DATA PROCESSING AGREEMENT

Usercentrics Contract – Data Processing Agreement

Agreement between

(hereinafter **„Controller“**)

and

Usercentrics A/S

Havnegade 39

1058 Copenhagen

Denmark

(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 following tasks by the Processor in accordance with the service description in the terms and conditions (https://www.cookiebot.com/en/terms-of-service/) of the Processor agreed between the Parties (Main Agreement): collection, management, documentation and transfer of the consent of the Controller's users or personal data collected on the basis of legitimate interests via the technology provided by the Controller and, if applicable, other services agreed with the Controller in accordance with the 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.

2.2. Type of Data

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

- User data:
    - Consent Data (Consent ID, Consent date and time, User Agent of the browser and Consent State.)
    - Device data (HTTP Agent, HTTP Referrer)
    - URL visited
    - User language
    - IP address
    - Geolocation

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 (end-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). Annex 3, the Main Agreement, this Agreement and, if applicable, the settings made by the Customer 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 client reserves the right to issue comprehensive instructions on the type, scope and procedure of data processing, which the client 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. For the purposes of this Agreement, "Standard Contractual Clauses" or "SCCs" means the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914. 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 under Union law or the law of an EU member state 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 its area of responsibility, the Processor shall design the internal organisation in such a way that it meets the special requirements of data protection. The Processor 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.

5.3. The technical and organisational measures are listed in Annex 1 to this Agreement.

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 within the CMP, the end-user can accordingly exercise the right to withdraw consent. 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 the data subject's 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. In the case the security incident results from the risk sphere of the Processor, the Controller is not obliged to reimburse costs.

9. Other obligations of the Processor

9.1. 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.

9.2. 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 its obligations and implementation of the technical and organizational measures. Convincing documentation can be provided by presenting a written report displaying the compliance covering the security by the Processor.

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 verify the Processor's compliance with this Agreement within the Processor’s 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 its 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 utilization 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.

11.2. 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. The Processor 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 or in a separate agreement between the parties. For the external legal liability, the regulations according to Art. 82 GDPR apply.

13. Miscellaneous

13.1. Changes and additions to this Agreement and all of its components, must be made in a written agreement, which may also be made in an electronic format (text form), and the express statement that it constitutes a change or addition to the present terms and conditions. This also applies to any waiver of this written-form requirement.

13.2. The provisions of this Agreement shall survive the termination of the Main Agreement and remain in force until such time as all personal data of Controller have been destroyed in full or returned to Controller.

13.3. In other respects, the provisions of the Main Agreement / the contract shall apply in like manner.

13.4. If any individual part of this Agreement is invalid, this shall not affect the validity of the remainder of the Agreement.

Annex 1 - Technical-Organisational Measures/ Safety Concept of the Usercentrics A/S (Cookiebot)

Technical and organizational measures (TOM)

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

Usercentrics A/S, Havnegade 39, 1058 Copenhagen, Denmark (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

- Personal data, subject to processing, is stored in accordance with industry standards.
- Data is stored and processed in Microsoft Azure datacenters and Usercentrics does not have physical access to this data.
    - Access to Microsoft Azure infrastructure - more information on measures can be found here: https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-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:
    - Outside normal working hours, access to the coworking building and office space is only possible for employees and service providers (e.g. cleaning service) which have access with a key and a code. Some employees have been assigned their own key - in addition, there is one key to each of the offices, which is locked inside a key box next to the entrance to the offices. During normal working hours, the office is not locked if employees are in the office and can monitor access.
    - The use of surveillance cameras.

Electronic Access control

Usercentrics defines two approaches to access data:

- Access to data with the intent to process
- Access to systems with the intent to change the system infrastructure

Access to data with the intent to process

- Data access operates within the following constraints:
    - Only identified resources can access data and access is only via encrypted means (HTTPS, TLS/SSL).
    - Anonymous access to data is not allowed and is actively prohibited.
    - A central directory resource provides the identity of users and systems. IT operates within these core principles:
        - User accounts must adhere to the following;
            - A combination must username and password grants access
            - Passwords must be strong as defined by industry standards
            - Account access is verified with multi-factor (e.g. two-factor) authentication, adhering to industry standards
            - Passwords are transmitted unencrypted during account creation. A user is forced to change the initial password upon first usage
        - Systems accounts adhere to the following:
            - Managed accounts are preferred
            - Where managed systems accounts are not possible, the infrastructure stores account information in a highly secure manner utilizing strong encryption and access control
        - A least-privilege approach defines access rights and grants to users and systems.
        - Inactive users and systems are disabled or removed regularly in predefined intervals.
        - Audit trails on user creation are actively stored and monitored.
        - Administration of the directory operates within the following constraints:
            - Only a select few accounts have administrative access to the directory.
            - Administrative access is audited.
            - Administrative access is granted on a time-constrained basis.

- 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).

Access to systems with the intent to change the cloud infrastructure:

- Access to the underlying infrastructure compromising Usercentrics's systems operates within the following constraints:
  - Access to production system infrastructure is audited.
  - Access to production system infrastructure is granted on a time-constrained basis.
  - Only break-glass accounts have permanent administrative access to production system infrastructure.
  - Temporary administrative access to production system infrastructure is audited.
  - Temporary administrative access to production system infrastructure requires acceptance from multiple trusted employees.

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 and RDP are deactivated wherever possible.
- Graduated authorizations are assigned depending on the employee's area of activity. The minimum principle is always applied here.

Further measures

- Data at rest is stored using industry-standard encryption schemes.
- Data in transport, outside of the data centers, is encrypted using industry-standard encryption schemes.
- Each system in its respective stage is operated on its own system 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 data minimization principle in Article 5, para.1, lit. C GDPR

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.

Data management systems (DBMS) store personal data at rest. These have implied integrity checks at the physical storage level.

Following measures are employed to ensure integrity when processing data:

- Direct access to the DBMS is only allowed from a restricted set of IP addresses.
    - Users access DBMS systems through restricted VPN tunneling - Anonymous access is prohibited.
    - Systems access the DBMS systems through network restricted zones - Anonymous access is prohibited
    - Access is audited and monitored.

- Data inputs is validated using the following measures:
    - Constraints in the underlying database structures ensure integrity at the relational level.
    - Input validation in the software systems ensures integrity at the processing level.
    - High standards in the legally compliant drafting of contracts for processing 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)
    - Obtain information from service providers regarding the measures taken to implement data protection requirements.

- Data output is validated using the following measures:
    - Access restrictions in the software systems processing the data – only authorized users and systems have access to personal data.
    - Systems and users operate under the least privilege strategy.

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 (Consent Management Platform) & related systems

Usercentrics does not operate its own server resources in its own data centers. For the production system (CMP) and related systems, **Microsoft Azure** resources (Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18 D18) are used.

The following measures are employed to ensure the availability of systems and data:

- All systems and data exist in Microsoft Azure datacenters and are dependent on their availability as described here: https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure-availability.
- Data is stored in geo-redundant systems.
- Our productive environment is backed up at regular intervals or data mirroring procedures are used.
- The systems are protected by an uninterruptible power supply (UPS).
- A multi-layer virus protection and firewall architecture is used.
- 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.
- For specific Usercentrics systems, the following measures are implemented:
    - Systems health and activities are monitored both by automatic sub-systems and human employees.
    - Intrusion Detection Systems (IDS) are employed at the network access endpoints to the critical systems.

- Access to critical systems is load balanced and utilizes auto-scaling functionality to cope with increased demands.
- Content Delivery Networks (CDN) are deployed to ensure the high availability of critical systems.

Further information can be found at:

https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA - Appendix A

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.
- 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 data related to this processing by the hosting provider (Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18 D18).

- 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).
- Alarm monitoring.

Further information:

https://docs.microsoft.com/en-us/compliance/assurance/assurance-network-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).
- No personal data is stored as part of the consent log or anywhere else.
- A user's ID in the consent log is not reused across multiple sites and it is not possible for Usercentrics to track a user across multiple sites.

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.

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 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 Legal and the IT Department internally in Usercentrics.

Further measures

- Reviewing information on newly emerging vulnerabilities and other risk factors, including revision of the risk analysis and assessment, if necessary.

Contact details of the Internal data protection coordination:

Legal Department, Havnegade 39, 1058 Copenhagen, Denmark, privacy@cookiebot.com

Annex 2 - Sub-processors

Authorized subprocessor

#	Name	Operating company	Address of the Subcontractor	Place of data processing	Scope of Application under the Contract	Data Subject
1	Microsoft Azure	Microsoft Ireland Operations Ltd, Dublin	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18 D18	Databases are hosted on servers within EU member states, specifically Ireland with a hot fail-over mechanism to Microsoft's datacenter in Amsterdam, the Netherlands	Data hosting	Controller's end user
2	Akamai	Akamai Technologies, Inc.	145 Broadway Cambridge MA 02142 USA	Database in the US	CDN provider Geolocation to show the right cookie banner IP address stripping at edge layer for Visitor Attribution Add-On requests.	Controller's end user
3	Bunny	BunnyWay, d.o.o.	Cesta komandanta Staneta 4A 1215 Medvode Slovenia	Database in the European Union	CDN provider (used by the CB customers who choose the EU CDN provider)	Controller's end user
4.	Privacy Analytics	Visitor Analytics GmbH	Seestraße 76, 82335 Berg, Germany	Database in the European Union	Analytics Provider	Controller's end user

Annex 3 - Service Description

1. Consent Management Platform

Usercentrics offers a Consent Management Platform (CMP) as a Software as a Service (SaaS) solution. This solution is used to collect and document consents granted by the Controller's users. By using the CMP, elements on the Controller's website, such as scripts, images, iFrames etc are blocked and unblocked according to the consent granted by the user, when the website is opened. Elements that require consent are only unblocked after the user has granted consent.

Elements on the Controller's website that require consent are automatically detected and categorized according to the required consent categories by Usercentrics on a regular basis, through daily or monthly scans of the website.

It is possible for users to revoke or change their granted consent categories (via a privacy trigger or link).

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

- Consent Data
    - Consent ID - A unique ID that is required so a user can utilize it to request the Controller for a proof of consent
    - Consent State - 1) Consent categories granted - required to allow the CMP script to block and unblock tracking elements on the Controller's website according to the user's choice and 2) Version - required to maintain a record of which version of the Controller's consent and privacy policies the user granted consent to, so the Controller can ask a user to renew consents in case of policy updates
    - Consent date and time
- URL visited - Required to document where a user gave consent.
- User language - required to show the consent banner in the language defined by the Controller
- User agent (browser vendor and version, operating system) - required to separate traffic from real and synthetic users
- IP address - required to enable basic routing of messages on the Internet, to determine the user's geographical location and to separate real and synthetically generated consents
- Geolocation - required to ensure that consent banners shown correspond to the user's geographical location and legal jurisdiction

Before consent is given by the end user

When loading the Consent Banner from consent.cookiebot.com or consent.cookiebot.eu, Cookiebot receives and processes the following data:

- The website URL that is used to serve the correct consent banner
- The end user's browser language that is used to serve the consent banner in the correct language
- The end user's user agent that is used to filter synthetic traffic from real traffic
- The end user's IP that is required to enable basic routing of messages on the Internet, and to determine the users geo-location (country and state) to serve the correct banner, fitting the end user's geographical location and legal jurisdiction

The above data Usercentrics receives is only processed to serve the end user the consent banner and none of this data is retained after processing. After the consent banner is returned and shown to the visitor, the end user usually takes a consent decision, that involves either denying all consent, giving full consent or partial consent.

After consent is given by the end user

This consent decision is sent to Usercentrics where Usercentrics receives the following data:

- The website URL that is used to log the Consent State correctly
- The end user's user agent that is used to filter synthetic traffic from real traffic
- The Consent State to log the consent choice of the end user

The data Usercentrics receives is processed to document the end user's consent choice. To document the consent for potential auditing purposes, Usercentrics generates a Consent ID and saves it along with the Consent State on behalf of the customer within Usercentrics' consent log database. The storage of the Consent ID along with the Consent State is necessary to exercise the end user's right to receive proof of consent from the Controller at any time.

After the consent is stored, Usercentrics returns the generated Consent ID to the website. The Consent ID, along with the Consent State, is stored client side inside a first-party consent cookie. Using first-party cookies as the technology prevents any tracking use case of the consent cookie across multiple websites.

The consent cookie is not accessible to other websites or third parties. It is also never transmitted to Usercentrics, which does not track end users to the website across different visits. The Consent ID is used solely for the purpose described above and never for any kind of user tracking by Usercentrics.

After consent has been given by the end user, Usercentrics will process and retain the data listed above included in this data processing agreement on behalf of the website owner with help from the data processors listed in annex 2 and does not share or process the data any further.

Usercentrics does not collect data regarding a particular end user's or device's activity across multiple data controllers. Any data processed and collected as part of the CMP's processes are only done so in the context of the controller's websites. Users or devices will not be fingerprinted, tracked or otherwise matched across visits to different controllers, even if those sites all happen to use our CMP solution. The sharing and matching of data throughout the websites of a single controller remains untouched by this.

Find more information here.

2. Privacy Analytics

Usercentrics offers a website intelligence solution. It can be used to provide statistics, behavior analytics features, and direct visitor communication tools that help understand website performance and guide optimization.

When using the Privacy Analytics service, the following categories of personal data of the Controller's end users may be processed, depending on the selected privacy mode and the applicable consent status::

- Page views, sessions, and general traffic statistics
- Device information, Browser information, and Device Operating System information
- Non-precise geographic data (e.g., country or region)
- Click-paths, scroll behavior, and general interaction patterns on the website
- A hashed identifier used for statistical and analytical purposes

The scope, granularity, and availability of the above data categories depend on the privacy configuration selected by the Controller and may differ before and after a consent decision by the end user. Certain data elements may be aggregated, limited, or not collected at all in pre-consent scenarios.

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. Visitor Attribution Add-On

Usercentrics offers a Visitor Attribution Add-On as an optional feature available to Controllers with an active Cookiebot CMP account. The Add-On enables Controllers to deploy a configurable visitor question on their website for the purpose of collecting anonymous marketing attribution data. The Add-On is delivered as a feature of the existing Cookiebot CMP JavaScript tag and does not require separate installation.

The Add-On is designed to operate without collecting personal data. When a visitor responds to the Add-On, the following data is collected:

- A visitor's selected answer
- A domain identifier
- Configured page path
- Device type
- Timestamp

No IP address, cookie, persistent identifier, or other personal data is collected or retained by Usercentrics in connection with Add-On responses. Add-On dismissal and completion state is recorded in the visitor's browser sessionStorage for the duration of the browser session only and is not transmitted to Usercentrics.

Because no personal data is collected, the Add-On operates independently of the visitor's consent state and renders for all visitors regardless of their consent decision under the CMP. No legal basis under GDPR Art. 6 is required for the Add-On's operation.

Individual response records that do not meet the minimum aggregation threshold are automatically deleted within a defined retention period and are not made available to the Controller in any form. Aggregated response data is made available to the Controller via the Cookiebot CMP Manager dashboard.

The Add-On data pipeline is maintained architecturally separate from the CMP consent log database. No Add-On response data is commingled with personal data processed under this Agreement.