge that if data importer cannot provide such compliance for whatever reason, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the affected parts of the Service in accordance with the terms of the Main Agreement.

3. If the data exporter intends to suspend the transfer of personal data and/or terminate the affected parts of the Service, it shall first provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("**Cure Period**").

4. In addition, the data exporter and data importer shall reasonably cooperate with each other during the Cure Period to agree what additional safeguards or other measures, if any, may be reasonably required to ensure the data importer's compliance with the Clauses and applicable data protection law.

5. If after the Cure Period, the data importer has not or cannot cure the non-compliance then the data exporter may suspend or terminate the affected part of the Service in accordance with the provisions of the Main Agreement without liability to either party (but without prejudice to any fees incurred by the data exporter prior to suspension or termination).

Clause 5(f): Audit

1. Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) by instructing data importer to comply with the audit measures described in Section 5 (Audit and Records) of the DPA to which these Clauses are appended.

Clause 5(j): Disclosure of subprocessor agreements

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.

2. The parties further acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be contractually limited from disclosing certain aspects of onward subprocessor agreements to data exporter.

3. Even where data importer cannot disclose the entirety of a subprocessor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably can in connection with such subprocessing agreement to data exporter.

Clause 6: Liability

1. Any claims brought under the Clauses shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Main Agreement. In no event shall any party limit its liability to a data subject with respect to any data subject rights under these Clauses.

Clause 11: Onward subprocessing

1. The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "*FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC*" the data exporter may provide a general consent to onward subprocessing by the data importer.

2. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward subprocessors. Such consent is conditional on data importer's compliance with the subprocessing requirements set out in the DPA.