

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 is only possible for employees and service providers (eg cleaning) which have access with a key and a code. Some employees have been assigned their own key to the office - 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 (the Coworking buildings where we are located have surveillance cameras in - e.g. the entrance areas).

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 comprising 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.

- o Access to critical systems is load balanced and utilizes auto-scaling functionality to cope with increased demands.
- o 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, legal@usercentrics.com