

Data Processing Agreement

This Data Processing Agreement ("DPA") forms part of and supplements the agreement between Customer and Cyberly that governs Customer's use of the Application Access services (the "Agreement"), including the Cyberly Terms of Service available at <https://cyberly.ai/assets/cyberly-terms.pdf>, as updated from time to time. This DPA is entered into between the Customer (being you and/or the entity you represent, as applicable) and the applicable Cyberly contracting entity identified in the Agreement ("Cyberly" or "Processor").

Whereas, in connection with the performance of its obligations under the Agreement, the Processor may Process Controller Personal Data (both as defined below) on behalf of the Controller; and

Whereas, the parties wish to set forth mutual obligations with respect to the processing of Controller Personal Data by the Processor;

Now, therefore, intending to be legally bound, the Parties hereby agree as follows:

1. **Definitions.** In addition to capitalized terms defined elsewhere in this DPA, the following terms shall have the meanings set forth below:
 - 1.1. **"Affiliate"** means any entity that directly or indirectly controls, is controlled by or is under common control with the subject entity. "Control" for purposes of this definition means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.
 - 1.2. **"Applicable Law"** means all laws and regulations that apply to and are binding on the processing of Personal Data in connection with the provision of the Applicable Access services, including the Regulation 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, and repealing Directive 95/46/EC (General Data Protection Regulation) ("**GDPR**") where applicable;
 - 1.3. **"Controller Personal Data"** means any Personal Data Processed by Processor on behalf of Controller pursuant to or in connection with the Agreement;
 - 1.4. **"Sub Processor"** means any person (excluding an employee of Processor) or entity, including a Processor Affiliate, appointed by or on behalf of Processor or any Processor Affiliate and approved in advance and in writing by Controller to Process Personal Data on behalf of the Controller in connection with the Agreement; and

- 1.5. The terms "**Controller**", "**Data Subject**", "**Data Protection Officer**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processor**", "**Processing**" and "**Supervisory Authority**" shall have the meanings ascribed to them in the Applicable Law.

2. Processing of Controller Personal Data.

- 2.1. Processor shall Process Controller Personal Data on Controller's behalf and at the Controller's instructions as specified in this DPA, including without limitation, with regard to transfers of Controller Personal Data to a third country or international organization. Any other Processing shall only be permitted in the event that such Processing is required by Applicable Law to which the Processor is subject. In such event, Processor shall, unless prohibited by such EU Data Protection Laws, inform Controller of that requirement before engaging in such Processing. The Controller guarantees that it is entitled to entrust Processor with the Processing of the Personal Data covered by this DPA.
- 2.2. Controller instructs Processor (and authorizes Processor to instruct each Sub Processor) to (i) Process Controller Personal Data in accordance with Controller's written instructions, for the sole purpose of provision of the services, as detailed in the Agreement ("**Services**"), as set forth in this DPA and/or as otherwise directed by Controller; and (ii) transfer Controller Personal Data to a country or territory as strictly necessary for the provision of the Services, subject to Applicable Law and the Controller's prior written consent. The Controller's instructions which relate to a change in the scope or manner of provision of the Services constitute an order to the Processor of an additional service for the performance of which the Processor is entitled to additional remuneration.
- 2.3. Processor will not solicit Personal Data from Controller's Data Subjects except as expressly directed by Controller in writing. Processor is expressly prohibited from collecting and/or using data obtained from any source not specifically detailed in the Agreement and/or this DPA, including illegal sources. Processor will not disclose any Controller Personal Data to any person or entity without the prior written approval of Controller, unless in accordance with GDPR and/or this DPA
- 2.4. Processor will document its activities and decision-making processes regarding the implementation of this DPA.
- 2.5. Controller sets forth the details of the Processing of Controller Personal Data, as required by Article 28(3) of the GDPR in **Schedule 1** (*Details of Processing of Controller Personal Data*), attached hereto.

Processor Employees.

- 3.1. Processor shall ensure that access to the Controller Personal Data is limited on a need-to-know and/or access basis and that all Processor employees receiving such access are subject to written confidentiality undertakings or professional or statutory obligations of confidentiality in connection with their access to and use of Controller's Personal Data. Processor's employees and categories of personnel who shall have access to the Controller Personal Data, as well as levels of permitted access are as set forth in **Schedule 2** hereto.
- 3.2. Processor shall implement appropriate organizational controls and security measures and training programs to train those of its personnel authorized to access the Controller Personal Data in order to ensure compliance with the Agreement, this DPA, and Applicable Law.

4. Security.

- 4.1. Processor shall implement and maintain appropriate technical and organizational measures to ensure an appropriate level of security of the Controller Personal Data, including, as appropriate and applicable, structural and corporate segregation of the Controller Personal Data and other security measures commensurate with the type of Controller Personal Data and the risk of a data security breach, including as may be set forth in the Applicable Law and Binding Security Document appended hereto as **Schedule 2**. The parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures. The Processor will therefore evaluate the measures as implemented in accordance with this Section 4 on an ongoing basis and will, at its own cost, tighten, supplement and improve these measures in order to maintain compliance with the requirements set out in this Section.
- 4.2. Without limitation of the foregoing, Processor is obliged to comply with obligations under Applicable Law and will maintain the Controller Personal Data processed separately from data processed for third parties including, without limitation, Processor's other clients.
- 4.3. If required under Applicable Law, Processor will appoint a Data Protection Officer.

5. Personal Data Breach.

- 5.1. Processor shall notify Controller immediately by written notice, no later than 60 hours upon Processor becoming aware of a Personal Data Breach.
- 5.2. In such event, Processor shall provide Controller with all available information relating to (i) the nature of the Personal Data Breach including, where possible, the categories and an approximate number of Data

Subjects concerned; (ii) the likely consequences of the Personal Data Breach; (iii) the name and contact details of the Processor's Data Protection Officer or another contact point where more information can be obtained; and (iv) a description of the measures taken or proposed to be taken by the Processor to address the incident including, where appropriate, measures to mitigate its possible adverse effects.

- 5.3. Processor shall cooperate with Controller in connection with the investigation, mitigation, and remediation of such Personal Data Breach and shall take all necessary and appropriate corrective action.

Sub Processing.

- 5.4. Controller authorizes Processor to appoint (and permits each Sub Processor appointed in accordance with this Section 6 to appoint) Sub-Processors including collaborators, for further processing provided in **Schedule 3**. Accordingly, including to the extent that the Personal data is processed by the Sub Processor concerned, the processing of the Personal data is also subject to the terms and conditions laid down by that Sub Processor.
- 5.5. Processor shall notify Controller of the appointment of any Sub Processor, including full details of the Processing to be undertaken by such Sub Processor thereby giving Controller the opportunity to object to such changes.
- 5.6. With respect to each new Sub Processor, Processor shall:
 - 5.6.1. before the Sub Processor first Processes Controller Personal Data and to the extent reasonably possible, carry out adequate due diligence to ensure that the Sub Processor is committed and able to provide the level of protection for Controller Personal Data required by the Agreement and will provide evidence of such due diligence where requested by Controller or a Supervisory Authority; and
 - 5.6.2. ensure that the arrangement between the Processor and the Sub Processor is governed by a contract or other legal act, including terms that offer a materially similar level of protection for Controller Personal Data as those set out in this DPA and that meet the requirements of Applicable Law, and shall provide a copy of such agreements to Controller upon Controller's request.

7. Data Subject Rights.

- 7.1. Processor shall assist Controller to comply with any of Controller's statutory obligations concerning requests to exercise Data Subject rights under Applicable Law (e.g., for access, rectification, deletion of Controller Personal Data, etc.)

7.2. When a Data Subject whose Personal Data is being Processed by the Processor submits a written request to the Processor to inspect his or her Personal Data, Processor shall:

7.2.1. provide Controller with written notice of the inquiry together with all relevant details within seven (7) days of being approached by the Data Subject; and

7.2.2. not respond to that request except on the written instructions of Controller or as required by Applicable Law to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Law inform Controller of that legal requirement before the Processor responds to the request.

8. Data Protection Impact Assessment and Prior Consultation.

8.1. At Controller's request, the Processor shall provide assistance to Controller for any data protection impact assessments or prior consultations with Supervisory Authorities or other competent data privacy authorities, as required under any Applicable Law.

9. Retention, Deletion, or Return of Controller Personal Data.

9.1. Processor will retain Controller Personal Data only for as long as necessary to satisfy the purposes for which it was provided to Processor by Controller.

9.2. Processor shall promptly delete, return, or destroy all copies of any Controller Personal Data or any portion thereof, including, without limitation deletion from its hard drives, backup devices, and any magnetic or optic media, once such data is no longer necessary to be retained in accordance with Section 9.1 or upon the request of the Controller.

9.3. Notwithstanding the foregoing, Processor may retain Controller Personal Data to the extent required by Applicable Law, provided that such Controller Personal Data shall continue to be retained in accordance with the terms of this DPA.

10. Inspection and Audit Rights.

10.1. Processor and shall make available to Controller or any auditor mandated by Controller, upon Controller's request, all material and information necessary to enable Controller to confirm compliance with this DPA, and shall allow for audits, including inspections, by the Controller or an auditor on its behalf in relation to the Processing of the Controller Personal Data by the Processor.

- 10.2. The audit must meet the following requirements:
- 10.2.1. during the audit, those participating in the audit are required to comply with Processor's internal security and confidentiality procedures;
 - 10.2.2. Processor may make participation in the audit subject to the prior conclusion of an appropriate confidentiality agreement with Processor;
 - 10.2.3. the audit may not be carried out more than once per calendar year and may not last longer than 2 days.
 - 10.2.4. The audit will be carried out with a minimum of 14 days' notice, which should be sent to the e-mail address: legal@cyberly.ai
 - 10.2.5. Each Party shall bear its own costs in carrying out the audit.
 - 10.2.6. Any non-compliance with the Applicable Law found during the audit should be remedied by Processor within the timeframe agreed between the Parties.

11. International transfers

- 11.1. The Parties acknowledge that, due to the nature of the Application Access Services and the technical infrastructure used to provide them, the provision of the Services may involve the transfer of Personal Data to countries outside the jurisdiction in which the Personal Data was originally collected ("Data Transfers"), and the Processor may accordingly undertake such Data Transfers to third-country entities in compliance with Applicable Laws. In such cases, the Parties will ensure that all Data Transfers are carried out in compliance with an appropriate lawful transfer mechanism under Applicable Law, including the mechanisms set out in Schedule 1 (EU SCCs).

EU SCC

- 11.2. Where GDPR applies and a Data Transfer from the EU Controller to Processor occurs, the EU Standard Contractual Clauses (SCCs) adopted by the European Commission under Implementing Decision (EU) 2021/914 are incorporated as part of this DPA by reference and apply as set out in Schedule 1 (EU SCCs).

Alternative Transfer Mechanisms

- 11.3. The EU SCCs will not apply where Processor implements another lawful and recognised transfer mechanism (such as Binding Corporate Rules or an approved certification) that ensures an adequate level of protection under Applicable Laws. Any such mechanism will automatically replace the EU SCCs for the relevant Data Transfers.

12. Liability and Indemnity.

- 12.1. Processor's liability and/or indemnity towards Controller arising directly or indirectly out of or in connection with a breach of this DPA and/or the Applicable Law is governed by the Agreement.
- 12.2. The Controller shall indemnify the Processor against claims, damages, costs, charges or any other demands in connection with this DPA made against the Processor, in particular by any Controller within the meaning of GDPR.

13. General Terms.

- 13.1. **Termination.** This DPA shall terminate automatically upon the termination of the Agreement.
- 13.2. **Governing Law and Jurisdiction.**
 - 13.2.1. The Parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity, or termination or the consequences of its nullity; and
 - 13.2.2. This DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.
- 13.3. **Order of Precedence.**
 - 13.3.1. Nothing in this DPA reduces the Processor's obligations under the Agreement in relation to the protection of Personal Data or permits Processor to Process (or permit the Processing of) Personal Data in a manner that is prohibited by the Agreement. In the event of any conflict or inconsistency between this DPA and the Controller's Privacy Notice, the DPA shall prevail with regard to the processing of Personal Data subject to Applicable Law.
 - 13.3.2. Subject to this Section 12.3, with regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the Parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail. In case of discrepancies between English and Polish version of this DPA, the English version is binding.
- 13.4. **Changes in Applicable Law.**

- 13.4.1. Controller may by prior written notice to Processor, request in writing any variations to this DPA if they are required as a result of any change in, or decision of a competent authority under any applicable EU Data Protection Law in order to allow Controller Personal Data to be Processed (or continue to be Processed) without breach of that EU Data Protection Law; and
- 13.4.2. If Controller gives notice with respect to its request to modify this DPA under Section 12.4.1, Processor shall make best efforts to accommodate such modification request.
- 13.5. **Severance.** Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall either be (i) amended as necessary to ensure its validity and enforceability while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

Schedule 1:

This Schedule sets out the scope, nature and duration of the data processing carried out under the Data Processing Agreement, and also provides the information required for the application of the EU SCCs¹.

Part 1 – details required for EU SCCs

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (time period)	Clause 13 (Supervisory Authority)	Clause 17 (Governing Law)	Clause 18 (Choice of forum and jurisdiction)
2	Yes (to the extent customer as a Controller)	No	No	General Authorisation	7 days	Polish Data Protection Authority	Laws of Poland	Courts of Poland
3	Yes (to the extent customer acts as a Processor)	No	No	General Authorisation	7 days	Polish Data Protection Authority	Laws of Poland	Courts of Poland

Part 2 – details required for Appendix of EU SCCs

A. List of parties

¹ The full text of the EU SCCs is available at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj

Data exporter(s):

Name: The Customer entity indicated in the Agreement.

Address: The address for Customer associated with its account on Cyberly platform or as otherwise specified in the Agreement.

Contact person's name, position and contact details: The contact details associated with Customer's account, or as otherwise specified in the Agreement.

Activities relevant to the data transferred under these Clauses: recipient of the Services under the Agreement.

Role (controller / processor): Controller or Processor where relevant

Data importer(s):

Name: Cyberly contracting entity as identified in the Agreement.

Address: The address specified in the Agreement.

Contact person's name, position and contact details: The contact details for Cyberly specified in the Agreement.

Activities relevant to the data transferred under these Clauses: The activities specified in Section B below.

Role (controller / processor): Processor

B. Description of transfer**The categories of Data Subjects whose personal data is transferred:**

Data Subjects who are Controller's employees, persons employed under contracts other than an employment contract, end users of the Controller's web and mobile application services or other Data Subjects whose Personal Data was received by the Controller for the provision of the Services.

The types of Personal Data transferred:

The personal data transferred includes data related to the performance of duties between the Controller and the Controller's staff member or contractors, including e-mail address, first name, last name, device location, IP, Controller's e-mail language; personal photos sent to Cyberly.ai by its clients (end users of the Controller's web and mobile application services).

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for

instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

The Controller does not transfer sensitive data to the Processor. If such transfers were to occur in accordance with the law, strict purpose restrictions, access restrictions (including access only to employees who have received specialized training), retention of records of instances of data sharing, restrictions on onward transfers, or additional security measures will be applied

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Continuous.

Nature of the processing

Rendering Services in the nature of cloud-based image processing, as detailed in the Agreement. This includes operations such as collection, structuring, storage, analysis, and deletion of data. These activities are carried out in the context of providing Cyberly SaaS applications and cyber-security services, which include, among others, phishing attack simulations, email reporting functionalities, and data collection for risk management purposes.

Purpose of the data transfer and further processing:

Processing necessary to provide the Application Access services as set out in the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

For the duration of the Agreement and, where applicable, for any additional period required by Applicable Law; provided, however, that the Processor shall not be required to purge, or to cause others to purge, electronic archival media automatically generated by backup systems.

For transfers to (sub) processors, also specify subject matter, nature and duration of the processing:

The subject matter, nature and duration of the processing and transfers to subprocessors are described in this schedule and in Schedule 3.

C. COMPETENT SUPERVISORY AUTHORITY

President of the Personal Data Protection Office
Office for Personal Data Protection

D. TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA (AS REQUIRED BY ANNEX II TO EU SCC)

The technical and organizational measures are described in the Schedule 2 to this DPA.

Schedule 2: Binding Security Document

Processor implements the following organizational and technical measures to ensure security of data processing:

1.1. Confidentiality:

All personnel of Processor indicated in Schedule 1 to the DPA have assumed confidentiality obligations as regards Controller's data;

1.2. Physical Security:

Data is stored and processed in Google Cloud Platform data centers, secured in accordance with the Cloud Data Processing Addendum – Appendix 2: Security Measures: <https://cloud.google.com/terms/data-processing-addendum>. Google applies, among other measures, physically secured data centers, access control, CCTV monitoring, alarms, and restricts access exclusively to authorized personnel;

1.3. Electronic Access Control

Processor ensures there is no unauthorized use of the data processing and data storage systems: secure passwords, automatic blocking/locking mechanisms, two-factor authentication;

1.4. Internal access control

Processor ensures there is no unauthorized reading, copying, changes, or deletion of data. Access to data is granted on a need-to-know basis; keeping an updated list of persons with access rights;

1.5. Automated Processing

Processor ensures that, where possible, data is processed automatically and without human access to it. Human access rights are limited to what is inevitably necessary;

1.6. Data entry and deletion control

Processor ensures pre-access verification and logging control so as to define, whether and by whom personal data is entered, changed, or deleted control; policy regarding the removal of magnetic and optical data (including hard drives, portable storage media, backup platforms, etc.);

1.7. Personnel training

Processor provides its personnel with training as regards confidentiality, integrity and availability, and resilience of personal data;

1.8. Availability control

Processor implements measures for prevention of accidental or willful destruction or loss; restoration of access to personal data in a timely manner in the event of a physical or technical incident;

1.9. Security Checks

Processor will perform monitoring for the discovery of breaches of data integrity, as well as regular (at least once per half a year) checks in order to identify what and how information is stored, accessed, used, and processed in any other manner, as well as whether requirements of this DPA and Applicable Laws are met. Processor will take necessary measures to mitigate any identified security risk.

1.10. Contractual Control

Processor ensures there is no third-party data processing without corresponding instructions from Processor and/or Controller, e.g.: through clear and unambiguous contractual arrangements.

Schedule 3. CONSENT FOR APPOINTMENT OF SUB-PROCESSORS

WHEREAS

the Data Processing Agreement was concluded by and between you as user of the Site as defined in the Data Processing Agreement ("**Controller**") and Cyberly ("**Processor**") (the "**Data Processing Agreement**"),

Controller hereby gives its consent to Processor for appointing Sub-processors listed below to assist it in providing the Services and processing Personal Data on behalf of Controller.

List of Subprocessors:

1. Google Cloud

Name	Google Cloud Poland Sp. z o.o., with its headquarters in Warsaw, KRS number: 0000840059
Address	Rondo Ignacego Daszyńskiego 2C, 00-843 Warsaw, Poland
Data Processing Description	https://cloud.google.com/terms and https://cloud.google.com/privacy/gdpr?hl=pl

Contact	https://support.google.com/cloud/contact/dpo
Further processors	Then-current list is available at: Google Cloud Platform Subprocessors Google Cloud

2. OpenAI

Name	OpenAI Ireland Limited, a company registered in the Republic of Ireland, company number 737350
Address	1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland
Data Processing Description	https://openai.com/policies/row-terms-of-use/ and https://openai.com/policies/privacy-policy/
Contact	privacy@openai.com or dpo@openai.com
Further processors	Then-current list is available at: Sub-processor list OpenAI

3. Mailgun (Sinch)

Name	Sinch Sweden AB, a company registered in the Kingdom of Sweden, company number 556747-5495
Address	Sinch Sweden AB, Lindhagensgatan 112, 112 51 Stockholm, Sweden
Data Processing Description	https://www.mailgun.com/legal/terms/ and Explore Data Processing Agreement - Sinch
Contact	privacy@mailgun.com
Further processors	Then-current list is available at: Explore Sub-Processors - Sinch

4. Sendgrid (Twilio)

Name	Twilio Ireland Limited, a company registered in the Republic of Ireland, company number 557454
Address	70 Sir John Rogerson's Quay, Dublin 2, D02 R296, Ireland
Data Processing Description	LINK and https://www.twilio.com/en-us/gdpr
Contact	privacy@twilio.com
Further processors	Then-current list is available at: Twilio Sub-Processors Twilio

5. Cyberly Poland (applicable when Cyberly Inc. is contracting entity)

Name	Cyberly Poland Sp. z o.o., with its headquarters in Warsaw, KRS number: 0001157277
Address	Ul. Krakowskie Przedmieście 13/5, 00-071 Warsaw, Poland

Data Processing Description	Provision of hosting services
Contact	legal@cyberly.ai
Further processors	Cyberly Poland uses the services of the same further processors as indicated in points 1, 2, 3, 4, 6, 7, 8, 9.

5a. Cyberly INC ((applicable when Cyberly Poland sp. z o.o. is contracting entity)

Name	CYBERLY INC with EIN Assigned: 33-2052505 an American company
Address	131 CONTINENTAL DRIVE SUITE 301 NEWARK DE 19713
Data Processing Description	Provision of hosting services
Contact	legal@cyberly.ai
Further processors	Cyberly INC uses the services of the same further processors as indicated in points 1, 2, 3, 4, 6, 7, 8, 9.

6. Superlative Enterprises Pty Ltd (Have I Been Pwned)

Name	Superlative Enterprises Pty Ltd (ABN 62 085 442 020)
Address	Level 11, 2 Corporate Court, Bundall, Queensland, Australia
Data Processing Description	Have I Been Pwned: Data Processing Addendum
Contact	Submit a request – Have I Been Pwned
Further processors	Then-current list is available at (ANNEX 3): Have I Been Pwned: Data Processing Addendum

7. Vapi Inc.

Name	Vapi Inc. incorporated in Delaware
Address	Principal place of business at 95 3rd Street, 2nd Floor, San Francisco, CA 94103, USA
Data Processing Description	Privacy Policy
Contact	support@vapi.ai
Further processors	Then-current list is available at (section: "Service Providers"): Privacy Policy

8. Vonage Business Inc.

Name	Vonage Business Inc.
Address	A company incorporated under the laws of the State of Delaware, USA Registered address: 251 Little Falls Drive, Wilmington, Delaware 19808, USA

Data Processing Description	https://www.vonage.com/legal/data/dpa/ and https://www.vonage.com/legal/privacy-policy/
Contact	privacy@vonage.com
Further processors	Then-current list is available at https://www.vonage.com/legal/subprocessors/applicable-ericsson-affiliates/

9. ElevenLabs Inc.

Name	ElevenLabs Inc.
Address	A company incorporated under the laws of the State of New York, USA Registered address: 169 Madison Ave #2484, New York, NY 10016, United States, Delaware 19808, USA
Data Processing Description	https://elevenlabs.io/dpa and https://elevenlabs.io/privacy-policy
Contact	legal@elevenlabs.io
Further processors	Then-current list is available at https://compliance.elevenlabs.io/

Nothing in this Consent discharges the Data Processor from its obligations under the Data Processing Agreement.