



## **DATA PROCESSING AGREEMENT**



## Usercentrics Contract – Data Processing Agreement

Agreement between

Contracting Party

(hereinafter „**Controller**“)

and

Usercentrics<sup>1</sup>

(hereinafter „**Processor**“)

For the processing of personal data acting on behalf of a third party ("**Agreement**").

### 1. Subject and Duration of the Agreements

#### 1.1. Subject of the Agreement

The subject of the Agreement is the execution of the tasks as described under Annex 3 by the Processor in accordance with the service description in the offer (Main Agreement). In doing so, the Processor processes personal data for the Controller within the meaning of Art. 4 No. 2 and Art. 28 GDPR on the basis of the Main Agreement. Definitions in the Main Agreement shall also apply in this Agreement. Definitions in this Agreement shall only apply to this Agreement.

#### 1.2. Duration of the Agreement

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

### 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 result from the main agreement and Annex 3, with Annex 3 taking precedence in the event of a conflict.

---

<sup>1</sup> The Usercentrics entity that is the party to this Agreement is the same as that of the General Terms and Conditions agreed to between either Usercentrics GmbH, Usercentrics A/S, or Usercentrics, Inc. and the Controller.

## 2.2. Type of Data

Subjects of the collection, processing and / or use of personal data are the data as described in Annex 3.

## 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 are defined in Annex 3.

### **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). Annex 3, the Main Agreement, this Agreement and, if applicable, the settings made by the Controller for the use of the Processor's Product shall constitute the Controller's instructions. Within the scope of the description of the data processing mandate in this Agreement, the controller 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. Any transfer, including transfers of sub-operations, to a third country outside the territory of the EU/EEA or to an international organization requires Controller's prior consent as described below in 6.1.2 and may only take place if the special requirements of Art. 44 et seq. GDPR (e.g., adequacy decision of the Commission, standard contractual clauses and authorized code of conduct) have been fulfilled.

#### **4. Confidentiality**

- 4.1. 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 Consent Management Platform (CMP) provided by the Processor serves as an automated system to obtain consent from the Controller's users (end-user) and to document the measures required for data processing based on the Client's legitimate interests. Within the CMP, the end-user can accordingly exercise the right to withdraw consent as well as to object to processing based on legal basis of the Controller's choice. With regard to other data subject rights, the exercise of which is not enabled via the functionality of CMP, the Processor shall only provide information on the data processed on behalf of the Controller, correct or delete such data or restrict the data processing accordingly upon instruction of the Controller. Insofar as a data subject should contact the Processor directly for the purpose of information, correction, or deletion of his/her data as well as with regard to the restriction of data processing, the Processor shall forward this request to the Controller without undue 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 without undue delay 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 Controller's 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 Processor 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**

- 11.1. In the event of termination of the Agreement, the Processor shall, at the Controller's option and request, hand over to the Controller without undue delay, at the latest within 30 days, all documents, processing and utilisation results produced and data files connected with the contractual relationship which have come into the Processor's possession within the scope of the implementation of the Agreement or destroy them in accordance with data protection law after prior consent. The same shall apply to test

and reject material. The protocol of the deletion shall be submitted upon request. By way of derogation, a deletion or surrender period of no longer than 6 months shall apply to back-ups made by the Processor.

Documentation that 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 Controller at the end of the contract to exonerate him.

## **12. Liability**

- 12.1. 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.

**Annex 1** - Technical-Organisational Measures/ Safety Concept of the Usercentrics GmbH**Technical and organizational measures (TOM)**

Within the meaning of Art. 28 para. 3 lit. c 32 GDPR

**Usercentrics GmbH**, Sendlinger Straße 7, 80331 Munich, Germany (hereinafter "Usercentrics") processes personal data on behalf of its customers. Usercentrics is aware of its responsibility as a processor. Accordingly, technical and organizational measures have been taken to significantly reduce risks and potential hazards that arise in connection with the processing of personal data. How a level of security and data protection that complies with the GDPR is achieved can be found in the following technical and organizational measures. These are deemed to be agreed upon with the controller.

**Table of contents**

1. Measures to ensure confidentiality (Art. 32 para. 1 lit. b GDPR)
2. Measures to ensure integrity (Art. 32 para. 1 lit. b GDPR)
3. Measures to ensure resilience & availability (Art. 32 para. 1 lit. b GDPR)
4. Measures to restore availability (Art. 32 para. 1 lit. c GDPR)
5. Measures for the pseudonymization of personal data (Art. 32 para. 1 lit. a GDPR)
6. Procedures for the regular review, assessment and evaluation of the effectiveness of the technical and organizational measures (Art. 32 para. 1 lit. d GDPR)

## 1. Ensuring confidentiality (Art. 32 para. 1 lit. b GDPR)

Usercentrics takes measures to implement the requirement of confidentiality. This includes, among other things, measures for physical access, electronic access control and internal access control. The technical and organizational measures taken in this context are intended to ensure appropriate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

### Physical Access control

- Where personal data is the subject of processing, it is stored in systems that are secure (e.g. ISO/IEC 27001/27017/27018/27701).
- Access to Google Cloud infrastructure - more information on measures can be found here: <https://cloud.google.com/security>
- All systems and devices are updated at regular intervals (software update).
- All systems are regularly checked for vulnerabilities.
- There is no critical IT infrastructure (server systems) on the premises of Usercentrics. Nevertheless, physical access to office space is protected with security measures to the greatest possible extent. These include:
  - o Access to the office is only possible for employees and service providers (e.g. cleaning service) with personalized door transponders/locking cylinders and logged key/transponder issue/return.
  - o The use of surveillance cameras (inside - e.g. entrance area).
  - o Visitors must ring the bell, register in person, identify themselves and are not allowed to move freely around the premises.

### Electronic Access control

- Access to personal data is restricted to a limited group of employees, requires their designated login credentials (user ID and password) and access is only via encrypted means (HTTPS, TLS/SSL).
- Group accounts / system logins only for specific applications.
- Separate user IDs for privileged authorizations.
- User IDs are deactivated/deleted immediately when employees leave the company.
- Passwords are not stored in clear text or transmitted unencrypted.
- For user authentication, password requirements are: 8-12 characters long; 3-4 character types are to be used; upper & lower case; no common terms; the password is to be changed immediately if there is a reason/indication of misuse; temporary passwords are to be updated immediately after account activation by the user.

- Two-factor authentication is used wherever possible.
- Session Management.
- Internal IT security policies.
- Automatic locking of clients (e.g. employee workstations) after a defined period of time without user activity (also password-protected screen saver or automatic pause).

## Internal Access control

- Access is in accordance with an authorization concept and crypto concept.
- Use of a user and user group management system and access rights management.
- SSH is deactivated wherever possible.
- Graduated authorizations are assigned depending on the employee's area of activity. The minimum principle is always applied here.

## Further measures

- Strict separation control: If there are different purposes, data is not processed together. Here, a client separation (logical or physical) / function separation is supported.
- Each system in its respective stage is operated on its own server for its respective function (separation of development, test and production systems, separation of functions).
- If the respective purpose for data processing ceases to exist, the data is deleted. This is done in accordance with the deletion concept.
- The encryption of data-at-rest is done via AES256 with different keys per data segment. Data-in-transport is encrypted using TLS 1.3.

## **2. Ensuring integrity (Art. 32 para. 1 lit. b GDPR)**

Measures are taken that serve the requirement of integrity. This includes, among other things, measures to control input, but also those that generally contribute to protection against unauthorized or unlawful processing, destruction or unintentional damage.

### Transfer control

Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons during electronic transmission or while being transported or stored on data media, and that it is possible to verify and establish to which bodies personal data is intended to be transmitted by data transmission equipment:

- The transmission of data (e.g. emails) is encrypted.

- Data encryption is always used when data is transported to devices. This regulation applies, for example, to the work computers used by our employees, as well as external hard drives or USB sticks. Internal encryption requirements also apply to memory cards and CDs/DVD-ROMs.
- Only secure wireless networks (WLAN) are used, all of which are encrypted with WPA-2.
- If necessary, VPN technology is used.
- If data carriers, data and printouts are no longer used, they are securely deleted or destroyed. This ensures to the greatest possible extent that data cannot be recovered.
- If necessary, the data transfer is logged.

## Input control

Measures to ensure that it is possible to check and establish retroactively whether, at what time and by whom personal data have been entered, changed or removed in data processing systems:

- High standards in the legally compliant drafting of contracts for the processing of personal data with subcontractors, which contain provisions of control options.
- Use of logging and log evaluation systems to document user input. If adjustments are made to systems that process personal data, this is recorded and kept as required (e.g. in the form of log files).
- The logic of data input and output is checked (checking file paths, etc.).
- Obtain information from service providers regarding the measures taken to implement data protection requirements.
- Verbal instructions are confirmed in writing.

### **3. Ensuring availability (Art. 32 para. 1 lit b GDPR)**

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

#### Specific measures for our production environment & related systems

Usercentrics does not operate its own server resources in its own data centers. Where processing is carried out by subcontractors, the following measures, among others, apply, before and during data processing:

- Monitoring/supervision of system activities by our employees.
- Our productive environment is backed up at regular intervals or data mirroring procedures are used.
- Hardware (especially servers) is decommissioned after a check of the data carriers used in it and, if necessary, after the relevant data records have been backed up.



- The systems are protected by an uninterruptible power supply (UPS).
- A multi-layer virus protection and firewall architecture is used.
- The data centers used have fire/water and temperature early warning systems in the server rooms as well as fire doors.
- Data files collected for different purposes are stored separately.
- Regular patch management.
- Load balancing.
- Data storage is added as part of dynamic processes.
- Penetration and load tests are carried out regularly.
- The load limit for each data processing system is set above the necessary minimum in advance of data processing.
- Regular training of the personnel deployed.

For the production system and related systems, **Google Cloud** resources are used.

A distinction is made between the following resource categories: static hosting, APIs and databases.

**Statically hosted** resources are stored on servers within the member states of the EU (excluding Zurich and London) and are provided by a global CDN network cache with an availability of at least 99.95% (<https://cloud.google.com/cdn/sla>).

**APIs** or dynamically hosted resources are hosted on servers within EU member states, primarily Frankfurt and Belgium. For some resources, a global CDN network cache is in use.

**Databases** are hosted on servers within EU member states, primarily Frankfurt and Belgium.

Further information can be found at:

<https://cloud.google.com/terms/data-processing-terms#appendix-2-security-measures>

#### Further measures

If companies are commissioned with the processing of personal data, this is always subject to the condition of an existing order processing contract that complies with the requirements of Article 28 of the GDPR. Corresponding sample contracts are provided for this purpose. These also ensure that Usercentrics is informed of possible threats to availability at an early stage.

- Use of virus software on employee computers.
- The storage of data on employee computers is reduced as much as possible. Data is stored on secure cloud systems.

- Standard software used is subject to a preliminary check and may only be obtained from limited secure sources.
- The internal office IT is protected by an uninterruptible power supply (UPS) in the routing room.
- Emergency plans with concrete instructions for action have been established for security and data protection breaches.

#### **4. Ensuring recoverability (Art. 32 para. 1 lit. b GDPR)**

In the event of a physical or technical incident, measures are in place to ensure rapid availability and, as part of a plan of action, go beyond mere data backup. In order to be able to restore ongoing operations in these disaster scenarios, the following is undertaken:

##### Specific measures for our production environment (CMP) & related systems

- Daily backup of all server resources by the hosting provider (Google Cloud).
- Disaster recovery.
- Conclusion of service level agreements (SLAs) with service providers.
- Multi-level backup procedures.
- Redundant storage (cluster setups / geo-redundancy) of data (e.g. hard disk mirroring).
- Use of firewall, IDS/IPS.
- Fire and extinguishing water protection.
- Alarm monitoring.
- Failure, disaster and recovery plans and scenarios.

Further information:

<https://cloud.google.com/security>

#### **5. Measures for pseudonymization of personal data**

Pseudonymization is 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 to ensure that the personal data are not attributed to an identified or identifiable natural person. The following measures are taken for this purpose:

- Establish a strict privacy-by-design approach.

- Establish a pseudonymization concept (including definition of the data to be replaced; pseudonymization rules, description of procedure).
- A SHA-256 cryptographic hash is used for pseudonymization.

## **6. Procedures for the regular review, assessment and evaluation of the effectiveness of technical and organizational measures**

A regular review, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure the secure processing of personal data is carried out through the following measures:

### Data protection management system

All procedures, any requests from authorities, contracts and directories are kept for documentation and transparency purposes. Changes are also documented.

### Information Security Management System

All concepts, processes and risk analyses are kept in an internal ISMS.

### Processing of data on behalf of Usercentrics or by subcontractors

Commissioning is always preceded by an extensive selection process and a PreCheck. We check whether our high standards described here are also met by potential processors. Only when this has been done and a processing contract that complies with the requirements of Article 28 GDPR has been concluded may processing take place. In addition to the PreChecks, we also carry out recurring audits in order to permanently maintain the required level. The agreed-upon services are specifically set out in the order processing contracts in order to clearly delineate the scope of the order.

### Training and employee awareness

At the start of their employment with Usercentrics, all employees receive all important information on the topic of data protection and information security and are obligated to maintain confidentiality. With regular (refresher) training and selective provision of information (articles, cases, etc.), we ensure a constantly high level of employee awareness.

### Up-to-dateness of the security concept

The security concept is subject to regular revision and adapted as necessary.

### Responsibilities

Responsibility for the implementation of the measures and processes described here lies within the responsible departments or specialist areas. Regular monitoring is carried out in part by the Data Protection Officer and the Information Security Officer.

### Further measures



- Reviewing information on newly emerging vulnerabilities and other risk factors, including revision of the risk analysis and assessment, if necessary.
- Auditing of the Data Protection Officer and the Information Security Officer as well as regular process controls through appropriate quality management.

Contact details of the data protection officer:

**SECUWING GmbH & Co. KG** Maximilian Hartung, Frauentorstr. 9, 86152 Augsburg, Germany, [epost@datenschutz-agentur.de](mailto:epost@datenschutz-agentur.de), Tel. +49 (0) 821 907 86 450

Contact details of the Information Security Officer:

**activeMind AG** Christoph Burghardt, Potsdamer Str. 3, 80802 Munich, Germany, [burghardt@activemind.de](mailto:burghardt@activemind.de)

Tel. +49 (0) 89 9192 94 900

Internal data protection coordination:

Legal Department, Sendlinger Str. 7, 80331 Munich, Germany, [legal@usercentrics.com](mailto:legal@usercentrics.com)

**Annex 2 to the Data Processing Agreement**

Authorised subprocessor

#	Name	Operating company	Address of the Subcontractor	Place of data processing	Scope of Application under the Contract	Data Subject	Service
1	Google	Google Cloud EMEA Ltd.*	70 Sir John Rogerson's Quay, Dublin 2, Ireland	Server in the European Union	Hosting	Controller's user	Consent Management Platform, Preference Manager, Server-Side Tagging
2	BUNNY WAY	BUNNY WAY, informacijske storitve d.o.o.	Cesta komandanta Staneta 4A 1215 Medvode, Slovenia	European Union	Content Delivery Network (CDN)	Controller's user	Consent Management Platform (if applicable)
3	Hetzner	Hetzner Online GmbH	Industriestr. 25, 91710, Gunzenhausen, Germany	European Union	Hosting	Controller's user	Consent Management Platform (if applicable)

\*In addition, the standard contractual clauses between Usercentrics and Google Cloud EMEA 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/sccs/eu-p2p>), as well as additional measures, as far as this is necessary, to ensure an adequate level of data protection (see 3.4. of the Agreement).

## Annex 3 - Service Description

Below you can find the description of the services provided by Usercentrics GmbH and their processing activities. Based on the services provided to you, the relevant clause applies.

### 1. Consent Management Platform

Usercentrics offers a Consent Management Platform (CMP) as a Software as a Service (SaaS) solution. This is used to collect, manage, document and transmit consent decisions, as well as to document and transmit the processing activities based on a legal basis chosen by the Controller. By using the CMP, the scripts of the individually implemented technologies are blocked when the website is opened. These technologies are served only after consent has been given. Technologies that are used on the basis of legitimate interest are not blocked and served automatically.

The CMP makes it possible to track and document the end-user's consent as well as future changes in the decision. It is also possible to revoke consent via an embedded button (privacy button/link). Through this, the user has the option to subsequently adjust their decision.

The following data of the Controller's users is collected when using the CMP:

- User data:
  - Consent Data
  - Device data
  - IP address
  - Geolocation

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.

In addition, the Controller is provided with a database containing the latest version of the data protection texts (Data Processing Services) of the technologies used as a template. These serve only as a template and Usercentrics does not assume any liability for their correctness. It is also possible to create own customized texts for the technologies used. It is up to the Controller which version is switched live in the CMP.

Furthermore, an initial scan of the Controller's website is performed, which provides an overview of the Data Processing Services (DPS) used. After implementation of the CMP, the Usercentrics script integrated on the website regularly and extremely accurately scans for new DPS based on live user activity and updates the results accordingly.



## 2. Preference Management Platform

Usercentrics offers a Preference Management Platform. This platform can be used to provide the option to capture and store end-users choices regarding their preferences and permissions, as well as allowing end-users to manage such choices via a dedicated preference center. The purpose of this data is to provide the option to make individual decisions through the preference management platform.

The following data of the Controller's users is collected when using the PMP:

- Unique User Identifier provided by Controller,
- Preference decisions.

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.

## 3. Server-Side Tagging (SST)

Usercentrics offers a Server-Side Tagging Solution. This solution can be used to handle the execution of scripts and manage data flows server-side, instead of client-side (browsers, apps, or other sources). Through this solution, the data collected is first sent to a server that the Controller manages, before being shared with third-party services.

The following data of the Controller's users is collected when using the SST service:

- Device data
- IP address
- Geolocation
- Consent Data (if integrating with the Usercentrics CMP).

Additionally, data of the Controller's users may be passed through the Usercentrics Server-Side Tagging solution and processed by third party service providers.

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

- Visitors and users from any channel the customer integrates their SST server with.

Usercentrics only provides the Server-Side Tagging solution and is not responsible or liable for the data collected by the Controller and processed through the solution. It is the responsibility of the Controller to make sure that the data used is processed in a manner that is compliant with the relevant privacy laws.



## Annex 4 - United States of America Addendum

This Annex applies to the processing of data on the behalf of Controller and/or its affiliates who are subject to US Data Protection Laws (as defined below).

### 1. Definitions

1.1. Capitalised terms used in the Main DPA shall have the same meaning when used in this Addendum. The following capitalised terms used in this Addendum shall be defined as follows:

**"Applicable Data Protection Laws"** means all applicable US Data Protection Laws, rules, regulations, and governmental requirements relating to the privacy, confidentiality, or security of Personal Data, as they may be amended or otherwise updated from time to time

**"Covered Data"** means the data that is (a) provided by or on behalf of Controller to Processor in connection with the Services; or (b) obtained, developed, produced or otherwise Processed by Processor, or its agents or subcontractors, for the purposes of providing the Services, in each case as further specified in section 2.2 of the Main DPA.

**"Data Subject"** means a natural person whose Personal Data is Processed.

**"Deidentified Data"** means data created using Covered Data that cannot reasonably be linked to such Covered Data, directly or indirectly.

**"Main Agreement"** means the agreement entered into between Controller and Processor on the terms set out (or such other terms as the parties may agree in writing).

**"Main Data Processing Agreement" ("Main DPA")** means the Data Processing Agreement to which this addendum is attached.

**"Personal Data"** means any data or information that: (a) is linked or reasonably linkable to an identified or identifiable natural person; or (b) is otherwise **"personal data," "personal information," "personally identifiable information,"** or similarly defined data or information under Applicable Data Protection Laws.

**"Processing"** means any operation or set of operations which are performed on data or on sets of data, whether or not by automated means. **"Process," "Processes"** and **"Processed"** will be interpreted accordingly.

**"Security Incident"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, Covered Data.

**"Services"** means the services to be provided by Processor pursuant to the Main Agreement, as further described in Annex 3.

**"Standard Contractual Clauses" or "SCCs"** means the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914.



"**Subprocessor**" means an entity appointed by Processor to Process Covered Data on its behalf.

"**US Data Protection Laws**" means all applicable federal and state laws, rules, regulations, and governmental requirements relating to data protection, the Processing of Personal Data, privacy and/or data protection in force from time to time in the United States, including (without limitation): the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2018, the Virginia Consumer Data Protection Act, Code of Virginia Title 59.1 Chapter 52 § 59.1-571 et seq., the Colorado Privacy Act, Colorado Revised Statute Title 6 Article 1 Part 13 § 6-1-1301 et seq., the Utah Consumer Privacy Act, Utah Code § 13-6-101 et seq., Connecticut Senate Bill 6, An Act Concerning Personal Data Privacy and Online Monitoring (as such law is chaptered and enrolled).

Except as described otherwise, the definitions of: "Controller" includes "Business"; "Processor" includes "Service Provider"; "Data Subject" includes "Consumer"; "Personal Data" includes "Personal Information"; in each case as defined under the US Data Protection Laws.

## **2. Scope, nature and purpose of the processing**

See Annex 3 of the Main DPA.

## **3. Additional obligations in regards to the instructions for processing**

3.1. In addition to the obligations set out in the Main DPA, the Processor shall not:

- 3.1.1. use the Covered Data for any purpose other than for the business purposes specified in the Main Agreement or as otherwise permitted by Applicable Data Protection Laws;
- 3.1.2. sell Covered Data, or otherwise, make Covered Data available to any third party for monetary or other valuable consideration;
- 3.1.3. share Covered Data with any third party for cross-context behavioural advertising;
- 3.1.4. retain, use or disclose Covered Data for any purpose other than for the business purposes specified in the Main Agreement or as otherwise permitted by Applicable Data Protection Laws;
- 3.1.5. retain, use or disclose Covered Data outside of the direct business relationship between the parties; and
- 3.1.6. except as otherwise permitted by Applicable Data Protection Laws, combine Covered Data with Personal Data that the Processor receives from or on behalf of another person or persons, or collects from its own interaction with the Data Subject.

3.2. The Processor shall:

- 3.2.1. comply with its obligations under Applicable Data Protection Laws;
- 3.2.2. inform the Controller if it decides it can no longer meet its obligations under Applicable Data Protection Laws; and
- 3.2.3. inform the Controller without delay if it believes that an instruction violates Applicable Data Protection Laws. 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.



- 3.3. To the extent the Processor receives De-identified Data from Controller, the Processor agrees:
- 3.3.1. not to attempt to reidentify the data;
  - 3.3.2. to take reasonable measures to maintain and use the information in a deidentified manner, except as permitted by law;
  - 3.3.3. to commit publicly to Process the Deidentified Data solely in deidentified form and not to attempt to reidentify the information;
  - 3.3.4. to contractually obligate any authorized recipients of Deidentified Data to comply with Applicable Data Protection Laws and the foregoing requirements.
- 3.4. Notwithstanding any use restriction contained elsewhere in this Addendum, the Processor may de-identify or aggregate Covered Data as part of performing the Services.

#### **4. Confidentiality**

See clause 4 of the Main DPA.

#### **5. Security**

- 5.1. The Processor shall implement appropriate technical and organizational measures to ensure the security, confidentiality, integrity and availability of the Covered Data. The technical and organizational measures implemented by the Processor are described in Annex 1 of this Agreement. The Controller represents that it has reviewed these technical and organizational measures and is satisfied that they provide an adequate level of protection for the risks of the data to be processed under this Agreement.
- 5.2. The technical and organizational measures implemented by the Processor are subject to technical progress and further development. The Processor may implement alternative or additional measures, provided that such changes do not reduce the overall level of security afforded to Covered Data.

#### **6. Subprocessors**

- 6.1. The Controller grants Processor a general authorization to engage 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 of further Subprocessors, or other change in the identity of Subprocessors, provided that the Processor shall notify the Controller of the 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 Controller shall be deemed to have approved the change. The Controller acknowledges that in certain cases the Services can no longer be provided without the use of a specific Subprocessor. If there is an important data protection reason for the objection and if the parties are unable to reach an acceptable solution that prevents the Subprocessor from Processing Covered Data without affecting the provision of the Services, each party is entitled to terminate the contract without notice or liability.



6.1.3. The Processor shall enter into agreements with Subprocessor(s) that contain substantially the same data protection obligations as defined in this Addendum, taking into account the nature and extent of the Processing undertaken by the Subprocessor.

6.1.4. The Processor shall remain liable to the Controller for each Subprocessor's compliance with the obligations under this Addendum.

## **7. Data Subject Rights**

7.1. The Processor shall provide the Controller with reasonable assistance as necessary for the Controller to fulfil its obligation under Applicable Data Protection Laws to respond to requests from Data Subjects to exercise their rights in relation to Covered Data ("**Data Subject Requests**").

7.2. The Processor shall:

7.2.1. allow Data Subjects to withdraw consent or object to processing based on the Controller's legitimate interests directly through the features and functionalities of the Services; and

7.2.2. notify the Controller without undue delay if a data subject contacts the Processor directly with respect to Data Subject Requests relating to access, correction, restriction or deletion of their Personal Data, and provide information on the Personal Data Processed on behalf of the Controller, correct or delete such Personal Data or restrict the Processing of such Covered Data on the instruction of the Controller.

## **8. Processor's Obligations to Cooperate**

8.1. The Processor shall assist the Controller in complying with its obligations to conduct data protection impact assessments under Applicable Data Protection Laws.

8.2. The Processor shall (i) inform the Controller without undue delay of any Security Incidents suffered by the Processor; and (ii) provide the Controller with such information as required by the Controller to fulfil its obligations to notify Data Subjects or supervisory authorities under Applicable Data Protection Laws. The Processor shall not itself notify Data Subjects or supervisory authorities of the Security Incident unless it receives instructions to do so from the Controller 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 shall support the Controller at the Controller's expense.

## **9. Controller's right to information and inspection**

9.1. The Processor will notify the Controller promptly if it determines that it can no longer meet its obligations under Applicable Data Protection Laws.

9.2. The Controller may take reasonable and appropriate steps to:

9.2.1. ensure that the Processor uses Covered Data in a manner consistent with the Controller's obligations under Applicable Data Protection Laws;



- 9.2.2. upon reasonable notice, stop and remediate unauthorized use of Covered Data.
- 9.3. The Processor shall provide the Controller with any information reasonably required by the Controller to demonstrate the Processor's compliance with this Agreement. The Controller may carry out audits, including inspections, of the Processor's compliance with this Agreement, or, appoint a third-party auditor to carry out such inspections, in each case by prior written agreement with the Processor on the scope and timing of such audits.
- 9.4. The parties agree that the Processor may submit documentation to the Controller in order to prove its adherence to its obligations under this Agreement and implementation of the technical and organizational measures set out in this Addendum, including 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.
- 9.5. The Controller shall not conduct on-site inspections of the Processor unless it reasonably believes that such inspections are necessary after receipt of the documentation referred to in Section 9.4.
- 9.6. Any documentation provided by the Processor to the Controller under Section 9.4, and the results of any audit conducted by the Controller in accordance with Section 9.3, shall be the Confidential Information of the Processor.

## **10. Deletion of Data and Return of Data**

Processor shall, if requested to do so by Controller within thirty (30) days of termination or expiry of the Main Agreement, hand over to the Controller without undue delay, at the latest within 30 days, all Covered Data. Otherwise, the Processor shall destroy the Covered Data unless the Processor is required to retain it under applicable law.

Notwithstanding the above, the Processor may retain any backups of Covered Data made by the Processor for a period of up to 6 months.

Notwithstanding termination of the Main Agreement, this Addendum shall remain in effect until, and automatically expire upon, the Processor's deletion of all Covered Data as described above.

## **11. Liability**

The parties' liability under this Addendum shall be governed by the liability provisions in the Main Agreement.



## **Annex 5 - Swiss Federal Act on Data Protection Addendum**

This annex shall apply to any processing of Personal Data subject to Swiss Federal Act on Data Protection (FADP).

1. Any references to the "GDPR", "Directive 95/46/EC" or "Regulation (EU) 2016/679" will be interpreted as references to the Swiss FADP, and references to specific Articles of "Regulation (EU) 2016/679" will be replaced with the equivalent article or section of the Swiss FADP;
2. References to "EU", "Union", "Member State" and "Member State law" will be interpreted as references to Switzerland and Swiss law, as the case may be, and will not be interpreted in such a way as to exclude data subjects in Switzerland from exercising their rights in their place of habitual residence;
3. Data subjects as defined in the Swiss FADP may enforce their data subject rights as defined in the FADP;
4. The Federal Data Protection and Information Commissioner ("FDPIC") of Switzerland will have authority over data transfers governed by the Swiss FADP;
5. References to the "competent supervisory authority" and "competent courts" will be interpreted as references to the FDPIC and competent courts in Switzerland;
6. The DPA will be governed by the laws of Switzerland; and
7. Disputes will be resolved before the applicable courts of Switzerland.