Remerge

Data Processing Agreement

In accordance with the European Commission Implementing Decision of 04.06.2021 of the Standard Contractual Clauses between Controllers and Processors in the EU under Article 28 of GDPR.

between

_____
_____
_____
_____

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

and

remerge GmbH
Heidestraße 9
10557 Berlin
Germany

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

Preamble

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

II. This Data Processing Agreement ("**Agreement**"), including all Annexes and the Standard Contractual Clauses (the "**Clauses**"), specifies the data protection obligations of the parties from the underlying Principal Agreement ("**Principal Agreement**").

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1 - Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 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.

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2 - Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3 - Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4 - Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

SECTION II - OBLIGATION OF THE PARTIES

Clause 5 - Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 6 - Obligations of the Parties

6.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

6.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

6.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

6.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and

monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

6.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

6.7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 (thirty) days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a subprocessor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) 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 subprocessor contract and to instruct the sub-processor to erase or return the personal data.

6.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 6.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the subprocessor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 7 - Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the 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') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies 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 controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 8 - Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

8.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(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;

(2) the likely consequences of the personal data breach;

(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.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay 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.

8.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III - FINAL PROVISIONS

Clause 9 - Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its

instructions infringe applicable legal requirements in accordance with Clause 6.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

****** End of Standard Contractual Clauses******

Additional Clauses in line with Clause 2 (b) Invariability of the Clauses

Clause 10 - 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.

Clause 11 - Miscellaneous

(1) 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.

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

(3) 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.

_____	DocuSigned by: Panteleimon Katsukis 8DE7385C8E17429... _____
Controller Signature	remerge GmbH Signature
_____	Berlin, 7/5/2021 _____
Place, date:	Place, date:

Schedule of Annexes

ANNEX I:	List of Parties
ANNEX II:	Description of The Processing
ANNEX III:	Technical And Organisational Measures Including Technical And Organisational Measures To Ensure The Security of The Data
ANNEX IV:	List of Sub-processors

ANNEX I: LIST OF PARTIES

Controller(s):

1. **Name:** (insert here)

Address: (insert here)

Contact person's name: (insert here)

Position: (insert here)

Contact details: (insert here)

Data Protection Officer (if applicable): (insert here)

Address: (insert here)

E-mail: (insert here)

Processor(s):

2. **Name:** remerge GmbH

Address: Heidestraße 9, 10557 Berlin, Germany

Contact person's name: Panteleimon Katsukis

Position: CEO

Contact details: pan@remerge.io

Data Protection Officer: Ilan Leonard Selz

E-mail: privacy@remerge.io

ANNEX II: DESCRIPTION OF THE PROCESSING

1 - Subject matter and duration of the data processing

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

b) The subject-matter of the processing is to match data provided by Controller with bid requests on supply side platforms to deliver online advertising in order to re-engage Controller's users or acquire new users as agreed upon in the Principal Agreement.

c) The duration of this Agreement corresponds to the duration of the Principal Agreement.

2 - 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, according to the type of campaign chosen by the Controller, may include some or all of 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, and/or
- matching of advertising identifiers for the purpose of excluding known users, and
- the processing of IP addresses, Click ID, specified URL, and user agent for purposes of displaying the advertising.

3 - Categories of data subjects:

The categories of data subjects include:
- end users of the apps of the Controller, its affiliates and counterparties

4 - Types of personal data

The following types of personal data shall be processed under this Agreement:
- advertising identifier (such as IDFA and AAID), if provided
- IP addresses, Click ID, specified URL, and User Agent

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.

ANNEX III: TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

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 protects 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. Keys 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 these 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 follow 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 are 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.

ANNEX IV: LIST OF SUB-PROCESSORS

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

Company	Location	Processing
LeaseWeb Deutschland GmbH Kleyerstraße 75-87 60326 Frankfurt am Main	Frankfurt, DE	dedicated server for transfer and storage of advertising identifiers
LeaseWeb Netherlands B.V. Luttenbergweg 8 1101 EC Amsterdam	Amsterdam, NL	dedicated server for transfer and storage of advertising identifiers
LeaseWeb USA, Inc. 9301 Innovation Drive / Suite 100 Manassas, VA 20110	Washington, DC, USA	dedicated server for transfer and storage of advertising identifiers
LeaseWeb USA, Inc. 9301 Innovation Drive / Suite 100 Manassas, VA 20110	San Francisco, CA, USA	dedicated server for transfer and storage of advertising identifiers
LeaseWeb Asia Pacific Pte. Ltd. 11 Collyer Quay, The Arcade #16-02 049317, Singapore	Singapore, SG	dedicated server for transfer and storage of advertising identifiers
Amazon Web Services EMEA SARL* 38 avenue John F. Kennedy, L-1855, Luxemburg	Luxembourg, LUX	Backup server and data transfer and reporting to and from Controller via **Amazon S3 (if requested)**
Google Ireland Limited** Gordon House, Barrow Street Dublin 4, Ireland	Dublin, IRL	Incrementality reporting to Controller via **Google Cloud Platform**

*additional AWS Terms and Conditions may apply: https://aws.amazon.com/service-terms
**additional Google Cloud Platform Terms of Service may apply: https://cloud.google.com/terms