Data Processing Addendum

2026-01-28 - India

This Data Processing Addendum ("DPA") sets forth the terms and conditions relating to the Processing of Client Personal Data. This DPA constitutes an Attachment to the Agreement and is entered into by the parties in accordance with Section 5.3.2 of the SaaS GTC regarding the processing of European Data. Capitalized terms not defined in this DPA shall have the meanings given in the SaaS GTC or the DPA Setup Page.

1. Definitions.

1.1. "**Audit**" and "**Audit Parameters**" are defined in Section 9.3 below.

1.2. "**Audit Report**" is defined in Section 9.2 below.

1.3. "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data.

1.4. "**Client Instructions**" is defined in Section 3.1 below.

1.5. "**Client Personal Data**" means Personal Data in Client Data (as defined in the Agreement).

1.6. "**Data Protection Laws**" means all laws and regulations applicable to the Processing of Client Personal Data under the Agreement, including, as applicable: (i) the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and any binding regulations promulgated thereunder ("**CCPA**"), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**" or "**GDPR**"), (iii) the Swiss Federal Act on Data Protection ("**FADP**"), (iv) the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**") and (v) the UK Data Protection Act 2018, and (vi) the Digital Personal Data Protection Act, 2023 (India); in each case, as updated, amended or replaced from time to time.

1.7. "**Data Subject**" means the identified or identifiable natural person to whom Client Personal Data relates.

1.8. "**DPA Effective Date**" is specified on the DPA Setup Page.

1.9. "**DPA Setup Page**" means a separate document executed by Client and Optel which causes this DPA to become an Attachment to their Agreement.

1.10. "**EEA**" means European Economic Area.

1.11. "**Personal Data**" means information about an identified or identifiable natural person or which otherwise constitutes "personal data", "personal information", "personally identifiable information" or similar terms as defined in Data Protection Laws.

1.12. "**Processing**" and inflections thereof refer to any operation or set of operations that is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use,

disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.13. "**Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

1.14. "**Restricted Transfer**" means: (i) where EU GDPR applies, a transfer of Client Personal Data from the EEA to a country outside the EEA that is not subject to an adequacy determination, (ii) where UK GDPR applies, a transfer of Client Personal Data from the United Kingdom to any other country that is not subject to an adequacy determination or (iii) where FADP applies, a transfer of Client Personal Data from Switzerland to any other country that is not subject to an adequacy determination.

1.15. "**Schedules**" means one or more schedules incorporated by the parties in their DPA Setup Page. The default Schedules for this DPA are:

Schedule 1	Subject Matter and Details of Processing
Schedule 2	Technical and Organizational Measures
Schedule 3	Cross-Border Transfer Mechanisms
Schedule 4	Region-Specific Terms

1.16. "**Security Incident**" means any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Client Personal Data being Processed by Optel.

1.17. "**Specified Notice Period**" is 72 hours.

1.18. "**Subprocessor**" means any third party authorized by Optel to Process any Client Personal Data.

1.19. "**Subprocessor List**" means the list of Optel's Subprocessors as identified or linked to on the DPA Setup Page.

2. Scope and Duration.

2.1. Roles of the Parties. This DPA applies to Optel as a Processor of Client Personal Data and to Client as a Controller or Processor of Client Personal Data.

2.2. Scope of DPA. This DPA applies to Optel's Processing of Client Personal Data under the Agreement to the extent such Processing is subject to Data Protection Laws. This DPA is governed by the governing law of the Agreement unless otherwise required by Data Protection Laws.

2.3. Duration of DPA. This DPA commences on the **DPA Effective Date** and terminates upon expiration or termination of the Agreement (or, if later, the date on which Optel has ceased all Processing of Client Personal Data).

2.4. Order of Precedence. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) any Standard Contractual Clauses or other measures to which the parties have agreed in Schedule 3 (Cross-Border Transfer Mechanisms) or Schedule 4 (Region-Specific Terms), (2) this DPA and (3) the Agreement. To the fullest extent permitted by Data Protection Laws, any claims brought in connection with this DPA (including its Schedules) will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations, set forth in the Agreement.

3. Processing of Personal Data.

3.1. Client Instructions.

(a) Optel will Process Client Personal Data as a Processor only: (i) in accordance with Client Instructions or (ii) to comply with Optel's obligations under applicable laws, subject to any notice requirements under Data Protection Laws.

(b) "**Client Instructions**" means: (i) Processing to provide the Cloud Services and perform Optel's obligations in the Agreement (including this DPA) and (ii) other reasonable documented instructions of Client consistent with the terms of the Agreement.

(c) Details regarding the Processing of Client Personal Data by Optel are set forth in Schedule 1 (Subject Matter and Details of Processing).

(d) Optel will notify Client if it receives an instruction that Optel reasonably determines infringes Data Protection Laws (but Optel has no obligation to actively monitor Client's compliance with Data Protection Laws).

3.2. Confidentiality.

(a) Optel will protect Client Personal Data in accordance with its confidentiality obligations as set forth in the Agreement.

(b) Optel will ensure personnel who Process Client Personal Data either enter into written confidentiality agreements or are subject to statutory obligations of confidentiality.

3.3. Compliance with Laws.

(a) Optel and Client will each comply with Data Protection Laws in their respective Processing of Client Personal Data.

(b) Client will comply with Data Protection Laws in its issuing of Client Instructions to Optel. Client will ensure that it has established all necessary lawful bases under Data Protection Laws to enable Optel to lawfully Process Client Personal Data for the purposes contemplated by the Agreement (including this DPA), including, as applicable, by obtaining all necessary consents from, and giving all necessary notices to, Data Subjects.

3.4. Changes to Laws. The parties will work together in good faith to negotiate an amendment to this DPA as either party reasonably considers necessary to address the requirements of Data Protection Laws from time to time.

4. Subprocessors.

4.1. Use of Subprocessors.

(a) Client generally authorizes Optel to engage Subprocessors to Process Client Personal Data. Client further agrees that Optel may engage its Affiliates as Subprocessors.

(b) Optel will: (i) enter into a written agreement with each Subprocessor imposing data Processing and protection obligations substantially the same as those set out in this DPA and (ii) remain liable for compliance with the obligations of this DPA and for any acts or omissions of a Subprocessor that cause Optel to breach any of its obligations under this DPA.

4.2. Subprocessor List. Optel will maintain an up-to-date list of its Subprocessors, including their functions and locations, as specified in the **Subprocessor List**.

4.3. Notice of New Subprocessors. Optel may update the **Subprocessor List** from time to time. At least 30 days before any new Subprocessor Processes any Client Personal Data, Optel will add such Subprocessor to the **Subprocessor List** and notify Client through email or other means specified on the DPA Setup Page.

4.4. Objection to New Subprocessors.

(a) If, within 30 days after notice of a new Subprocessor, Client notifies Optel in writing that Client objects to Optel's appointment of such new Subprocessor based on reasonable data protection concerns, the parties will discuss such concerns in good faith.

(b) If the parties are unable to reach a mutually agreeable resolution to Client's objection to a new Subprocessor, Client, as its sole and exclusive remedy, may terminate the Order for the affected Cloud Services for convenience and Optel will refund any prepaid, unused fees for the terminated portion of the Subscription Term.

5. Security.

5.1. Security Measures. Optel will implement and maintain reasonable and appropriate technical and organizational measures, procedures and practices, as appropriate to the nature of the Client Personal Data, that are designed to protect the security, confidentiality, integrity and availability of Client Personal Data and protect against Security Incidents, in accordance with Optel's Security Measures referenced in the Agreement and as further described in Schedule 2 (Technical and Organizational Measures). Optel will regularly monitor its compliance with its Security Measures and Schedule 2 (Technical and Organizational Measures).

5.2. Incident Notice and Response.

(a) Optel will implement and follow procedures to detect and respond to Security Incidents.

(b) Optel will: (i) notify Client without undue delay and, in any event, not later than the Specified Notice Period, after becoming aware of a Security Incident affecting Client and (ii) make reasonable efforts to identify the cause of the Security Incident, mitigate the effects and remediate the cause to the extent within Optel's reasonable control.

(c) Upon Client's request and taking into account the nature of the applicable Processing, Optel will assist Client by providing, when available, information reasonably necessary for Client to meet its Security Incident notification obligations under Data Protection Laws.

(d) Client acknowledges that Optel's notification of a Security Incident is not an acknowledgement by Optel of its fault or liability.

(e) Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Client Personal Data, including unsuccessful login attempts, pings, port scans, denial of service attacks or other network attacks on firewalls or networked systems.

5.3. Client Responsibilities.

(a) Client is responsible for reviewing the information made available by Optel relating to data security and making an independent determination as to whether the Cloud Services meets Client's requirements and legal obligations under Data Protection Laws.

(b) Client is solely responsible for complying with Security Incident notification laws applicable to Client and fulfilling any obligations to give notices to government authorities, affected individuals or others relating to any Security Incidents.

6. Data Protection Impact Assessment. Upon Client's request and taking into account the nature of the applicable Processing, to the extent such information is available to Optel, Optel will assist Client in fulfilling Client's obligations under Data Protection Laws to carry out a data protection impact or similar risk assessment related to Client's use of the Cloud Services, including, if required by Data Protection Laws, by assisting Client in consultations with relevant government authorities.

7. Data Subject Requests.

7.1. Assisting Client. Upon Client's request and taking into account the nature of the applicable Processing, Optel will assist Client by appropriate technical and organizational measures, insofar as possible, in complying with Client's obligations under Data Protection Laws to respond to requests from individuals to exercise their rights under Data Protection Laws, provided that Client cannot reasonably fulfill such requests independently (including through use of the Cloud Services).

7.2. Data Subject Requests. If Optel receives a request from a Data Subject in relation to the Data Subject's Client Personal Data, Optel will notify Client and advise the Data Subject to submit the request to Client (but not otherwise communicate with the Data Subject regarding the request except as may be required by Data Protection Laws), and Client will be responsible for responding to any such request.

8. Data Return or Deletion.

8.1. During Subscription Term. During the Subscription Term, Client may, through the features of the Cloud Services or such other means specified on the DPA Setup Page, access, return to itself or delete Client Personal Data.

8.2. Post Termination.

(a) Following termination or expiration of the Agreement, Optel will, in accordance with its obligations under the Agreement, delete all Client Personal Data from Optel's systems.

(b) Deletion will be in accordance with industry-standard secure deletion practices. Optel will issue a certificate of deletion upon Client's request.

(c) Notwithstanding the foregoing, Optel may retain Client Personal Data: (i) as required by Data Protection Laws or (ii) in accordance with its standard backup or record retention policies, provided that, in either case, Optel will (x) maintain the confidentiality of, and otherwise comply with the applicable provisions of this DPA with respect to, retained Client Personal Data and (y) not further Process retained Client Personal Data except for such purpose(s) and duration specified in such applicable Data Protection Laws.

9. Audits.

9.1. Optel Records Generally. Optel will keep records of its Processing in compliance with Data Protection Laws and, upon Client's request, make available to Client any records reasonably necessary to demonstrate compliance with Optel's obligations under this DPA and Data Protection Laws.

9.2. Third-Party Compliance Program.

(a) Optel will describe its third-party audit and certification programs (if any) and make summary copies of its audit reports (each, an "**Audit Report**") available to Client upon Client's written request at reasonable intervals (subject to confidentiality obligations).

(b) Client may share a copy of Audit Reports with relevant government authorities as required upon their request.

(c) Client agrees that any audit rights granted by Data Protection Laws will be satisfied by Audit Reports and the procedures of Section 9.3 (Client Audit) below.

9.3. Client Audit.

(a) Subject to the terms of this Section 9.3, Client has the right, at Client's expense, to conduct an audit of reasonable scope and duration pursuant to a mutually agreed-upon audit plan with Optel that is consistent with the Audit Parameters (an "**Audit**").

(b) Client may exercise its Audit right: (i) to the extent Optel's provision of an Audit Report does not provide sufficient information for Client to verify Optel's compliance with this DPA or the parties' compliance with Data Protection Laws, (ii) as necessary for Client to respond to a government authority audit or (iii) in connection with a Security Incident.

(c) Each Audit must conform to the following parameters ("**Audit Parameters**"): (i) be conducted by an independent third party that will enter into a confidentiality agreement with Optel, (ii) be limited in scope to matters reasonably required for Client to assess Optel's compliance with this DPA and the parties' compliance with Data Protection Laws, (iii) occur at a mutually agreed date and time and only during Optel's regular business hours, (iv) occur no more than once annually (unless required under Data Protection Laws or in connection with a Security Incident), (v) cover only facilities controlled by Optel, (vi) restrict findings to Client Personal Data only and (vii) treat any results as confidential information to the fullest extent permitted by Data Protection Laws.

10. Cross-Border Transfers/Region-Specific Terms.

10.1. Cross-Border Data Transfers.

(a) Optel (and its Affiliates) may Process and transfer Client Personal Data globally as necessary to provide the Cloud Services.

(b) If Optel engages in a Restricted Transfer, it will comply with Schedule 3 (Cross-Border Transfer Mechanisms).

10.2. Region-Specific Terms. To the extent that Optel Processes Client Personal Data protected by Data Protection Laws in one of the regions listed in Schedule 4 (Region-Specific Terms), then the terms specified therein with respect to the applicable jurisdiction(s) will apply in addition to the terms of this DPA.