COMPLINITY DATA PROCESSING ADDENDUM

Last Updated: February 2026

1. PURPOSE AND SCOPE

This Data Processing Addendum ("**DPA**") forms part of the Complinity Terms of Service, Master Services Agreement, or any other written or electronic agreement, including any service orders, purchase orders, or order forms (collectively, the "**Agreement**"), entered into between **Complinity Technologies Pvt. Ltd**. ("**Complinity**", "**Processor**") and the customer entering into the Agreement ("Customer", "Controller").

Under the Agreement, Complinity provides access to its compliance management software platform and related services (the "**Services**").

The purpose of this DPA is to set out the parties' respective rights and obligations with respect to the Processing of Personal Data by Complinity on behalf of the Customer, including any international or cross-border transfers, in accordance with:

- Regulation (EU) 2016/679 (**General Data Protection Regulation – GDPR**);
- Applicable EU Member State data protection laws; and
- Applicable Indian data protection laws.

For the avoidance of doubt, applicable Indian data protection laws include the **Digital Personal Data Protection Act, 2023** ("**DPDP Act**), together with all rules, notifications, directions, and amendments issued thereunder from time to time.

This DPA shall take effect on the date on which it is accepted by or becomes binding upon the Customer ("DPA Effective Date") and shall remain in force for the duration of the Agreement. Notwithstanding termination or expiry of the Agreement, this DPA shall continue to apply until all Customer Data has been deleted or returned in accordance with this DPA.

This DPA incorporates by reference the **Standard Contractual Clauses** annexed as **Exhibit 1**, together with:

(i) **Appendix 1** (Description of the Transfer)

(ii) **Appendix 2** (Technical and Organisational Security Measures)

(iii) **Appendix 3** (List of Sub-Processors)

2. DEFINITIONS

For the purposes of this DPA, the following terms shall have the meanings set out below. Capitalised terms not defined in this Section shall have the meanings given to them in the Agreement, the GDPR, or the DPDP Act, as applicable.

1) "**Controller**" means the Customer, as the entity that determines the purposes and means of the Processing of Personal Data.
2) "**Customer Data**" means any information, data, or material submitted to, stored in, generated by, or otherwise processed through the Services by or on behalf of the Customer, including Personal Data.
3) "**Data Subject**" (or "Data Principal", where applicable under the DPDP Act) means an identified or identifiable natural person to whom Personal Data relates.
4) "**DPA Effective Date**" means the date on which this DPA is accepted by or becomes binding upon the Customer, including through execution of the Agreement or use of the Services.
5) "**EU Data Protection Laws**" means the GDPR and all applicable laws of EU Member States implementing, supplementing, or replacing the GDPR, as amended from time to time.
6) "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council.
7) "**Instructions**" means the documented instructions issued by the Controller to the Processor regarding the Processing of Personal Data, including as set out in the Agreement, this DPA, and any written instructions provided by the Controller from time to time.
8) "**Personal Data**" means any information relating to an identified or identifiable natural person that is contained within Customer Data and processed by Complinity on behalf of the Customer.
9) "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data.

10) "**Processing**" means any operation or set of operations performed on Personal Data, whether or not by automated means, as defined under Article 4(2) of the GDPR.
11) "**Processor**" means Complinity Technologies Pvt. Ltd., acting as a data processor under the GDPR and as a data processor under the DPDP Act, as applicable.
12) "**Standard Contractual Clauses**" or "**SCCs**" means the standard contractual clauses adopted by the European Commission pursuant to Commission Decision (EU) 2021/914, Module 2 (Controller to Processor), as may be amended or replaced from time to time.

3. DETAILS OF THE PROCESSING

3.1 CATEGORIES OF DATA SUBJECTS.

Depending on the Customer's use of the Services, Personal Data processed may relate to:

- Employees, directors, officers, and authorised users of the Customer;
- Contractors, consultants, auditors, and advisors engaged by the Customer;
- Vendors, suppliers, and other third parties whose details are entered into the Services by the Customer; and
- Individuals whose information forms part of statutory, regulatory, or compliance records managed through the Services.

3.2 TYPES OF PERSONAL DATA

Depending on the Customer's configuration and use of the Services, Personal Data may include:

- Identification and contact information;
- Compliance roles, assignments, and workflow-related data;
- System usage data, audit trails, logs, and timestamps;
- Documents, records, and other content uploaded by or on behalf of the Customer; and
- Application-generated metadata.

The Services are **not intended** to process special categories of Personal Data as defined under Article 9 of the GDPR, and the Customer agrees not to intentionally provide such data through the Services.

3.3 SUBJECT-MATTER AND NATURE OF THE PROCESSING

The Processing consists of the hosting, storing, organising, structuring, retrieving, transmitting, and deleting of Personal Data as necessary to provide the Services in accordance with the Agreement, through a secure, cloud-based software-as-a-service (SaaS) platform.

3.4 PURPOSE OF THE PROCESSING.

Personal Data shall be processed solely for the purposes of providing, maintaining, supporting, and improving the Services, as set out in the Agreement and any applicable Order Form, and in accordance with the Customer's documented Instructions.

3.5 DURATION OF THE PROCESSING

Personal Data shall be processed for the duration of the Agreement and any active Customer licence, subject to the deletion and retention provisions set out in **Section 9 (Deletion or Return of Personal Data)** of this DPA.

3.6 DATA STORAGE LOCATION

Complinity processes and stores all Customer Data **within India**, using cloud infrastructure provided by Amazon Web Services (AWS), as follows:

- **Primary processing region:** AWS Mumbai (ap-south-1)
- **Backup and disaster recovery region:** AWS Hyderabad (ap-south-2)

Complinity maintains appropriate technical and organisational measures to ensure the confidentiality, integrity, and availability of Customer Data within these regions.

If Complinity proposes to change the location of Processing or storage of Customer Data, it shall notify the Customer at least **thirty (30)** days in advance and ensure that any such change complies with applicable data protection laws and this DPA.

4. CUSTOMER RESPONSIBILITY

4.1 Compliance with Data Protection Laws

Within the scope of the Agreement and its use of the Services, the Customer, acting as Controller (and Data Fiduciary where applicable), is responsible for complying with all applicable data protection and privacy laws with respect to the disclosure, transfer, and Processing of Personal Data provided to Complinity.

> Without limiting the foregoing, the Customer warrants that its documented Instructions for the Processing of Personal Data comply with all applicable laws and regulations, including the GDPR and applicable Indian data protection laws.

4.2 Instructions to Complinity

The Customer's Instructions for Processing shall be as set out in the Agreement, this DPA, and any applicable Order Form. The Customer may amend, supplement, or replace such Instructions from time to time by providing documented written instructions to Complinity, provided that such Instructions are lawful and technically feasible.

4.3 Accuracy and Updates of Personal Data

The Customer shall inform Complinity without undue delay of any errors, inaccuracies, required corrections, or other issues relating to the Personal Data or the applicable legal basis for Processing, and shall take reasonable steps to ensure that Personal Data provided to Complinity is accurate and up to date.

5. OBLIGATIONS OF PROCESSOR

5.1 Processing on Documented Instructions

The parties acknowledge that the Customer acts as the Controller (and Data Fiduciary, where applicable) and that Complinity acts as the Processor (and Data Processor, where applicable).

Complinity shall process Personal Data only on the basis of documented Instructions from the Customer, including as set out in the Agreement, this DPA, and any applicable Order Form.

Where Complinity reasonably believes that an Instruction infringes applicable data protection laws, it shall promptly inform the Customer. Where Complinity is required by applicable law to process Personal Data in a manner inconsistent with the Customer's Instructions, Complinity shall notify the Customer of such legal requirement to the extent permitted by law and shall limit Processing to what is legally required.

5.2 Security of Processing

Complinity shall implement and maintain appropriate technical and organisational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data.

Such measures are described in Appendix 2 and include, as appropriate:

- physical and logical access controls;
- user access management and authorisation controls;
- encryption and secure transmission mechanisms;
- audit logging and monitoring;
- protection against data loss and unauthorised modification; and
- availability, resilience, and disaster recovery controls.

Complinity shall consider the state of the art, costs of implementation, and the nature, scope, context, and purposes of the Processing, and shall assist the Customer in meeting its own security obligations under applicable data protection laws.

5.3 Confidentiality

Complinity shall ensure that all personnel authorised to process Personal Data are subject to appropriate confidentiality obligations, whether contractual or statutory, which shall survive termination of their engagement or of the Processing activities.

5.4 Personal Data Breaches

Complinity shall notify the Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Data. Where the GDPR applies, such notification shall be made no later than **twenty-four (24) hours** after awareness, unless a longer period is permitted by applicable law.

Complinity shall provide reasonable assistance to the Customer to enable compliance with breach notification obligations under applicable data protection laws and shall take appropriate measures to mitigate the effects of the Personal Data Breach and prevent its recurrence.

5.5 Data Subject and Data Principal Requests

Considering the nature of the Processing, Complinity shall provide reasonable assistance to enable the Customer to respond to requests from Data Subjects or Data Principals exercising their rights under applicable data protection laws, including:

- access, rectification, erasure, restriction, portability (GDPR); and
- access, correction, erasure, grievance redressal, consent withdrawal, and nomination (DPDP Act).

If Complinity receives such a request directly, it shall promptly inform the Customer and shall not respond directly unless required by law. Any reasonable costs incurred by Complinity in providing such assistance may be borne by the Customer, as agreed under the Agreement.

5.6 Sub-Processors

1. The Customer authorises Complinity to engage the sub-processors listed in Appendix 3 for the provision of the Services.
2. Complinity may engage additional sub-processors by providing prior written notice to the Customer and allowing the Customer thirty (30) days to object on reasonable data protection grounds. If the parties are unable to resolve such objection, either party may terminate the affected Services.
3. Complinity shall enter into a written agreement with each sub-processor imposing data protection obligations materially equivalent to those set out in this DPA.
4. Complinity shall remain fully liable for the acts and omissions of its sub-processors in accordance with this DPA and applicable law.

5.7 International Data Transfers

To the extent Personal Data originating in the European Economic Area is processed outside the EEA, including in India, such transfers shall be governed by the **Standard Contractual Clauses (Module 2)** set out in Exhibit 1.

Where required by EU Data Protection Laws, Complinity shall conduct and document a **Transfer Impact Assessment (TIA)** and shall implement supplementary technical and organisational measures as appropriate.

5.8 Deletion or Return of Personal Data

5. During the term of an active Customer licence, Personal Data shall be retained to provide the Services.
6. Upon termination or expiry of the Agreement, and subject to applicable law, Complinity shall, within thirty **(30) days,** delete or return Customer Data in accordance with the Customer's documented Instructions.
7. Complinity may retain Personal Data, audit logs, system logs, and compliance records to the extent required for statutory, regulatory, or contractual purposes, including retention of logs for a minimum period of **four (4) years**, after which such data shall be deleted or de-identified in accordance with documented retention policies.

6. AUDITS

6.1 Audit Rights

The Customer may, no more than **once in any twelve (12) month period**, audit Complinity's compliance with this DPA and applicable data protection laws, provided that such audit:

- is conducted on at least **thirty (30) days' prior written notice**;
- is limited to information and systems relevant to the Processing of Customer Data; and
- does not unreasonably interfere with Complinity's business operations.

6.2 Audit Methods

Audits shall, in the first instance, be satisfied by one or more of the following, at the Customer's choice:

- written responses to reasonable information requests;
- review of Complinity's relevant policies, procedures, and controls; or
- review of independent third-party attestations or certifications (including ISO or SOC reports), where available.

On-site audits may be conducted only where the above measures are insufficient to demonstrate compliance and must be carried out during regular business hours by a qualified, independent auditor that is not a competitor of Complinity.

6.3 Costs and Confidentiality

All costs associated with an audit, including third-party professional fees, shall be borne by the Customer. Any information disclosed in connection with an audit shall be treated as Confidential Information under the Agreement.

6.4 Cooperation

Complinity shall provide reasonable cooperation and information necessary to demonstrate compliance with this DPA, to the extent such information is within Complinity's control and not restricted by applicable law, contractual obligations, or duties of confidentiality owed to third parties.

7. INDEMNIFICATION

Each party shall be responsible for, and shall indemnify the other party against, claims, losses, damages, liabilities, costs, and expenses (including reasonable legal fees) arising out of its own breach of this DPA or applicable data protection laws, subject to the liability limitations set out in the Agreement and to the extent permitted by law.

For the avoidance of doubt:

- Complinity shall not be liable for claims arising from Processing carried out in accordance with the Customer's lawful Instructions; and
- The Customer shall not be liable for claims arising solely from Complinity's failure to comply with this DPA or applicable data protection laws.

8. GENERAL PROVISIONS

1) General provisions of the Agreement shall, in so far as they are not inconsistent herewith, apply to this DPA.
2) In case of any conflict between the terms of this DPA and the Agreement, the terms of this DPA shall take precedence in so far as the subject matter to which it relates. Where individual provisions of this DPA are invalid or unenforceable, the validity and enforceability of the other provisions of this DPA shall not be affected.

9. OTHERS

9.1 Assistance with Compliance Obligations

Complinity shall provide reasonable assistance to the Customer in meeting its obligations as Controller or Data Fiduciary under applicable data protection laws, including the GDPR and the Digital Personal Data Protection Act, 2023, considering the nature of the Processing and the information available to Complinity.

9.2 Privacy by Design and Security

Complinity implements appropriate technical and organisational measures designed to ensure privacy by design and by default, and to achieve a level of security of Processing appropriate to the risks associated with the Processing of Personal Data.

9.3 Breach Notification Support

Complinity shall support the Customer in complying with applicable breach notification obligations to supervisory authorities, Customers, and Data Subjects or Data Principals, as required under applicable data protection laws and as further set out in this DPA.

9.4 Impact Assessments and Regulatory Consultations

Where required under applicable data protection laws, Complinity shall provide reasonable assistance to the Customer in connection with data protection impact assessments and, where applicable, prior consultations with competent data protection authorities.

9.5 Lawfulness of Instructions

Complinity shall notify the Customer without undue delay if, in its reasonable opinion, an Instruction infringes applicable data protection laws or regulations.

9.6 Use Limitation

Complinity shall not process Personal Data for purposes of marketing, advertising, or any purpose other than providing the Services and fulfilling its obligations under the Agreement and this DPA.

9.7 Audit Cooperation

Complinity shall coordinate with the Customer and provide reasonable information necessary to enable the Customer to demonstrate compliance with its data protection obligations, subject to the audit provisions set out in Section 6 (Audits).

9.8 Use of Cloud Infrastructure and Sub-Processors

The Customer acknowledges that Complinity uses reputable cloud service providers, including Amazon Web Services (AWS), as sub-processors, in accordance with the security and privacy requirements set out in this DPA and Appendix 3.

9.9 Standards Alignment

Complinity maintains its information security and privacy management practices aligned with the principles of ISO/IEC 27001:2022 and ISO/IEC 27701:2019, as well as applicable statutory and regulatory data protection requirements.

9.10 Data Deletion and Retention

Personal Data shall be deleted or de-identified following completion of the Processing, subject to applicable statutory, regulatory, contractual, and documented retention requirements, as further described in this DPA.

9.11 Government and Law Enforcement Requests

Complinity shall notify the Customer promptly, and where legally permitted prior to disclosure, of any legally binding request for access to or disclosure of Personal Data by a competent authority.

9.12 Data Protection Contact

Where required under applicable law, the Customer may contact Complinity's data protection contact for matters relating to Personal Data:

Name: Neera Singh
Email: neera.singh@complinity.com
Phone: +91-8800499040

complinity™

EXHIBIT 1

STANDARD CONTRACTUAL CLAUSES

MODULE 2 (Controller → Processor) – COMMISSION DECISION (EU) 2021/914

SECTION I – GENERAL PROVISIONS

Clause 1 – Purpose and Scope

1. These Standard Contractual Clauses (the "Clauses") apply to the transfer of Personal Data by the data exporter, acting as Controller, to the data importer, acting as Processor, where such transfer is subject to Regulation (EU) 2016/679 ("GDPR") and involves a transfer of Personal Data to a third country not recognised by the European Commission as providing an adequate level of protection.
2. These Clauses are intended to provide appropriate safeguards, enforceable rights, and effective legal remedies for Data Subjects in accordance with Articles 44–46 and 49 GDPR.
3. These Clauses shall apply only to the extent that Personal Data originating in the European Economic Area ("EEA") is transferred to the data importer outside the EEA.

Clause 2 – Effect and Invariability of the Clauses

4. These Clauses set out appropriate safeguards for the protection of Personal Data and shall be binding on the Parties.

5. The Parties may not modify or contradict these Clauses, except to:
   - select options expressly permitted by the Clauses; or
   - add information to the Annexes, provided such additions do not contradict or undermine the Clauses.

6. Where the Clauses are incorporated into a broader commercial contract or data processing agreement, the Clauses shall prevail in case of conflict with respect to international data transfers.

Clause 3 – Third-Party Beneficiaries

1. Data Subjects may invoke and enforce the following Clauses as third-party beneficiaries:
   - Clause 8 (except Clause 8.7),
   - Clauses 10, 11, 12, 13,
   - Clauses 14 and 15,
   - Clause 16.
2. This shall be without prejudice to the rights of Data Subjects under GDPR.

Clause 4 – Interpretation

1. Where these Clauses use terms defined in GDPR, those terms shall have the same meaning.
2. These Clauses shall be read and interpreted in light of GDPR and shall not restrict or prejudice any rights granted to Data Subjects under applicable data protection laws.

Clause 5 – Hierarchy

In the event of any inconsistency between these Clauses and the provisions of any other agreement between the Parties, including the Data Processing Addendum ("DPA") or the Master Services Agreement, these Clauses shall prevail with respect to matters concerning international transfers of Personal Data.

Clause 6 – Description of the Transfer

The details of the transfer, including:

- the categories of Data Subjects,
- the categories of Personal Data,
- the nature and purpose of Processing,
- the frequency and duration of Processing,

are specified in Annex I, which forms an integral part of these Clauses.

Clause 7 – Docking Clause

This Clause is not used.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 – Data Protection Safeguards

8.1 Instructions

1. The data importer shall process Personal Data only on documented instructions from the data exporter, including with regard to onward transfers, unless required to do so by applicable Union or Member State law.
2. Where the data importer is required by law to process Personal Data otherwise than in accordance with the instructions, it shall inform the data exporter of that legal requirement prior to processing, unless prohibited by law.

8.2 Purpose Limitation

The data importer shall process Personal Data solely for the specific purposes described in Annex I and shall not process Personal Data in a manner incompatible with those purposes.

8.3 Transparency

The data importer shall assist the data exporter in meeting its obligations under Articles 12–14 GDPR, including by providing information necessary to ensure transparent Processing of Personal Data.

8.4 Accuracy

Where relevant to the Processing, the data importer shall take reasonable steps to ensure that Personal Data is accurate and kept up to date, including by implementing mechanisms for correction or deletion where appropriate.

8.5 Duration of Processing and Erasure or Return

1. Processing shall continue only for the duration specified in Annex I.
2. Upon termination or expiry of the Services, the data importer shall, at the choice of the data exporter, delete or return all Personal Data, unless retention is required by applicable law.
3. Where retention is required by law, the data importer shall ensure continued confidentiality and shall not further process the retained Personal Data.

8.6 Security of Processing

1. The data importer shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including measures to protect against:
   - accidental or unlawful destruction,
   - loss,
   - alteration,
   - unauthorised disclosure or access.
2. The security measures are described in Annex II and shall take into account the state of the art, implementation costs, and the nature, scope, context, and purposes of Processing.

8.7 Sensitive Data

The Parties do not intend to transfer special categories of Personal Data under Article 9 GDPR. Where such data is transferred inadvertently, enhanced safeguards shall apply.

8.8 Onward Transfers

1. The data importer shall not engage another processor without prior authorisation of the data exporter.
2. Where a sub-processor is engaged, the data importer shall ensure that the sub-processor is bound by obligations equivalent to those set out in these Clauses.
3. The data importer shall remain fully liable for the performance of sub-processors.

8.9 Documentation and Compliance

The data importer shall make available to the data exporter all information necessary to demonstrate compliance with these Clauses and shall allow for audits in accordance with the DPA.

8.10 Data Subject Rights

The data importer shall assist the data exporter, by appropriate technical and organisational measures, in responding to requests from Data Subjects exercising their rights under GDPR.

Clause 9 – Use of Sub-Processors

Sub-processing shall be permitted only in accordance with the DPA and Annex III.

Clause 10 – Data Subject Rights

Data Subjects may exercise their rights under GDPR and these Clauses directly against the data exporter and, where applicable, the data importer.

Clause 11 – Redress

The data importer shall inform Data Subjects of a contact point and cooperate in good faith with supervisory authorities.

Clause 12 – Liability

Each Party shall be liable for damages caused by its breach of these Clauses, subject to the liability limitations set out in the Agreement, to the extent permitted by law.

Clause 13 – Supervision

The supervisory authority of the EU Member State in which the data exporter is established shall act as the competent supervisory authority.

SECTION III – LOCAL LAWS AND ACCESS BY PUBLIC AUTHORITIES

Clause 14 – Local Laws and Practices Affecting Compliance

1. The data importer represents that it has no reason to believe that the laws and practices of the destination country prevent it from fulfilling its obligations under these Clauses.
2. The data importer shall notify the data exporter if this representation can no longer be maintained.

Clause 15 – Obligations in Case of Access Requests

1. The data importer shall notify the data exporter of any legally binding request for disclosure of Personal Data, where legally permitted.
2. The data importer shall challenge any request that it believes to be unlawful or disproportionate.
3. The data importer shall document and make available information regarding access requests upon reasonable request.

SECTION IV – FINAL PROVISIONS

Clause 16 – Non-Compliance and Termination

In the event of non-compliance, the data exporter may suspend data transfers or terminate the Agreement without penalty.

Clause 17 – Governing Law

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

Clause 18 – Choice of Forum

Disputes arising from these Clauses shall be resolved before the courts of the EU Member State in which the data exporter is established.

APPENDIX 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

1. **Data exporter**
   The data exporter is the Customer, as defined in the Complinity Customer Terms of Service ("**Agreement**").
2. **Data importer**
   The data importer is Complinity – India's Leading Compliance Software
3. **Data subjects**
   Categories of data subjects set out under Section 2 of the Data Processing Addendum to which the Clauses are attached.
4. **Categories of data**
   Categories of personal data set out under Section 2 of the Data Processing Addendum to which the Clauses are attached.
5. **Special categories of data (if appropriate)**
   The parties do not anticipate the transfer of special categories of data.
6. **Processing operations**
   The processing activities set out under Section 2 of the Data Processing Addendum to which the Clauses are attached.

Appendix 2 to the Standard Contractual Clauses (Technical and Organizational Security Measures)

This Appendix forms part of the Clauses.

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Complinity currently observes the security practices described in this Appendix 2. Notwithstanding any provision to the contrary otherwise agreed to by data exporter,

Complinity may modify or update these practices at its discretion provided that such modification and update does not result in a material degradation in the protection offered by these practices. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the Agreement.

a) Access Control

- Preventing Unauthorized Product Access Outsourced processing: Complinity hosts its Services with outsourced cloud infrastructure providers. Additionally, Complinity maintains contractual relationships with vendors in order to provide the Services in accordance with our Data Processing Addendums. Complinity relies on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors. Physical and environmental security: Complinity hosts its product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are aligned with SOC 2 Type II and ISO 27001, among other standards. Authentication: Complinity implements a uniform password policy for its customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public Customer Data. Authorization: Customer data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of Complinity's products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set. Application Programming Interface (API) access: Public product APIs may be accessed over secured socket layer (SSL) or Transport Layered Security (TLS) based HTTPS using and security API key only.
- Preventing Unauthorized Product Use

Complinity implements industry standard access controls and detection capabilities for the internal networks that support its products. Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules. Intrusion detection and prevention: As part of its commitment to protecting customer data and websites, access to Complinity is aligned with best practice guidelines documented by the Open Web Application Security Project (OWASP) in

the OWASP Top 10 and similar recommendations. Protections from Distributed Denial of Service (DDoS) attacks are also incorporated, helping to ensure that customers' sites and other parts of the Complinity products are available continuously. Complinity is configured with a combination of industry standard and custom rules that are capable of automatically enabling and disabling appropriate controls to best protect our customers. We employ tools that actively monitor real-time traffic at the application layer with ability to alert or deny malicious behaviour based on behaviour type and rate. Static code analysis: Security reviews of code stored in Complinity's source code repositories is performed, checking for coding best practices and identifiable software flaws. Penetration testing: Complinity maintains relationships with industry recognized penetration testing service providers for penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

- Limitations of Privilege & Authorization Requirements Product access: A subset of Complinity's employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through "just in time" requests for access; all such requests are logged. Background checks: All Complinity employees undergo a third-party background check prior to being extended an employment offer, in accordance with the applicable laws. All employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

b) Transmission Control

In-transit: Complinity makes HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces. Complinity's HTTPS implementation uses industry standard algorithms and certificates.

All sensitive interactions with the Complinity products (e.g., API calls, login, authenticated sessions to the customer's portal, etc.) are encrypted in-transit with TLS 1.2.

Certain information is encrypted or hashed at rest, based on the sensitivity of the information. For instance, user passwords are hashed. Contact Data like Lead information is encrypted at rest. Other information, like public web content, images, documents are not encrypted at rest.

c) Input Control

Detection: Complinity designed its infrastructure to log extensive information about the system behaviour, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. Complinity personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: Complinity maintain a security incident response and tracking mechanism. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, Complinity will take appropriate steps to minimize product and Customer damage or unauthorized disclosure.

Communication: If Complinity becomes aware of unlawful access to customer data stored within its products, Complinity will: 1) notify the affected customers of the incident; 2) provide a description of the steps Complinity is taking to resolve the incident; and 3) provide status updates to the Customer contact, as Complinity deems necessary. Notification(s) of incidents, if any, will be delivered to one or more of the Customer's contacts in a form Complinity selects, which may include via email or telephone.

d) Availability Control

Complinity maintains business continuity and disaster recovery plans focusing both on preventing outage through redundancy of telecommunications, systems, and business operations, and on rapid recovery strategies in the event of an availability or performance issue. Whenever customer-impacting situations occur, Complinity's goal is to quickly and transparently isolate and address the issue. Identified issues are published on Complinity's status site and are subsequently updated until the issue is resolved.

Business continuity testing is part of Complinity normal processing. Complinity recovery processes are validated continuously through normal maintenance and support processes. We follow continuous deployment principles and create or destroy many server instances as part

of our regular daily maintenance and growth. We also use those procedures to recover from impaired instances and other failures, allowing us to practice our recovery process every day.

Complinity primarily relies on infrastructure redundancy, real time replication and backups. All Complinity product services are built with full redundancy. Server infrastructure is strategically distributed across 2 distinct availability zones within our data centre provider.

Complinity ensures data is replicated and backed up in multiple durable data-stores. The retention period of backups depends on the nature of the data. Data is also replicated across data-centre availability zones in order to provide fault-tolerance within an availability zone as well as scalability and responsive recovery, when necessary. In addition, the following policies have been implemented and enforced for data resilience:

- Customer (production) data is backed up leveraging multiple online replicas of data for immediate data protection. All production databases have no less than 1 primary (master) and 1 replica (slave) copy of the data live at any given point in time. Ten days' worth of backups are kept for any database in a way that ensures restoration can occur easily.
- Because we leverage private cloud services for hosting, backup, and recovery, Complinity does not implement physical infrastructure or physical storage media within its products. Complinity does also not generally produce or use other kinds of hard copy media (e.g., paper, tape, etc.) as part of making our products available to our customers.
- By default, all backups will be protected through access control restrictions on Complinity product infrastructure networks, access control lists on the file systems storing the backup files and/or through database security protections.

Appendix 3 to the Standard Contractual Clauses (List of Sub-Processor)

- Amazon Web Services, Inc.
  - Primary Server geographical location – AWS Mumbai region (ap-south-1)
  - Backup Server geographical location – AWS Hyderabad region (ap-south-2)

- CloudThat
  - Geographical location – Bengaluru, Karnataka, India

- TrueCopy
  - Geographical location – Pune, Maharashtra, India