Data Processing Agreement

Agreement on the processing of personal data on behalf of a controller pursuant to Art. 28 GDPR between the customer (hereinafter referred to as "**Customer**") and CA Customer Alliance GmbH, Ullsteinstr. 130, 12109 Berlin, Germany (hereinafter referred to as "**Supplier**").

1. Subject of the Agreement

In the course of rendering services as per the service agreement (hereinafter referred to as "**Main Agreement**"), it is necessary that the Supplier deals with personal data with regard to which the Customer acts as a controller in terms of data protection law (hereinafter referred to as "**Customer Data**"). This agreement specifies the data protection obligations and rights of the parties in connection with the Supplier's use of Customer Data to render the services under the Main Agreement.

2. Scope of the commissioning

2.1. The Supplier shall process the Customer Data on behalf and in accordance with the instructions of the Customer within the meaning of Art. 28 GDPR (Processing on Behalf). The Customer remains the controller in terms of data protection law.

2.2. The processing of Customer Data by the Supplier occurs in the manner and the scope and for the purpose determined in **Annex 1** to this agreement; the processing relates to the types of personal data and categories of data subjects specified therein. The duration of processing corresponds to the term of the Main Agreement.

2.3. The processing of Customer Data by the Supplier shall in principle take place inside the European Union or another contracting state of the European Economic Area (EEA). The Supplier is nevertheless permitted to process Customer Data in accordance with the provisions of this agreement outside the EEA if he informs the Customer in advance about the place of data processing and if the requirements of Art. 44 to 48 GDPR are fulfilled or if an exception according to Art. 49 GDPR applies.

3. Right of the Customer to issue instructions

3.1. The Supplier processes the Customer Data in accordance with the instructions of the Customer, unless the Supplier is legally required to do otherwise. In the latter case, the Supplier shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3.2. The instructions of the Customer are in principle conclusively stipulated and documented in the provisions of this agreement. Individual instructions which deviate from the stipulations of this agreement or which impose additional requirements require mutual agreement and shall be made writing.

3.3. The Supplier shall ensure that the Customer Data is processed in accordance with the

instructions given by the Customer. If the Supplier is of the opinion that an instruction given by the Customer infringes this agreement or applicable data protection law, he is after correspondingly informing the Customer entitled to suspend the execution of the instruction until the Customer confirms the instruction.

4. Legal Responsibility of the Customer

4.1. The Customer is solely responsible for the permissibility of the processing of the Customer Data and for safeguarding the rights of data subjects in the relationship between the parties.

4.2. The Customer is responsible to provide the Supplier with the Customer Data in time for the rendering of services according to the Main Agreement and he is responsible for the quality of the Customer Data. The Customer shall inform the Supplier immediately and completely if during the examination of the Supplier's results he finds errors or irregularities with regard to data protection provisions or his instructions.

4.3. If the Supplier is required to provide information to a governmental body or person on the processing of Customer Data or to cooperate with these bodies in any other way, the Customer is obliged at first request to assist the Supplier in providing such information and in fulfilling other cooperation obligations.

5. Requirements for personnel

The Supplier shall commit all persons engaged in processing Customer Data to confidentiality with respect to the processing of Customer Data.

6. Security of processing

6.1. The Supplier takes according to Art. 32 GDPR necessary, appropriate technical and organizational measures, taking into account the state of the art, the implementation costs and the nature, scope, circumstances and purposes of the Customer Data, as well as the different likelihood and severity of the risk to the rights and freedoms of the data subjects, in order to ensure a level of protection of Customer Data appropriate to the risk. The current measures can be found in **Annex 2**.

6.2. The Supplier shall have the right to modify technical and organizational measures during the term of the agreement, as long as they continue to comply with the statutory requirements.

7. Engagement of further processors

7.1. The Customer grants the Supplier the general authorization to engage further processors with regard to the processing of Customer Data. Further processors consulted at the time of conclusion of the agreement result from **Annex 3**. In general, no authorization is required for contractual relationships with service providers that are concerned with the examination or maintenance of data processing procedures or systems by third parties or that involve other additional services, even if access to Customer Data cannot be excluded, as long as the Supplier takes reasonable steps to protect the confidentiality of the Customer Data.

7.2. The Supplier shall notify the Customer of any intended changes in relation to the consultation or replacement of further processors. In individual cases, the Customer has the right to object to the engagement of a potential further processor. An objection may only be raised by the Customer for important reasons which have to be proven to the Supplier. Insofar as the Customer does not object within 14 days after receipt of the notification, his right to object to the corresponding engagement lapses. If the Customer objects, the Supplier is entitled to terminate the Main Agreement and this agreement with a notice period of three (3) months.

7.3. The agreement between the Supplier and the further processor must impose the same obligations on the latter as those incumbent upon the Supplier under this agreement. The parties agree that this requirement is fulfilled if the contract has a level of protection corresponding to this agreement, respectively if the obligations laid down in Art. 28 para. 3 GDPR are imposed on the further processor.

8. Data subjects' rights

8.1. The Supplier shall support the Customer within reason by virtue of technical and organizational measures in fulfilling the latter's obligation to respond to requests for exercising data subjects' rights.

8.2. As far as a data subject submits a request for the exercise of his rights directly to the Supplier, the Supplier will forward this request to the Customer in a timely manner.

8.3. The Supplier shall inform the Customer of any information relating to the stored Customer Data, about the recipients of Customer Data to which the Supplier shall disclose it in accordance with the instruction and about the purpose of storage, as far as the Customer does not have this information at his disposal and as far as he is not able to collect it himself.

8.4. The Supplier shall, within the bounds of what is reasonable and necessary enable the Customer to correct, delete or restrict the further processing of Customer Data, or at the instruction of the Customer correct, block or restrict further processing himself, if and to the extent that this is impossible for the Customer.

9. Notification and support obligations of the Supplier

9.1. Insofar as the Customer is subject to a statutory notification obligation due to a breach of the security of Customer Data (in particular pursuant to Art. 33, 34 GDPR), the Supplier shall inform the Customer in a timely manner of any reportable events in his area of responsibility. The Supplier shall assist the Customer in fulfilling the notification obligations at the latter's request to the extent reasonable and necessary.

9.2. The Supplier shall assist the Customer to the extent reasonable and necessary with data protection impact assessments to be carried out by the Customer and, if necessary, subsequent consultations with the supervisory authority pursuant to Art. 35, 36 GDPR.

10. Deletion of Customer Data

10.1. The Supplier shall delete the Customer Data upon termination of this agreement, unless the Supplier is obligated by law to further store the Customer Data.

10.2. The Supplier may keep documentation, which serves as evidence of the orderly and accurate processing of Customer Data, also after the termination of the agreement.

11. Evidence and audits

11.1. The Supplier shall provide the Customer, at the latter's request, with all information required and available to the Supplier to prove compliance with his obligations under this agreement.

11.2. The Customer shall be entitled to audit the Supplier with regard to compliance with the provisions of this agreement, in particular the implementation of the technical and organizational measures; including inspections.

11.3. In order to carry out inspections in accordance with Section 11.2, the Customer is entitled to access the business premises of the Supplier in which Customer Data is processed within the usual business hours (Mondays to Fridays from 10 a.m. to 6 p.m.) after timely advance notification in accordance with Section 11.5. at his own expense, without disruption of the course of business and under strict secrecy of the Supplier's business and trade secrets.

11.4. The Supplier is entitled, at his own discretion and taking into account the legal obligations of the Customer, not to disclose information which is sensitive with regard to the Supplier's business or if the Supplier would be in breach of statutory or other contractual provisions as a result of its disclosure. The Customer is not entitled to get access to data or information about the Supplier's other customers, cost information, quality control and contract management reports, or any other confidential data of the Supplier that is not directly relevant for the agreed audit purposes.

11.5. The Customer shall inform the Supplier in good time (usually at least two weeks in advance) of all circumstances relating to the performance of the audit. The Customer may carry out one audit per calendar year. Further audits are carried out against reimbursement of the costs and after consultation with the Supplier.

11.6. If the Customer commissions a third party to carry out the audit, the Customer shall obligate the third party in writing the same way as the Customer is obliged vis-à-vis the Supplier according to this Section 11 of this agreement. In addition, the Customer shall obligate the third party to maintain secrecy and confidentiality, unless the third party is subject to a professional obligation of secrecy.

11.7. At the discretion of the Supplier, proof of compliance with the obligations under this agreement may be provided, instead of an inspection, by submitting an appropriate, current opinion or report from an independent authority (e.g. auditor, audit department, data protection officer, IT security department, data protection auditors or quality auditors) or a suitable certification by IT security or data protection audit – e.g. according to "BSI-Grundschutz" – ("audit report"), if the audit report makes it possible for the Customer in an appropriate manner to convince himself of compliance with the contractual obligations.

12. Contract term and termination

The term and termination of this agreement shall be governed by the term and termination provisions of the Main Agreement. A termination of the Main Agreement automatically results in a cancellation of this agreement. An isolated termination of this contract is excluded.

13. Liability

13.1. The Supplier's liability under this agreement shall be governed by the limitations of liability provided in the Main Agreement. As far as third parties assert claims against the Supplier which are caused by the Customer's culpable breach of this agreement or one of his obligations as the controller in terms of data protection law affecting him, the Customer shall upon first request indemnify and hold the Supplier harmless from these claims.

13.2. The Customer undertakes to indemnify the Supplier upon first request against all possible fines imposed on the Supplier corresponding to the Customer's part of responsibility for the infringement sanctioned by the fine.

14. Final provisions

14.1. Disputes arising from this contract shall be governed by German law. The place of performance and jurisdiction shall be the Contractor's registered office. In the event of contradictions in the two language versions, the German version shall prevail.

14.2. In case individual provisions of this agreement are ineffective or become ineffective or contain a gap, the remaining provisions shall remain unaffected. The parties undertake to replace the ineffective provision by a legally permissible provision which comes closest to the purpose of the ineffective provision and that thereby satisfies the requirements of Art. 28 GDPR.

14.3. In case of conflicts between this agreement and other arrangements between the parties, in particular the Main Agreement, the provisions of this agreement shall prevail.

Annex:

Annex 1: Purpose, type and extent of the processing of Customer Data, types of personal data and categories of data subjects

Annex 2: Technical and organizational measures

Annex 3: Further Processors

Annex 1 - Purpose, type and extent of the processing of Customer Data, types of personal data and categories of data subjects

1. Purpose of data processing

The Supplier sends messages to end customers of and on behalf of the Customer before and during provision of its service to obtain feedback, improve, standardize and automate communication between Customer and its end customers. The results are processed and evaluated on behalf of the Customer. In addition, evaluations from indirect and derived feedback, such as information from internal and/or public sources, are used to fully represent the voice of the end customer. The Supplier aggregates and thereby anonymizes Customer data collected through the platform in order to offer Customer additional services such as reporting, benchmarking, and KPI monitoring features related to feedback given by Customer's end customers.

2. Types of personal data

a) Master data (e.g. name, gender, language);
b) Contact data (e.g. e-mail address, address, telephone no.);
c) Communication data (e.g. e-mail correspondence);
d) Contract data (e.g. contract duration, information on service provision such as turnover or costs);
e) If applicable, existing individual segmentation data of the Customer for its end customers such as way of contract conclusion (internet, telephone, etc.), country of origin, service category or age group;
f) Evaluation of the Customer by the end customer (customer review);
g) Satisfaction analyses (e.g. text-, topic- and expression evaluations).

3. Categories of data subjects

a) Customer's personnel;
b) End customers of the Customer;
c) Customer's Supplier.

Annex 2 – Technical and organizational measures

The following technical and organisational measures have been taken to protect personal data:

1. Entry control

Unauthorised persons shall be denied access to data processing equipment with which the personal data are processed and used.

Ensured by:

a) Definition of security areas and authorised persons
b) Room security (key, roller blind, etc.)
c) Attendance record
d) Exterior security of the building (fencing, security doors/windows)
e) Care in the selection of security guards
f) Care in the selection of cleaning services
g) Video surveillance of the entrances
h) Key management / documentation of key allocation
i) Automatic access control system
j) Chip cards / transponder systems
k) Manual locking system
l) Security locks
m) Doors with knob (outside)

2. Access control (external)

It must be prevented that data processing systems can be used by unauthorised persons.

Ensured by:

a) Lockability of the data station
b) Login with user name & password and specifications for changing them
c) Encryption of passwords
d) Anti-Virus Software Server
e) Anti-Virus Software Clients
f) Firewall
g) Mobile Device Management
h) Use of VPN tunnels for remote access
i) Locking external interfaces (USB)
j) Encryption of notebooks / tablets
k) Manage user permissions
l) Create user profiles
m) Central password assignment
n) Secure Password Policy
o) Delete / Destroy Policy
p) Data Protection and Security Policy

3. Access control (internal)

Care shall be taken to ensure that those authorised to use a data processing system can only access the data subject to their access authorisation and that personal data cannot be read, copied, modified or removed without authorisation during processing, use and after storage.

Ensured by:

a) User-specific graded rights management
b) Management of user rights by administrators
c) Minimum number of administrators
d) Documentation of rights management
e) Screen darkening during work interruption
f) Regular security updates
g) Shredder (min. level 3, cross cut)
h) Logging of access to applications, specifically when entering, changing and deleting data

4. Separation control

Ensure that data collected for different purposes can be processed separately.

Ensured by:

a) Separate software systems
b) Separate databases and storage
c) Control via authorisation concept
d) Separation through access regulations
e) Setting database rights

5. Transfer control

It shall be ensured that personal data cannot be read, copied, altered or removed without authorisation during electronic transmission or during their transport or storage on data carriers, and that it is possible to check and establish at which points a transmission of personal data is provided for by data transmission equipment.

Ensured by:

a) Determination of powers for the processing of data
b) Determination of the authorised transmitting parties, transmitting recipients and transmission paths
c) Transport security of data carriers
d) Secured W-LAN
e) Regulations on the destruction of data media
f) Encryption

6. Input control

Care must be taken to ensure that it is possible to check and establish retrospectively whether and by whom personal data have been entered into data processing systems, altered or removed.

Ensured by:

a) Read / Write Access Management
b) Logging of read/write accesses and programme calls
c) Marking of data entry documents with name and date after entry
d) Provisions on changing access rights and data responsibility
e) Strict responsibilities for deletions

7. Availability control

Care shall be taken to ensure that personal data is protected against accidental destruction or loss.

Ensured by:

a) Creation of periodic backup copies
b) UPS protection in case of power failure
c) Virus protection/firewall
d) Emergency plan
e) Recovery plan
f) Permanently active DDoS protection

8. Order processing control

It must be ensured that personal data processed on behalf of the client can only be processed in accordance with client's instructions.

Ensured by:

a) Determination of rights and obligations of the contractor
b) Contract for commissioned data processing
c) Training of all employees with access rights
d) Regular data protection audits
e) Agreement on control and audit rights

Annex 3 – Further Processors			
Company, Address	**Service / Type of Processing**	**Legal Coverage**	**Measures for a Comparable Level of Protection (only in Third Countries)**
ALL-INKL.COM - Neue Medien Münnich, Hauptstraße 68, 02742 Friedersdorf Germany	Web-Hosting	Data Processing Agreement	/
CHARGEBEE INC., 340 S. Lemon Avenue, Suite #1537, Walnut, CA 91789 USA	Billing	Standard contractual clause and individual assessment to a level of protection comparable to standard within the EU.	3rd-party-certifications & audits; ISO 27001 certificate; SOC 1/SOC 2 and MFA standards; network, application and operational level security policies; AWS security setup - multiple certifications for data centers, including ISO 27001 compliance, PCI certification and SOC reports.
Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043 USA	Google Workspace Google Analytics	Standard contractual clause and individual assessment to a level of protection comparable to standard within the EU.	ISO-certificates (ISO 27001, 27017, 27018); Data Protection Guideline; Compliance Center & Reports.
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen Germany	Hosting	Data Processing Agreement	/
HubSpot, Inc., 25 First Street, Cambridge, MA 02141 USA	Inbound-Marketing and Sales	Standard contractual clause and individual assessment to a level of protection comparable to standard within the EU.	Binding Corporate Rules; Data Center (ISO 27001 certificate / SOC 2 audit); HTTPs encryption.

Intercom, Inc., 55 2nd Street, 4th Fl., San Francisco, CA 94105 USA	Live-Chat	Standard contractual clause and individual assessment to a level of protection comparable to standard within the EU.	External audits, pentests and bug bounties; SOC 2 audit; ISO 27001 certificate; HIPAA audit; AWS security setup; API and application endpoints are TLS/ SSL only; security policy; security and awareness training.
Impala Travel Technology Ltd., 70 White Lion Street, London, N1 9PP UK	PMS-data-extraction (API)	Data Processing Agreement	Adequate protection of personal data in UK - EU Commission Implementing Decision as of June 28, 2021 - C(2021) 4800.
Mailgun Technologies, Inc., 548 Market Street, Suite 43099, San Francisco, CA 94101 USA	Email-provider (e-mail-API)	Standard contractual clause and individual assessment to a level of protection comparable to standard within the EU.	External network scan and penetration test; data encryption; intrusion detection; vendor management procedure - control and frequent auditing of all sub-processors.
Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA	Office 365	Standard contractual clause and individual assessment to a level of protection comparable to standard within the EU.	External trust & audit reports; ISO 27001, 27017, 27018, 22301, 277701 certificates; data loss prevention policy; SSAE 18 SOC 1 Type II & SSAE 18 SOC 2 Type II compliant.
OVH GmbH, St. Johanner Str. 41-43, 66111 Saarbrücken Germany	Hosting	Data Processing Agreement	/
Scaling Technologies GmbH, Pfarrer-Hillmann-Weg 1, 51069 Köln Germany	Web Operations	Data Processing Agreement	/

Stripe, Inc. 510 Townsend Street San Francisco, CA 94103 USA	Payment Solution	Standard contractual clause and individual assessment to a level of protection comparable to standard within the EU.	Data encryption at rest and for data in transit - HTTPS for all services using TLS (SSL); all card numbers are encrypted at rest with AES-256; audit logs; access management policy; PCI Service Provider Level 1 certificate.
SugarCRM, Inc., 10050 N Wolfe Road, SW2-130 Cupertino, CA 95014 USA	Customer Relationship Management	Standard contractual clause and individual assessment to a level of protection comparable to standard within the EU.	SOC II certificate; encryption for all passwords, key data and backups; all production and customer data is encrypted in transit and at rest; multifactor authentication; data loss prevention tools; hosted in Ireland (EU); AWS security setup - multiple certifications for data centres, including ISO 27001 compliance, PCI certification and SOC reports.
Twilio, Inc., 375 Beale Street, Suite 300, San Francisco, CA 94105 USA	Provider for Short-Messages (SMS)	Standard contractual clause and individual assessment to a level of protection comparable to standard within the EU.	Binding Corporate Rules; security framework based on ISO 27001; ISO/IEC 27001, ISO/IEC 27017 & 27018, SOC 2 Type II, PCI DSS Level 1 certificates; AWS security setup - multiple certifications for data centres, including ISO 27001 compliance, PCI certification and SOC report; databases (customer data) are encrypted using the Advanced Encryption Standard and customer data is encrypted when in transit between customer's software application and the services using TLS v1.2; penetration testing; security incident management policies and procedures in accordance with NIST SP 800-61.