OpenSlides

Das digitale Antrags- und Versammlungssystem

Data Processing Agreement in accordance with Article 28 of the General Data Protection Regulation (GDPR)

Agreement

between

(Client's address)

– controller, hereinafter referred to as the Client –

and

Intevation GmbH
Neuer Graben 17
49074 Osnabrück
Germany
– processor, hereinafter referred to as the Contractor –

1. Subject-Matter and Term of the Contract

(1) The subject-matter of the contract is the provision of hosting services in the context of the OpenSlides product package provided by the Contractor.

(2) The term of this contract (duration) is determined by the duration of the provision of hosting services by the Contractor to the Client. The contract ends when the Client ceases to use the Contractor's hosting services in accordance with the service agreements / quotations set out in individual order confirmations for the Contractor's hosting services.

2. Specification of the Contractual Content

(1) Nature and purpose of the intended processing of data:

The subject-matter of the contract relates to the hosting of OpenSlides on a web server administered by the Contractor. The scope, nature and purpose of the intended collection, processing and/or use of data arise from the hosting service agreements. The provision of data processing as stipulated in the contract shall take place exclusively in a Member State of the European Union or in another Contracting State to the Agreement on the European Economic Area.

(2) Type of data:
The following types/categories of data are the subject-matter of the processing of personal data:

- Personal master data (first and last name)
- Communications data (email address)
- Structure level at the Client
- Membership data (see Article 9(1) GDPR)
- Political opinion (see Article 9(1) GDPR)
- Image and sound (for optional use of audio or video conferencing services)

(3) Categories of data subjects:
The categories of data subjects affected by the processing include:

- The Client's employees
- Delegates or members of the Client
- Guest participants

3. Technical and Organisational Measures

(1) The Contractor shall ensure the technical and organisational measures required for the proper performance of the contract in accordance with Articles 28 and 32 GDPR. The technical and organisational measures described in Annex 1 are detailed to match the data security risk, taking into account the protection goals of confidentiality, availability, integrity, purpose limitation, transparency and intervenability, and with particular regard to the IT systems and processing procedures used by the processor.

(2) The contractor administers the OpenSlides servers, which are operated exclusively in certified data centres in Germany. The data centres' technical and organisational measures in accordance with Article 32 GDPR can be accessed here:

- kyberio GmbH:
  `https://www.kyberio.com/wp-content/uploads/Vereinbarung-ueber-Auftragsverarbeitung-kyberio-gmbh.pdf`
- Hetzner Online GmbH:
  `https://www.hetzner.com/AV/TOM.pdf`

(3) The software used on the servers complies with current security requirements. The Contractor regularly ensures that security updates are installed and documented on the servers.

(4) For configurations that include the optional video streaming feature, OpenSlides uses services provided by the subcontractor nanocosmos Informationstechnologien GmbH. The contractor's technical and organisational measures are being provided here: `https://www.nanocosmos.de/documents/GDPR-DSGVO-DPA-nanocosmos.pdf`.

4. Processing of Data

(1) The Contractor may only process the data processed on behalf of the Client within the scope of the mandate and exclusively on behalf of and in accordance with the Client's documented instructions. If the Contractor is required to carry out further processing by the law of the Union or the Member States to which it is subject, the Contractor shall notify the Client of the legal requirements prior to the processing.

(2) Where included in the scope of services, the Contractor shall directly ensure the deletion concept, the right to be forgotten, rectification, data portability and access to personal data in accordance with the Client's documented instructions.

5. Quality Assurance and other Obligations of the Contractor

(1) The Contractor ensures that all persons it appoints to process and perform this Agreement are bound by written confidentiality obligations. The Contractor may not disclose the information obtained from the Client's domain to third parties; it is obliged to maintain confidentiality regarding such information, even after termination of the contractual relationship.

(2) In addition to complying with the provisions of this Agreement, the Contractor also has legal obligations in accordance with Articles 28 to 33 GDPR.

(3) The Contractor shall, where possible, support the Client with appropriate technical and organisational measures in fulfilling the Client's obligations under Articles 12 to 22 GDPR.

6. Subcontracting Relationships

(1) The Client agrees in principle that the Contractor may subcontract to carefully selected third-party companies. The Contractor shall inform the Client in good

time before any intended change with regard to the engagement or replacement of other third-party companies. In this case, the Client may object to the engagement or replacement. If this makes it impossible for the Contractor to perform the subject-matter of this Agreement, the Contractor may extraordinarily terminate this Agreement and the contract for the provision of hosting services at the time of the intended engagement or replacement.

(2) When subcontracting, the Contractor shall comply with the requirements of Article 28(2)–(4) GDPR and shall draft the contractual agreement with the subcontractor in such a way that they comply with the data protection requirements between the Contractor and the Client stipulated in this Agreement.

(3) The only subcontractors commissioned are:

- kyberio GmbH:
  `https://www.kyberio.com/impressum/`
- nanocosmos Informationstechnologien GmbH:
  `http://www.nanocosmos.de/v6/imprint.html`
- Hetzner Online GmbH:
  `https://www.hetzner.com/de/rechtliches/impressum`

7. Control Rights of the Client

(1) The Client has the right, in consultation with the Contractor, to carry out inspections or to have inspections carried out by auditors to be appointed on a case-by-case basis. It has the right to satisfy itself of compliance with this Agreement by the Contractor in its business establishment by means of spot checks, which must usually be announced in good time.

(2) The Contractor shall ensure that the Client can satisfy itself of the Contractor's compliance with its obligations under Article 28 GDPR. The Contractor undertakes to provide the Client with the necessary information on request and, in particular, to provide evidence of the implementation of the technical and organisational measures.

(3) Evidence of such measures, which do not only relate to the specific contract, can be provided by way of compliance with approved codes of conduct as referred to in Article 40 GDPR or by way of reports produced by the data protection officer responsible for the Contractor.

(4) The Contractor may claim remuneration for enabling the Client to carry out inspections. Unless otherwise agreed with the Client, the hourly rate for support agreed in the main contract shall be used as the basis for resource-related billing.

8. Communication in the Event of Non-Compliance by the Contractor

(1) The Contractor shall assist the Client in ensuring compliance with obligations relating to the security of personal data, the notification of data breaches, data protection impact assessments and prior consultations pursuant to Articles 32 to 36 GDPR. These include

a) Ensuring an adequate level of protection by means of technical and organisational measures that take into account the circumstances and purposes of the processing as well as the predicted likelihood and severity of a possible infringement due to security vulnerabilities and that facilitate the immediate detection of relevant infringement events.

b) The obligation to immediately report personal data breaches to the Client

c) The obligation to assist the Client in the context of its duty to inform the data subject and, in this connection, to immediately provide the Client with all relevant information

d) Provision of support to the Client in conducting its data protection impact assessment

e) Provision of support to the Client in the context of prior consultations with the supervisory authority.

(2) The Contractor may claim remuneration for support services that are not included in the specification of services or that are not attributable to any misconduct on the part of the Contractor. Unless otherwise agreed with the Client, the hourly rate for support agreed in the main contract shall be used as the basis for resource-related billing.

9. Client's Authority to Issue Instructions

(1) As a general rule, the Client shall issue instructions to the Contractor in text form. The Client shall immediately confirm verbal instructions (at least in text form). The Contractor shall document the instructions and their implementation.

(2) The Contractor shall immediately inform the Client if it believes an instruction breaches data protection rules. The Contractor is entitled to suspend the execution of the relevant instruction until it is confirmed or amended by the Client.

10. Qualified Confidentiality Agreement for Anonymous or Secret Votes and Ballots

(1) Where OpenSlides is to be used for holding anonymous or secret votes and ballots, the Contractor is required to abstain from any measure that could compromise the secrecy of the ballot or vote. In particular, no records may be made of the content of individual votes and no corresponding data may be read out if this could lead to a link being established to the person voting. If any such data is obtained nevertheless (e.g. due to a program error), the Contractor is obliged to maintain absolute confidentiality and to destroy the data immediately.

(2) The Client's control rights and authority to issue instructions referred to in Nos 7 and 9 of this Agreement are limited, insofar as the obligation under Paragraph 1 suffices. In particular, the Client may not give any instructions aimed at sounding out the secrecy of the ballot or vote; nor may the Client exercise its control rights in such a way that the secrecy of the ballot or vote would be sounded out.

(3) The Contractor may not be released from its obligation under Paragraph 1 even after conclusion of the contract, not even by an express declaration by the Client or its legal representative or its bodies authorised to represent the Client. The same applies to any deviating unilateral or bilateral change of the Agreement in the first sentence. The same applies to the abolition of the restrictions set out in Paragraph 2.

11. Deletion and Return of Personal Data

(1) No copies or duplicates of data may be made without the knowledge of the Client. This does not apply to backups, where they are necessary to ensure proper data processing, or to data required to comply with legal retention obligations.

(2) After completion of the contractually agreed work, or earlier at the request of the Client – at the latest upon the termination of the service agreement – the Contractor shall hand over to the Client all documentation that it has obtained, all results generated from the processing and usage of the data, and all databases associated with the contractual relationship, or, after prior consent, shall destroy such materials in accordance with data protection regulations. The same applies to test and scrap material. The deletion protocol shall be presented on request.

(3) Documentation that serves the purpose of proving proper data processing as per the contract shall be kept by the Contractor beyond the end of the contract in accordance with the relevant retention periods. It may hand them over to the Client to its discharge at the end of the contract.

12. Contractor's Data Protection Officer

(1) The following person has been appointed as the Contractor's data protection officer: Dr. Johannes Schröder <datenschutz@intevation.de>.

(2) The Contractor shall be notified immediately if there is a change of data protection officer.

Osnabrück, 13th September 2024
(This contract was generated automatically and is valid without a signature.)

A. Annex 1 – Technical and Organisational Measures

A.1. Confidentiality (Point (b) of Article 32(1) GDPR)

A.1.1. Physical Access Control

Hosting takes place in the German data centres of kyberio GmbH and Hetzner GmbH. These data centres are certified according to IT-Grundschutz / ISO 27001. The hardware is accessed via an access control system that excludes unauthorised physical access.

A.1.2. Logical Access Control

OpenSlides servers are connected through dedicated switches. Connections between data centres (cf. A.3.1) are established over a dedicated VLAN. The setup ensures that all data traffic between OpenSlides servers runs over a trusted network.

OpenSlides has an access concept consisting of encrypted transmission and user authentication by user name and password (login process).

At the administration level, access is OpenSSH encrypted with key authentication.

OpenSlides systems run on dedicated servers with LUKS-encrypted data carriers. When switched off, therefore, all client data on the systems is encrypted. This means that when a data carrier is replaced or disposed of, the confidentiality of stored data is ensured from the beginning. Data carriers are additionally deleted or destroyed by the data centre operators.

A.1.3. Data Access Control

OpenSlides servers are connected through dedicated switches. Connections between data centres (cf. A.3.1) are established over a dedicated VLAN. The setup ensures that all data traffic between OpenSlides servers runs over a trusted network.

OpenSlides manages the processes of individual customer instances in separate virtualised networks. Instance data is stored on dedicated database servers. Instances can each only access their own separate databases using their specific database user accounts (multitenancy).

Regular security updates (according to the state of the art) prevent unauthorised access by exploiting security vulnerabilities.

OpenSlides systems run on dedicated servers with LUKS-encrypted data carriers. When switched off, therefore, all client data on the systems is encrypted. This means that when a data carrier is replaced or disposed of, the confidentiality of stored data is ensured from the beginning. Data carriers are additionally deleted or destroyed by the data centre operators.

A.1.4. Separation Control

OpenSlides manages the data of individual client instances in separate databases on its database servers which can only be accessed by the respective OpenSlides instances.

A.1.5. Pseudonymisation (Point (a) of Article 32(1) GDPR; Article 25(1) GDPR)

An OpenSlides instance is transferred to the Client with an individual user account with administrative rights. The Client makes all other entries, including the creation of additional user accounts and their authorisations.

It is up to the Client to decide whether the event can be held using pseudonyms or whether participants must be directly identified. OpenSlides does not enforce the use of real names.

No personal data, including IP addresses, is recorded.

A.2. Integrity (Point (b) of Article 32(1) GDPR)

A.2.1. Disclosure Control

No disclosure is intended within the commissioned processing.

The input/output of data is encrypted via HTTPS in the context of data access control.

A.2.2. Input Control

Access to OpenSlides, and therefore also to data processing, takes place via individual user accounts created by the Contractor. Detailed access permissions can be granted or removed from user accounts in OpenSlides.

Access to OpenSlides servers by system administrators is automatically logged.

A.3. Availability and Resilience (Point (b) of Article 32(1) GDPR)

A.3.1. Availability Control

Systemic measures OpenSlides systems are designed to be redundant. Two hot standby systems are provided for each database cluster. If the primary cluster fails, a standby system automatically takes on the role of the primary cluster. The third system ensures redundant data storage even if a server fails.

In addition, regular backups are made and all operations that run on the databases are saved. This enables point-in-time recovery.

Spatial measures The data centres are equipped with fire alarm systems, uninterruptible emergency power systems and mains backup systems (emergency diesel power).

Servers of the redundant OpenSlides systems are distributed over two fire protection areas within the data centres to absorb the effects of potential physical destruction by protecting data in separate areas.

In addition to performing backups on local servers, backups are also copied to backup storage of Hetzner GmbH. Data transmission to the backup storage and storage in the backup memory is encrypted.

Access is restricted exclusively to the administrators at Intevation GmbH.

A.3.2. Rapid Restorability (Point (c) of Article 32(1) GDPR)

Databases and individual data sets can be restored from the various levels of data backup as required. The necessary steps are documented in the operations manual.

A.4. Process for Regular Testing, Assessment and Evaluation (Point (d) of Article 32(1) GDPR; Article 25(1) GDPR)

A.4.1. Data Protection Management

Together with its externally appointed data protection officer, Intevation GmbH has established a data protection management system based on the PDCA cycle.

A.4.2. Incident Response Management

Disruptions in operation are identified by automatic monitoring by Intevation GmbH and reported directly to the system administration or the IT Operations team. In the case of incident reports received personally (phone, email, ticket system), there is a policy of forwarding these directly to the system administration or to the IT Operations team without delay.

On the basis of point 8 b) of this Agreement, incident response management is based on the TDODAR decision-making model used in aviation.

1. *Time*: A check to determine how quickly a decision has to be made and action taken. If you have more time, it may be possible to make better decisions, but if you wait too long, some actions may no longer be feasible or appropriate. The decision on how to proceed is taken within 15-30 minutes. A longer amount of time is only available if it can be ruled out that sensitive data will fall into the wrong hands.
2. *Diagnosis*: What exactly is the problem and how severe are the consequences?
3. *Options*: What are the options for action? Who can provide support?
4. *Decide*: What is the best option for action?
5. *Act or Assign*: The chosen option starts to be implemented. It may make sense to share tasks or assign them to someone with more experience in this area.
6. *Review*: When implementing the chosen option, it is important to constantly review whether that option continues to be the right one. It may make sense to restart the decision-making process with the information gained during implementation.

If the diagnosis reveals a risk or a breach of the protection of personal data, the Client will be appropriately informed and involved in the individual steps. A summary email is sent to the Client no later than after the decision has been taken (*Decide*).

As a general rule, if there is a risk of data requiring greater protection falling into the wrong hands, the systems must be shut down immediately or disabled.

A.4.3. Data Protection by Default (Article 25(2) GDPR)

At the start of commissioned processing, the Contractor creates a new OpenSlides instance with an individual user account for the Client.

The account has administrative rights within the booked OpenSlides instance. The Client makes all other entries, including the creation of additional user accounts and their authorisations.

It is up to the client to decide whether the event can be held using pseudonyms or whether participants must be directly identified. OpenSlides does not enforce the use of real names.

OpenSlides systems consistently refrain from logging IP addresses.

A.4.4. Control of Commissioned Processing

The basis of data processing is the Client's mandate to process data on behalf of the Client. It is stipulated that all instructions must be in writing or in an electronic form (text form) and that the Client is able to exert full control.

Intevation keeps documentation of the current state of the servers (hardware, installed software), which can be requested by the Client at any time; Intevation also regularly checks the hosting service provider for the existence of a valid ISO 27001 / IT-Grundschutz certificate.