

Service Description

SWITCHcast

Version 3.1

Effective 1st of January 2023

Note: This template exists in several languages. In case of contradictions, the German version takes precedence over the other language versions.

1	Definitions	4
2	Overview and Purpose	5
3	Functionality and Components of the Service	5
3.1	Subject Matter	5
3.2	Application Software	5
3.3	Set-Up	6
3.4	Operation of the Application Software	6
4	Contact Information and SWITCHcast Helpdesk	6
5	Service Level / Support Services	7
6	Usage Data Collection	8
7	Instructions to Organisation / Contracting Party	8

8	Legal Terms of Use	9
8.1	Applicable Provisions	9
8.2	Copyright and other Intellectual Property Rights	9
8.3	Data Protection and Data Security	10
8.3.1	Data Processing by SWITCH	10
8.3.2	Purposes of Data Processing	10
8.3.3	Categories of Data Subjects	11
8.3.4	Categories of Personal Data	11
8.3.5	Data Location and Origin	11
8.3.6	Recipients or Categories of Recipients of Personal Data	11
8.3.7	Subcontractors	11
8.3.8	Duration of Data Processing	12
8.3.9	Rights of Data Subjects	12
8.3.10	Access to Employee Data	12
8.3.11	Data Security	13
8.4	Acceptable Use of the Service	15
8.5	Unacceptable Use of the Service	15
8.6	Warranty	16
8.7	Liability	16

1 Definitions

<p>End Users</p>	<p>In this document, End Users are members of an Organisation or Contracting Party (including but not limited to employees, researchers, lecturers, staff members and students) who use a SWITCH service directly or indirectly through an Organisation or Contracting Party.</p>
<p>Extended SWITCH Community</p>	<p>Organisations that are closely related to the SWITCH Community, including but not limited to university policy organisations, academies, funding institutions, libraries and hospitals, as well as private research facilities and schools in the tertiary sector that are not part of the SWITCH Community.</p>
<p>Organisation</p>	<p>An organisation within the SWITCH Community or the Extended SWITCH Community.</p>
<p>Kaltura</p>	<p>Kaltura (www.kaltura.com); Kaltura Inc., 860 Broadway, 3rd Floor, New York, NY 10003</p>
<p>SWITCH Community</p>	<p>The Organisations in the field of education and research that are affiliated with SWITCH (in accordance with the Appendix to the Regulations on the Purchase of SWITCH Services, as amended from time to time).</p>
<p>Scale of Charges</p>	<p>Periodically adjusted schedule that applies to Organisations in the SWITCH Community for the purpose of purchasing SWITCH services.</p>
<p>Contracting Party</p>	<p>The person who has concluded a contract with SWITCH for the service but is not an Organisation as defined above.</p>

2 Overview and Purpose

SWITCHcast is a powerful video management system that can receive video content from various sources, process it further and publish it in other systems. At the same time, SWITCHcast enables the central management of large collections of content in combination with decentralised elements by delegating tasks and/or competencies. The video content can be seamlessly integrated into third-party systems via interfaces.

3 Functionality and Components of the Service

3.1 Subject Matter

SWITCHcast relates to the use of the functionalities of the application software ordered by the Organisation / Contracting Party and provided and operated by SWITCH as well as the provision of storage capacity on the SWITCH infrastructure.

3.2 Application Software

The application software provided and operated by SWITCH as part of SWITCHcast is based on the order of the Organisation / Contracting Parties.

The following application software may be ordered by the Organisations / Contracting Party:

- Kaltura Media Space (KMS) is the web frontend for creating, managing and publishing video content (Campus Portal).
- Interactive, the solution for creating interactive videos. (Quizzes and hotspots are included in the standard package)
- LMS integration, e.g. Moodle, Blackboard, Canvas, Sakai, and LTI interface
- Webcasting (6 webcasts are included in the webcast licence; additional webcasts may also be ordered)
- Lecture Capture (LC), the classroom recording solution including live streaming, is an app regardless of the number of installations required.
- MS Teams Integration, for the use of video content in teams.

The technical specifications and user documentation for the individual application software are available on the SWITCH website or portal. SWITCH may make minor changes to the technical specifications, terms of use and user documentation at any time. Notice of significant changes will be given within a reasonable period.

3.3 Set-Up

SWITCH sets up the application software for use by the Organisation / Contracting Party. This includes the following services:

- Set-up of the tenant
- Providing access to the application software
- Setting all necessary permissions
- Initial introduction of the contact person in accordance with Section 7 below

3.4 Operation of the Application Software

SWITCH makes the application software available to the Organisation or Contracting Party in the form of a Software-as-a-Service solution.

The servers on which the application software runs can be accessed directly from the networks of the Organisations connected to the SWITCHlan fibre-optic network. In other cases, the application software is accessed via the public internet.

The application software is provided by SWITCH at the service interconnection point. Unless otherwise specified in the technical specifications, the service interconnection point is the connection of SWITCH's servers to the SWITCHlan fibre-optic network or the public Internet.

In order to use SWITCHcast, the End User generally uses their SWITCHaai or SWITCH edu-ID user account. Other login procedures can be supported upon request. Such an implementation would be paid for individually.

The application software shall be available to the Organisation / Contracting Party in the then-current version. SWITCH shall update the Software to new versions at its own discretion and make these updates available to the Organisation / Contracting Party as part of this Agreement. The Organisation / Contracting Party shall be given reasonable advance notice of updates that significantly alter the existing functions of the software.

4 Contact Information and SWITCHcast Helpdesk

Fault reports, support requests or specific enquiries regarding SWITCHcast may be submitted at any time to the email address cast-support@switch.ch.

Any legal questions concerning the service may be addressed to legalteam@switch.ch.

Requests to assert the rights of data subjects under the Data Protection Act must be addressed to privacy@switch.ch.

5 Service Level / Support Services

Operating time	The service is generally available for use 24 hours a day, 7 days a week except in case of disruptions that adversely affect the service.
Maintenance windows	SWITCH generally performs maintenance work outside normal office hours. If such work will cause interruptions or restrictions of service quality, SWITCH will inform the affected customers via email at least 14 days in advance. Maintenance work shall, as far as possible, take account of important customer events (exam days/periods according to the academic calendar).
Availability	SWITCH strives for 99.5% availability of the service, less the time required for maintenance and repairs and taking support times into account.
Support times	During its normal business hours, SWITCH undertakes to initiate or execute, as applicable, measures to remedy service disruptions and malfunctions.
Response times	SWITCH undertakes to respond to customer complaints no later than the next working day, within its support times.
Repair times	SWITCH undertakes to correct errors within a reasonable period of time.
Restoration	SWITCH undertakes to restore the service within a reasonable time in the event of an outage.

Normal office hours are set out in the [Service Regulations](#) or in the [General Terms and Conditions for the Purchase of SWITCH Services](#), as amended from time to time. Depending on the urgency of the matter, SWITCH may also, at its own discretion, take measures to maintain good service quality outside of these periods.

1st Level Support is covered by the Organisation / Contracting Party. First Level Support may escalate to 2nd Level Support at SWITCH if a request cannot be resolved independently. SWITCH is responsible for 2nd and 3rd Level Support. The Organisation / Contracting Party can conclude a different agreement with SWITCH regarding the provision of 1st Level Support.

6 Usage Data Collection

SWITCH collects data on the use of the service by the End Users, the Organisation or the Contracting Party. Where possible, this is done on a per-Organisation / Contracting Party basis. SWITCH provides the Organisations / Contracting Parties with anonymous statistics on their use of SWITCHcast.

7 Instructions to Organisation / Contracting Party

In order to make full use of the service, the Organisations / Contracting Parties undertake the following obligations:

- The Organisations and Contracting Parties shall be responsible for equipping the premises with the necessary recording hardware. On its help page (<https://help.switch.ch/cast/recording/>), SWITCH recommends a variety of recording hardware as well as software for recording courses that enable optimum use of the service.
- The Organisations / Contracting Parties shall be responsible for the operation, maintenance, management and maintenance of the recording hardware.
- The Organisations / Contracting Parties are responsible for planning, implementing and processing their records.
- The Organisation / Contracting Party is responsible for ensuring the correct operation and handling of the recording hardware and application software by the End Users.
- The Organisations / Contracting Parties shall be responsible for provisioning and connecting third-party systems or their interface to SWITCHcast, as applicable.
- The Organisation / Contracting Party shall designate a contact person and their alternate and shall notify SWITCH thereof. SWITCH must also be notified immediately of any change of contact person or their alternate.

8 Legal Terms of Use

8.1 Applicable Provisions

The following provisions, as amended from time to time, shall apply to the use of the service by Organisations, Contracting Parties and End Users:

- For Organisations in the SWITCH Community and for End Users who are members of an Organisation in the SWITCH Community:
 - the [Regulations on the Purchase of SWITCH Services \(hereinafter: Regulations\)](#);
 - the Scale of Charges in effect from time to time

In case of discrepancies, this Service Description shall take precedence over the Scale of Charges, which in turn shall take precedence over the Regulations.

- For Organisations in the Extended SWITCH Community, for End Users who are members of an Organisation in the Extended SWITCH Community, for Contracting Parties and for End Users who are members of a Contracting Party:
 - the [General Terms and Conditions for the Purchase of SWITCH Services](#) (hereinafter: General Terms and Conditions);
 - the Service Agreement

In case of discrepancies, this Service Description shall take precedence over the Service Agreement, which in turn shall take precedence over the General Terms and Conditions.

SWITCH may modify this Service Description at any time. Any modification of the Service Description shall be duly reported to the Organisations, the Contracting Parties and the End Users and, barring objection, shall take effect within 30 days after the date of notice of the modification.

Any objection shall result in termination of the contract.

8.2 Copyright and other Intellectual Property Rights

The Organisations / Contracting Parties retain all rights to the content vis-à-vis SWITCH. The Organisations / Contracting Parties are solely responsible for their use of the content and for compliance with all laws that apply to such content, including but not limited to those that require the Organisations / Contracting Parties to obtain a third party's consent to use the content and provide reasonable notice of third-party rights.

The Organisations / Contracting Parties represent and warrant that they have the right to process this content and that such use does not infringe any third-party rights. SWITCH shall not under any circumstances be liable in any way for the content of the Organisations / Contracting Parties.

8.3 Data Protection and Data Security

8.3.1 Data Processing by SWITCH

In terms of processing personal data, SWITCH shall abide by the Regulations or the General Terms and Conditions, as applicable and as amended from time to time. For the purposes of this data processing, the Organisations / Contracting Parties are deemed to be the **Controllers** and SWITCH is deemed to be the **Processor**. The End Users shall be deemed to be **data subjects**. This Service Description sets out the information

- that must be disclosed to the data subjects (duty to provide information),
- that controllers must include in their record of processing activities (documentation obligation) and
- that data controllers need in order to guarantee the rights of data subjects.

In addition, the Service Description, together with the information contained in the Service Regulations or the General Terms and Conditions, as applicable, contains all information that must be included in a data processing agreement pursuant to the applicable data protection laws.

8.3.2 Purposes of Data Processing

SWITCH processes personal data mainly in order to provide the SWITCHcast service and to comply with its statutory obligations.

In addition, SWITCH also processes personal data of Organisations, Contracting Parties and End Users, in line with applicable law and where appropriate, for the following purposes, in which SWITCH (and sometimes third parties) have a legitimate interest corresponding to the above purposes:

- Offering and further developing our offers, services and websites, apps and other platforms on which SWITCH is represented;
- Communication with third parties and processing of their inquiries (e.g. applications, media inquiries);
- Examining and optimising processes for analysing needs for the purpose of directly addressing customers as well as collecting personal data from publicly available sources for the purpose of acquiring customers;
- Advertising and marketing (including organising events), provided that you have not objected to the use of your data for this purpose (if you are part of our existing customer base and receive advertising from us, you may object at any time and we will place you on a blacklist against further advertising mailings);
- Market and opinion research, media surveillance;
- Assertion of legal claims and defending against claims in connection with legal disputes and regulatory proceedings;
- Prevention and investigation of criminal offences and other misconduct (e.g., conducting internal investigations, data analysis to combat fraud);
- Ensuring our operation, including our IT, our websites, apps and other platforms;
- Other measures for IT, building and system security and the protection of our employees and other persons and assets owned or entrusted to us (such as access controls, visitors logs, network and email scanners, telephone recordings);

- Processing of personal data for the detection, analysis, elimination or prevention of ICT security incidents.

In addition, SWITCH generates anonymous statistics for the Organisations and Contracting Parties. The foregoing shall be without prejudice to cases of abuse.

8.3.3 Categories of Data Subjects

Data subjects are End Users as defined in Section 1 above.

8.3.4 Categories of Personal Data

The following categories of personal data may be processed in connection with the service:

- Surname, first name, email address,
- Employer or associated Organisation / Contracting Party,
- Language, identifiers,
- Training and development,
- Login data (login name), server logs, IP addresses,
- Any content data that End Users share when using the service.

8.3.5 Data Location and Origin

Subject to the statements in sections 8.3.6 and 8.3.7, data is held, stored and processed exclusively on physical hardware of SWITCH in Swiss data centres (Zurich and Lausanne).

The personal data processed by SWITCH originate either directly from the data subject who registers as an End User for the use of a SWITCH service and enters personal data in the process, or from the Organisation or Contracting Party of which the data subject is a member. If the login to use a SWITCH service is made, e.g., by means of a SWITCH edu-ID, the origin of the data is based on this service.

8.3.6 Recipients or Categories of Recipients of Personal Data

SWITCH may disclose personal data to the following categories of recipients:

- Subcontractors (contract data processing),
- Authorities,
- Suppliers and other business partners,

8.3.7 Subcontractors

The following subcontractors are currently engaged in connection with the provision of the service:

Company name	Purpose of data processing:	Location of data processing	If non-secure third country: Warranty
Kaltura Europe Limited	Maintenance and Support	EU, UK, Israel, Singapore and Ukraine	Contractual safeguarding

The subcontractors listed above shall be deemed approved upon use of the service by the Organisation or Contracting Party. SWITCH may engage further subcontractors. Before SWITCH engages a new subcontractor, SWITCH shall

inform the Organisation / Contracting Party. The Organisation or Contracting Party has the right to object in writing to the engagement of a subcontractor. If the Organisation / Contracting Party does not agree with a subcontractor, it shall be entitled to terminate the contract without notice.

SWITCH concludes contracts with all subcontractors that guarantee a level of data protection equivalent to the present Service Description and the Service Regulations or the GTC.

8.3.8 Duration of Data Processing

SWITCH will process personal data in connection with the SWITCHcast service for as long as this is necessary for the purposes of the processing. In addition, statutory retention and documentation obligations apply.

Unless the Organisation / Contracting Party agrees otherwise in a binding written agreement with SWITCH, personal data will be stored as follows:

- Service content data: Content data will be stored for as long as the Organisation / Contracting Party uses the service. If use of the service is discontinued, the content data will be deleted within 180 days or after the actual migration, but at the latest after 360 days.
- Log data: 1 year;
- Master data of End Users (personal data required in order to use their accounts): 30 days after cancellation of the User's account.

As an exception and on a case-by-case basis, certain data may also be retained for as long as legal claims can be asserted against SWITCH. Such extended storage will only take place if SWITCH anticipates that the relevant data could be required for evidentiary or documentation purposes.

8.3.9 Rights of Data Subjects

Data subjects may have the following rights vis-à-vis the Organisation or Contracting Party of which they are members as Controllers under data protection law, depending on the applicable data protection law:

- Right of access,
- Right of rectification,
- Right to erasure,
- Right to restrict processing,
- Right to object to the processing,
- Right to data portability.

In order to exercise these rights, data subjects must contact the responsible Organisation or the Contracting Party, as the case may be. If SWITCH receives such enquiries, it will forward them to the Organisation / Contracting Party.

8.3.10 Access to Employee Data

When data are transferred to SWITCH for processing, occasions may arise where, for operational reasons, an Organisation / Contracting Party requires access to data that was stored on its behalf by an employee who cannot be reached.

In any case, the Organisation / Contracting Party must provide detailed and verifiable evidence that it is entitled to access the relevant data. If such evidence is not clear and unambiguous, or if any unacceptable liability risk remains for SWITCH for any other reason, SWITCH may refuse such access.

8.3.11 Data Security

SWITCH shall use appropriate technical and organisational measures to protect the personal data against accidental or unlawful erasure, loss, destruction or alteration or unauthorised disclosure or access. To protect the personal data, SWITCH shall take measures including but not limited to the following:

SWITCH may amend these measures at any time without prior notice, as long as a comparable or higher security level is maintained. This may mean replacing individual measures with new ones that serve the same purpose without reducing the security level.

SWITCH shall regularly review and optimise the effectiveness of the measures utilised. The measures shall be examined by way of internal IT security reviews.

8.3.11.1 Control of Users and User Access

Data processing systems utilised to provide the services are protected against unauthorised use:

- Access to sensitive systems, including systems for storing and processing personal data, is granted via several authorisation levels. Appropriate processes ensure that the authorised persons have the appropriate authorisation to add, delete or change users.
- All users must access the systems with a unique ID (user ID).
- SWITCH has established procedures to ensure that requested changes to authorisations are only implemented in accordance with SWITCH's internal policies. If a user leaves the company, their access rights are revoked and access is blocked.
- SWITCH has established a password policy that prohibits the disclosure of passwords, determines the procedure to follow if a password is disclosed and for changing default passwords. For authentication, personalised user IDs are assigned. All passwords must meet certain minimum requirements and are stored in encrypted form. Every computer has a password-protected screensaver.
- The company network is protected from the public network by firewalls.
- Security patch management ensures that security updates are applied regularly.

8.3.11.2 Physical Access Control

Physical access to facilities, buildings and premises containing data processing systems that process or use personal data is denied to unauthorised persons:

- In general, buildings are secured by access control systems (e.g. access by chip card).
- As a minimum requirement, the external entrances to a building must be equipped with a locking system, including modern, active key management.
- Access rights are granted to authorised persons on an individual basis in accordance with SWITCH's internal guidelines on system and data access control. This also applies to visitor access.

8.3.11.3 Data Carrier and Storage Control

Persons authorised to use data processing systems shall only be granted access to the personal data to which they have access rights. Personal data may not be read, copied, altered or removed without authorisation during processing, use or storage:

- As part of the SWITCH ISMS concept, personal data require at least the same protection as “confidential” information as defined in the Directive “Processing and Classification of Business Data”.
- Access to personal, confidential or sensitive information is only granted where necessary (“need-to-know” principle). In other words, employees or service companies are only granted access to the information they need to perform their work. SWITCH uses an authorisation concept that documents how authorisations are assigned and which authorisations are assigned to whom. All personal, confidential and other sensitive data are protected in accordance with SWITCH’s security guidelines and standards.
- All servers are operated in data centres. The security measures to protect the applications for processing personal, confidential and other sensitive data are reviewed on a regular basis.
- The directive “Erasure and Disposal of Electronic Data Carriers” governs the manner in which data and data carriers are to be erased or destroyed when they are no longer needed.

8.3.11.4 Transport Control

Transport control ensures that personal data cannot be read, copied, altered or removed without authorisation during transmission or storage, except as necessary for the provision of the services under the service agreement.

For the transfer of data between SWITCH and the Organisations, Contracting Parties and End Users, the personal data to be transferred are secured by state-of-the-art encryption techniques. In any event, the Organisation, Contracting Party or End Customer assumes responsibility for the data transfer as soon as it takes place outside the systems controlled by SWITCH.

8.3.11.5 Entry and Disclosure Control

It shall be possible to subsequently investigate and establish whether and by whom personal data have been collected, modified or removed from SWITCH’s data processing systems:

- SWITCH shall only allow authorised persons to access personal data as part of their work assignment.
- Within its products and services, SWITCH has implemented a logging system for recording, amending and deleting or blocking personal data by SWITCH or its subcontractors/business partners to the greatest extent possible.
- The Organisation / Contracting Party is responsible for the proper handling and amendment of the processed data.

8.3.11.6 Availability and Restoration

Personal data shall be protected against accidental or unauthorised destruction or loss:

- SWITCH has backup processes and other measures in place to restore the availability of data as required in accordance with the SLA.
- SWITCH uses uninterrupted power supplies (UPS, batteries, generators, etc.) to ensure the power supply for the data centres.

8.3.11.7 Reliability

Malfunctions are detected on data processing systems and evaluated centrally. Based on the evaluation, alerts are given in various forms:

- SWITCH operates a central monitoring system for all services.
- SWITCHcast is integrated into the monitoring and individual threshold values have been defined. If thresholds are exceeded, the relevant operational teams are informed.

8.3.11.8 Data Integrity

Personal data shall remain intact, complete and up-to-date during processing activities.

SWITCH has implemented a multi-layered security strategy to protect against unauthorised changes.

Specifically, SWITCH uses the following means to implement the above sections on controls and measures. In particular, these are:

- Firewalls
- Anti-virus software
- Creating backups and restoring data

8.4 Acceptable Use of the Service

Any use of the service is acceptable only insofar as it does not result in an infringement of these terms of use, the rights of third parties or any applicable laws.

8.5 Unacceptable Use of the Service

Any unauthorised use of the service is subject to the provisions of the Regulations or the General Terms and Conditions, as applicable and as amended from time to time.

The Organisations / Contracting Parties of which the infringing End Users of the service are members may be held responsible or fully liable, as the case may be, together with the End Users, for all losses incurred by SWITCH or any third party as a result of the unauthorised use of the service by its End Users.

Upon first request by SWITCH, the Organisation or Contracting Party of which the infringing person is a member shall defend SWITCH, and its own expense, against any third-party claims made against SWITCH in connection with the improper use of the service. The Organisation or Contracting Party of which the infringing person is a member shall jointly and severally assume the costs, licence fees and/or compensation obligations imposed on SWITCH by court order or settlement,

provided that SWITCH has informed the affected Organisation or Contracting Party in writing of the claim brought and has authorised it, in accordance with the applicable procedural law, to conduct and settle the legal dispute, including by means of an in-court or out-of-court settlement.

SWITCH reserves the right, in the event of a reasonable suspicion that the service has been used in a manner contrary to the law or the contract, to immediately and without prior notification to the affected End Users or Organisations / Contracting Party, delete the affected [virtual rooms; accounts; access; etc.] and/or temporarily or permanently block the registered End Users concerned, without the data subjects or Organisations / Contracting Parties being entitled to any claims for compensation on account thereof.

Furthermore, in order to ensure proper operation, and even barring suspicion of improper use, SWITCH may at any time require the registered End Users to reset their PIN, moderator PIN, and/or the URL of their virtual room; lock up the room; etc.].

End Users and their Organisations / Contracting Parties are obligated to support SWITCH in investigating incidents of unauthorised use, the elements constituting the crime, and other loss events.

SWITCH further reserves the right, in all cases where SWITCH is required by law or otherwise deems it appropriate to do so, to collaborate with the responsible government authorities and to provide them with all information necessary to prosecute the legal offences in question.

8.6 Warranty

SWITCH's warranty is subject to the provisions of the Regulations or the General Terms and Conditions, as applicable and as amended from time to time, in connection with the service level warranted in section 5.

8.7 Liability

SWITCH's liability to the Organisations in the SWITCH Community shall be governed by the provisions of the Regulations, as amended from time to time.

SWITCH shall not be liable in any way for the lawful use of the service.

SWITCH's liability to the Organisations in the Extended SWITCH Community and to the Contracting Parties shall be governed by the provisions of the General Terms and Conditions, as amended from time to time. SWITCH shall not be liable in any way for the lawful use of the service.

SWITCH's liability to End Users and third parties who use its service other than under contract with SWITCH but with the consent of the Organisation or the Contracting Parties is hereby waived except where prohibited by law.

The Organisations, Contracting Parties and End Users shall be jointly and severally liable to SWITCH to the extent permitted by law for losses incurred by SWITCH as a result of the unauthorised use of the Service, as well as for other indirect losses.