TELEPHOS LLC DATA PROCESSING AGREEMENT

Last Updated: September 24, 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 all Personal Data that Telephos processes on behalf of the Client in connection with the Services, from any source, including Personal Data that the Client provides, or that Telephos obtains on the Client's behalf, through any Integrated Recording Platform or other Connected Service, upload, or other means, whether made available now or in the future. Client Personal Data excludes Telephos Data and De-Identified Data. Client Personal Data does not become Telephos Data, and Telephos Data does not become Client Personal Data, by being associated with the other within the Services.

• **Personal Data:** means personal data under the definition set out in GDPR.

• **Telephos Data:** means Personal Data provided by Telephos.

• **Connected Service:** means any Integrated Recording Platform and any other third-party platform, application, or data source (including calendar, customer relationship management, messaging, and email services) that the Client connects to the Services or authorises Telephos to access on the Client's behalf, including any such platform, application, or data source made available through the Services in the future.

• **Personal Data Breach:** has the meaning given in Article 4(12) of the GDPR, and applies to Client Personal Data.

• **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.

• **Client Content and End-User:** have the meanings given in the Terms of Service.

• **De-Identification Standard:** means the standard set out in Annex C, as maintained and updated in accordance with Section 15.2.

• **De-Identified Data:** means data derived from Client Content that has been aggregated with data derived from multiple Clients or other sources and de-identified in accordance with the De-Identification Standard (Annex C), such that it does not identify, and cannot reasonably be used, alone or in combination with other information reasonably available to the recipient or publicly available, to identify the Client, any End-User, any natural person, or any individual merchant or business that is a customer of, or a participant in or subject of communications processed for, any Client. De-Identified Data expressly excludes (a) any verbatim transcript excerpt or quotation, (b) any direct or indirect identifier of a natural person, and (c) any output

© 2026 Telephos LLC. All rights reserved.

that does not satisfy the minimum-cohort threshold in the De-Identification Standard. Notwithstanding the foregoing, De-Identified Data may identify commercially available products and services, and the vendors of such products and services (including a vendor that is or was itself a Client), solely in their capacity as market participants and only where the supporting signal satisfies the De-Identification Standard; identification of a vendor or product solely in that capacity does not constitute identification of "the Client" or of an "individual merchant or business" for purposes of this definition, provided the output does not identify the vendor in its capacity as a Client of Telephos or attribute to it any specific Client Content as its source.

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 for Client Personal Data made available through any Integrated Recording Platform (Gong, Fireflies, Zoom, or similar service) or other Connected 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, including for data labeling and analysis services and the creation of De-Identified Data as described in Section 15 (Aggregated and De-Identified Data), which the parties agree is a permitted purpose under this DPA and within the Objective. 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 will ensure that De-Identified Data is de-identified in accordance with the De-Identification Standard (Annex C) such that it does not constitute Personal Data under the Data Protection Legislation; data meeting that standard is not Client Personal Data for the purposes of this DPA. 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

© 2026 Telephos LLC. All rights reserved.

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 will not use Client Personal Data to train any machine learning model or artificial intelligence system. Telephos will not process Client Personal Data for any purpose other than providing the Services to Client, except that Telephos may create De-Identified Data as described in Section 15 (Aggregated and De-Identified Data). Each Client's Personal Data, and any Client Content that identifies the Client, an End-User, a natural person, or an individual business (in each case other than references to commercially available products, services, and their vendors solely as market participants, as permitted by the definition of De-Identified Data), remains isolated: Telephos will never disclose it to any other Client, and will never include it in any output made available to any other Client, except Shared Data that the Client itself directs Telephos to make available to a Sharing Partner under Section 16 (Optional Data Sharing), and then only as that Section permits. Separately, Telephos may create and use De-Identified Data — which by definition contains no such identifying information — as described in Section 15.

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 United States, 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

© 2026 Telephos LLC. All rights reserved.

process Client 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 Client Personal Data. Telephos will implement and maintain technical and organizational measures to protect Client Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Annex B (the "Security Measures"). As described in Annex B, 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 Location of processing. Telephos stores and processes Client Personal Data in the United States, and the Client authorises Telephos, and the sub-processors listed in Annex B, to process Client Personal Data there. Telephos must not transfer or otherwise process Client Personal Data in any other country without the Client's prior written consent, such consent not to be unreasonably withheld, conditioned or delayed. All transfers of Client Personal Data, into or out of the United States, including onward transfers by Telephos to its sub-processors, shall (to the extent required under the Data Protection Legislation) be effected by way of appropriate safeguards and in accordance with the Data Protection Legislation.

© 2026 Telephos LLC. All rights reserved.

8.2 EU transfers. Where the Client (or any of its affiliates) transfers Client Personal Data to Telephos, directly or through a Connected Service, and that transfer is subject to the GDPR and is to a country not recognised by the European Commission as providing an adequate level of protection (a "Restricted Transfer"), the Standard Contractual Clauses approved by Commission Implementing Decision (EU) 2021/914, Module Two (controller to processor), set out in full in Annex A with the options selected there (the "SCCs"), apply to that transfer and are incorporated into this DPA. Execution of this DPA or of the Agreement constitutes each party's execution of the SCCs.

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.

8.4 UK transfers. Where a transfer of Client Personal Data to Telephos is subject to the UK GDPR and would be a Restricted Transfer under it, the SCCs apply as amended by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B1.0) issued by the UK Information Commissioner under S119A(1) of the Data Protection Act 2018 (the "UK Addendum"), which is incorporated into this DPA. For the purposes of the UK Addendum: Table 1 is completed with the information in Annex I.A; Table 2 is completed by reference to the Module and options selected in Annex A; Table 3 is completed with the information in Annexes I.B, I.C, B, and the Approved Sub-processors list; and in Table 4, either party may end the UK Addendum as set out in its Section 19.

8.5 Swiss transfers. Where a transfer of Client Personal Data to Telephos is subject to the Swiss Federal Act on Data Protection ("FADP"), the SCCs apply with the following amendments: references to the GDPR are to be read as references to the FADP to the extent the transfer is subject to the FADP; the Swiss Federal Data Protection and Information Commissioner is the competent supervisory authority under Clause 13 for such transfers; and the term "Member State" in the SCCs is not to be interpreted to exclude data subjects in Switzerland from bringing legal proceedings in their place of habitual residence under Clause 18(c).

8.6 Precedence. In the event of any conflict or inconsistency between the SCCs (including as amended by the UK Addendum or Section 8.5) and this DPA or the Agreement, the SCCs prevail with respect to the applicable transfer. Nothing in this DPA or the Agreement modifies the SCCs or limits the rights of data subjects under them.

9. Subcontractors

9.1 The Client grants to Telephos general written authorisation to engage sub-processors in connection with the Objective, in accordance with Section 9.2, and specifically authorises the sub-processors listed in the Approved Sub-processors list in Annex B.

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.

© 2026 Telephos LLC. All rights reserved.

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 6.2 and Annex B ("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

© 2026 Telephos LLC. All rights reserved.

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 Client 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, except that data subjects may invoke and enforce the SCCs (including as amended by the UK Addendum or Section 8.5) as third-party beneficiaries in accordance with Clause 3 of the SCCs, and except that a Sharing Partner may enforce Section 16.4 as provided there.

14.3 Where the Client's 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, except that Section 16 (Optional Data Sharing) applies to the Client once the Client accepts it by enabling a Sharing Feature in the Services (or, for Section 16.4, receives Shared Data), and that recorded acceptance satisfies this Section 14.5 for Section 16.

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. Nothing in this Section 14.6 limits either party's liability to data subjects under the SCCs (including as amended by the UK Addendum or Section 8.5).

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. Notwithstanding the foregoing, the SCCs are governed by the law specified in Clause 17 of the SCCs, and disputes arising from the SCCs are subject to Clause 18 of the SCCs (in each case, as amended by the UK Addendum or Section 8.5 where applicable).

15. Aggregated and De-Identified Data

15.1 Protections; no re-identification. Except for Shared Data made available at the Client's direction under Section 16 (Optional Data Sharing), Telephos will not disclose to any other Client, or include in any De-Identified Data or other cross-Client output: Client Personal Data; any Client Content that identifies the Client, an End-User, a natural person, or an individual business (in each case other than references to commercially available products, services, and their vendors solely as market participants, as permitted by the definition of De-Identified Data and the De-Identification Standard); or any verbatim transcript excerpt or quotation. Telephos will not attempt to re-identify De-Identified Data, and will contractually require any recipient of De-Identified Data not to attempt re-identification.

© 2026 Telephos LLC. All rights reserved.

15.2 Creation; standard; attestation. Telephos may create De-Identified Data from Client Content, in each case in accordance with the De-Identification Standard (Annex C). Telephos will make the then-current De-Identification Standard available to Client, and may update it from time to time, provided that no update materially reduces the protection it provides; Telephos will notify Client of any material update. Upon Client's written request, no more than once in any twelve-month period, Telephos will provide a written attestation of Telephos's conformance with the De-Identification Standard, which may be accompanied by a summary of the most recent review conducted under Telephos's security program (Annex C, paragraph 6).

15.3 Use. Client retains all right, title, and interest in and to Client Content. As between the parties, Telephos owns the De-Identified Data it creates, which — by definition — does not identify Client, any End-User, any natural person, or any individual business. Telephos may use, combine, retain, and make available De-Identified Data to: (a) operate, provide, maintain, secure, analyze, improve, and develop the Platform and Services, including developing, training, and evaluating the statistical models, machine-learning systems, and algorithms used to provide them, through machine-learning techniques applied to De-Identified Data (and, per Section 3.5, never to Client Personal Data); (b) create and make available to Clients (including Client) aggregate ecosystem, category, benchmarking, and trend intelligence through the Platform and Services; (c) produce and publish industry- and category-level research, reports, and statistics; and (d) purposes substantially similar to the foregoing — in each case in accordance with the De-Identification Standard.

15.4 Termination. Upon termination, Telephos will delete or return Client Personal Data and Client Content as required by this DPA, and will not create new De-Identified Data from Client Content following termination. Because De-Identified Data does not identify Client or any person or business, the deletion and return obligations of this DPA do not apply to De-Identified Data, which Telephos may continue to use, combine, and re-aggregate as described in this Section (including by continuing to maintain, recompute, and update aggregates that incorporate De-Identified Data created prior to termination); De-Identified Data already created will continue to be maintained in accordance with the De-Identification Standard. This Section 15 survives termination.

16. Optional Data Sharing

16.1 Scope; optional. The Services may offer features through which the Client can choose to share data with another Client ("Sharing Features"). Sharing Features are off by default, and no Client Personal Data or Client Content is shared with another Client unless the Client chooses to share it. This Section applies to a Client that enables a Sharing Feature, and Section 16.4 also applies to any Client that receives Shared Data. Subject to Section 8.6, where this Section conflicts with any other part of this DPA, this Section governs Shared Data, and only Shared Data.

16.2 Definitions. "Shared Data" means the data the Client chooses to share through a Sharing Feature. "Sharing Partner" means a Client with which the Client chooses to share, or from which it receives, Shared Data.

16.3 The Client's instruction. The Client's choice to share through a Sharing Feature is its documented instruction to Telephos under Section 3.1 and Article 28(3)(a) of the GDPR. Telephos will make available only the Shared Data the Client selects, only to the Sharing Partner it selects, and only while the Client keeps that sharing enabled. The Client may stop sharing at any time, and Telephos will then stop making the Client's Shared Data available to the Sharing Partner.

16.4 Obligations of a recipient. A Client that receives Shared Data from a Sharing Partner, whether or not it has itself enabled a Sharing Feature: (a) will use it only within the Services and only for its business relationship with that Sharing Partner; (b) will treat it as the Sharing Partner's confidential information; (c) will not sell, license, publish, or disclose it to any third party; (d) will not attempt to re-identify any person or business from any aggregate or de-identified form of it; and (e) will stop using any copy of it within thirty (30) days after the sharing ends, save as required by law. The Sharing Partner may enforce this Section 16.4 against the recipient directly.

© 2026 Telephos LLC. All rights reserved.

16.5 Roles. For Shared Data, Telephos remains the sharing Client's Processor, and making Shared Data available to a Sharing Partner is a disclosure made on that Client's instruction. To the extent Shared Data includes Personal Data, the Sharing Partner receives it as an independent Controller, and Section 8 and the SCCs apply to any transfer as they apply to Client Personal Data.

16.6 Acceptance and records. The Client accepts this Section by enabling a Sharing Feature. Telephos records the acceptance, the user who gave it, the time, and the version of the terms shown, and will provide that record to the Client on request.

16.7 Client warranty; responsibility. The Client warrants that it has the rights, notices, and consents needed for Telephos to make its Shared Data available to the Sharing Partners it selects. Telephos is not responsible for a Sharing Partner's use of Shared Data in breach of Section 16.4; any claim arising from such a breach lies between the Client and that Sharing Partner. Section 14.6 applies to Telephos's liability under this Section.

16.8 De-Identified Data. Telephos will not use Shared Data, or the existence of any sharing between Clients, to create De-Identified Data.

Annex A: Standard Contractual Clauses

The following are the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, approved by Commission Implementing Decision (EU) 2021/914 of 4 June 2021, Module Two (transfer controller to processor), reproduced in full with the options selected by the parties. Official text: **eur-lex.europa.eu/eli/dec_impl/2021/914/oj**.

> **Options selected:** Module Two. Clause 7 (docking): not used. Clause 9(a): Option 2 (general written authorisation), with thirty (30) days' notice. Clause 11(a): optional independent dispute resolution body not selected. Clause 13: as applicable to the data exporter, as indicated in Annex I.C. Clause 17: Option 1, the law of Ireland. Clause 18(b): the courts of Ireland.

STANDARD CONTRACTUAL CLAUSES (MODULE TWO: TRANSFER 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) [1] 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.

© 2026 Telephos LLC. All rights reserved.

(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.

Clause 3 - Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 - Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5 - Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6 - Description of the transfer(s)

© 2026 Telephos LLC. All rights reserved.

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional - Docking clause

Not used. The parties have not selected the optional docking clause.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 - Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

© 2026 Telephos LLC. All rights reserved.

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union [4] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

© 2026 Telephos LLC. All rights reserved.

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9 - Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. [8] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter

© 2026 Telephos LLC. All rights reserved.

shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10 - Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11 - Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 - Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

© 2026 Telephos LLC. All rights reserved.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13 - Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14 - Local laws and practices affecting compliance with the Clauses

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

© 2026 Telephos LLC. All rights reserved.

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards [12];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 - Obligations of the data importer in case of access by public authorities

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

© 2026 Telephos LLC. All rights reserved.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16 - Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

© 2026 Telephos LLC. All rights reserved.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17 - Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18 - Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Footnotes to the Clauses

- [1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.
- [4] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

© 2026 Telephos LLC. All rights reserved.

• [8] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

• [12] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

APPENDIX

Annex I.A - List of Parties

Data Exporter	The Client, as identified in the Agreement or Order Form, including its name, address, and contact person's name, position, and contact details. Activities relevant to the data transferred: use of the Services described in the Agreement. Role: controller. Signature and date: the Client's execution of the Agreement or Order Form constitutes its signature of this Annex I.A.
Data Importer	Telephos LLC, a Delaware limited liability company located in the United States. Contact: dpo@telephos.ai. Activities relevant to the data transferred: data labeling and analysis services as described in the Agreement. Role: processor. Signature and date: Telephos's execution of the Agreement or Order Form constitutes its signature of this Annex I.A.

Annex I.B - Description of Transfer

Categories of Data Subjects	Business contacts, meeting attendees, call participants, the Client's personnel (including sales and customer success personnel) and users of the Services, and other individuals whose Personal Data is contained in data the Client makes available through an Integrated Recording Platform or other Connected Service.

© 2026 Telephos LLC. All rights reserved.

Categories of Personal Data	• Call transcript content (spoken words, conversation context) • Speaker identification (names, email addresses) • Meeting and calendar metadata (date, time, duration, title, attendee names and email addresses) • Customer relationship management records (contact names, email addresses, job titles, company, and deal information) • Messages and related metadata from messaging or email services the Client connects • Business context (company names, deal information mentioned in calls or other Client Content) • Account data of the Client's users of the Services (names, email addresses) • Personal Data contained in any other Connected Service the Client connects, now or in the future
Sensitive Data	None intentionally processed. Any sensitive data incidentally captured in Client Content is not specifically extracted or processed and is subject to the same security measures as all Client Personal Data.
Frequency of Transfer	Continuous, as data is synced from Integrated Recording Platforms and other Connected Services.
Nature and Purpose of Processing	Data labeling, classification, and analysis of Client Content to extract business intelligence, identify key insights, and provide analytics as described in the Agreement; and, where the Client chooses to share, disclosure of Shared Data to a Sharing Partner on the Client's instruction under Section 16 (Optional Data Sharing).
Duration of Processing and Retention	The term of the Agreement, after which Client Personal Data is deleted or returned in accordance with Section 11 of this DPA, subject to any retention period specified in Section 11.
Transfers to Sub-processors	The sub-processors in the Approved Sub-processors list in Annex B process Client Personal Data for the purposes described there, for the duration of the Agreement.

Annex I.C - Competent Supervisory Authority

Determined in accordance with Clause 13(a) of the SCCs: where the data exporter is established in an EU Member State, the supervisory authority of that Member State; where the data exporter is not established in an EU Member State but has appointed a representative under Article 27(1) of the GDPR, the supervisory authority of the Member State in which that representative is established; otherwise, the supervisory authority of the Member State in which the data subjects whose Personal Data is transferred are located. For transfers subject to the UK GDPR, the UK Information Commissioner; for transfers subject to the FADP, the Swiss Federal Data Protection and Information Commissioner.

Annex II - Technical and Organisational Measures

The technical and organisational measures set out in Annex B (Technical and Security Measures) of this DPA.

Annex III - List of Sub-processors

© 2026 Telephos LLC. All rights reserved.

Not required, because Clause 9(a), Option 2 (general written authorisation) is selected. The agreed list of sub-processors referred to in Clause 9(a) is the Approved Sub-processors list in Annex B, as updated in accordance with Section 9 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

© 2026 Telephos LLC. All rights reserved.

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

Annex C: De-Identification Standard

This Annex sets out the De-Identification Standard referenced in Section 15 and in the definition of De-Identified Data. Telephos maintains and reviews this standard as part of its security program (paragraph 6); the then-current version is made available to Client per Section 15.2.

1. **No verbatim.** No transcript excerpt, quotation, or distinctive phrase is included in any De-Identified Data unit; only derived labels, themes, counts, and bands.

2. **Identifiers removed or generalized.** No direct or indirect identifiers of any natural person. Names of merchants and other businesses that are customers of, or participants in or subjects of communications processed for, any Client are removed or generalized to role or segment; raw firmographic values (such as revenue or traffic) are generalized to bands, never point values. Names of commercially available products and services, and their vendors (including vendors that are themselves Clients, solely in that market-participant capacity), may be retained solely as market participants, subject to paragraph 3.

3. **Minimum cohort, post-filter.** Any output cell — any combination of attribute bands (for example, vertical × revenue band × region × technology stack), and any statement concerning a named vendor or product — must be supported by data from no fewer distinct source businesses, after all filters are applied, than the minimum-cohort threshold published in the then-current De-Identification Standard documentation made available to Client, or it is suppressed; Telephos may apply higher thresholds. The count is on the combination and its supporting source set, not the total row count. Per Section 15.2 and paragraph 6, no update to the published threshold will materially reduce the protection this standard provides.

4. **Re-identification screen.** A named-entity and uniqueness review runs before publication to catch descriptive re-identification (for example, a description that identifies a business without naming it) even where no identifier field is present.

5. **No re-identification.** Per Section 15.1, Telephos does not attempt re-identification, and recipients of De-Identified Data are contractually barred from attempting it.

6. **Review; no weakening.** The De-Identification Standard is reviewed at least annually as part of Telephos's security program and is not updated in any way that materially reduces the protection it provides (Section 15.2).

© 2026 Telephos LLC. All rights reserved.