TELEPHOS LLC DATA PROCESSING AGREEMENT

Last Updated: June 1, 2026

> This Data Processing Agreement ("DPA") sets out the terms, requirements, and conditions on which Telephos will process Client Personal Data for the purposes of the Objective. This DPA contains the mandatory clauses required by Article 28(3) of the General Data Protection Regulation (EU) 2016/679 ("GDPR") for contracts between controllers and processors, as well as compliance with the applicable provisions of the GDPR and related EU data protection laws, including the European Data Protection Board (EDPB) guidelines and the EU Commission's standard contractual clauses (SCCs) where applicable.

1. Definitions

The following definitions apply in this DPA:

1.1 Definitions:

- **Client Personal Data:** means Personal Data provided by the Client through integrated third-party recording platforms.
- **Personal Data:** means personal data under the definition set out in GDPR.
- **Telephos Data:** means Personal Data provided by Telephos.
- **Objective:** means the Services to be provided by Telephos according to the Terms of Service, which together with the Order Form constitute a legally binding agreement between the parties ("Agreement").
- **Data Labeling Services:** means the processing of call transcripts to identify, classify, and label data elements for analytics and business intelligence purposes.
- **Integrated Recording Platform:** means third-party services (such as Gong, Fireflies, Zoom, or similar platforms) that capture and provide call transcripts to Telephos with appropriate consent already obtained.

Data Protection Legislation:

means all applicable data protection and privacy legislation in force from time to time, including without limitation:

1. The UK GDPR.
2. The Data Protection Act 2018 (and regulations made thereunder) (DPA 2018).
3. The Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended.
4. The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) as applicable.
5. The ePrivacy Directive (Directive 2002/58/EC) as amended and national implementations thereof.
6. The California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA).
7. Any successor legislation or regulations applicable in the UK, EU, and United States.

2. Personal Data Types and Processing Purposes

2.1 The Client and Telephos acknowledge and agree that for the purpose of the Data Protection Legislation:

- (a) the Client is the Controller and Telephos is the Processor, save with respect to Telephos Data for which Telephos is a Controller.
- (b) the Client retains control of Client Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including ensuring that appropriate consent has been

obtained by the Integrated Recording Platform (Gong, Fireflies, Zoom, or similar service), providing any required notices, and for the processing instructions it gives to Telephos; and

• (c) Annex A describes the subject matter, duration, nature and purpose of processing and the Personal Data categories and Data Subject types in respect of which Telephos may process.

3. Telephos's Obligations

3.1 Telephos will only process the Client Personal Data to the extent, and in such a manner, as is necessary for the Objective, specifically for data labeling and analysis services. Telephos will not process the Client Personal Data for any other purpose or in a way that does not comply with this DPA or the Data Protection Legislation. Telephos must promptly notify the Client if, in its opinion, the Client's instructions do not comply with the Data Protection Legislation.

3.2 Telephos will maintain the confidentiality of the Client Personal Data and will not disclose the Client Personal Data to third parties unless the Client or this DPA specifically authorises the disclosure, or as required by domestic or EU law, court, or regulator (including the Commissioner). If a domestic or EU law, court, or regulator (including the Commissioner) requires Telephos to process or disclose the Client Personal Data to a third-party, Telephos must first inform the Client of such legal or regulatory requirement and give the Client an opportunity to object or challenge the requirement, unless the domestic or EU law prohibits the giving of such notice.

3.3 Telephos will reasonably assist the Client, at no additional cost to the Client for standard requests, with meeting the Client's compliance obligations under the Data Protection Legislation, taking into account the nature of Telephos's processing and the information available to Telephos, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with the Commissioner under the Data Protection Legislation.

3.4 Telephos must notify the Client promptly of any changes to the Data Protection Legislation that may reasonably be interpreted as adversely affecting Telephos's performance of the Objective or this DPA.

3.5 Telephos confirms that Client Personal Data will not be used to train any machine learning models, artificial intelligence systems, or for any purpose other than providing data labeling services specific to the individual Client's requirements. Each Client's data remains isolated and is never combined with data from other clients.

4. Telephos Data

4.1 Telephos Data is made available only for use for the purposes of the Objective and must not be made public by the Client. By making Telephos Data public or using it other than for the purposes for which it is provided, the Client may be in breach of the Data Protection Legislation and the terms of this DPA. The Client shall not transfer or access Telephos Data outside of the UK or the European Economic Area ("EEA") except with the prior written consent of Telephos and subject to appropriate safeguards.

4.2 The Client is responsible for keeping Telephos Data safe and using appropriate security measures to prevent unauthorised access, copying, modification, storage, reproduction, display, or distribution of the data. If any unauthorised access occurs, the Client must take immediate action to remedy the situation. The security measures used by the Client must be at least as good as the security measures used by the Client to protect their personal data or confidential information.

4.3 If the Client becomes aware of any misuse of any Telephos Data, or any security breach in connection with the DPA that could compromise the security or integrity of Telephos Data or otherwise adversely affect Telephos, or if the Client learns or suspects that any password or other security feature has been revealed to or obtained by any unauthorised person, the Client shall promptly notify Telephos and fully co-operate with Telephos to remedy the issue as soon as reasonably practicable.

4.4 The Client understands and acknowledges that Telephos gives no opinion and makes no recommendation in relation to any persons appearing in Telephos Data.

5. Telephos Employees

5.1 Telephos shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data as well as any security obligations with respect to such Data.

5.2 Telephos will take appropriate steps to ensure compliance with the Security Measures (defined below) by its personnel to the extent applicable to their scope of performance, including ensuring that all persons authorized to process your Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and that any such obligations survive the termination of that individual's engagement with Telephos.

5.3 Telephos shall ensure that access to Personal Data is limited to authorized personnel who require such access to perform the Services, following zero-trust architecture principles.

6. Security

6.1 Telephos is required to take necessary steps to prevent unauthorised or illegal processing, access, disclosure, copying, modification, storage, reproduction, display, or distribution of Client Personal Data. Additionally, Telephos must take measures to prevent accidental or illegal loss, destruction, alteration, disclosure, or damage of Client Personal Data.

6.2 Telephos shall maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of your Personal Data. Telephos will implement and maintain technical and organizational measures to protect your data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 1 (the "Security Measures"). As described in Appendix 1, the Security Measures include measures to protect Personal Data; to help ensure ongoing confidentiality, integrity, availability and resilience of Telephos's systems and services; to help restore timely access to Personal Data following an incident; and for regular testing of effectiveness. Telephos 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 Services.

6.3 Telephos is actively working with Vanta to achieve SOC 2 Type II certification and maintains the necessary posture for SOC 2 Type I certification upon request.

7. Personal Data Breach

7.1 Telephos shall, without undue delay and within 72 hours, notify the Client if it becomes aware of:

- (a) any accidental, unauthorised, or unlawful processing of the Client Personal Data; or
- (b) any Personal Data Breach.

7.2 Following any Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. Telephos will reasonably co-operate with the Client in the Client's handling of the matter, including:

- (a) assisting with any investigation;
- (b) making available all relevant records, logs, files, data reporting and other materials required to comply with Data Protection Legislation or as otherwise reasonably required by the Client; and
- (c) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the personal data breach.

8. Cross-border Transfers of Personal Data

8.1 Telephos must not transfer or otherwise process Client Personal Data outside the EEA or UK without obtaining the Client's prior written consent, such consent not to be unreasonably withheld, conditioned or delayed provided that all transfers by Telephos of Client Personal Data shall (to the extent required under the Data Protection Legislation) be affected by way of appropriate safeguards and in accordance with Data Protection Legislation.

8.2 If any Client Personal Data transfer between the Client and Telephos requires execution of Standard Contractual Clauses ("SCC's") in order to comply with the Data Protection Legislation (where the Client is the entity exporting Client Personal Data to Telephos outside the EEA), the parties will complete all relevant details in, and execute the SCC's, and take all other actions required to legitimise the transfer. The SCC's are part of this DPA as Annex A.

8.3 For enterprise customers, Telephos can implement Private Storage options including EU data localization and customer-controlled storage solutions, subject to separate agreement and additional terms.

9. Subcontractors

9.1 The Client grants to Telephos specific authorisation to appoint the sub-processors listed in Annex A in connection with the Objective.

9.2 Subject to clause 8.1, Telephos may only authorise a new subcontractor to process the Client Personal Data if:

- (a) the Client is provided with an opportunity to object to the appointment of each subcontractor within thirty (30) days after Telephos supplies the Client with details regarding such subcontractor via email notification to the designated contact; and
- (b) Telephos enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this DPA, in particular, in relation to requiring appropriate technical and organisational data security measures.

9.3 Where the subcontractor fails to fulfil its obligations under such written DPA, Telephos remains fully liable to the Client for the subcontractor's performance of its DPA obligations.

9.4 If the Client objects to a new subcontractor within the 30-day period, Telephos and the Client will work in good faith to find a mutually acceptable resolution. If no resolution is reached within 30 days of the objection, the Client may terminate the affected Services without penalty by providing written notice within 10 days following the resolution period.

10. Complaints, Data Subject Requests and Third-party Rights

10.1 Telephos shall provide such information to the Client as the Client may reasonably require, to enable the Client to comply with:

- (a) the rights of data subjects under the Data Protection Legislation, including subject access rights, the rights to rectify and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and
- (b) information or assessment notices served on the Client by any supervisory authority under the Data Protection Legislation.

10.2 Telephos must notify the Client immediately if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Client Personal Data or to either party's compliance with the Data Protection Legislation.

10.3 Telephos must notify the Client within seven (7) working days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their related rights under the Data Protection Legislation.

10.4 Telephos will give the Client its full co-operation and assistance in responding to any complaint, notice, communication, or data subject request.

10.5 Telephos must not disclose the Client Personal Data to any Data Subject or to a third party other than at the Client's request or instruction, as provided for in this DPA or as required by law.

11. Data Return and Destruction

11.1 At the Client's request, Telephos will give the Client a copy of or access to all or part of the Client's Personal Data in its possession or control in a commonly used and machine-readable format.

11.2 On expiry or termination of this DPA, Telephos will securely delete or destroy or, if directed in writing by the Client, return, all or any Client Personal Data related to this DPA in its possession or control, including any labeled data outputs.

11.3 If any law, regulation, or government or regulatory body requires Telephos to retain any documents or materials that Telephos would otherwise be required to return or destroy, it will notify the Client in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

12. Records

12.1 Telephos will keep accurate and up-to-date written records regarding any processing of Client Personal Data it carries out for the Client, including but not limited to, the access, control and security of the Client Personal Data, approved subcontractors and affiliates, the processing purposes, categories of processing, any transfers of personal data to a third country and related safeguards, and a general description of the technical and organisational security measures referred to in clause 6.1 ("Records").

12.2 Telephos will ensure that the Records are sufficient to enable the Client to verify Telephos's compliance with its obligations under this DPA and Telephos will provide the Client with copies of the Records upon request.

12.3 Telephos will maintain comprehensive audit logs of all data labeling activities, including timestamps, user actions, and data modifications.

13. Audits and Compliance Verification

13.1 Telephos will, upon reasonable notice and not more than once per year (unless required by a competent supervisory authority or following a data breach), permit the Client or its authorized representative to conduct audits of Telephos's compliance with this DPA.

13.2 Telephos may provide its SOC 2 Type II report (once obtained) or SOC 2 Type I attestation as evidence of compliance with security obligations under this DPA.

14. Miscellaneous

14.1 This DPA will take effect on the execution date (the "Effective Date") and will remain in effect until, and automatically expire upon, the deletion of all of your Personal Data by Telephos as described in this DPA.

14.2 Nothing in this DPA shall confer any benefits or rights on any person or entity other than the parties to this DPA.

14.3 Where Your Affiliates are Data Controllers of the Personal Data, they may enforce the terms of this DPA against Telephos directly.

14.4 This DPA may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all the counterparts shall together constitute the one DPA.

14.5 Any amendments to this DPA must be made in writing and signed by both parties.

14.6 Limitation of Liability. Telephos's total aggregate liability under this DPA shall not exceed the total fees paid by the Client to Telephos in the twelve (12) months preceding the claim. For claims arising from breach of confidentiality obligations under Section 3.2, Telephos's liability shall not exceed twenty-four (24) months of fees paid by Client. The foregoing limitations shall not apply to claims arising from Telephos's gross negligence or willful misconduct.

14.7 Governing Law and Jurisdiction. This DPA shall be governed by and construed in accordance with the laws of the State of Delaware, United States, without regard to its conflict of laws principles. Any disputes arising under this DPA shall be subject to the exclusive jurisdiction of the state and federal courts located in Delaware.

Annex A: Standard Contractual Clauses

(MODULE TWO – CONTROLLER TO PROCESSOR)

SECTION I

Clause 1 - Purpose and scope

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) for the transfer of personal data to a third country.
- (b) The Parties: (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2 - Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Note: The Standard Contractual Clauses continue with detailed provisions covering data protection safeguards, obligations of the parties, local laws and obligations in case of access by public authorities, and final provisions. The complete clauses are incorporated by reference and form an integral part of this DPA.

Annex I.A - List of Parties

Data Exporter	The Client, as defined in the Agreement. The data exporter is the controller of Client Personal Data and is responsible for ensuring appropriate consent has been obtained via the Integrated Recording Platform.
Data Importer	Telephos LLC, a Delaware limited liability company located in the United States. The data importer provides data labeling and analysis services as described in the Agreement.
Competent Supervisory Authority	The supervisory authority of the EU Member State in which the data exporter is established, or where the data exporter is not established in an EU Member State, the supervisory authority of the EU Member State where the data exporter's EU representative is established.

Annex I.B - Description of Transfer

Categories of Data Subjects	Business contacts, call participants, sales representatives, customer success personnel, and other individuals whose communications are captured by the Integrated Recording Platform.
Categories of Personal Data	• Call transcript content (spoken words, conversation context) • Speaker identification (names, email addresses) • Meeting metadata (date, time, duration, participants) • Business context (company names, deal information mentioned in calls)
Sensitive Data	None intentionally processed. Any sensitive data incidentally captured in call transcripts is not specifically extracted or processed and is subject to the same security measures as all Client Personal Data.
Frequency of Transfer	Continuous, as call transcripts are synced from the Integrated Recording Platform.
Nature and Purpose of Processing	Data labeling, classification, and analysis of call transcripts to extract business intelligence, identify key insights, and provide analytics as described in the Agreement.
Duration of Processing	The term of the Agreement, plus any retention period specified in Section 11 of this DPA.

Annex B: Technical and Security Measures

Confidentiality

• **Electronic Access Control:** Telephos's systems implement zero-trust architecture to prevent unauthorised use of our data processing and storage systems. We utilize strong passwords with complexity requirements, automatic blocking/locking mechanisms after failed attempts, and mandatory multi-factor authentication (MFA) for all administrative access.

• **Internal Access Control:** We maintain strict Role-Based Access Control (RBAC) with principle of least privilege. All access requests to our systems seeking access to personal data are authenticated and authorized. Each user and subsystem has access only to the minimal set of resources required for their function. We maintain comprehensive audit logs of all access events, data modifications, and administrative actions.

• **Data Segregation:** Client data is logically segregated with strict access controls ensuring that data from one client cannot be accessed by another client.

Integrity

• **Data Transfer Controls:** All data is encrypted in transit using TLS 1.3 (with TLS 1.2 as minimum). At rest, we encrypt files using 256-bit Advanced Encryption Standard (AES-256). We utilize industry-standard encryption techniques and regularly review our cryptographic implementations.

• **Data Processing Integrity:** All labeled data outputs are versioned and tracked, with comprehensive audit trails showing what transformations were applied, when, and by whom. Quality assurance processes ensure accuracy of data labeling.

• **API Security:** All API endpoints are secured with authentication tokens, rate limiting, and request validation to prevent unauthorized data manipulation.

Availability and Resilience

• **Infrastructure Redundancy:** Telephos utilizes geographically distributed cloud infrastructure with automatic failover capabilities to eliminate single points of failure.

• **Backup Strategy:** Automated daily backups with point-in-time recovery capabilities. Backups are encrypted and stored in geographically separate locations. Regular restoration testing ensures backup integrity.

• **Incident Response:** 24/7 monitoring with automated alerting for security events and system anomalies. Documented incident response procedures with defined escalation paths.

• **Business Continuity:** Documented disaster recovery procedures with Recovery Time Objective (RTO) of 4 hours and Recovery Point Objective (RPO) of 1 hour for critical systems.

Security Governance

• **Security Program:** Comprehensive information security management system aligned with ISO 27001 standards. Currently pursuing SOC 2 Type II certification through Vanta.

• **Security Awareness:** All employees receive security training upon onboarding and annually thereafter. Specialized training for personnel handling customer data.

• **Vendor Security:** All sub-processors undergo security assessment before onboarding and are bound by equivalent security obligations.

Approved Sub-processors

Anthropic (USA)	Large Language Model Service for Data Analysis
Google Workspace (USA)	Identity Provider, Email, and Google Meet Transcripts
HubSpot (USA)	Customer Relationship Management
OpenAI (USA)	Large Language Model Service for Data Labeling

Perplexity AI (USA)	AI Research and Enrichment
Render (USA)	Application Hosting and PostgreSQL Database
Slack (USA)	Notification Delivery and Customer-Facing Shared Channels
Stripe (USA)	Payment Processing
Vercel (USA)	Frontend Application Hosting
Zoom (USA)	Call Recording and Transcript Source