Remerge

Data Processing Agreement with Advertiser in accordance with Art. 28 GDPR

between

_____
_____
_____
_____

hereinafter referred to as the "**Controller**"

and

remerge GmbH
Heidestraße 9
10557 Berlin
Germany

hereinafter referred to as the "**Processor**"

Preamble

The Controller has selected the Processor to act as a service provider in accordance with Art. 28 of Regulation (EU) 2016/679 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**").

This Data Processing Agreement, including all Annexes (hereinafter referred to collectively as the "**Agreement**"), specifies the data protection obligations of the parties from the underlying insertion order and Remerge's general terms and conditions (hereinafter referred to collectively as the "**Principal Agreement**").

The Processor guarantees to the Controller that it will fulfil the Principal Agreement and this Agreement in accordance with the following terms:

Sect. 1 Scope and definitions

(1) The following provisions shall apply to all services of data processing provided by the Processor on behalf of the Controller under Art. 28 GDPR, which the Processor performs under the Principal Agreement.

(2) The terms “data processing” and “processing” of data, shall have the meanings set out in the GDPR. Data processing or the processing of data shall mean any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(3) Reference is made to the further definitions set forth in Art. 4 GDPR.

Sect. 2 Subject matter and duration of the data processing

(1) The Processor shall process personal data on behalf and in accordance with the instructions of the Controller.

(2) The subject-matter of the processing is to match data provided by Controller with bid requests on supply side platforms to deliver ads in order to re-engage Controllers users as agreed upon in the Principal Agreement.

(3) The duration of this Agreement corresponds to the duration of the Principal Agreement.

Sect. 3 Nature and purpose of the data processing

The nature and purpose of the processing of personal data by the Processor is specified in the Principal Agreement. The Principal Agreement includes the following activities and purposes:

- the provision of advertising identifiers (IDFA, AAID) from Controller to Processor (and vice versa for reporting purposes) in encrypted form via a secure interface provided by Processor;
- the creation of a database based on the collected data in order to provide services for the Controller (e.g. user segmentation);
- the recognition of these users on the publisher and supply side platforms;
- the targeting of these users with personalized marketing messages.

Sect. 4 Categories of data subjects

The categories of data subjects include:

- end users of the apps of the Controller, its affiliates and counterparties

Sect. 5 Types of personal data

The following types of personal data shall be processed under this Agreement:

- advertising identifier (such as IDFA and AAID)

From time to time, the Controller may supply the Processor with additional, so-called attribution data which typically relates to the behavior of users inside the apps of the Controller, its affiliates and counterparties. This data may consist of

- installation and first opening of an app on user's mobile device;
- user interactions within an app (e.g. in-app purchases, registration);
- information regarding which advertisements users have seen or clicked on;
- certain metadata, such as timestamp, device type and model, app and app version, country.

Sect. 6 Rights and duties of the Controller

(1) The Controller is responsible for assessing the lawfulness of the data processing and for safeguarding the rights of data subjects, and is hence a controller within the meaning of Art. 4 (7) GDPR.

(2) The Controller is entitled to issue instructions concerning the nature, scale and method of data processing. Upon request by the Controller, the Processor shall confirm verbal instructions immediately in writing or in text form (e.g. by email).

(3) The Controller agrees to provide the app user with the required information about the data processing according to Art. 13 GDPR, in particular the processing for direct marketing and the transfer to third parties such as Processor, at the time personal data (as specified in section 5) is obtained. In particular, the Controller shall inform the user in the app's privacy policy about the collection of advertising identifiers and the user's right to object to the processing. Furthermore, the Controller agrees to provide the user with a link to Processor's privacy policy upon users request.

(4) Insofar as the Controller deems it necessary, persons authorized to issue instructions may be appointed. The Processor shall be notified of such in writing or in text form. In the event that the persons authorized to issue instructions change, the Controller shall notify the Processor of this change in writing or in text form, naming the new person in each case.

(5) The Controller shall notify the Processor immediately of any errors or irregularities that are detected by it in relation to the processing of personal data by the Processor.

Sect. 7 Duties of the Processor

(1) Data processing

The Processor shall process personal data exclusively in accordance with this Agreement and/or the underlying Principal Agreement and in accordance with the Controller's instructions.

(2) Data subjects' rights

a. The Processor shall, within its capabilities, assist the Controller in complying with the rights of data subjects, particularly with respect to rectification, restriction of processing, deletion of data, notification and information. If the Processor processes the personal data specified under Sect. 5 of this Agreement on behalf of the Controller and these data are the subject of a data portability request under Art. 20 GDPR, the Processor shall, upon request, make the dataset in question available to the Controller within a reasonably set time frame, otherwise within seven business days, in a structured, commonly used and machine-readable format.

b. If so instructed by the Controller, the Processor shall rectify, delete or restrict the processing of personal data specified under Sect. 5 of this Agreement. The same applies if this Agreement stipulates the rectification, deletion or restriction of the processing of data.

c. If a data subject contacts the Processor directly to have his or her personal data specified under Sect. 5 of this Agreement rectified, deleted or the processing restricted, the Processor shall forward this request to the Controller immediately upon receipt.

(3) Monitoring duties

a. The Processor shall ensure, by means of appropriate controls, that the personal data processed on behalf of the Controller are processed solely in accordance with this Agreement and/or the Principal Agreement and/or the relevant instructions as applicable.

b. The Processor shall organize its business and operations in such way that the data processed on behalf of the Controller are secured to the extent necessary in each case and protected from unauthorized access by third parties.

c. The Processor shall grant the Controller access to reporting on the advertising campaigns via the Remerge Platform, via an API and/or by receiving an XLS or CSV-file upon request.

d. The Processor confirms that it has appointed a Data Protection Officer in accordance with Art. 37 GDPR and and that the Processor shall monitor compliance with data protection and security laws. The Processor's Data Protection Officer currently is:

Ilan Leonard Selz
privacy@remerge.io

(4) Information duties

a. The Processor shall inform the Controller immediately if, in its opinion, an instruction issued by the Controller violates legal regulations. In such cases, the Processor shall be entitled to suspend execution of the relevant instruction until it is confirmed or changed by the Controller.

b. The Processor shall assist the Controller in complying with the obligations set out in Articles 32 to 36 GDPR taking into account the nature of processing and the information available to the Processor.

(5) Location of processing

The processing of the data shall in principle take place in the territory of the Federal Republic of Germany, in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area. Any transfer to a third country may only take place if the special requirements of Art. 44 et seqq. GDPR are fulfilled.

(6) Deletion of personal data after order completion

After termination or expiry of the Principal Agreement, the Processor shall delete or return all the personal data processed on behalf of the Controller to the Controller after the end of the provision of services relating to processing and delete existing copies, provided that the deletion of these data does not conflict with any statutory storage obligations of the Processor. The deletion in accordance with data protection and data security regulations must be documented and confirmed upon request to the Controller.

Sect. 8 Monitoring rights of the Controller

(1) The Controller shall be entitled, after prior notification in good time and during normal business hours, to carry out an inspection of compliance with the provisions on data protection and the contractual agreements to the extent required, either himself or through third parties, without disrupting the Processor's business operations or endangering the security measures for other controllers and at his own expense. Controls can also be carried out by accessing existing industry-standard certifications of the Processor, current attestations or reports from an independent body (such as auditors, external data protection officers or external data protection auditors) or self-assessments. The Processor shall offer the necessary support to carry out the checks.

(2) The Processor shall inform the Controller of the execution of inspection measures by the supervisory authority to the extent that such measures or requests may concern data processing operations carried out by the Processor on behalf of the Controller.

Sect. 9 Subprocessing

(1) The Controller authorizes the Processor to make use of other processors in accordance with the following subsections in Sect. 9 of this Agreement. This authorization shall constitute a general written authorization within the meaning of Art. 28 (2) GDPR.

(2) The Processor currently works with the subcontractors specified in **Annex 2** and the Controller hereby agrees to their appointment.

(3) The Processor shall be entitled to appoint or replace other processors. The Processor shall inform the Controller in advance of any intended change regarding the appointment or replacement of other processors. The Controller may object to an intended change.

(4) The objection to the intended change must be notified to the Processor within 2 weeks after receipt of the information on the change. In the event of an objection, the Processor may, at his own discretion, either provide the service without the intended change or propose an alternative subcontractor and coordinate it with the Controller. Insofar as the provision of the service is unreasonable for the Processor without the intended modification - for example, due to the associated disproportionate costs for the Processor - or the agreement on an alternative subcontractor fails, the Controller and the Processor may terminate this Agreement as well as the Principal Agreement with a notice period of one month to the end of the month.

(5) A level of protection comparable to that of this Agreement must always be guaranteed when other processors are involved. The Processor is liable to the Controller for all acts and omissions of other processors it appoints.

Sect. 10 Confidentiality

(1) The Processor is obliged to maintain confidentiality when processing data for the Controller.

(2) In fulfilling its obligations under this Agreement, the Processor undertakes to employ only employees or other agents who are committed to confidentiality in the handling of personal data provided and who have been appropriately familiarized with the requirements of data protection. Upon request, the Processor shall provide the Controller with evidence of the confidentiality commitments.

(3) Insofar as the Controller is subject to other confidentiality provisions affecting the data transferred under this Agreement, it shall inform the Processor accordingly. The Processor shall oblige its employees to observe these confidentiality rules in accordance with the requirements of the Controller.

Sect. 11 Technical and organizational measures

(1) The technical and organizational measures described in **Annex 1** are agreed upon as appropriate. The Processor may update and amend these measures provided that the level of protection is not significantly reduced by such updates and/or changes and that these measures are always in compliance with provisions of appropriate data protection legislation.

(2) The Processor shall observe the principles of due and proper data processing in accordance with Art. 32 in conjunction with Art. 5 (1) GDPR. It guarantees the contractually agreed and legally prescribed data security measures. It will take all necessary measures to safeguard the data and the security of the processing, in particular taking into account the state of the art, as well as to reduce possible adverse consequences for the affected parties. Measures to be taken include, in particular, measures to protect the confidentiality, integrity, availability and resilience of systems and measures to ensure continuity of processing after incidents. In order to ensure an appropriate level of processing security at all times, the Processor will regularly evaluate the measures implemented and make any necessary adjustments.

Sect. 12 Liability/Indemnification

(1) The Processor shall be liable to the Controller for any and all loss or damage culpably caused in the performance of the services under the Principal Agreement or by a breach of applicable statutory data protection obligations on the part of the Processor, its employees or parties commissioned by it to implement the Principal Agreement. The Processor shall not be obliged to pay compensation if the Processor proves that it has processed the data provided by the Controller solely in accordance with the instructions of the Controller and that it has complied with its obligations arising from the GDPR specifically directed to processors.

(2) The Controller shall indemnify the Processor against any and all claims for damages asserted against the Processor based on the Controller's culpable breach of its own obligations under this Agreement or under applicable data protection and security regulations.

Sect. 13 Miscellaneous

(1) In case of contradictions between the provisions contained in this Agreement and provisions contained in the Principal Agreement, the provisions of this Agreement shall prevail.

(2) Amendments and supplements to this Agreement shall be subject to the mutual consent of the contracting parties, with specific reference to the provisions of this Agreement to be amended. Verbal side agreements do not exist and shall also be excluded for any subsequent changes to this Agreement.

(3) This Agreement is subject to the laws of the Principal Agreement.

(4) In the event that access to the data which the Controller has transmitted to the Processor for data processing is jeopardized by third-party measures (measures taken by an insolvency administrator, seizure by revenue authorities, etc.), the Processor shall notify the Controller of such without undue delay.

_____	_____
Place, date	Place, date
_____	_____
Signature Customer (Controller)	Signature Remerge (Processor)

Schedule of Annexes

Annex 1 Technical and organizational measures taken to ensure the security of processing

Annex 2 Subprocessors pursuant to Sect. 9 of this Data Processing Agreement

Annex 1

Technical and organizational measures to ensure the security of processing

The Processor guarantees that the following technical and organizational measures have been taken:

A. Pseudonymization measures

Measures that reduce direct references to persons during processing in such a way that it is only possible to associate data with a specific person if additional information is included. The additional information must be kept separately from the pseudonym by appropriate technical and organizational measures.

Description of the pseudonymization:

Processor does not collect, process or store any data that would allow association with a specific person with a pseudonym as further data points are unavailable to Processor.

For internal and external aggregated reporting pseudonyms are dropped therefore anonymizing the data.

B. Encryption measures

Measures or operations in which a clearly legible text/information is converted into an illegible, i.e. not easily interpreted, character string (secret text) by means of an encryption method (cryptosystem).

Description of the encryption measure(s):
Processor uses TLS (1.2) for all communication that does not use a private channel.
Data at rest is encrypted using standard block encryption algorithms.

C. Measures to ensure confidentiality

1. Physical access control

Measures that physically deny unauthorized persons access to IT systems and data processing equipment used to process personal data, as well as to confidential files and data storage media.

Description of physical access control:

Processor's office is protected by an electronic door lock system. Tokens to open doors are assigned to individual employees on an as needed basis and can be centrally revoked on demand at any time without access to the token. Lock access is centrally logged.

Processor's data center providing sub-processors protect Processor's servers against any physical access besides sub-processors maintenance staff employing industry standard data center protection techniques.

2. Logical access control

Measures to prevent unauthorized persons from processing or using data which is protected by data privacy laws.

Description of logical access control system:

Processor uses a centrally managed SSO solution with 2FA support. The system enforces personal and individual login user credentials with strong password rules and regular password changes.

Authentication attempts are logged. After a number of unsuccessful attempts credentials are suspended temporarily.

Access is granted on a as needed basis using a role based rights management system.

A standardized employee on- and offboarding process is in place to ensure access rights are only granted as long as necessary and based on the role of the employee.

Production systems are completely separated from other company systems and only support public/private key based authentication. Key are managed centrally and only employees that need to interact with production systems (developers, ops) hold time limited keys.

Data at rest is encrypted.

3. Data access control

Measures to ensure that persons authorized to use data processing systems can only access personal data according to their access rights, so that data cannot be read, copied, changed or removed without authorization during processing, use and storage.

Description of data access control:

Processor uses a role based approach to determine access rights for all user and system combinations. Roles are based on job function and defined responsibilities using the concepts of need-to-know and least-privilege. They are assigned during the onboarding process and reviewed if the job function changes or if the employees role changes. Role application, approval, allocation and reset are reviewed and signed off by the responsible manager. Granted roles are tied to a personal identifier and an account. Resource authorization is tied to specific roles. If the foundation for an authorization ceases to apply, the authorization/role is withdrawn immediately.

Access to personal data via the Remerge Platform is limited to operational personnel and restricted in the scope of access capabilities to the minimum need to fulfil operational duties.

Interaction with Processor's systems is logged in an immutable log and can be audited afterwards.

To ensure that data can not be read or copied by unauthorized personnel Processor encrypts data in transit (HTTPS) and at rest.

4. Separation rule

Measures to ensure that data collected for different purposes are processed separately and separated from other data and systems in such a way as to preclude the unplanned use of such data for other purposes.

Description of the separation control process:

Processor employs different data processing systems for different purposes. These systems are architecturally (logical and physically) separated. All systems require a valid authorization to be accessed.

Changes to the structure of Processor's systems that affect data separation are documented in a revision safe manner and follow a strict review process by the technical operations personnel.

To ensure against unintentional amalgamation of data Processor separates development, testing, staging and production environments.

Controller data is logically separated.

D. Measures to ensure integrity

1. Data integrity

Measures to ensure that stored personal data cannot be corrupted by means of a malfunctioning of the system.

Description of data integrity:

Processor employs an automated testing system for new releases which verifies the correctness of the changed component. Components that fail this tests will not be deployed to a production environment.

Changes to Processor's main database are logged, can be audited and rolled back on a per change basis.

To ensure against unintentional data corruption the production system is segregated from other environments.

2. Transmission control

Measures to ensure that it is possible to verify and establish to which bodies personal data may be or have been transmitted or made available using data communication equipment.

Description of transmission control:

Processor offers Controllers the ability to access their own data via several APIs. Access to these APIs is governed by a per Controller authentication and authorization process. Transactions are logged and are available for auditing.

Data that is transmitted to Controller by Processor's operations personnel is governed by a transport process with individual responsibilities (encryption & signing).

3. Transport control

Measures to ensure that the confidentiality and integrity of data is protected during transmission of personal data and transport of data carriers.

Description of transport control:

Personal data that is transmitted (sent and received) to or from Processor over public channels is encrypted (TLS 1.2). If changes to the data are detected during transmission the data is discarded and the channel is considered compromised.

4. Input control

Measures to ensure that it can be subsequently verified and ascertained whether and by whom personal data have been entered or modified in data processing systems.

Description of the input control process:

Personal data that is submitted by Controller using Processor's APIs is verified and associated with its source by a Controller specific verification token.

All interactions with the Processor's main database via the Remerge Plattform are verified and logged. This change log includes information about who added, modified or deleted data and what point in time.

E. Measures to ensure availability and resilience

1. Availability control

Measures to ensure that personal data are protected against accidental destruction or loss.

Description of the availability control system:

To ensure against a loss of data all storage systems are multi-way redundant (hardware and logical). In addition data is automatically backed up in regular intervals to physically separated systems and can be restored on demand. Backups are encrypted.

Furthermore Processor's data center sub-processors provide a highly available infrastructure that is secured against major physical risks by providing: alarm systems, fire alarms, air conditioning, waterproof server rooms, uninterrupted power supplies and redundant upstream connectivity.

2. Quick recovery

Measures to ensure the ability to quickly restore the availability of and access to personal data and used systems in the event of a physical or technical incident.

Description of the measures for quick recovery:

Due to the redundant storage a quick recovery is ensured.

3. Reliability

Measures to ensure that the functions of the system are available and malfunctions are reported.

Description of measures for reliability:

All systems in the Processor's infrastructure are monitored with the help of a software based system. An automated alerting system notifies Processor's personnel 24/7 via SMS, eMail, call or custom notifications in case any systems behave outside of well defined normal conditions. In case of a malfunction Processor's personnel follows a standardized incident management & communication process which clearly defines steps and responsibilities.

F. Measures for the regular testing and evaluation of the security of data processing

1. Verification process

Measures to ensure that the data are processed securely and in compliance with data protection regulations.

Description of verification process:

Processor employs an external auditing service that regularly verifies compliance with data protection regulations. Furthermore a regular internal audit by Processor's legal department ensures compliance.

Processor's personnel is regularly trained with regard to data protection and security best practices.

The Controller is entitled to carry out an inspection of compliance with the provisions on data protection and the contractual agreements to the extent required, either himself or through third parties.

The Controller shall notify the Processor immediately of any errors or irregularities detected in relation to the processing of personal data by the Processor.

2. Order control

Measures to ensure that personal data processed on behalf of the Controller can only be processed in accordance with the instructions of the Controller.

Description of the order control measures:

The Controller is entitled to issue instructions concerning the nature, scale and method of data processing. Upon request by the Controller, the Processor shall confirm verbal instructions immediately in writing or in text form (e.g. by email).

Instructions received by the Controller are documented and acted upon by the Processor as applicable. This includes data request, retention and deletion policies.

Insofar as the Controller deems it necessary, persons authorized to issue instructions to Processor may be appointed.

The Controller is entitled to carry out an inspection of compliance with the provisions on data protection and the contractual agreements to the extent required, either himself or through third parties.

Remerge

Remerge

Annex 2

Subprocessors pursuant to Sect. 9 Data Processing Agreement

The Processor currently works with the following subcontractors and the Controller hereby agrees to their appointment.

Company	Location	Processing
LeaseWeb Deutschland GmbH	Frankfurt, DE	dedicated server for transfer and storage of advertising identifiers
LeaseWeb Netherlands B.V.	Amsterdam, NL	dedicated server for transfer and storage of advertising identifiers
LeaseWeb USA, Inc.	Washington, DC, USA	dedicated server for transfer and storage of advertising identifiers
LeaseWeb USA, Inc.	San Francisco, CA, USA	dedicated server for transfer and storage of advertising identifiers
LeaseWeb Asia Pacific Pte. Ltd.	Singapore, SG	dedicated server for transfer and storage of advertising identifiers

The Controller appoints the Processor to additionally work with the following subcontractors if reporting via AWS S3 is requested:

Company	Location	Processing
Amazon Web Services EMEA SARL*	Luxembourg	data transfer and reporting to and from Controller via **Amazon S3**

*additional AWS Terms and Conditions may apply: https://aws.amazon.com/service-terms