Quick facts about application & platform security

In the following list we provide a brief description of the measures we have implemented, which are part of the security standard of the MEA, Polario, Registr services.

Client separation:

Databases and file storage are separated on a client-specific basis. Business logic is encapsulated in Docker containers.

Penetrationstests:

External pentests are carried out regularly every year to identify and fix weaknesses. The last tests for MEA & Polario took place at the end of 2023.

Vulnerability scans:

Our DevOps use Trivy for vulnerability scans in the cloud environments. Findings from scan reports are evaluated and fixed.

Hacking:

Attack scenarios are covered in the pentests and vulnerabilities are addressed.

Ethical hacking tests:s:

No specific implementations to date.

Plattformsicherheit:

Google Cloud offers comprehensive documentation on security measures.

- https://cloud.google.com/solutions/security?hl=en
- https://cloud.google.com/docs/security

Development guidelines:

Specified requirements for employees are known to everyone and are monitored.

Web application firewall:

Is implemented.

Encryption:

Data at rest and in transit are encrypted in the Google Cloud. Documentation is available.

- https://cloud.google.com/docs/security/encryption/default-encryption
- https://cloud.google.com/docs/security/encryption-in-transit

Access control:

All access is monitored and limited to the need-to-know principle. Google only accesses data for support purposes. API and CMS accesses are recorded by the monitoring system. Robust authentication and authorization to ensure that only authorized users can access the API/CMS/platform.

Avoiding sensitive information in URLs:

We do not transmit confidential data such as passwords or access tokens in URLs. We use headers or request bodies instead.

TLS encryption:

We use secure Transport Layer Security (TLS) encryption to protect communication between client and server.

Narrowly defined requests and responses:

We limit the allowed requests and responses for RESTful APIs to prevent unwanted access.

Monitoring and detection of API attacks:

We have implemented a feature to monitor and detect attacks on our API.

Patches and updates:

Automatic security patches and updates to the Google Cloud. Individual updates and patches of the application.

Secure configuration:

Connected services (GCP, All-Inkl) are securely configured according to the provider‘s specifications.

Backups:

Daily backups of databases with 7-day retention period. Can be set individually.

Emergency planning:

ISO27001-compliant emergency management.

Monitoring:

Continuous monitoring of access and other values of the hosting platform. (utilization, transmission, identification)

Detailed descriptions and further details can be found in our DPA template.