Records of Processing Activities

according to Art. 30 of the GDPR

Table of Contents

Order data processor

InterMedia Solutions GmbH
(hereinafter referred to as IMS)
Ahornstr. 7, 82041 Oberhaching near Munich

Contact person: Robert Holzer
Phone: +49 89-244 151 51
Email: datenschutz@intermedia-solutions.de

Product description – IMS webcast platform

IMS develops and operates a web-based streaming and webcast platform whose basic function is the publication of live video streams and on-demand video recordings over the internet. The following systems are used for operation.

IMS streaming and hosting services:
A cloud server network enables the storage and high-performance delivery of streaming video and web/download content.

IMS webcast CMS:
The CMS (content management system) allows you to create your own website or websites for publishing and controlling videos and live streams. With additional functionalities, the website can be designed individually, access can be protected, and interactive modules can be added.

Publication is done via a link that opens the webcast project in a browser, or via existing websites in which it is integrated.

Users and rights

There is basically only one (main) access to the customer account. Additional (partial) accesses can be (optionally) created within the customer account.

Customer/owner (administrator)	Has full access to all functionalities and can (optionally) create password-protected (partial) accesses to subsequent areas and functionalities.
IMS (optional)	According to the customer's order IMS can be commissioned by the customer for setup and support.
Event manager (optional)	Participant management Create, edit, export, delete participants/data

Event manager (optional)	Survey management Create, display, edit, evaluate, export, delete surveys
Moderator (optional)	Message management View, sort, prioritise, export, delete incoming messages
Event manager (optional)	Web RTC Create, moderate, delete web meetings

Invitation management/registration

IMS supports the following invitation options:

- Participants can be invited via email. Other options include a link on a public or internal website, social networks, forums, or intranet applications.
- Data transfer via csv/xls files
  Participant data can be imported into the system.
- Self-registration
  Any number of data fields can be freely defined, optional mandatory fields can be defined as well as pure text fields or fields for free text input.
- Password options
  Passwords are automatically assigned by the system or predefined by the customer/owner.
- Login with customised username and password

Participant management/data usage

The querying and storage of participants' data in a central database is optionally possible.

The following webcast modules require access to the user database or enable the use and publication of participant data:

- Login/registration
  Access data is compared with the stored participant data to enable access to protected pages of the webcast project.

- Message box and message box viewers (sending and displaying messages)
  Messages sent by the participant can be (optionally) displayed with the participant data in the backend (admin area). In addition, it is possible to display participant data within the webcast interface (visible to other participants) along with the sent message.

- Surveys/tests:
  Survey or test results can (optionally) be assigned to the participant.

- Participation and participant tracking:
  Usage behaviour (time and duration of use) can be (optionally) assigned to the participant.

- IMS web RTC – (web meeting):

Participant data can be (optionally) used to register for the web meeting functionality and displayed within a web meeting (visible to other participants).

In the cases mentioned, safeguarding the rights of those affected lies solely with the customer/owner, since the system does not independently assign, store or publish any participant data.

Records

The IMS streaming and hosting services offer the possibility to record live streams, edit them and publish them as VOD (video on demand). The live stream as well as the recording can record persons as well as people in the background.

In this case, the protection of the rights of those affected lies exclusively with the customer/owner, since the system does not produce any live streams or recordings on its own.

Deletion concept

If a webcast project is deleted, all participant and project data associated with it will be irretrievably deleted. The deletion process is initiated manually by an authorised user.

Guarantee of data subject rights

According to Chapter III of the GDPR, IMS grants data subjects the right to information, correction, deletion or blocking, data portability and revocation. Insofar as deletion does not affect statutory, contractual or commercial or tax retention periods or other legal reasons, the data will not be deleted but blocked.
To exercise the aforementioned rights, data subjects can contact:

InterMedia Solutions GmbH
Ahornstr. 7, 82041 Oberhaching near Munich

Phone: +49 89-244 151 51
Email: datenschutz@intermedia-solutions.de

Applications and systems

The platform consists of the following systems:

- Web and download servers
- Streaming server cloud

Hosting, services and streaming systems

IMS uses the following service partners:

- Microsoft Azure, cloud services (streaming)
  Server location: Netherlands
  Further information: https://docs.microsoft.com/de-de/compliance/regulatory/gdpr

Data transmission (SSL/SSH) to all servers is encrypted. IMS is responsible for the processing, management and storage of the
data. The service partners mentioned are responsible for the operation of the hardware and for the provision of the data processing infrastructure, and shall be provided exclusively within the EU and in accordance with the GDPR (General Data Protection Regulation).

Cookies

For using the platform, IMS uses technically required cookies, so-called "session cookies". These are deleted as soon as the user closes their browser. A "session cookie" does not store any information that serves to identify a user, but is only a session identifier (session ID). The user does not have to agree to the use of these "session cookies
"."Session cookies" are used for the following:

IMS customer login – affects only administrators and users of the platform
- Login page

Event and video platform – affects participants when using the following modules
- Login/registration
- Surveys
- Chats
- i-frame/token/server authentication (only with special applications)
- Real-time video conferences

Certifications

Microsoft Azure, cloud services have the following certifications, among others, which guarantee data protection within Europe:
- ISO 27001
- ISO 27018
- FedRAM
- FERPA
- HIPAA/HITECH
- SOC 1 and SOC 2 type 2 reports

Ionos by 1&1 server systems have the following certifications, among others, which guarantee data protection within Europe:
- ISO 9001
- ISO 27001
- PCI DSS

Security measures

The technical and organisational measures used are described below.

Confidentiality – access

Regulated physical access to data processing centres
Access control to server rooms is guaranteed by the spatial structure of the respective data centres and their operators.

Access – regulation of digital access to IT

Systems/applications

- Encrypted data transmission (SSL/SSH)
- Password-protected system access
- Role-based access control
- Multi-factor authentication (MFA)
- Logging of system usage

Access – access to information

- Strict regulation and compliance with an access scheme in the application
- Prevention of unauthorised reading or manipulation of application data
- The granting of access on a "need-to-know" basis

Data separation

Personal data may only be used for the purpose for which it was originally collected. That data collected for different purposes can be separately processed is ensured by the following:

- Software-based exclusion (separation of mandates; multi-tenancy architecture, role-based
- access control)
- The principle of least privilege
- The database principle, separation via access regulation
- Separation of test and production data
- Separation of development and production programs

Integrity

Disclosure – prohibition of unauthorised reading of data when being transmitted

- Tap-proof transmission of data (SSL/SSH)
- Firewalls
- Anti-virus protection

Input – traceability of the data source

Whether and by whom data has been entered, changed or removed in data processing systems can
subsequently be checked and determined by the following:

- User identification
- Logging of entered data (processing log).

Availability

Availability – security versus loss or accidental destruction of data and recoverability

- Hosting in N+1 configurations
- Use of RAID systems
- The regular automatic creation of backups
- Additional manual backup options
- Multiple, separate storage of the backup data

Loadability

The IMS system and the servers were last checked in 11/2021 with the following penetration and resilience tests.

- Rapid7 Insightvm
- Arachni scanner

Procedures for periodic review, assessment, and evaluation

- Default privacy settings
- Regular review and revision of the measures (on an annual basis at least)

Data processing order

There is guarantee that commissioned external service providers process transferred personal data with the same care and according to the intended purpose.

Peer-to-peer enterprise CDN
The peer-to-peer ECDN is based on native browser features, i.e., connectivity between peers, and the security aspects associated with it are part of browser implementation (WebRTC peer-to-peer connections).

It is a native platform component of IMS, meaning no additional
data processors are required. The connections are limited to the local network and therefore do not introduce network bridges. They are subject to firewall rules at the network and client ends.

Peer-to-peer enterprise CDN

The peer-to-peer ECDN is based on native browser features, i.e., connectivity between peers, and the security aspects associated with it are part of browser implementation (WebRTC peer-to-peer connections).
It is a native platform component of IMS, meaning no additional
data processors are required. The connections are limited to the local network and therefore do not introduce network bridges. They are subject to firewall rules at the network and client ends.

Annex: External service providers

Microsoft Ireland Operations Ltd. South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland	Operation of servers and cloud server networks, content delivery network for storing and delivering audio/video streams
1&1 IONOS SE Elgendorfer Str. 57, 56410 Montabaur	Operation of servers and cloud server networks, content delivery network for storing and delivering websites and web content and databases
TenshiTec Neustift 7, 85622 Weissenfeld	Server administration and development

Annex: Collected, stored and processed data

IMS collects, stores and processes data as follows:

Data	Scenario	Legal basis	Access	Storage and deletion
Audio/video streams	Incoming live A/V signals can be recorded on the server end	Order fulfilment	Owner/customer	Storage within the platform until the webcast project is deleted (manually or automatically after the relevant deadlines have expired)
Participant data	During registration, any participant data can be queried and stored	Order fulfilment	Owner/customer, participant (optionally, participant data can be displayed within the webcast – for details, see pt. Participant management	
Incoming messages, information	The customer can use their own functionalities as well as those provided by the system for data input by the participant.	Order fulfilment		