Status: 24th of February 2023

RFI Q/A

The following information for our customers and partners provides an overview of relevant questions regarding the operational structure of our Cookiebot CMP, IT security, and data privacy at Usercentrics. These questions are supplementary to the explanations in our technical, organizational measures (TOM) and our data processing agreement (DPA).

Q What services are included in the solution?

A Usercentrics offers a Consent Management Platform (CMP) as a Software as a Service (SaaS) -the Cookiebot CMP. The Cookiebot CMP is used to properly inform your website visitors or app users about any data processing activities and to collect, manage, document, and share user consent data with other applications that require the information. The Cookiebot CMP allows you to block or unblock tools in your website or app based on whether or not a user consented to the use of those tools.

The Cookiebot CMP makes it possible to track and document the end user's consent as well as future changes to their consent preferences. Via an optional privacy button you enable the user to subsequently adjust their privacy/consent preferences at any point in time - building trust by putting the user in control over the privacy choice.

The Cookiebot CMP also monitors your website regularly and reports on any tools or technologies identified, to ensure that all data processing activities are properly captured.

Q Is personal data being processed by the solution?

A The Cookiebot CMP service is provided via the Internet and hence the IP address of users' must be processed to exchange data with our servers. Usercentrics further processes the following data for the purpose of recording end users' consent decisions: Consent ID, consent data and time, User Agent of the browser State, device data (e.g. HTTP agent and HTTP Referrer), URL visited, User language, geolocation and the consent data itself.

Q Is data encrypted?

A Data at rest is stored using industry-standard encryption schemes. Data in transit, outside of the data centers, is encrypted using industry-standard encryption schemes. And only identified resources can access data and access is only via encrypted means (HTTPS, TLS/SSL).

© Copyright 2023 Usercentrics A/S

Q What availability does Usercentrics offer for its services?

A We organize our resources to provide a high level of service with at least 99.9% uptime on the operation of the cloud service and a response time of less than 1 business day for support requests related to critical bugs (high impact, high urgency) and unscheduled downtime of Cookiebot.

Q Is Usercentrics a data controller or processor?

A In the context of providing the Cookiebot CMP to our customers, we take the role of data processor, acting on behalf of our customers. In this regard, our customers are the data controller.

Q Where can I find a current overview of the sub-processors?

A Information about relevant sub-processors can be found in the DPA. We inform our customers about changes in accordance with the GDPR.

Q Are appropriate agreements in place with the sub-processors and other external vendors to ensure IT security and data privacy?

A Yes, the selection process for any of our sub-processors includes a data privacy and IT security screening process. Data processing and confidentiality agreements are in place with all our sub-processors. We apply the same standards to these measures as we do to our own processing.

Q Is data processed outside the EU, and, if so, what measures are taken to safeguard it?

A We operate the Cookiebot CMP on regional Microsoft Azure servers in European data centers (Ireland with a hot fail-over mechanism to Microsoft's datacenter in Amsterdam, Netherlands). But for our CDN provider, Akamai Technologies Inc., we are using a US company which may be subject to the US CLOUD Act and FISA 702 and therefore the possibility of potential access by the US government cannot be fully excluded. We have therefore concluded the current variants of the standard contractual clauses, evaluated transfer risks in a comprehensive transfer impact assessment, and work with secure encryption technology (AES256). To further reduce potential risks, we provide additional optional technical solutions that ensure processing of end user IP addresses in the EU, as well as management of our own encryption keys.

© Copyright 2023 Usercentrics A/S

Q **Can we share our Transfer Impact Assessment (TIA) for the providers/sub-processors we are using for processing data?**

A No, it is not possible for us to share our TIAs. We have created these as the required documentation needed for the processing of personal data for the providers we are using located in a third country (including the USA).

Q **How are confidentiality, integrity, resilience and availability ensured?**

A A wide range of technical and organizational measures (TOM) are in place, such as access control on various levels, input and transfer controls, system monitoring and a redundancy to ensure your data is securely stored and processed and the solution operates reliably. You can find our current TOM here in our DPA.

Q **How is the subject of data privacy and data security established in the company?**

A For data privacy, we have established a data privacy management system (DPMS).
For information security, we are working after the ISO27001 standards. Both contain extensive documentation of processes and procedures, (possible) incidents, guidelines for dealing with the challenges within the company, risk analyzes, regular audits and training for all our employees.

Q **Do we have a data protection officer (DPO) for Usercentrics A/S?**

A As it is not required for us to have a DPO in regard to Danish law, we do not have a DPO for Usercentrics A/S.

Q **Does Usercentrics have certifications that show successful use of an information security management system?**

A No, it is not possible to share an ISO certification for Usercentrics A/S. But in our daily work we are working under the standards and requirements of a certification like this.

Q **Are there established processes for (potential) security and/or data privacy incidents?**

A There are processes for (potential) data privacy breaches and information security incidents, for internal systems and systems that affect the operation of our Cookiebot CMP. The processes include internal standardized and documented measures that take legal requirements (e.g. incident notification and documentation) into account. Dedicated data protection information security officers ensure clear ownership within the organization and that processes are regularly reviewed and updated where required, as well as that all employees are adequately informed and educated on the subject.

© Copyright 2023 Usercentrics A/S

Q **How is secure data erasure of personal data ensured?**

A We have documented the blocking and erasure of data in a corresponding concept as part of our data privacy management system. This concept is based on a technical deletion guideline that specifies the corresponding deletion periods for each type of data in the company. Based on these deletion periods, and if otherwise required, data is deleted and blocked at Usercentrics. Data deletion actions are documented in an erasure log.

Q **Are penetration tests performed? If so, at what intervals?**

A We work with different service providers to perform detailed penetration tests regularly. The results are reviewed within the teams concerned. If necessary, measures are taken to remedy the findings. Issues with high risk attached are addressed immediately, medium risk issues are addressed within 6 months.

Q **Is there a role and authorization/permission concept?**

A At Usercentrics, a role and authorization concept as part of our data privacy management system regulates when an employee is granted access to the systems. We always ensure that only absolutely necessary access and rights are assigned. Roles/permissions are granted and revoked using standardized and documented processes.

Q **Is there a documented process for exercising the rights of data subjects in accordance with Article 15-22 GDPR?**

A Yes, we have internal documentation and a process for how to handle requests like this.

Q **What measures are in place for physical access to systems and data?**

A We use managed services hosted in secure server environments of the Microsoft Azure. Further information on the Microsoft Azure infrastructure and the security used can be found here. Usercentrics does not have physical access to this data.

The Coworking building where our office is located is secured with video surveillance of various areas. We have a clean desk policy, and outside normal working hours access to the Coworking building and office is only for employees and service providers (cleaning) which have access with a kay and a code.

© Copyright 2023 Usercentrics A/S

Q **Organization of Information Security: are risk assessments performed?**

A Risk management around critical assets is in place. As part of the information security management system. Risk assessments are carried out at least annually. Identified risks are managed and mitigation strategies identified and implemented.

Q **How are employees sensitized and/or trained on the topic of IT security and data privacy?**

A There is a training concept for IT security and data privacy. Employees undergo relevant training modules when they join the company (e.g.~45-minute interactive online training), which must be repeated at annual intervals to refresh the knowledge. In addition, employees are consistently made aware of the issues using practical examples within their respective teams and during topical workshops.

Q **How is it ensured that employees process personal data in secure work environments (hardware/software)?**

A An IT use policy regulates how an employee must handle hardware and software in the company. Each employee's computer is protected by an end user protection software and equipped with a device management software that enforces policies based on an employee's profile. All devices are password protected and have hard drive encryption enabled. Any software used undergoes extensive preliminary screenings (data privacy, data security, reputation, etc.). The same applies to system updates. Access to the relevant software is strictly regulated via a roles/permissions concept. In addition, we work with personal access (user ID, password), avoid group accounts, and set strict password policies. We use multi-factor authentication where possible.

Q **How is it ensured that employees have the correct roles/permissions when working with internal systems?**

A Employees are only given precisely those roles/permissions that are necessary for the job. If an employee joins the company, they receive access relevant to their role (e.g. sales employee, developer, customer success manager). These may vary over time. Accordingly, the correctness of the assignments is also regularly audited. Changes in roles/permissions must be applied for and approved and are subsequently documented. Especially in the case of particularly sensitive systems (e.g., Cloud Consoles), a granular classification of the assigned rights and roles is carried out. For production systems, only cloud admins have privileged access to the production system. Non privileged access is provided to 24×7 staff for monitoring and logs.

© Copyright 2023 Usercentrics A/S

Q **Are BCM tests performed on a regular basis?**

A For both internal systems and the systems used to operate the Cookiebot CMP there are appropriate BCM templates to ensure business continuity at all times. BCM measures are reviewed and tested at least annually.

Q **Are there central regulations on how to ensure safe development?**

A Internal guidelines that provide policies and instructions for the entire lifecycle of our software and/ or services that must be followed during the everyday operational/development work are in place.

The following aspects are covered:

- Security in Software Development (Requirements, Design, Implementation, Testing and Verification)
- Security in software deployment/release
- Security in operation (reaction to identified faults and vulnerabilities)

We are always available for further inquiries. In this case, please contact your respective contact person at Usercentrics.

© Copyright 2023 Usercentrics A/S