Data Processing in Accordance with Article 28
General Data Protection Regulation (GDPR)

Agreement

between

.....
the Controller – hereinafter referred to as the Client –

and

Ciara GmbH
Karl-Theodor-Str. 55
80803 Munich
Germany

.....
the Processor - hereinafter referred to as the Supplier

1. Subject matter and duration of the Order or Contract

(1) Subject Matter: The Subject matter of the Order or Contract results from The Ciara Terms of Service dated May 2020, which is referred to here (hereinafter referred to as The Ciara Terms of Service).

(2) Duration: The duration of this Order or Contract corresponds to the duration of The Ciara Terms of Service.

2. Specification of the Order or Contract Details

(1) Nature and Purpose of the intended Processing of Data: Nature and Purpose of Processing of personal data by the Supplier for the Client are precisely defined in The Ciara Terms of Service.

(2) The undertaking of the contractually agreed Processing of Data shall be carried out exclusively within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA). Each and every Transfer of Data to a State which is not a Member State of either the EU or the EEA requires the prior agreement of the Client and shall only occur if the specific Conditions of Article 44 et seq. GDPR have been fulfilled.

(3) The Subject Matter of the processing of personal data comprises the following data types: Key Personal Data, Contact Data, Conversation Data, and Customer History.

The Categories of Data Subjects comprise Customers, Potential Customers, Subscribers, Employees, Suppliers, Authorised Agents, and Contact Persons.

3. Technical and Organisational Measures

(1) Before the commencement of processing, the Supplier shall document the execution of the necessary Technical and Organisational Measures, set out in advance of the awarding of the Order or Contract, specifically with regard to the detailed execution of the contract, and shall present these documented measures to the Client for inspection. Upon acceptance by the Client, the documented measures become the foundation of the contract. Insofar as the inspection/audit by the Client shows the need for amendments, such amendments shall be implemented by mutual agreement.

(2) The Supplier shall establish the security in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR must be taken into account. Please refer to Appendix 1 for a detailed description of the Technical and Organisational Measures taken by the Supplier.

(3) The Technical and Organisational Measures are subject to technical progress and further development. In this respect, it is permissible for the Supplier to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

4. Rectification, restriction and erasure of data

(1) The Supplier may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Client, but only on documented instructions from the Client.

(2) Insofar as a Data Subject contacts the Supplier directly concerning a rectification, erasure, or restriction of processing, the Supplier will immediately forward the Data Subject's request to the Client.

(3) Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the Supplier in accordance with documented instructions from the Client without undue delay.

5. Quality assurance and other duties of the Supplier

(1) In addition to complying with the rules set out in this Order or Contract, the Supplier shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, the Supplier ensures, in particular, compliance with the following requirements:

(2) Appointed Data Protection Officer, who performs his/her duties in compliance with Articles 38

and 39 GDPR.

- The Client shall be informed of his/her contact details for the purpose of direct contact. The Client shall be informed immediately of any change of Data Protection Officer.
- The Supplier has appointed a Data Protection Officer according to the Ciara Privacy Policy accessible via the Ciara website (https://www.getciara.com/privacy-policy/). The Client shall be informed immediately of any change of Data Protection Officer.

6. Subcontracting

(1) Subcontracting for the purpose of this Agreement is to be understood as meaning services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The Supplier shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Client's data, even in the case of outsourced ancillary services.

(2) The Supplier may commission subcontractors (additional contract processors) only after prior explicit written or documented consent from the Client. The Client agrees to the commissioning of the following subcontractors on the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR:

Company	Address/country	Service
Heroku Inc., a Salesforce Company	Salesforce Tower, 415 Mission Street, 3rd Floor, San Francisco, CA 94105, USA	Data Hosting
Hubspot Inc.	25 First Street, 2nd Floor, Cambridge, MA 02141, USA	Customer Relationship Management
Intercom Inc.	55 Second Street, San Francisco, CA 94105, USA	Customer Communications
Mixpanel Inc.	405 Howard Street, 2nd Floor, San Francisco, CA 94105, USA	Customer Analytics
Heap Inc.	460 Bryant Street 3rd Floor, San Francisco, CA 94107 USA	Product Analytics

Outsourcing to subcontractors or changing the existing subcontractor are permissible when:

- The Supplier submits such an outsourcing to a subcontractor to the Client in writing or in text form with appropriate advance notice; and
- The Client has not objected to the planned outsourcing in writing or in text form by the date of handing over the data to the Supplier; and
- The subcontracting is based on a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR.

(3) The transfer of personal data from the Client to the subcontractor and the subcontractor's commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved.

(4) If the subcontractor provides the agreed service outside the EU/EEA, the Supplier shall ensure compliance with EU Data Protection Regulations by appropriate measures. The same applies if service providers are to be used within the meaning of Paragraph 1 Sentence 2.

(5) Further outsourcing by the subcontractor requires the express consent of the Supplier (at the minimum in text form);

All contractual provisions in the contract chain shall be communicated to and agreed with each and every additional subcontractor.

7. Supervisory powers of the Client

(1) The Client has the right, after consultation with the Supplier, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to convince itself of the compliance with this agreement by the Supplier in his business operations by means of random checks, which are ordinarily to be announced in good time.

(2) The Supplier shall ensure that the Client is able to verify compliance with the obligations of the Supplier in accordance with Article 28 GDPR**.** The Supplier undertakes to give the Client the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.

(3) Evidence of such measures, which concern not only the specific Order or Contract, may be provided by

- Compliance with approved Codes of Conduct pursuant to Article 40 GDPR;
- Certification according to an approved certification procedure in accordance with Article 42 GDPR;
- Current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor)
- A suitable certification by IT security or data protection auditing.

(4) The Supplier may claim remuneration for enabling Client inspections.

8. Communication in the case of infringements by the Supplier

(1) The Supplier shall assist the Client in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. These include:

a) Ensuring an appropriate level of protection through Technical and Organizational Measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.
b) The obligation to report a personal data breach immediately to the Client.
c) The duty to assist the Client with regard to the Client's obligation to provide information to the Data Subject concerned and to immediately provide the Client with all relevant information in this regard.
d) Supporting the Client with its data protection impact assessment.
e) Supporting the Client with regard to prior consultation of the supervisory authority.

(2) The Supplier may claim compensation for support services which are not included in the description of the services and which are not attributable to failures on the part of the Supplier.

9. Authority of the Client to issue instructions

(1) The Client shall immediately confirm oral instructions (at the minimum in text form).

(2) The Supplier shall inform the Client immediately if he considers that an instruction violates Data Protection Regulations. The Supplier shall then be entitled to suspend the execution of the relevant instructions until the Client confirms or changes them.

10. Deletion and return of personal data

(1) Copies or duplicates of the data shall never be created without the knowledge of the Client, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

(2) After conclusion of the contracted work, or earlier upon request by the Client, at the latest upon termination of the Service Agreement, the Supplier shall hand over to the Client or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into its possession, in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on request.

(3) Documentation which is used to demonstrate orderly data processing in accordance with the Order or Contract shall be stored beyond the contract duration by the Supplier in accordance with the respective retention periods. It may hand such documentation over to the Client at the end of the contract duration to relieve the Supplier of this contractual obligation.

[Signature Page]

(Date, Place)

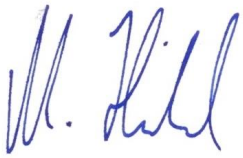
(Signature Controller / Client

Company:

Name:

Title:)

Munich, May 26th, 2020



(Ort, Datum)

(Signature Processor
Ciara GmbH
Dr. Martin Heibel
Managing Director)

Appendix 1 - Technical and Organisational Measures

1. **Confidentiality (Article 32 Paragraph 1 Point b GDPR)**

- Physical Access Control
  No unauthorised access to Data Processing Facilities, keys, electronic door openers
- Electronic Access Control
  No unauthorised use of the Data Processing and Data Storage Systems, secure passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media
- Internal Access Control (permissions for user rights of access to and amendment of data)
  No unauthorised Reading, Copying, Changes or Deletions of Data within the system, rights authorisation concept, need-based rights of access
- Isolation Control
  The isolated Processing of Data, which is collected for differing purposes, multiple Client support, sandboxing;
- Pseudonymisation (Article 32 Paragraph 1 Point a GDPR; Article 25 Paragraph 1 GDPR)
  The processing of personal data in such a method/way, that the data cannot be associated with a specific Data Subject without the assistance of additional Information, provided that this additional information is stored separately, and is subject to appropriate technical and organisational measures.

2. **Integrity (Article 32 Paragraph 1 Point b GDPR)**

- Data Transfer Control
  No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, Encryption, electronic signature;
- Data Entry Control
  Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, Logging, Document Management

3. **Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)**

- Availability Control
  Prevention of accidental or wilful destruction or loss, Backup Strategy (online, on-site & off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning
- Rapid Recovery (Article 32 Paragraph 1 Point c GDPR) (Article 32 Paragraph 1 Point c GDPR);

4. **Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)**

- Data Protection Management;
- Incident Response Management;
- Data Protection by Design and Default (Article 25 Paragraph 2 GDPR);
- Order or Contract Control
  No third party data processing as per Article 28 GDPR without corresponding instructions from the Supplier, clear and unambiguous contractual arrangements, strict controls on the selection of the Service Provider, duty of pre-evaluation, supervisory follow-up checks.