DATA PROCESSING AGREEMENT

1. INITIAL PROVISIONS

This Data Processing Agreement (the "**DPA**") is an integral part of the Agreement between CloudTalk and the Customer and is incorporated by reference therein.

2. DEFINITIONS

Any capitalized terms not specifically defined in this DPA shall have the meanings assigned to them in the Agreement. Additional definitions relevant to this DPA are specified below.

"**CCPA**" means the California Consumer Privacy Act of 2018, as amended, including as amended by the California Privacy Rights Act of 2020, together with all implementing regulations.

"**Data Breach**" means a breach of security of the Services leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by CloudTalk under this DPA.

"**Data Protection Legislation**" means, as applicable to a party and its Processing of Personal Data: (i) EU/UK Data Protection Laws, and (ii) CCPA and any national data protection laws made under the CCPA.

"**EU/UK Data Protection Laws**" means all laws and regulations of the European Union, Switzerland, and the United Kingdom applicable to the Processing of Personal Data under the Agreement, including, where applicable, (i) Regulation 2016/679 of the European Parliament and of the Council 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) (the "**EU GDPR**"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (the "**UK GDPR**"); (iii) the Swiss Federal Act on Data Protection of 1 September 2023 and its corresponding ordinances ("**Swiss FADP**"); (iv) the EU e-Privacy Directive (Directive 2002/58/EC); and (v) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii), (iii), (iv).

"**Personal Data**" means any information that (i) is protected as "personal data", "personal information" or "personally identifiable information" under Data Protection Legislation; and (ii) is Processed by CloudTalk on behalf of Customer in the course of providing the Services, as more particularly described in Annex A of this DPA.

"**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of Personal Data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; (ii) where UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not subject based on adequacy regulations pursuant to Section 17A of the UK Data Protection Act 2018; and (iii) where the Swiss FADP applies, a transfer of Personal Data from Switzerland to any other country which is not determined to provide adequate protection for personal data by the Federal Data Protection and Information Commission or Federal Council (as applicable).

"**Sub-processor**" means any third party engaged by CloudTalk to assist in fulfilling its obligations with respect to providing the Services and that Processes Personal Data as Processor.

"Standard Contractual Clauses" or **"EU SCCs"** means the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021.

"Swiss Addendum" means adaptation of the EU SCCs to comply with Swiss FADP as specified in Annex C of this DPA.

"**UK Addendum**" means the International Data Transfer Addendum to the EU SCCs, Version B1.0, issued by Information Commissioners Office under the UK Data Protection Act 2018 as specified in Annex C of this DPA.

The terms "Controller", "Processor", "Process", "Processing" and "Data Subject" shall have the same meanings given to them under the EU/UK Data Protection Laws, and the terms "Business", "Service Provider," "Share," "Sell" and "Sale" have the same meanings given to them under the CCPA.

3. RELATIONSHIP AND ROLES OF THE PARTIES

The Parties acknowledge and agree that, with respect to the Processing of Personal Data, the Customer (or a third party on whose behalf the Customer is authorized to instruct CloudTalk) is the Controller and CloudTalk acts as a Processor (or sub-Processor, as applicable to the Customer's use of the Services). For the purposes of the CCPA, to the extent the CCPA is applicable, the Customer is the Business and CloudTalk is the Service Provider.

4. CLOUDTALK'S OBLIGATIONS

4.1. **Permitted Purposes**. CloudTalk shall Process Personal Data for the permitted purposes described in Annex A of this DPA (the "**Permitted Purposes**").

4.2. **Compliance with Customer Instructions.** CloudTalk shall Process Personal Data in accordance with Customer's documented lawful instructions, except where otherwise required by laws that are compatible with applicable Data Protection Legislation. The Agreement, including this DPA, along with the Customer's configuration of any settings or options in the Services, constitute Customer's complete and final instructions to CloudTalk regarding the Processing of Personal Data, including for the purposes of the Standard Contractual Clauses. Any additional or alternate instructions must be consistent with the terms of the Agreement and this DPA. CloudTalk shall inform the Customer if it becomes aware that Customer's instructions infringe Data Protection Legislation (but without obligation to actively monitor Customer's or, where applicable its Controller's, compliance with Data Protection Legislation).

4.3. **Technical and Organizational Measures.** CloudTalk shall implement and maintain reasonable and appropriate technical and organizational measures designed to protect data, including the Personal Data, from Data Breaches and to preserve security and confidentiality of Personal Data, in accordance with the measures identified in Annex D of this DPA ("**Technical and Organizational Measures**"). Customer acknowledge that the Technical and Organizational Measures are subject to technical progress and development and that CloudTalk may update or modify the Technical and Organizational Measures from time to time, provided that such updates and modifications do not degrade or diminish the overall security of the Services.

4.4. **Personnel Confidentiality and Training.** CloudTalk shall ensure that any person CloudTalk authorizes to Process the Personal Data (including CloudTalk's staff, agents, and sub-processors) ("**Personnel**") is under appropriate obligations of confidentiality (whether a contractual or statutory duty), has received proper training, is informed about the confidential nature of the Personal Data and their obligations related to it, and has access to Personal Data only on a need-to-know basis. CloudTalk shall ensure that Personnel Processes the Personal Data only as necessary for the Permitted Purposes.

4.5. **Data Deletion or Return upon Termination.** Upon termination or expiration of the Agreement, CloudTalk shall delete or return to the Customer all Personal Data in its possession or control, except for one copy for archival and compliance purposes.

4.6. **Processing Subject to the CCPA.** To the extent the CCPA is applicable, CloudTalk shall not: (i) Sell or Share any Personal Data; (ii) retain, use, or disclose any Personal Data (1) for any purpose other than for the business purposes specified in the Agreement, or (2) outside of the direct business relationship between the Customer and CloudTalk; or (iii) combine Personal Data received from, or on behalf of, Customer with Personal Data received from or on behalf of any third party, or collected from CloudTalk's own interaction with Data Subjects, except to perform any business purpose permitted by the CCPA. CloudTalk certifies that it understands the foregoing restrictions under this clause and will comply with them. CloudTalk will comply with applicable obligations under the CCPA

and provide the same level of privacy protection to Personal Data as is required by the CCPA. CloudTalk will notify Customer if it can no longer comply with its obligations under the CCPA. Customer has the right to take reasonable steps to help ensure that CloudTalk uses the Personal Data in a manner consistent with Customer's obligations under the CCPA by exercising Customer's audit rights in Section 5 of this DPA. Customer's transfer of Personal Data to CloudTalk is not a Sale and does not constitute Sharing, and CloudTalk provides no monetary or other valuable consideration to Customer in exchange for Personal Data.

4.7. **Data Protection Impact Assessment**. To the extent required by Data Protection Legislation, CloudTalk shall provide reasonable cooperation regarding the Services to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by Data Protection Legislation.

4.8. **Request for Disclosure**. CloudTalk shall promptly notify the Customer about any legally binding request for disclosure of the Personal Data by a judicial or regulatory authority unless otherwise prohibited, such as the obligation under criminal law to preserve the confidentiality of a judicial enquiry and to assist the Customer accordingly (at Customer's expense).

4.9. **Data Subject Rights**. To the extent that the Customer is unable to access the relevant Personal Data within the Services independently, CloudTalk shall, taking into account the nature of the Processing, provide assistance (including by appropriate technical and organizational measures) to provide reasonable cooperation to the Customer in order to (i) respond to any requests from a Data Subject seeking to exercise any of its rights under Data Protection Legislation (including its right of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a Data Subject, regulator or other third party in connection with the Processing of the Personal Data (collectively "**Correspondence**"). In the event that any such Correspondence is made directly to CloudTalk, it shall promptly notify the Customer and shall not respond directly unless legally compelled to do so. If CloudTalk is required to respond to such Correspondence, CloudTalk shall promptly notify the Customer and provide it with a copy of the request, unless legally prohibited from doing so.

5. CUSTOMER'S RIGHTS

5.1. **Audit Rights.** The Customer shall have the right to conduct an audit to verify CloudTalk's compliance with its obligations under Data Protection Legislation and in this DPA. CloudTalk shall permit the Customer to carry out the audit under the following conditions: (i) the Customer requests to carry out the audit via a written notice at least 30 (thirty) days in advance; (ii) the Customer will specify the agenda for such audit in such notice; (iii) the audit shall not take place more than once a year; (iv) all associated costs and expenses shall be borne by the Customer or reimbursed to CloudTalk on demand; and (v) the audit shall last no longer than the equivalent of 1 working day (8 hours) of CloudTalk's representative. On the request of the Customer, CloudTalk will provide the Customer with the estimated cost that it expects to incur during such audit according to the extent specified in the agenda provided by the Customer.

5.2. **Independent Audit by External Licensed Auditor**. In case the Customer requests the audit by an independent party – external licensed auditor, CloudTalk may object to an external licensed auditor appointed by the Customer to conduct the audit if the auditor is, in CloudTalk's reasonable opinion, not suitably qualified or independent, a competitor of CloudTalk, or otherwise manifestly unsuitable. Any such objection will require the Customer to appoint another auditor.

6. CUSTOMER'S OBLIGATIONS

6.1. Customer's Processing of Personal Data. The Customer shall, in its use of the Services, Process Personal Data in accordance with Data Protection Legislation. The Customer shall have the sole responsibility for the accuracy, quality, and legality of Personal Data and how the Customer acquired Personal Data.

6.2. **Customer's Compliance**. The Customer agrees that (i) it shall comply with its obligations as a Controller under Data Protection Legislation in respect of its Processing of Personal Data and any Processing instructions it issues to CloudTalk; (ii) it has provided notice and obtained (or shall obtain) all consents or any other necessary authorizations (as applicable) under Data Protection Legislation for CloudTalk to Process Personal Data for the Permitted Purposes; (iii) it shall be responsible for providing any notices required by Data Protection Legislation to its permitted users and other relevant Data Subjects with respect to sharing their Personal Data with CloudTalk; (iv) it has fulfilled (or shall fulfil) all registration or notification obligations to which the Customer is subject to under the Data Protection Legislation; and (v) it is responsible for its own Processing of Personal Data, including integrity, security, maintenance, and appropriate protection of Personal Data under Customer's control.

6.3. **Technical and Organizational Measures**. Without prejudice to CloudTalk's obligations under Section 4.3 (Technical and Organizational Measures), the Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Personal Data when in transit to and from the Services, and taking any appropriate technical, organizational, and security measures to securely encrypt or backup any Personal Data uploaded to the Services. The Customer is also responsible for the use of the Services by any person the Customer authorized to access or use the Services, and any person who gains access to its Personal Data or the Services as a result of its failure to use reasonable security precautions, even if the Customer did not authorize such use. The Customer agrees to, immediately upon awareness, notify the CloudTalk of any unauthorized use of the Services or of any other breach of security involving the Services.

7. DATA BREACHES

7.1. **Data Breach Notification**. Upon becoming aware of a Data Breach, CloudTalk shall notify the Customer without undue delay and provide timely information and cooperation as the Customer may reasonably require to fulfill its data breach reporting obligations under Data Protection Legislation. This includes details about the type of data affected and the identity of the affected person(s) as soon as such information becomes known or available to CloudTalk.

7.2. **Disclaimer of Fault or Liability in Data Breach Notifications**. The Customer agrees that any notification provided by CloudTalk to the Customer in relation to a Data Breach shall not be construed or understood as an acknowledgment of any fault or liability.

7.3. **Mitigation.** CloudTalk shall take all reasonable measures and actions to remedy or mitigate the effects of any Data Breach. CloudTalk shall also keep the Customer informed of all developments related to the Data Breach.

7.4. **Customer Caused Data Breaches.** If a Data Breach is caused or materially contributed to by the Customer, CloudTalk will cooperate in the investigation of the Data Breach subject to Customer's obligation to compensate CloudTalk for its expenses and costs.

8. SUB-PROCESSING

8.1. **Authorized Sub-processors.** The Customer provides a general authorization for CloudTalk to engage Sub-processors to Process Personal Data on Customer's behalf. The Sub-processors currently engaged by CloudTalk are specified in Annex B to this DPA.

8.2. **New Sub-processors**. CloudTalk shall provide prior written notice to the Customer before engaging any new Sub-processor, either at the email address associated with the Customer’s Account or via a pop-up window through the Services, as decided by CloudTalk at its sole discretion.

8.3. **Objections**. The Customer may reasonably object to the engagement of a new sub-processor by sending an email to privacy@cloudtalk.io. If the Customer does not send any objection to CloudTalk within ten (10) days of receiving the notification, it will be deemed to have consented to the new

sub-processor and waived its right to object. If the Customer timely objects, the Parties agree to negotiate to resolve the matter in good faith.

8.4. **Liability for Sub-processors**. CloudTalk remains liable for any breach of this DPA caused by an act, error, or omission of its Sub-processors.

9. DATA TRANSFERS FROM THE EUROPEAN ECONOMIC AREA, SWITZERLAND AND THE UNITED KINGDOM

9.1. **Restricted Transfer**. When and to the extent that the transfer of Personal Data from the Customer to CloudTalk is a Restricted Transfer and EU/UK Data Protection Laws require that appropriate safeguards are put in place, the Parties agree that (i) the Standard Contractual Clauses (including the UK Addendum and Swiss Addendum), incorporated by reference into this DPA, shall apply to such transfer; (ii) the Parties will comply with their respective obligations under such Standard Contractual Clauses, UK Addendum and Swiss Addendum; and (iii) the Standard Contractual Clauses, UK Addendum and Swiss Addendum shall be deemed completed as set forth in Annex C of this DPA.

9.2. **Further Restricted Transfer**. In respect of Restricted Transfers made to CloudTalk under clause 9.1 of this DPA, CloudTalk may participate in (or permit any sub-Processor to participate in) any further Restricted Transfers of Personal Data if such further Restricted Transfer is made in compliance with EU/UK Data Protection Laws and based on appropriate transfer mechanism.

10. LIMITATION OF LIABILITY

To the maximum extent permitted by law, each party and its Affiliates' aggregate liability to the other party arising out of or in relation to this DPA (including the Standard Contractual Clauses, Swiss Addendum, UK Addendum), whether in contract, tort or under any other theory of liability, will be subject to the limitations and exclusions of liability (including any agreed aggregate financial cap) set forth under the Agreement. For the avoidance of doubt, nothing in this DPA is intended to limit the rights a Data Subject may have against either Party arising out of such Party's breach of the Standard Contractual Clauses, where applicable.

11. FINAL PROVISIONS

11.1. **Third-Party Beneficiaries**. Data Subjects are the sole third-party beneficiaries of the Standard Contractual Clauses, and there are no other third-party beneficiaries to this DPA, unless specified to the contrary in the Agreement.

11.2. **Governing Law and Jurisdiction**. This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless and to the extent required otherwise by the Data Protection Legislation or the Standard Contractual Clauses (including the UK Addendum or Swiss Addendum).

11.3. **Scope of this DPA.** For the avoidance of doubt, the processing of information other than Personal Data for the Permitted Purposes does not fall under the scope of this DPA.

11.4. **Term.** This DPA will remain in effect for the term of the Agreement plus the period from the expiry of the Agreement until CloudTalk ceases to process Personal Data on behalf of the Customer (the "Processing Term").

Annex A

Description of the Data Processing and Transfer

Annex A (1) List of Parties to the Standard Contractual Clauses:

Data Exporter	**Data Importer**
Name: Customer, as identified in the Agreement	**Name**: CloudTalk, as identified in the Agreement
Address: As identified in the Agreement	**Address**: As identified in the Agreement
Contact details: As identified in the Agreement	**Contact details:** As identified in the Agreement
Activities relevant to the transfer: See Annex A (2) below	**Activities relevant to the transfer:** See Annex A (2) below
Signature and Date: By entering into the Agreement, Data Exporter is deemed to have signed the Standard Contractual Clauses.	**Signature and Date:** By entering into the Agreement, Data Exporter is deemed to have signed the Standard Contractual Clauses.
Role: Controller or Processor (as applicable)	**Role**: Processor or sub-processor (as applicable)

Annex A (2) Description of the Data Processing and Transfer

	Description
Categories of data subjects:	● **permitted users** – any of Customer's employees or other personnel, suppliers and other third parties authorized under the Agreement to use the Services. ● **end customers** – any individuals who contact or are contacted by the Customer using the Services or whose personal data is otherwise processed by Customer to the Services.
Categories of personal data:	● identification and contact data (name, address, title, contact and billing details, username) ● any information shared in calls between the permitted users and end customers ● financial information (credit card details, account details, payment information) ● employment details (employer, job title, geographic location, area of responsibility) ● IT related data (computer ID, user ID, password, IP address, log files) and any other Personal Data Customer configures the Services to collect.
Sensitive data:	CloudTalk does not require any special categories of data to provide the Services and does not intentionally collect or process such data in connection with the provision of the Services.

Frequency of the transfer:	Continuous
Nature and subject matter of processing:	The Personal Data may be subject to the following processing activities: ● storage (hosting) and other processing necessary to provide, maintain and improve the Services provided to Customer under the Agreement, ● technical support provided to the Customer on a case by case basis, ● disclosures in accordance with the Agreement and the DPA, as compelled by law, and ● collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
Duration of the processing:	Subscription Term
Purpose(s) of the data processing:	● Processing to provide, maintain, support, and improve the Services provided to the Customer in accordance with the Agreement; ● Processing initiated by the Permitted users in their use of the Services; ● Processing to comply with other documented reasonable instructions provided by the Customer (e.g., via email) where such instructions are consistent with the Agreement of the Agreement (including this DPA) ● Processing to comply and fulfill legal obligations.
Retention period (or, if not possible to determine, the criteria used to determine that period):	Processing Term

Annex A (3): Competent supervisory authority

With respect to EU Data the competent supervisory authority is to be determined depending on the Customer's competent supervisory authority in accordance with the GDPR, where applicable ("**Supervisory Authority**").

Annex B
List of Approved Sub-processors

The list of approved Sub-processors is available at https://www.cloudtalk.io/sub-processors/

Annex C

STANDARD CONTRACTUAL CLAUSES, SWISS ADDENDUM, UK ADDENDUM

1. **EU Transfers: in relation to Personal Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:**
   - **a)** Where the Customer is a Controller of Personal Data, Module Two (Controller to Processor Clauses) will apply and where the Customer is a Processor acting on behalf of third-party Controllers, Module 3 (Processor to Processor Clauses) will apply;
   - **b)** in Clause 7 (Docking Clause), the optional docking clause will apply;
   - **c)** in Clause 9 (Use of Sub-processors), Option 2 will apply, and the time period for prior notice of sub-processor changes shall be as set out in Section 8.2 of this DPA and the period for notification of objections in Section 8.3 of this DPA;
   - **d)** in Clause 11 (Redress), the optional language to permit data subjects to lodge complaints with an independent dispute resolution body will not apply;
   - **e)** in Clause 17 (Governing Law), Option 1 will apply, and the EU SCCs will be governed by the law of Slovakia;
   - **f)** in Clause 18(b) (Choice of forum and jurisdiction), disputes shall be resolved before the courts of Slovakia;
   - **g)** Annex I of the EU SCCs shall be deemed completed with the information set out in Annex A to this DPA;
   - **h)** Annex II of the EU SCCs shall be deemed completed with the information set out in Annex D to this DPA.

2. Swiss **Transfers: in relation to Personal Data that is protected by** (i) **the** Swiss FADP or (ii) Swiss FADP and EU GDPR**, the EU SCCs in accordance with paragraphs 1 (a) to 1 (d) above, with the following modifications (Swiss Addendum):**

   Where the transfer is exclusively subject to Swiss FADP:
   a) References to EU GDPR are replaced by references to the Swiss FADP;
   b) References to the "EU", "EU Member State", "European Union" and "Union" are replaced with references to Switzerland;
   c) References to the competent supervisory authority are replaced by references to the Federal Data Protection and Information Commissioner in Switzerland (or its replacement or successor) ("FDPIC");
   d) Clause 13 (Supervision): Competent supervisory authority is: FDPIC;
   e) Clause 17 (Governing law): Swiss law.

   Where the transfer is subject to both Swiss FADP and EU GDPR:
   a) References to EU GDPR are supplemented by references to the Swiss FADP
   b) References to the "EU", "EU Member State", "European Union" and "Union" are supplemented with references to Switzerland.
   c) References to competent supervisory authority are supplemented with references to FDPIC.
   d) References to the competent supervisory authority are supplemented by references to the Federal Data Protection and Information Commissioner in Switzerland (or its replacement or successor).
   e) Clause 13 (Supervision): Competent supervisory authority is:
      a. FDPIC, insofar as the transfer is governed by Swiss FADP; and
      b. The Slovak Data Protection Authority, insofar as the transfer is governed by GDPR.
   f) Clause 17 (Governing law): Slovak law

   The term "Member state" must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Standard Contractual Clauses.

3. UK Transfers: in relation to Personal Data that is protected by the UK GDPR, **the EU SCC, completed as set above, shall apply to transfers, expect that:**

a) The EU SCCs shall be deemed amended as specified by the UK Addendum, which shall be deemed executed between the transferring Customer and CloudTalk;
b) Any conflict between the terms of the EU SCCs and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum;
c) For the purposes of the UK Addendum, Tables 1 to 3 in Part 1 of the UK Addendum shall be deemed completed using the information contained in the Annexes of this DPA; and
d) (iv) Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting “neither party.”

UK ADDENDUM

Part 1: Tables
Table 1: Parties

Start date	See Annex A	
The Parties	Exporter	Importer
Parties' details	See Annex A (1)	See Annex A (1)
Key Contact	See Annex A (1)	See Annex A (1)

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs		☒ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:				
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1.	N/A					
2.	X	Applies	Does not apply	General authorisation	See clause 8 of this DPA	N/A
3.	X	Applies	Does not apply	General authorisation	See clause 8 of this DPA	N/A
4.	N/A					

Table 3: Appendix Information

Annex 1A: List of Parties:	See Annex A (1) of the DPA
Annex 1B: Description of Transfer:	See Annex A(2) of the DPA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:	See Annex D of the DPA
Annex III: List of Sub processors (Modules 2 and 3 only):	See Annex B of the DPA

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Neither Party

Part 2: Mandatory Clauses
Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses. By entering into the DPA, the parties are deemed to have signed the mandatory clauses, incorporated herein by reference, as of the Effective date of the DPA.

Annex D

Technical and Organizational Measures

Full description of the technical and organizational security measures implemented by CloudTalk is available at www.cloudtalk.io/security-whitepaper.

1. ACCESS CONTROL

1.1 Unauthorized persons shall be prevented from gaining physical access to premises, buildings or rooms, where data processing systems are located which process personal data. Exceptions may be granted for the purpose of auditing the facilities to third party auditors as long as they are supervised by CloudTalk and do not get access to the personal data themselves.

1.2 CloudTalk acknowledges that it has (without limitation) implemented the following controls:

1.2.1 controls to specify authorized individuals permitted to access personal data;

1.2.2 implemented an access control process to avoid unauthorized access to the company's premises;

1.2.3 implemented an access control process to restrict access to data centers / rooms where data servers are located;

1.2.4 utilizes video surveillance and alarm devices with reference to access areas; and

1.2.5 ensured that personnel without access authorization (e.g. technicians, cleaning personnel) are accompanied all times when accessing data processing areas.

2. SYSTEM ACCESS CONTROL

2.1 Data processing systems must be prevented from being used without authorization.

2.2 CloudTalk acknowledges that has (without limitation) implemented the following controls:

2.2.1 ensured that all systems processing personal data (this includes remote access) are password protected:

2.2.1.1 after boot sequences, and

2.2.1.2 when left even for a short period;

2.2.2 to prevent unauthorized persons from accessing any personal data;

2.2.3 provides dedicated user IDs for authentication against systems user management for every individual;

2.2.4 assigns individual user passwords for authentication;

2.2.5 ensured that access control is supported by an authentication system;

2.2.6 controls to grant access only to authorized personnel and to assign only the minimum permissions necessary for those personal to access personal data in the performance of their function;

2.2.7 implemented a password policy that prohibits the sharing of passwords and outlines processes after a disclosure of a password;

2.2.8 ensured that passwords are always stored in encrypted form;

2.2.9 implemented a proper procedure to deactivate user account, when a user leaves the company or function;

2.2.10 implemented a proper process to adjust administrator permissions, when an administrator leaves company or function; and

2.2.11 implemented a process to log all access to systems and review those logs for security incidents.

3. DATA ACCESS CONTROL

3.1 Persons entitled to use a data processing system shall gain access only to the data to which they have a right of access, and personal data must not be read, copied, modified or removed without authorization in the course of processing.

3.2 CloudTalk acknowledges that it has (without limitation) implemented the following controls:

3.2.1 restricted access to files and programs based on a "need-to-know-basis";

3.2.2 stored physical media containing personal data in secured areas;

3.2.3 established rules for the safe and permanent destruction of data that are no longer required; and

3.2.4 controls to grant access only to authorized personnel and to assign only the minimum permissions necessary for those personal to access personal data in the performance of their function.

4. DATA TRANSMISSION CONTROL

4.1 Personal data must not be read, copied, modified or removed without authorization during transfer or storage and it shall be possible to establish to whom personal data was transferred.

4.2 CloudTalk acknowledges that it has (without limitation) implemented the following controls:

4.2.1 encrypt data during any transmission and at rest;

4.2.2 transport physical media containing personal data in sealed containers; and

4.2.3 have shipping and delivery notes.

5. DATA ENTRY CONTROL

5.1 CloudTalk shall be able retrospectively to examine and establish whether and by whom personal data have been entered into data processing systems, modified or removed.

5.2 CloudTalk acknowledges that it has (without limitation) implemented the following controls:

5.2.1 controls to log administrators' and users' activities; and

5.2.2 controls to permit only authorized personnel to modify any personal data within the scope of their function.

6. JOB CONTROL

6.1 CloudTalk acknowledges that it has (without limitation) implemented the following controls:

6.1.1 established controls to ensure processing of personal data only for contractual performance;

6.1.2 controls to ensure staff members and contractors comply with written instructions or contracts; and

6.1.3 ensured that data is always physically or logically separated so that, in each step of the processing, the client from whom personal data originates can be identified.

7. AVAILABILITY CONTROL

7.1 Personal data shall be protected against disclosure, accidental or unauthorized destruction or loss.

7.2 CloudTalk acknowledges that it has (without limitation) implemented the following controls:

7.2.1 arrangements to create back-up copies stored in specially protected environments;

7.2.2 arrangements to perform regular restore tests from those backups;

7.2.3 contingency plans or business recovery strategies;

7.2.4 controls to ensure that personal data is not used for any purpose other than for the purposes it has been contracted to perform;

7.2.5 controls to prevent removal of personal data from the data importer's business computers or premises for any reason (unless data exporter has specifically authorized such removal for business purposes);

7.2.6 controls to use only authorized business equipment to perform the services;

7.2.7 controls to ensure that whenever a staff member leaves its desk unattended during the day and prior to leaving the office at the end of the day, he/she places materials containing personal data in a safe and secure environment such as a locked desk drawer, filing cabinet, or other secured storage space. (clean desk);

7.2.8 implemented a process for secure disposal of documents or data carriers containing personal data;

7.2.9 implemented network firewalls to prevent unauthorized access to systems and services and

7.2.10 ensured that each system used to process personal data runs an up to date antivirus solution.

8. ORGANIZATIONAL REQUIREMENTS

8.1 The internal organization of the data importer shall meet the specific requirements of data protection. In particular, the data importer shall take technical and organizational measures to avoid the accidental mixing of personal data.

8.2 CloudTalk acknowledges that it has (without limitation) implemented the following controls:

8.2.1 designated a data protection officer (or a responsible person if a data protection officer is not required by law);

8.2.2 obtained the written commitment of the employees to maintain confidentiality;

8.2.3 trained staff on data privacy and data security;

8.2.4 implemented a formal security incident response process that is consistently followed for the management of security incidents; and

8.2.5 trained staff in the security incident responder roles on the security incident process.