Contract Processing on Behalf (PoB)

per Article 28 of the General Data Protection Regulation (GDPR)

entered into by and between

The Client – hereinafter referred to as "**Controller**" –

and

CA Customer Alliance GmbH
Ullsteinstraße 130
12109 Berlin
Germany

as the order processor – hereinafter referred to as "**Processor**" –.

Section 1 Scope and Duration as to Contract Data Processing on Behalf

(1) The Processor helps the Controller analyse ratings of the Controller on the Internet, actively surveying its customers and receiving new booking, by implementing the order confirmation/customer contract. To do so, the Processor collects, uses and processes personal data of the Controller's customers in connection with performance of the Agreement. The Parties conclude this contract to ensure the resulting mutual data protection obligations.
(2) The Parties conclude the present contract to specify the mutual rights and obligations under data protection law. In cases of doubt, the provisions in the present contract have priority over the provisions of the Agreement.
(3) This PoB applies for all activities in conjunction with the Agreement, in which employees and/or sub processors of the Processor use personal data of the Controller.
(4) The duration of this contract corresponds to the duration of the Agreement, unless governed otherwise by the present PoB.
(5) The right of each Contract Party to terminate the PoB without notice for good cause remains unaffected.

Section 2 Nature and Purpose of Contract Processing on Behalf

(1) The type and purpose of the processing of personal data by the Processor is to contact and ask the Controller's customers to evaluate the performance of the Controller, record the customer rating and then analyse and provide it to the Controller.
(2) The Processor uses the following data types/categories as part of its service for the individual customers of the Controller:

(a) Name;
(b) Title;
(c) Gender;
(d) Language;
(e) Contract duration;
(f) E-mail address;
(g) Telephone number;

(h) Address;
(i) Information on service provision (costs, turnover, number of service subjects)
(j) Any segmentation data available to the Controller, such as contract conclusion method (Internet, telephone, etc.), country of origin, service category or age group;
(k) Assessment of the Controller by the customer (customer rating).

(3) The group of persons affected by handling of the personal data as part of this contract comprises the Controller's customers and can also include the Controller's employees with regard to processing the contract.
(4) The personal data is processed exclusively in the territory of the Federal Republic of Germany, a member of the European Union or another Member State of the Treaty on the European Economic Area.
(5) The Controller and the Processor and, where appropriate, its representatives shall cooperate with the responsible supervisory authority in performing its duties.

Section 3 Technical and Organisational Measures

(1) Within its sphere of responsibility, the Processor shall design the internal organisation such that it meets the legal data protection requirements. The technical and organisational security measures (Art. 32 of GDPR) to be taken by the Processor when processing the order data are based on the following data protection requirements and are ensured as presented below:

(a) Unauthorised persons must be prohibited from accessing the data processing systems used to process and utilise the personal data (**physical access control**):

This shall be ensured in particular via: keys, key distribution guideline, electric door openers, factory security, gatekeepers (for the entire building).

(b) Measures must be put into place to ensure that data processing systems cannot be used by unauthorised persons (**logical access control**):

This shall be ensured in particular via: locking the workstation; assigning user passwords; encryption of passwords

(c) It must be ensured that the authorised persons entitled to use a data processing system can only access the data for which they are authorised, and that personal data cannot be read, copied, changed or deleted during processing (**data access control**):

This shall be ensured in particular via: user-specific graduated rights management.

(d) It must be ensured that personal data cannot be read, copied, changed or deleted without authorisation while it is being electronically transferred or stored on data media, and that it can be checked and established where personal data is to be transferred via data transfer systems (**data transfer control**):

This shall be ensured in particular via: The Controller's customers enter and/or transfer the data themselves. That is implemented via an encrypted SSL connection.

(e) It must be ensured that retrospective checks and findings are possible of whether personal data is entered, changed and deleted in data processing systems, and by whom (**data entry control**):

This shall be ensured in particular via: The Processor's software has a user management feature. The Controller can set up its own users and specify the areas of the software they can access. Among other things, the time at which each user logs in is recorded.

(f) It must be ensured that personal data processed by order can only be processed in accordance with the instructions of the Controller **(control of Processing Instructions)**

This shall be ensured in particular via: Specification of authorisations and obligations of the Processor and Controller to agree control rights and company organisation of the Processor.

(g) It must be ensured that personal data is protected against accidental destruction or loss (**availability control**):

This shall be ensured in particular via: backup methods; hard drive mirroring; antivirus/firewall software. Also uninterruptible power supply (UPS) and emergency plan with the server provider (see Section 6 Par. 2).

(h) It must be ensured that data collected for different purposes can be processed separately (**separation control**):

This shall be ensured in particular via: Each user of the software receives their own area from the Controller, which is separated from the other areas. There is a functional separation between the production server and internal test servers.

(2) The technical and organisational measures are subject to technical progress and advances. Provided the security level does not fall below the measures specified, the Processor can implement alternative measures.

Section 4 Correction, Blocking and Deletion of Data

(1) The Processor must only correct, delete or block the data processed by order if instructed to do so by the Controller.

(2) If one of the affected persons asserts rights, e.g. for provision of information, correction or deletion, directly vis-à-vis the Processor, the Processor shall not react independently; it shall pass the affected persons immediately on to the Controller and await its instructions. (3) The Processor shall help the Processor to fulfil its obligations per Arts. 12 – 22, 32 and 36 of GDPR to the best of its ability with suitable technical and organisational measures.

§ 5 Other Obligations

In addition to complying with the provisions in this Contract, the Processor undertakes the following obligations:

(a) The Processor has appointed a company data protection officer. The Processor publishes the contact data of the data protection officer on its website and notifies the supervisory authority of it. The Processor shall provide evidence of the publication and notification in a suitable manner on request by the Controller.

(b) Persons employed by the Processor for data processing are prohibited from processing personal data without authorisation. The Processor shall oblige all persons commissioned to process and fulfil this Contract (hereinafter referred to as Employees) accordingly (Confidentiality Obligation, Art. 28 Par. 3 b of GDPR) and take due care to ensure compliance with this obligation. Suitable proof of the obligations must be provided to the Controller on request. (c)Implementation and compliance with all technical and organisational measures required for this Order in accordance with Art. 32 of GDPR.

(c) The Controller must be informed immediately of control activities and measures of the supervisory authority where they are related to this Order.

(d) Contract control is implemented via regular audits with regard to the contract implementation and/or fulfilment, in particular compliance and potentially necessary adaptation of provisions and measures to implement the contract.

Section 6 Subcontractors

(1) The Processor is entitled to use subcontractors. If and where personal data of the Controller becomes accessible to a subcontractor, the Processor shall not use this subcontractor without prior consent of the Controller. The Controller shall grant consent unless reasons under data protection laws prevent it, and the Processor proves that the subcontractor fulfils all obligations per this PoB, and in particular that the Controller has direct rights of control and information vis-à-vis the subcontractor. Consent can be revoked with future effect if the subcontractor violates provisions of this PoB. The subcontractors listed in Section 6 Par. 2 are approved by the Controller on conclusion of this PoB.

(2) The following list shows the subcontractors who work for the Processor as part of the services per Section 1 of the PoB.

Sub-Contractors	**Address**	**Service / Activity**
All-Inkl.com – Neue Medien Münich	Hauptstraße 68, D-02742 Friedersdorf	Server provider for our software
Scaling Technologies GmbH	Pfarrer-Hillmann-Weg 1, D-51069 Cologne	Server provider for our software
Datapine GmbH	Oranienstraße 185, D-10999 Berlin	Business intelligence tool

Section 7 Audit Obligations

(1) The Controller is entitled to perform order controls in coordination with the Processor or to have the order controlled by auditors to be named in individual cases. It is entitled to convince itself that the Processor is complying with this Contract in its business premises with random sample controls, which must be announced in good time. The Processor undertakes to provide the Controller with information required to comply with its order control obligation on request, and to make the corresponding proofs available.

(2) With regard to the Controller’s control obligations before starting data processing and during the term of the Contract, the Processor shall ensure that the Controller can convince itself of compliance with the technical and organisational measures taken. To do so, the Processor shall prove to the Controller on request the implementation of the technical and organisational measures. Proof of the implementation of such measures that not only concern the specific order can also be provided by submitting a current attestation or reports by independent bodies (e.g. auditors, reviews, data protection officers, IT security department) or suitable certification by an IT security or data protection audit (e.g. Basic IT Protection per Federal Office for Information Security [BSI]).

(3) With regard to the contractual relationship and the data to be processed by the Processor as part of its implementation, the Controller is responsible for compliance with all data protection laws. The Controller is “Herr der Daten”.

Section 8 Notification in the Event of Infringements in the Responsibility of the Processor

(1) If there is a suspicion of data protection infringements or a suspicion of security-relevant occurrences or other major irregularities in processing personal data by the Processor, by persons employed by it as part of the Contract, or by third parties, the Processor shall inform the Controller immediately in writing. The same applies for audits of the Processor by the data protection supervisory authority.

(2) The Processor shall immediately take the measures required to secure the data and mitigate possible adverse effects for the affected parties, inform the Controller of this and request additional instructions where necessary.

(3) Moreover, the Processor is obliged to provide information to the Controller at any time, where its data is affected by an infringement per Paragraph 1.

Section 9 Authority of the Controller

(1) It is hereby agreed that the data shall only be handled as part of the agreements made and based on instructions from the Controller. The Controller reserves a comprehensive authority to instruct the Processor on the type, scope and method of data processing, which it can specify with individual instructions, as part of the order description made in this Contract. Changes to the processing subject and method changes must be coordinated jointly and documented. The Processor may only provide information to third parties or affected persons after prior approval by the Controller.

(2) The instructions of the Controller are initially specified by this Contract and can thereafter be changed, supplemented or replaced by the Controller in written or text form with individual instructions (individual instructions). The Controller is entitled to issue corresponding instructions at any time. The Processor shall not use the data for any other purpose and in particular is not entitled to pass it on to third parties. Copies and duplicates shall not be produced without the knowledge of the Controller. This does not include backup copies, where they are required to ensure proper data processing, and data which is required to comply with legal archival obligations.
(3) The Processor is obliged to inform the Controller immediately if it is of the opinion that an instruction by the Controller infringes against the data protection laws. The Processor is entitled to delay performance of the corresponding instruction until it has been confirmed or changed by the responsible persons at the Controller.

Section 10 Return and Deletion of Data

(1) The Parties are in agreement that after completion of the contractual work or earlier on request by the Controller – on termination of the Main Contract at the latest – the Processor shall hand over to the Controller or destroy in accordance with data protection requirements after prior consent all documents it has received, any processing and use results produced and data related to the order relationship. This does not apply if there is an obligation to store personal data under Union law or the law of the Federal Republic of Germany.
(2) The Processor is entitled to store documentation that serves as evidence of the orderly and proper data processing beyond the end of the Contract in accordance with the corresponding archival periods. To relieve itself of this responsibility, it can hand it over to the Controller.

Section 11 Liability and Choice of Law

(1) In the internal relationship with the Processor, the Controller shall bear sole responsibility vis-à-vis the affected parties for compensation of damages suffered by an affected party due to illegal or improper data processing or use under the data protection laws as part of the order processing.
(2) The Parties shall mutually indemnify one another from liability if one Party proves that it is in no way responsible for the circumstance which caused the damage to the affected Party.
(3) The present Contract is subject to German law.
(4) The place of execution is the registered address of the Processor.
(5) The sole court of jurisdiction for disputes resulting from this contract is Berlin.

Section 12 Final Provisions

(1) No verbal subsidiary agreements have been made. Changes, supplements and additions to this contract shall only be valid if agreed in writing by the Parties. This shall also apply for amendment of this contract provision. The priority of individual contractual agreements shall remain unaffected by this.
(2) Should one provision of this Contract be or become invalid, the validity of the other provisions in this Contract shall not be affected. The Parties are obliged to replace the invalid provision with a valid provision that comes closest to the economic purpose of the invalid provision. The same applies accordingly for any contractual loopholes.