Data Processing Agreement

INTRODUCTION

The following European standard contract for order processing is concluded between the customer and etracker GmbH. It is important to note that the legal security of these contractual clauses is only guaranteed if their content remains unchanged.

The conclusion ensures that the processing is carried out in compliance with the requirements of the GDPR when processing personal data on behalf pursuant to Art. 28 (3) of the General Data Protection Regulation (GDPR).

Pursuant to Article 28 (7) of the GDPR, the European Commission may adopt standard contractual clauses to meet the requirements of Article 28 (3). With the Implementing Decision of 4.6.2021 on standard contractual clauses between controllers and processors pursuant to Article 28 (7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29 (7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council, the European Commission has adopted such standard contractual clauses. The full Implementing Decision can be found on the European Commission's website: https://eur- lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021D0915.

This is explicitly not the often-mentioned standard contractual clauses for international data transfer in third party countries, for example for data processing in the United States, but a model agreement for commissioned processing in the meaning of Art. 28 GDPR.
The standard contractual clauses for commissioned processing are legally secure and already fulfill all legal requirements based on the decision of the European Commission. In particular, a German supervisory authority does not have the possibility to declare the use of these standard contractual clauses insufficient if used correctly. "Checklists" or other expressions of opinion by supervisory authorities do not override the Commission's decision.

If you have any questions regarding data protection, please do not hesitate to contact us:

Elke Hollensteiner

Privacy Manager

privacy@etracker.com

Hamburg, May 2023

EUROPEAN
COMMISSION

Brussels, 4.6.2021
C(2021) 3701 final

ANNEX

ANNEX

to the

COMMISSION IMPLEMENTING DECISION

on standard contractual clauses between controllers and processors under Article 28 (7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29 (7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council

ANNEX

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.

Clause 5 - Optional

- not applicable -

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

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.

Clause7

Obligations of the Parties

7.1. 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.

7.2. 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.

7.3. Duration of the processing of personal data

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

7.4. 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.

7.5. 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.

7.6 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.

7.7. 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 ome month 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 sub-processor 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 sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. 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 7.7. 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 sub-processor 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 8

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 9

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.

9.1 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 [OPTION 1] Article 34 Regulation (EU) 2016/679 / [OPTION 2] Article 35 Regulation (EU) 2018/1725, 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.

9.2 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 10

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 7.1 (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.

ANNEX I - LIST OF PARTIES

Controller(s):

As stored in the settings of the service of etracker with the name, address and contact details.

Processor(s):

1. Name: etracker GmbH

Address: Erste Brunnenstraße 1, 20459 Hamburg, Germany
Contact person's name, position and contact details: Elke Hollensteiner, Privacy Manager, privacy@etracker.com
Signature and accession date: Oct., 7th, 2022

2. Processor's Data Privacy Officer

Thomas Brehm c/o BBS Rechtsanwälte, Brandstwiete 46, 20457 Hamburg, Germany, privacy@etracker.com

APPENDIX II - DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data are processed

Users of the client's offers for which the etracker services are used.

Categories of personal data that are processed

- Internet protocol addresses anonymized as soon as possible by default
- User identifiers, which can be stored in cookies after the user's consent, provided that cookie activation is used
- Device identifiers, if app tracking or app push is used
- Identifiers optionally handed over by the client
- Email addresses as part of overlay newsletter opt-in dialogs, provided the function is used in etracker Optimiser

Processed sensitive data

None

Type of processing

With the help of the etracker services used, data, characteristics and activities of users with regard to the use of websites, applications or other media offers of the client are recorded, processed or stored in accordance with the service agreement.

Purpose(s) for which the personal data are processed on behalf of the controller

etracker processes the customer's personal data for the purpose of providing the services to the customer in accordance with the General Terms and Conditions of etracke GmbH and as set forth in the Service Agreement for usage analysis, reach measurement, optimization and needs-based design as well as the sending of push messages.

The scope of the commissioned service or the service agreement is essentially determined by the product, the edition, the number of accounts, the associated hit quota, the service period and the license fee.

Processing duration

For the term using the etracker services plus the period after the expiry of the term until the anonymization, return or deletion of the data in accordance with this contract.

(Sub)Processors

None

International data transfers of personal data to third countries outside the territory of the European Union

Not applicable

APPENDIX III - TECHNICAL AND ORGANIZATIONAL MEASURES, INCLUDING THOSE TO ENSURE DATA SECURITY

A comprehensive data security concept was implemented at the contractor (etracker GmbH), which contains the necessary precautions in terms of construction, personnel and organization as well as technology to ensure the security of the objects and the data stock as well as the secure operation with regard to data protection and data security as well as the protection of the rights of the persons concerned in an optimized manner.

etracker GmbH's data center is operated by IPHH Internet Port Hamburg GmbH at Wendenstraße 408 in 20537 Hamburg, Germany, on behalf of etracker. IPHH provides the Internet connection and the physical accommodation of the etracker servers in so-called racks (server cabinets). The racks are located on the premises of IPHH and are rented by etracker. The server hardware is procured, configured, installed in the rack and maintained as well as disposed of solely by etracker. Thus, etracker uses pure housing from IPHH as a service.

The etracker services and their configurations take into account the objectives of data protection and the related specifications and guidelines of the legal provisions:

- The contractor shortens the IP addresses collected within the scope of the services in order to avoid a reference to persons wherever possible.
- The client is obligated not to transfer any further personal data to etracker within the scope of using the etracker solutions in order to ensure processing that is as anonymous as possible.

The following security measures are determined, which serve to implement the requirements of Art. 32 GDPR to ensure an adequate level of protection, taking into account the nature, scope, context and purposes of the processing, as well as the risks to the rights and freedoms of natural persons:

Measures of pseudonymization and encryption of personal data

The processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures.

Measures to ensure the continued confidentiality, integrity, availability, and resilience of systems and services related to processing

Physical entry control

Measures to prevent unauthorized persons from gaining access to data processing equipment used to process personal data:

- Access control guidelines and regulations
- Safety areas are clearly defined and few access routes are available

- Access to sensitive areas is secured by an electronic access control system with multi-factor authentication and logging
- Appropriate design of property security measures; entrance doors, window grilles, etc. are designed to be burglar-resistant, among other things
- All areas are secured with a burglar alarm system (VdS-approved) and redundantly connected to the permanently manned security service; in addition, alarm messages are transmitted to the IPHH on-call service
- Monitoring of all critical areas by means of vandalism-proof video cameras
- A person is granted access only to those areas to which access is necessary for the performance of the respective tasks
- Guidelines regulating the escort and identification of guests throughout the building
- Access to the office-internal server room is secured by a PIN
- Access to the data center requires a keycard, a PIN, and additionally a biometric feature (fingerprint); access can only be managed by employees who participate in the on-call service
- The system racks located in the server room are individually locked by means of locking cylinders
- Secured entrance for delivery and pick-up (control before entering the access points)

Digital entry control

Measures to prevent unauthorized persons from using data processing systems and procedures:

- Regulation of user authorization (administration incl. granting of rights, granting of special rights, revocation of authorizations, regular reviews)
- Password policy (strong passwords, regular reviews)
- Differentiated access control
- Assignment of identification keys (SSH keys)
- Use of encryption routines
- Use of encryption routines for mobile data carriers (e.g. notebooks, mobile telephones)
- Authentication of users with remote access (cryptographic techniques, VPN solutions)
- Obligation of data secrecy according to Art. 28, Para. 3 lit. b GDPR
- Controlled destruction of data carriers
- Two-factor authentication (VPN)

Access control

Measures to ensure that the equipment required to use the data processing procedures can only access the personal data subject to their access authorization, and that personal data are protected during processing, use and after the storage cannot be read, copied, modified or removed without authorization:

- Regulation of access authorization in the etracker back office (differentiated authorizations via profiles, roles)
- Access to the frontend at the client only with authentication (user name/password) Provision of appropriate functions for authentication
- Encryption

- Recording and evaluation of logs (unsuccessful and successful authentication attempts in the application)
- Guidelines for the pseudonymization of personal data

Separation control

Measures to ensure that data collected for different purposes can be processed separately:

- Data collected for different purposes is stored separately in the data processing system
- Data is processed on dedicated systems belonging to etracker GmbH

Transfer control

Measures to ensure that personal data cannot be read, copied, modified or delete without authorization during electronic transmission or while being transported or stored on data media:

- All data will remain within the data processing system and will not be disclosed to third parties
- Transmission of data between etracker and the data center takes place exclusively via encrypted channels
- Web pages of the client frontend are provided via an encrypted connection

Input control

Measures to ensure that it is possible to check and establish retrospectively whether and by whom personal data have been entered into data processing systems, modified or deleted:

- Custom rights assignment
- Logging of entries (in the etracker back office)
- Logging of data usage (in the etracker back office)
- Obligation of all employees involved in data processing to maintain secrecy and to process data in accordance with instructions (data secrecy)

Availability control

Measures to ensure that personal data is protected against accidental destruction or loss:

- Regulated process for ensuring business operations
- Extensive monitoring of all services
- Emergency plans
- Regular back-ups according to a back-up plan
- Securing systems against database failure, service level agreements with IT service providers
- Mirroring data
- Virus protection / Firewall
- Redundant hardware
- Uninterruptible power supply (UPS)

Rapid recoverability (Art. 32 (1) (c) GDPR)

Recovery / Back-up systems

Procedures for periodically reviewing, assessing and evaluating the effectiveness of technical and organizational measures to ensure the security of processing

- Data protection management
- Incident Response Management
- Data protection-friendly default settings (Art. 25 (2) GDPR)
- Order control: No order processing in the sense of Art. 28 GDPR without corresponding instruction of the client
- Clear contract design
- Formalized order management
- Rigorous selection of service provider
- Duty of prior conviction
- Follow-up checks

ANNEX IV - LIST OF SUBPROCESSORS

Not applicable