LatticeTechnical and Organisational 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 pseudonymisation 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 or higher. • Access to operational environments requires use of secure protocols such as HTTPS. • Data that resides in Amazon Web Services (AWS) 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 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 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 trainings 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 organisational measures in order to ensure the security of the processing	• Event reports are enabled. These reports are periodically reviewed by Lattice. • 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 authorisation	• 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. 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 • 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 asign-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 is 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 Head of Security and IT, 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 minimisation	• 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 returned and/or deleted in accordance with the customer contract 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.