Exhibit Data Processing Agreement

Standard Contractual Clauses

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

Counterparty

(the data controller)

and

Corti ApS

35669825

Kuglegårdsvej 2, 2 sal.

1434 København K

Denmark

(the data processor)

each a ‘party’; together ‘the parties’

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1. Table of Contents

2. Preamble

2.1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2.2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of 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).

2.3. In the context of the provision of Corti's products, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

2.4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

2.5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

2.6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

2.7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

2.8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

2.9. Appendix D contains provisions for other activities which are not covered by the Clauses.

2.10. Appendix E contains provisions for other activities which are not covered by the Clauses.

2.11. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

2.12. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the data controller

3.1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State data protection provisions and the Clauses.

3.2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3.3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

4.1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the

duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

4.2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

5.1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

5.2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

6.1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

6.1.1. Pseudonymisation and encryption of personal data;

6.1.2. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

6.1.3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

6.1.4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

6.2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

6.3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

7.1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

7.2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

7.3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 1 month in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

7.4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

7.5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

7.6. The processor shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the processor has factually disappeared, ceased to exist in law or has become insolvent – the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.7. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

8.1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

8.2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

8.3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

8.3.1. transfer personal data to a data controller or a data processor in a third country or in an international organization

8.3.2. transfer the processing of personal data to a sub-processor in a third country

8.3.3. have the personal data processed in by the data processor in a third country

8.4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

8.5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

9.1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

9.1.1. the right to be informed when collecting personal data from the data subject

9.1.2. the right to be informed when personal data have not been obtained from the data subject

9.1.3. the right of access by the data subject

9.1.4. the right to rectification

9.1.5. the right to erasure ('the right to be forgotten')

9.1.6. the right to restriction of processing

9.1.7. notification obligation regarding rectification or erasure of personal data or restriction of processing

9.1.8. the right to data portability

9.1.9. the right to object

9.1.10. the right not to be subject to a decision based solely on automated processing, including profiling

9.2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

9.2.1. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, Datatilsynet, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

9.2.2. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

9.2.3. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

9.2.4. the data controller's obligation to consult the competent supervisory authority, Datatilsynet, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

9.3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

10.1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

10.2. The data processor's notification to the data controller shall, if possible, take place within 48 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

10.3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

10.3.1. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

10.3.2. the likely consequences of the personal data breach;

10.3.3. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

10.4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

11.1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller by use of anonymization and certify to the data controller that it has done so unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

12.1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

12.2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

12.3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

13. The parties' agreement on other terms

13.1. The parties may agree to other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.


corti

14. Commencement and termination

14.1. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

14.2. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

14.3. If the provision of personal data processing services is terminated, and the personal data is deleted, the Clauses may be terminated by written notice by either party.

15. Data controller and data processor contacts/contact points

15.1. The parties may contact each other using the following contacts/contact points:

15.2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points

On behalf of the data controller:

Name

Position

Telephone

E-Mail

On behalf of the data processor:

Name: Sofia Moula

Position: Privacy Manager & Legal Associate

E-mail: snm@corti.ai

Appendix A Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

Providing the services detailed in the [Subscription Agreement (including the Exhibits) and/or the Reseller Agreement (including the Exhibits) and/or the Integration Partner Agreement (including the Exhibits)], mainly speech recognition, transcription services and/or coding.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

Access, transmission, modification, deletion, anonymization of personal data in connection with the provision of the above-mentioned services.

The services include the use of a machine learning model employed to transcribe audio data, converting audio input into textual output. This model is specifically fine-tuned using audio recordings from consultations, enhancing its accuracy for this particular domain. Importantly, no patient or consultation-specific metadata is utilized during either the inference process (audio to text conversion) or the fine-tuning phase.

For the prediction of medical codes, another machine learning model is utilized. This model processes both raw audio and the textual output generated by the transcription model. Its training involves periodic fine-tuning, incorporating user corrections to continually improve its performance and accuracy in code prediction.

The task of summarization is handled by a proprietary large language model (LLM). This model takes the text transcribed by the first model and processes it according to a specified template provided in the input prompt. Similar to the previous models, this summarization model also benefits from periodic fine-tuning, using corrections from users to refine its output and better meet user expectations.

A.3. The processing includes the following types of personal data about data subjects:

Ordinary and confidential personal data:

- Name
- Address
- Email address
- Phone number
- Date of birth
- ID number
- Recordings
- Transcripts
- Online identifiers
- Login details
- Employee ID
- Job position

Special categories of personal data:

- Health information.
- Possible : political, religious or philosophical belief.
- Possible : Racial and ethnic origin.
- Possible : Sex life or sexual orientation.

A.4. Processing includes the following categories of data subject:

- Personnel (including employees, users, decision makers, key contacts, IT staff, persons logging support case(s), personnel involved in support case(s); and
- Customers, patients and other individuals mentioned in dictations, tasks and files recorded on any Offering, provided to the relevant data controller.

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

The processing will continue until either the Agreement is no longer valid (e.g., because of termination, expiration etc.) All personal data will be deleted 30 days after contract's termination (including backups).

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

Data Processor	DataDog
Company Name	DataDog
CVR Number	36408235
Address in Denmark	Balticagade 14B, 8000 Aarhus C, Denmark
Headquarter Address	13-18 City Quay, 1st Floor, Dublin, D02 ED70 Ireland
Contact	Kerry Acocella General Counsel
Type of subprocessor agreement	We have a generic data processing agreement with Datadog, which can be found on their homepage: https://www.datadoghq.com/legal/data-processing-addendum/. From the agreement, all data from customers is encrypted at rest and in transit.
Description of Processing	Processing of usage telemetry data of Corti's applications.

Data Processor	Microsoft Azure
Company Name	Microsoft
CVR Number	13612870
Address in Denmark	Kanalvej 7, 2800 Kongens Lyngby, Denmark
Headquarter Address	South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland
Contact	Oliver Kaae Vinter SR PARTNER DEV MANAGER olkaaevi@microsoft.com
Type of subprocessor agreement	Standard contract with Microsoft Azure

Description of Processing	All customer data is stored within Microsoft Azure and all services are run within their systems. All data is encrypted in transit and at rest within Microsoft Azure.

Data Processor	Mixpanel
Company Name	Mixpanel
CVR Number	11379955
Address in Denmark	None
Headquarter Address	One Front Street, 28th floor San Francisco, CA, USA 94111
Contact	James Allee (VP of Legal at Mixpanel)
Type of subprocessor agreement	We have a generic data processing agreement with Mixpanel, which can be found on their homepage: https://mixpanel.com/legal/dpa.
Description of Processing	Processing of data of anonymized activity of users of Corti's frontend application.

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's general written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

B.2. Prior notice for the authorisation of sub-processors

The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 1 month in advance

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

The data processor is obliged to process the personal data in accordance with the data controller's instructions under the Reseller Agreement (including the Exhibits) and/or Subscription Agreement (including the Exhibits) and/or the Integration Partner Agreement (including the Exhibits) in a clear format to fulfill its obligations under these agreements including the Exhibits for the purposes stated above in A.1.

C.2. Security of processing

The level of security shall take into account:

Details of the technical and organizational measures to safeguard the rights of the project partners and details of the security measure to prevent unauthorised access to personal data:

Technical and organizational measures taken in order to control access to rooms, in particular to verify authorization: Corti uses a collocation provider with ISAE 3402 Type 2 approved and ISO 27001 certified physical security. This provides full access control and monitoring ensuring HIPAA compliance.

Technical (identity control/password) and organizational (user's personal data) measures taken for the identification and authentication of users: Data is only accessible from within the Corti premise and with an authorized device. Access to the colocation is only possible via an MPLS VPN tunnel from such authorized devices. Devices are authorized using user specific credentials and multi factor authentication.

Authorization and rights of access, as well as monitoring and registration of accesses: Data scientists have their own authentication credentials to access data, and they are only granted access to datasets on a case-by-case basis if deemed necessary by our Chief Technology Officer. Furthermore, we deploy access control, regular security updates, and employee NDA's to keep the data secure.

Measures taken which concern transport, transmission, and communication or archiving (manual or electronic) of the data through informatics support of data, as well as further control: If necessary, data is transferred via Secure FTP or HTTPS which are both using the FIPS approved TLS 1.2 encryption method. Data at rest is encrypted using AES256 which is FIPS approved as well. We have strict guidelines on how to handle the data when being processed including a full audit on who and when data was accessed.

Measures taken to grant the safety (physical and logical) of the data: We have built our entire solution, i.e. database infrastructure and interfaces, to be 100% redundant in case of sudden technical problems or emergencies. #

The technical and organizational measures are continuously improved by Corti according to feasibility and state of the art and brought to a higher level of security and protection.

Corti may change these security measures at any time without notice so long as Corti maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting personal data.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2.

The procedure for handling requests from data subjects and data breaches, including the technical and organizational measures implemented to support this assistance, is described in the data processor's data protection policies .

Upon request from the data controller, the data processor will provide the requested data or remove it, depending on a request, within a timely manner.


corti

C.4. Storage period/erasure procedures

Upon termination of the provision of personal data processing services, the data processor shall delete unless the data controller – after the signature of the contract – has modified the data controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

Microsoft Azure's datacenters in: Ireland & The Netherlands

C.6. Instruction on the transfer of personal data to third countries

Personal Data will be transferred from Denmark to the nearest Azure locations, currently located in

Ireland & The Netherlands.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

The data processor shall once a year at the data processor's expense obtain an auditor's

report from an independent third party concerning the data processor's compliance with the

GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The parties have agreed that the following types of Auditor's report may be used in compliance with the Clauses:

At least one of following:

ISO27001 Certificate incl. Scope and SOA

ISO27701 Certificate

ISAE3000

ISAE3402II or SOC2

And/or participation in audit questionnaires incl. relevant documentation

Or other relevant and similar reports or certifications

The auditor's report shall without undue delay be submitted to the data controller for information.

Appendix D STANDARD CONTRACTUAL CLAUSES (SCC)

Module Two: Controller to Processor

Module Three: Processor to Sub-Processor

If Corti processes any Customer Data that is subject to the GDPR within an EU Restricted Territory, such processing will be governed by the provisions of the EU Standard Contractual Clauses.

The EU Standard Contractual Clauses (Modules Two and Three) with the following modifications are hereby incorporated here:

1. **Module Two (Transfer Controller to Processor)** clauses shall apply to the processing activities concerning Customer's Data, where the Customer is the Controller (exporter) and Corti is the Processor (importer).
2. **Module Three (Transfer Processor to Processor)** clauses shall apply to the processing activities concerning End Customer Data, where the Customer is the Processor (exporter) and Corti is the sub-processor (importer)
    - Clause 7 (Docking Clause) - Optional - shall apply
    - Clause 9(a) (Use of Sub-processors):
        - Module Two - The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The applicable time period shall be 30 (thirty) days.
        - Module Three - The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The applicable time period shall be 30 (thirty) days.
    - Clause 11 (Redress): The option in paragraph (a) shall not apply.
    - Clause 17 (Governing Law): Option 1 shall apply. The applicable law shall be the law of Denmark.
    - Clause 18 (Choice of Forum and Jurisdiction): The courts of Denmark shall be inserted into paragraph (b).

Appendix A: shall be completed as follows:

- List of Parties: as set out in this DPA, with the Customer being the data exporter and Corti being the data importer.
- Description of Transfer: as set out in this DPA.
- Competent Supervisory Authority: The Danish Supervisory Authority.

Appendix B: shall be completed as follows:

- The sub-processors as set out in this DPA.

Appendix E The parties' terms of agreement on other subjects