Your Customers.
Convinced.



# ARCHITECTURE OF EXCENTOS PRODUCT GUIDE SAAS WEBSERVICES

This document describes the security architecture of the webservices provided by excentos.
Further regulations regarding the Service Level Agreements (SLA) and general privacy regulations
see the SLA and General Terms and Conditions documents as published on www.excentos.com/service-terms.

## 1) Overview of excentos SaaS webservices

excentos provides the Product Guides in a comfortable SaaS model and takes care that all services run smoothly. We know that our Product Guides play an important role in your user's purchase decision processes and thus take great care in providing extremely stable and scalable webservices:

(1) excentos is 100% responsible for providing the webservices for your Product Guide applications. You as our customer do not need to provide any IT resources to operate the Product Guides.

(2) We provide internet backbones in Europe and USA and whereever required for your operations.

(3) We can scale the webservice in terms of load and performance according to our customer's requirements.

(4) excentos provides automated deployment and load-balancing and off-datacenter monitoring with ping every 5 min from EU & US (see below in "Monitoring").

(5) All IT-related maintenance efforts, providing the webservice and all hardware costs are covered by the SaaS fee.

(6) Our customers do not need any modification on their security or IT infrastructure, except providing the integration site and mentioning excentos in your privacy policy or cookie / consent management solution.

## 2) Security of Product Guide webservices

(1) All external requests are forced to use HTTPS with modern TLS implementations and secure ciphers.

(2) Thread detection and mitigation is done by Cloudflare (see further information below), also denial-of-service prevention, provides firewall.

(3) All Product Guide service instances are shielded by Cloudflare, so IP addresses of our servers are not publicly available

(4) Each product guide service instances runs as a unique user so any breaches cannot influence other instances.

(5) Each server has a separate firewall to block all ports except SSH and HTTP(S).

(6) Each server scans log files to ban any IP addresses with malicious behavior.

(7) Root user is deactivated everywhere, access is only granted for excentos users.

(8) Product Guide service instances are only created and updated by excentos tools, never by employees manually.

(9) Product Guide instances provide no means for external users to change the configuration or store malicious data since the only action a user can do is select existing navigation or answer options for his profile.

## 3) Security of Workbench (self-service backend)

(1) All external requests are forced to use HTTPS with modern TLS implementations and secure cyphers.

(2) Each server has a separate firewall to block all ports except SSH and HTTP(S)

(3) Each server scans log files to ban any IP addresses with malicious behavior.

(4) Root user is deactivated everywhere, access is only granted for excentos users.

(5) Each account (e.g. https://workbench.excentos.com/your-account-name) has its own database; even user accounts (including excentos users) are only local to his database, so there is no risk to enter a wrong account accidentally.

(6) The Workbench infrastructure uses extensive security checks in the backend to ensure the user is only able to see and change things allowed by his permissions.

## 4) Stress test possibilities

excentos uses the following stress test possibilities to assure security and performance of our services:

(1) Own framework built upon an established open-source framework to measure latencies / server response times for a given number of concurrent users.
This testing framework can be used to test a scalable cluster of servers for their performance and response time with a simulation of

high-traffic impacts (e.g. TV advertisements, email marketing) to assure that certain load / performance criteria are met.

(2) Comparison tool to test if there are differences in API output for a simulation of user sessions. This tool is used to run revision tests of new software releases.

## 5) Data security standards

(1) excentos delivers its service according to highest GDPR (General Data Protection Regulation) standards. For an overview of the extensive GDPR measures that excentos provides, please see the Data Processing Agreement (DPA) published on https://www.excentos.com/service-terms (please refer especially to the chapter "Technical and Organizational Measures" at the end of the document).

## 6) Monitoring

For optimized performance, we use several levels of monitoring the excentos SaaS:

(1) Hardware monitoring: excentos runs permanent hardware monitoring tests every 20 seconds to ensure availability and health. Additionally, every of our hosting providers runs separate uptime tests.

(2) Global service monitoring: The end-to-end availability of our webservice is tested by a global monitoring solution every 5 minutes.
The monitoring solution provides real-life requests to the webservice to ensure availability. The monitoring is executed from several locations around the world.

(3) Dedicated global loadbalancer monitoring: Our loadbalancers are monitored by our network provider to assure availability.

## 7) Penetration tests

(1) excentos regularly performs penetration tests to assure the security of our SaaS. Several of our services (Workbench backend; service URLs and frontends of the productive Product Guides; analytics; hosting center) require different penetration tests to cover their individual requirements. Besides penetration tests, all applications are secured by HTTPS and TLS (see chapter 2) and 3)) and stress-tested (see chapter (4)).

(2) Upon request, we can run specific penetration tests by a third party and share the assessment results with you.

## 8) Hosting / network providers and certifications

The following list shows the default hosting / network providers used by excentos. For data security reasons, excentos will decide which servers will actually be used for your applications depending on your rollout plan.

| **Provider** | **Address and Server Location** | **Certification** |
|---|---|---|
| Hosting center for requests from **Europe** (and rest of world):<br><br>Hetzner Online GmbH or velia.net (address see below) | Industriestr. 25 91710 Gunzenhausen, Germany<br><br>Server location: Frankfurt, Nürnberg, Falkenstein (Germany) and Helsinki (Finland) and Strasbourg (France). | DIN ISO/IEC 27001<br><br>Further infos see here |
| Hosting center for requests from **USA**:<br><br>velia.net Internetdienste GmbH | Hansestr. 111<br>51149 Köln<br>Germany<br><br>Server locations: Los Angeles, St. Louis, Miami, USA. | SSAE16 SOC2<br><br>Further infos see here (colocation center of velia.net) |
| Hosting center for requests from **Asia**<br><br>velia.net Internetdienste GmbH | Hansestr. 111<br>51149 Köln<br>Germany<br><br>Server locations: Hongkong, China. | SSAE16 SOC2<br><br>Further infos see here |
| Network provider:<br><br>Cloudflare Inc. | 101 Townsend St,<br>San Francisco<br>CA 94107, USA.<br><br>Server location: around the world | ISO 27001:2013,<br>SOC 2 Type II,<br>SOC 3,<br>PCI DSS 3.2.1<br><br>Further infos see here |

In case we encounter specific hosting requirements, we will provide further regional hosting centers or also provide on premises-hosting in your IT / hosting center.