WE BELIEVE
PRIVACY
SHOULD
MATTER
TO OUR CLIENTS

DATA PROCESSING AGREEMENT

Usercentrics Contract – Data Processing Agreement (Annex 1 of the Order Form)

Agreement between

Contracting Party

...

...

(hereinafter **„Controller“**)

and

Usercentrics GmbH

Sendlinger Str. 7

80331 München

(hereinafter **„Processor“))**

for the processing of personal data acting on behalf of a third party ("**Agreement**"). Definitions in the General Terms and Conditions or the service description also apply to this Data Processing Agreement. Definitions in this Data Processing Agreement apply only to this Data Processing Agreement.

1. Subject and Duration of the Agreements

1.1. Subject of the Agreement

The subject of the Agreement is the execution of the following tasks by the Processor according to the service description in the offer: collection, administration, documentation and transfer of the consent of the Controller's users as well as other services, if applicable. For this purpose, the Processor is processing personal data for the Controller within the meaning of Art. 4 No. 2 and Art. 28 GDPR on the basis of the General Terms and Conditions.

1.2. Duration of the Agreement

The duration of this Agreement (term) shall correspond to the duration of the main Contract.

2. Specification of the Agreement content

2.1. Scope, Nature and Purpose

Scope, nature and purpose of the collection, processing and / or use of personal data by the Processor for the Controller are outlined in detail in the service description of the order.

2.2. Type of Data

Subject of the collection, processing and / or use of personal data are the following data:

- Customer data: Settings Login Data
- User data:
  - Consent Data (Consent ID, Consent Number, Timestamp of the Consent, implicit or explicit Consent, Opt-in or Opt-out, Banner Language, Customer Setting, Template Version)

- Device data (HTTP Agent, HTTP Referrer)

2.3. **Categories of Data Subjects**

The categories of data subjects affected by the processing of their personal data within the scope of this Agreement include:

- Website visitors or app users,
- Customers / Registered users

3. Controller's Authority to Issue Instructions / Location of the Data Processing

3.1. The data is handled exclusively within the framework of the agreements made and in accordance with documented instructions from the Controller (cf. Art. 28 Para. 3 lit. a GDPR). Within the scope of the description of the data processing mandate in this Agreement, the client reserves the right to issue comprehensive instructions on the type, scope and procedure of data processing, which he can specify in more detail by means of individual instructions. Changes to the object of processing and procedural changes are to be jointly agreed and documented. Any additional expenses incurred are to be remunerated by the Controller on a time and material basis. The Processor may only provide information to third parties or the person concerned with the prior written consent of the Controller.

3.2. Oral instructions will be confirmed by the Controller immediately in writing or by e-mail (in text form). The Processor shall not use the data for any other purposes and shall in particular not be entitled to pass them on to third parties. Excluded from this are back-up copies, insofar as they are necessary to ensure proper data processing, as well as data which is necessary in order to comply with legal obligations under Union law or the law of an EU member state, and to comply with retention obligations.

3.3. The Processor must inform the Controller without delay in accordance with Art. 28 para. 3 subpara. 2 GDPR if it believes that an instruction violates data protection regulations. The Processor is entitled to suspend the execution of the corresponding instruction until it is confirmed or amended by the person responsible at the Controller.

3.4. The processing of the Controller data by the Processor takes place within the EU / EEA. The Processor shall be obliged to inform the Controller prior to the commencement of the processing of the Controller's data of a legal obligation of the Processor to carry out the processing of the Controller's data at another location, unless such notification is prohibited by law. The processing and / or transfer to a third country outside the territory of the EU / EEA or to an international organization requires the prior written consent of the Controller. In this case, the Processor shall also be obliged to ensure an adequate level of data protection at the place of data processing in accordance with the applicable statutory provisions and the interpretations thereof by courts and authorities or - at the Controller's option - to give the Controller the opportunity to ensure an adequate level of data protection, including by concluding or acceding to standard EU contractual clauses.

4. Confidentiality

The Processor shall ensure that employees involved in the processing of personal data and other persons working for the Processor are prohibited from processing the personal data outside the scope of the instruction. Furthermore, the Processor shall ensure that the persons authorised to process the personal data have committed themselves to confidentiality or are subject to an appropriate legal obligation of secrecy. The confidentiality / secrecy obligation shall continue to exist after the termination of the Agreement.

5. Technical-organisational Measures

5.1. Within his area of responsibility, the Processor shall design the internal organisation in such a way that it meets the special requirements of data protection. He will take appropriate technical and organisational measures to protect the personal data of the Controller which meet the requirements of Art. 32 GDPR. In particular, the technical and organisational measures are to be taken in such a way that the confidentiality,

integrity, availability and resilience of the systems and services in connection with data processing are permanently guaranteed. These technical and organisational measures are described in Annex 1 of this agreement. The Controller is aware of these technical and organisational measures and is responsible for ensuring that they provide an adequate level of protection for the risks of the data to be processed.

5.2. The technical and organisational measures are subject to technical progress and further development. In this respect the Processor is permitted to implement alternative adequate measures. In doing so, the safety level of the specified measures may not be undercut. Significant changes must be documented.

6. Subprocessors

6.1. The engagement and/or change of Subprocessors by the Processor is only allowed with the consent of the Controller. The Controller agrees to the engagement of Subprocessors as follows:

6.1.1. The Controller hereby agrees to the engagement of the Subprocessors listed in Annex 2 to this Agreement.

6.1.2. The Controller agrees to the use or modification of further Subprocessors if the Processor notifies the Controller of the use or change in writing (email sufficient) thirty (30) days before the start of the data processing. The Controller may object to the use of a new Subprocessor or the change. If no objection is made within the aforementioned period, the approval of the use or change shall be assumed to have been given. The Controller acknowledges that in certain cases the service can no longer be provided without the use of a specific Subprocessor. In these cases, each party is entitled to terminate the contract without notice. If there is an important data protection reason for the objection and if an acceptable solution between the parties is not possible, the Controller is granted a special right of termination. The Controller shall declare its intention to terminate the contract in writing to the Processor within one week after the failure to reach an agreeable solution. The Processor may remedy the objection within two weeks of receipt of the declaration of intent. If the objection is not remedied, the Controller can declare the special termination, which becomes effective upon receipt.

6.2. The Processor shall design the contractual arrangements with the Subprocessor(s) in such a way that they contain the same data protection obligations as defined in this Agreement, taking into account the nature and extent of data processing within the scope of the Subcontract. The Subprocessor's commitment must be made in writing or in electronic format.

6.3. Subcontracting relationships within the meaning of this provision do not include services which the Processor uses with third parties as ancillary services to support the execution of the Agreement. These include, for example, telecommunications services, maintenance and user service, cleaning staff, inspectors or the disposal of data media. However, the Processor is obliged to make appropriate and legally compliant contractual agreements and to take control measures to ensure the protection and security of the Controller's data, even in the case of ancillary services contracted out to third parties.

7. Data Subject Rights

7.1. The Processor shall support the Controller within the scope of its possibilities in meeting the requests and claims of affected persons in accordance with Chapter III of the GDPR.

7.2. The Processor shall only provide information about the data processed in the order, correct or delete such data or restrict data processing accordingly, if instructed to do so by the Controller. If a data subject should contact the Processor directly for information, correction or deletion of his/her data or with regard to the restriction of data processing, the Processor shall forward this request to the Controller without delay.

8. Processor's Obligations to Cooperate

8.1. The Processor shall assist the Controller in complying with the obligations regarding the security of personal data, reporting obligations in the event of data breaches, data protection impact assessments and prior consultations as set out in Articles 32 to 36 GDPR.

8.2. With regard to possible notification and reporting obligations of the Controller according to Art. 33 and Art. 34 GDPR the following applies: The Processor is obliged (i) to inform the Controller immediately of any violation of the protection of personal data and (ii) in the event of such a violation, to provide the Controller with appropriate support, if necessary, in its obligations under Art. 33 and 34 GDPR (Art. 28 para. 3 sentence 2 lit. f GDPR). Notifications pursuant to Art. 33 or 34 GDPR (notifications and reports of violations of personal data protection) for the Controller may only be carried out by the Processor following prior instructions pursuant to Section 3 of this Agreement.

8.3. If the Controller has an obligation to notify or report in the event of a security incident, the Processor is obliged to support the Controller at the Controllers expense.

9. Other obligations of the Processor

9.1. To the extent required by law, the Processor shall appoint a data protection officer, who may resume his activities in accordance with Articles 38 and 39 GDPR, §§ 38, 6 BDSG. His contact details will be provided to the Controller for the purpose of direct contact upon request.

9.2. The Processor shall inform the Controller immediately of control actions and measures taken by the supervisory authority pursuant to Art. 58 GDPR. This shall also apply if a supervisory authority is investigating the Processor in accordance with Art. 83 GDPR.

9.3. The Processor shall ensure to execute the control of the proper contract performance and fulfillment by means of regular self-inspections, in particular the adherence to and, if required, the necessary adjustment of regulations and measures for the execution of the contract.

10. Controller's right to information and inspection

10.1. The Controller has the right to request the information required under Art. 28 Para. 3 h) GDPR to prove that the Processor has complied with the agreed obligations and to carry out inspections in agreement with the Processo or to have them carried out by auditors to be appointed in individual cases.

10.2. The parties agree that the Processor is entitled to submit convincing documentation to the Controller in order to prove adherence to his obligations and implementation of the technical and organizational measures. Convincing documentation can be provided by presenting a current audit certificate, reports or report extracts from independent institutions (e.g. auditors, auditing, data protection officer), appropriate certification through an IT security or data protection audit (e.g. ISO 27001) or certification approved by the responsible supervisory authorities.

10.3. This shall not affect the right of the Controller to conduct on-site visits. However, the Controller shall consider whether an on-site inspection is still necessary after submission of meaningful documentation, in particular taking into account the maintenance of the Processor's regular business operations.

10.4. The Controller has the right to assure himself of the Processor's compliance with this Agreement in his business operations by means of spot checks, which as a rule must be announced in good time. The Processor is committed to provide the Controller, upon request, with the information required to comply with his obligation to carry out inspections and to make the relevant documentation available.

11. Deletion of Data and Return of Data Carriers

At the discretion and request of the Controller - at the latest upon termination of the contract - the Processor shall hand over to the Controller all documents, processing and operating outputs as well as data resources that have come into his possession in the context of the contractual relationship, or destroy them in accordance with data protection laws after prior approval. The same applies to test and scrap material. The protocol of the deletion must be presented on request.

Documentation which serves as proof of the orderly and appropriate data processing shall be kept by the Processor in accordance with the respective retention periods beyond the end of the contract. He can hand them over to the customer at the end of the contract to exonerate him.

12. Liability

The parties' liability under this Agreement shall be governed internally by the liability provisions in the Processor's General Terms and Conditions, unless otherwise stated in the service description in the offer or in a separate agreement between the parties. For the external legal liability, the regulations according to Art. 82 GDPR apply.

Place, Date _____

Signature of the Controller

Place, Date _____

Usercentrics GmbH

Mischa Rürup, CEO

Annex 1 - Technical-Organisational Measures/ Safety Concept of the Usercentrics GmbH

Table of Contents

The following technical and organisational measures have been implemented by the Processor and have been agreed with the Controller.

1. Measures regarding the pseudonymisation of personal data

Pseudonymisation means the processing of personal data in such a way that the personal data can no longer be attributed to a specified data subject without additional information, provided that such additional information is kept separately and is subject to technical and organisational measures ensuring that the personal data are not attributed to an identified or identifiable natural person.
Measures related to the pseudonymisation of personal data are:

- Privacy-by-design
- All IDs of a user (consentID, processorID, consentID) are pseudonymized with a sha-256 cryptographic hash.
- A pseudonymization concept is available (including definition of the data to be replaced; pseudonymization rules, description of procedure, etc.).

2. Measures to ensure confidentiality

Measures to implement the requirement of confidentiality include measures for access or admission control. The technical and organisational measures taken in this context shall ensure adequate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Measures implemented by Usercentrics GmbH to prevent unauthorized access to data processing systems:

- Personal and individual user login when logging into the system (Google Cloud)
- Password procedure (specification of password parameters with regard to complexity and update interval)
- BIOS passwords
- Additional system login for certain applications
- Automatic blocking of the clients after a certain period of time without user activity (also password-protected screen saver or automatic pause switch)

- Electronic documentation of all passwords and encryption of this documentation to protect against unauthorized access
- two-factor authentication
- Regular software updates / patching
- Regular vulnerability scans

The servers are hosted by Google Cloud in Frankfurt, Germany. This provider guarantees reliability and protection against unauthorized access to the physical infrastructure.

Measures implemented by the subprocessor Google Cloud can be found here:
https://cloud.google.com/terms/data-processing-terms#appendix-2-security-measures

3. Measures to ensure integrity

Measures to implement the principle of integrity are, on the one hand, those which also belong to input control, but on the other hand, those which generally protect against unauthorised access or unlawful processing, destruction or accidental damage.

3.1 Transmission control

measures to ensure that personal data cannot be read, copied, altered or removed without authorisation during their electronic transmission or during their transport or storage on data carriers and that it is possible to verify and establish the points to which personal data are to be transmitted by data transmission facilities:

- E-mail encryption
- Encryption of CD/DVD-ROM, external hard disks and/or laptops
- Secured WLAN
- SSL-/TLS encryption
- Data protection-compliant destruction of data, data carriers and printouts
- Protocolling of data transfer

3.2 Input control

Measures to ensure subsequent verification and determination of whether, when and by whom personal data have been submitted, modified or removed in data processing systems:

- Contracts governing the processing of personal data with subprocessors in compliance with the law, containing appropriate control mechanisms.
- Obtaining self-disclosure from service providers with regard to their measures for implementing data protection requirements
- Written confirmation of verbal instructions
- Recording and demand-oriented provision of corresponding actions performed on systems (e.g. log files)
- Use of logging and protocolling evaluation systems
- Determination of the authorised persons for the creation of data carriers and the processing of data

4. Measures to ensure availability

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

- Use of centrally tested and approved standard software from secure sources
- Regular data backups and mirroring processes
- Hardware (in particular servers) is deactivated after a inspection of the data carriers used therein and, if necessary, after the relevant data records have been backed up.
- Uninterruptible power supply (UPS) in the server room
- Separate storage of data files collected for different purposes
- Multilayered anti-virus and firewall architecture
- Emergency planning (emergency plan for security and data protection violations with specific instructions)
- Fire/water and temperature detection system in the server rooms
- Fire doors

5. Ensuring the resilience of systems

This includes measures that must be implemented prior to data processing by the processor. In addition, continuous monitoring of the systems is necessary and planned.
The subprocessor Google Cloud has ensured the resilience of its systems through the following measures:

- Load-Balancing
- Dynamic processes and memory activation
- Penetration tests
- Regular load tests of the data processing systems
- Set the load limit for the respective data processing system in advance above the necessary minimum.
- Regular training of the personnel deployed in accordance with the requirement to ensure the integrity and confidentiality of data processing.

More information on the procedures can be found here: https://cloud.google.com/security/overview/

6. Measures to restore availability

To ensure recoverability, sufficient backups are required on the one hand, but also action plans that can restore ongoing operations in the sense of disaster scenarios on the other. The subprocessor Google Cloud has set up a multi-level backup system, including measures such as:

- Daily backup of the entire server
- Service Level Agreements (SLAs) with subprocessors
- Backup Process

- Redundancy (e.g. Mirroring hard drives)
- Firewall, IDS/IPS
- Fire protection and hydration water protection
- Monitoring von alarms
- Failure/emergency/restoration plans

More information on the procedures can be found here: https://cloud.google.com/security/overview/

7. Procedures for periodic review, assessment and evaluation

Regular review, assessment and evaluation of the effectiveness of the technical and organisational measures taken to ensure the security of the processing shall be carried out within the framework of the implementation of:

- Regular revisions of the safety concept
- Information on emerging vulnerabilities and other risk factors, revision of risk analysis and assessment as appropriate.
- Audits of the data protection officer, process controls through quality management

Annex 2 to the Data Processing Agreement

Authorised subcontractors

#	Name	Operating company	Address of the Subcontractor	Place of data processing	Scope of Application under the Contract	Betroffene
1	Google	Google Ireland Limited *	Gordon House, Barrow Street Dublin 4. Irland	Server in the European Union	Hosting	User of the Controller
1	Auth0	Auth0 Inc.*	10800 NE 8th Street, Suite 700, Bellevue, WA 98004, United States of America	Server in the European Union	Login Authentification	Controller

* In addition, the standard contractual clauses between Usercentrics and Google Ireland Ltd. apply here for any data transfer to the US as a result of the decision of the European Court of Justice of 16.07.2020 (ECJ, 16.7.2020 - C-311/18 "Schrems II", available under https://cloud.google.com/terms/eu-model-contract-clause) and Auth0 (available under https://cdn.auth0.com/website/legal/files/dpa/data-processing-addendum-8-20.pdf?_ga=2.176298087.393185399.1600347978-2067480355.1593507683) to ensure an adequate level of data protection (see 3.4. of the Agreement).