SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

Service Description

SWITCHdrive

Version 2.0

Effective 01.07.2023

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

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

1 Definitions

End Users	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.
Extended SWITCH Community	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.
Organisation	An organisation within the SWITCH Community or the Extended SWITCH Community.
External Product	SWITCHdrive is based on the ownCloud Enterprise Edition software of ownCloud.org.
SWITCH Community	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).

Scale of Charges	Periodically adjusted schedule that applies to Organisations in the SWITCH Community for the purpose of purchasing SWITCH services.
Contracting Party	The person who has concluded a contract with SWITCH for the service but is not an Organisation as defined above.
Quota	The maximum storage capacity available to an End User.

2 Overview and Purpose

SWITCHdrive enables End Users to

- store files in the Community Cloud
- align or synchronise files across multiple devices
- exchange files with other End Users and edit them at the same time.

With its servers located exclusively in Switzerland, SWITCHdrive meets the customer's requirements in terms of data security and data protection.

SWITCHdrive is described on the website at https://www.switch.ch/drive/. The service can be found at https://drive.switch.ch.

3 Functionality and Components of the Service

3.1 Setup and Access

SWITCHdrive is made accessible to the End Users of an Organisation / Contracting Party who have subscribed to the service. Registered End Users use a SWITCH edu-ID as authentication and can create a SWITCHdrive account and thereby access storage space on the technical infrastructure. They have full access to all of the functions available on SWITCHdrive. For example, they can upload a file into a folder and, by sending a link to that folder, they can invite other End Users to download or modify the contents of the folder. The first names, surnames and abbreviations of Organisations / Contracting Parties of potential recipients of invitations are suggested to the registered End User.

Unregistered End Users can also access the service through an invitation or a link received. Certain functions are only available to unregistered End Users on a limited basis, depending

upon how the registered End User has configured certain settings before sending the invitation or link.

Before uploading files, registered End Users must be aware that a recipient of an invitation or link received is also able to forward such invitation or link to third parties.

3.2 Administration of End Users

End Users register for the service themselves. However, the Organisation / Contracting Party of which they are a member has to have subscribed to the service. If End Users leave the Organisation / Contracting Party, they lose the right to continue to use SWITCHdrive as active End Users of the Organisation / Contracting Party. SWITCH periodically deletes the accounts of End Users who are no longer authorised as active End Users of an Organisation / Contracting Party or who have not used the service for an extended period of time. SWITCH will contact the End Users of the service before erasing any data and provide them the opportunity to secure the stored data on another medium prior to erasure.

3.3 Access to the Servers

The servers on which all End User data are stored are located within the SWITCH infrastructure in Switzerland. From the networks of the Organisations / Contracting Parties that are connected to the SWITCHlan, the servers can be accessed directly through SWITCHlan, which is also located in Switzerland. In all other cases, the service is accessed over the public internet.

3.4 WG Meeting

SWITCH organises regular working group meetings, to which representatives of the Organisations / Contracting Parties are invited to help determine the roadmap for the service.

4 Contact Information and SWITCHdrive Helpdesk

Support requests or specific enquiries regarding the service may be made at any time via the e-mail address drive-support@switch.ch.

On the service website, End Users can find FAQ and online documentation. The support website for the service (https://help.switch.ch/drive) contains detailed instructions. The status of the service is always visible at https://status.switch.ch/.

Any legal questions about the service may be sent to legalteam@switch.ch.

Requests to assert the rights of data subjects under the Data Protection Act must be sent 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. Disruptions which lead to an impairment of the service remain reserved.
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 https://help.switch.ch/drive at least 10 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 aims to achieve an availability of the service of 99.5%, less the time required for maintenance and repairs and taking support times into account.
Support times	SWITCH undertakes to initiate or carry out measures to remedy service disruptions and malfunctions within SWITCH's normal office hours.
Response times	SWITCH undertakes to respond to customer complaints within 2 working days, during its support times.

The normal office hours are set out in the Service Regulations (DFR) 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.

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 anonymised statistics regarding the use of SWITCHdrive.

7 Instructions for Admins & End Users

7.1 End Users

The maximum Quota available to an End User is displayed in the user interface. The End User’s data are stored redundantly on the infrastructure to avoid the risk of data loss due to defective hardware. Nevertheless, data loss cannot be entirely ruled out. In particular, data are not additionally secured by SWITCH alongside redundant storage (no backup). The End User must ensure that the data stored on the infrastructure are backed up.

7.2 Administrators

Administrators at the Organisations / Contracting Parties can manage the Quota of End Users, create project folders and add or remove credits (i.e. vouchers) for external employees.

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
  - ownCloud's GNU General Public License
  - For Android users: End-User License Agreement for Android from ownCloud
  - For iOS users: End-User License Agreement for the iOS App of ownCloud

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
  - ownCloud's GNU General Public License
  - For Android users: End-User License Agreement for Android from ownCloud
  - For iOS users: End-User License Agreement for the iOS App of ownCloud

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

All End Users and the Organisation / Contracting Party of which they are members must defend at their own cost any third party claims against SWITCH alleging infringement of copyrights or other intellectual property rights and/or any other applicable laws in connection with files processed in relation to the service by the End Users / Organisations / Contracting Parties, if so requested by SWITCH. End Users and the Organisation / Contracting Party of which they are members shall be jointly and severally liable for all costs, licence fees and/or compensation payments imposed on SWITCH by court order or under the terms of an out-of-court settlement, provided that they were informed by SWITCH in writing concerning the claim in question and were authorised by SWITCH to conduct and resolve such litigation in accordance with applicable procedural law, including by means of an in-court or out-of-court settlement.

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 SWITCHdrive 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 we (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;
- 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;

- Asserting legal claims and defending against claims in connection with legal disputes and regulatory proceedings;
- Preventing and investigating criminal offences and other misconduct (e.g., conducting internal investigations and performing data analyses 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 by 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 and non-registered End Users as defined in Section 3.1 above.

8.3.4 Categories of Personal Data

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

- SWITCHdrive account information (surname, first name, email address)
- Files stored in SWITCHdrive (content data)
- Employer or associated Organisation / Contracting Party,
- Language
- Education and further training
- Login data (login name)
- Server logs, IP addresses

8.3.5 Data Location and Origin

Subject to the statements in sections 8.3.6 and 8.3.7, data are 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,
- Third countries in the context of mutual assistance proceedings.

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
ownCloud	Support	Germany	

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 or 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 SWITCHdrive 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:

- Content data / account information / login data: These are stored for as long as the Organisation / Contracting Party uses the service, until the End Users' accounts are deleted after leaving the Organisation / Contracting Party (see Section 3.2) or until content data are deleted by the End Users. After the service has been ceased by the Organisation / Contracting Party, an account has been deleted or content data has been deleted by End Users, content data, account information and login data are retained for one year and then permanently deleted.
- Log data: 60 days
- Back-up: 90 days

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-a-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.

With regard to the transmission of data between SWITCH and the Organisations, Contracting Parties and End Users, the personal data to be transmitted is secured by modern 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.
- SWITCHdrive is integrated into the monitoring, and individual thresholds 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 law or the contract, to immediately delete the accounts concerned and/or to temporarily block or permanently block the registered End Users concerned, without prior notification to the affected End Users or Organisations / Contracting Parties and without the affected End Users or Organisations / Contracting Parties being entitled to any claims for compensation on account thereof.

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.