ETH Zurich Department of Architecture
ARCHITECTURE OF TERRITORY
Chair of Architecture
and Territorial Planning
Professor Milica Topalović

The Production of Cloud
Fall 2025

Atlas

Data Sovereignty

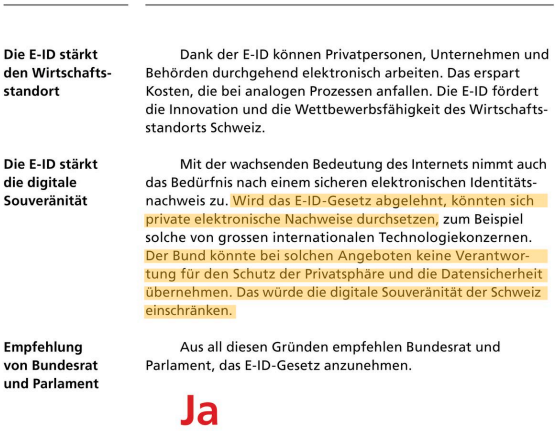
Esma Alili, Timo Feddern, Joanna Druey, and Valentin Egger

Switzerland aims for digital sovereignty and its people entrust their government with that responsibility, as confirmed with the recent approval of the E-ID act. The state categorises data into four stages of sensitivity and protects them accordingly. A certain interdependence with hyperscalers remains, which is mitigated through colocation, a type of data centre where equipment, space, and bandwidth are available for rental to retail customers. Swiss Fort Knox is the physical embodiment of data protection, the peak of digital sovereignty. Being located in a former military bunker in Saanen (BE), it intends to offer protection even against geopolitical threats. While private actors are crucial to shape the digital landscape and future of Switzerland, the Confederation directs the ecosystem according to the public interest and preserves digital sovereignty.

E-ID(entity) in Your Pocket



STATISTICS ON E-ID AND IPHONE USAGE IN SWITZERLAND. Source: admin.ch [https://www.admin.ch/gov/de/start/dokumentation/abstimmungen/20250928/e-id-gesetz.html], 2025/statista.ch [https://de.statista.com/themen/3581/smartphone-nutzung-in-der-schweiz/], 2023.



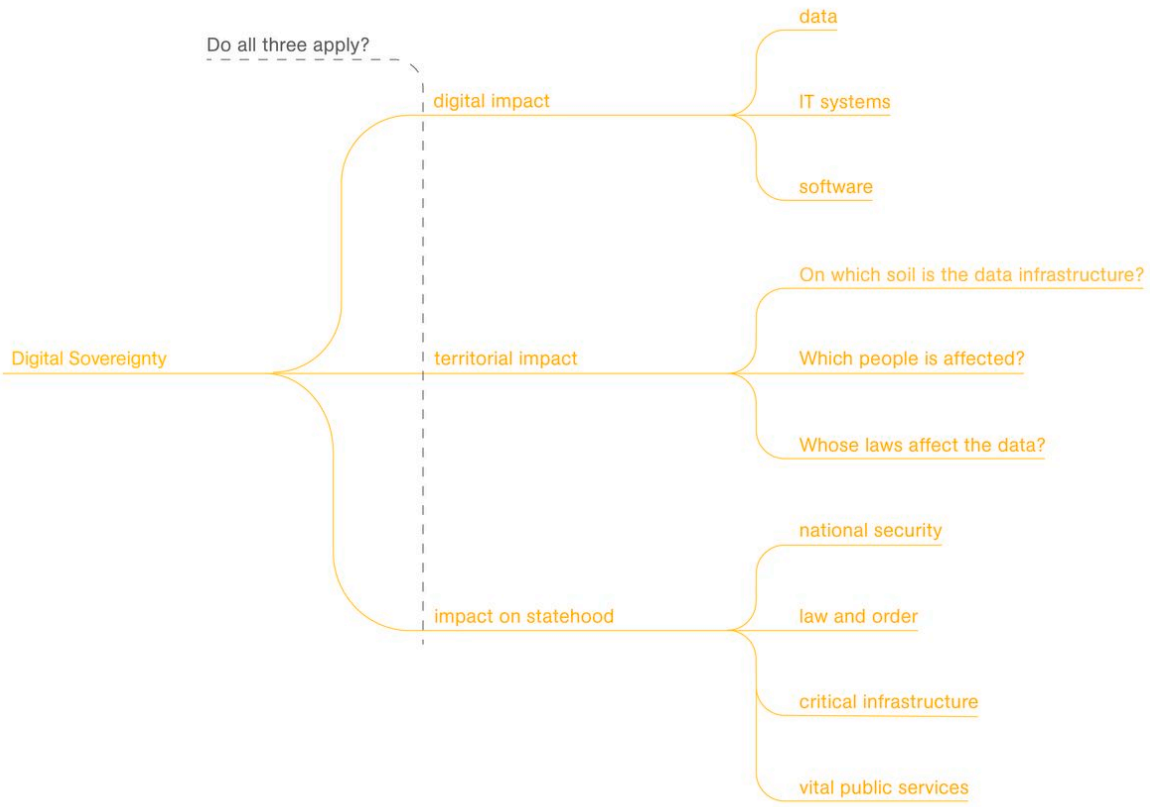
Die E-ID stärkt den Wirtschafts-standort	Dank der E-ID können Privatpersonen, Unternehmen und Behörden durchgehend elektronisch arbeiten. Das erspart Kosten, die bei analogen Prozessen anfallen. Die E-ID fördert die Innovation und die Wettbewerbsfähigkeit des Wirtschafts-standorts Schweiz.
Die E-ID stärkt die digitale Souveränität	Mit der wachsenden Bedeutung des Internets nimmt auch das Bedürfnis nach einem sicheren elektronischen Identitäts-nachweis zu. Wird das E-ID-Gesetz abgelehnt, könnten sich private elektronische Nachweise durchsetzen, zum Beispiel solche von grossen internationalen Technologiekonzernen. Der Bund könnte bei solchen Angeboten keine Verantwor-tung für den Schutz der Privatsphäre und die Datensicherheit übernehmen. Das würde die digitale Souveränität der Schweiz einschränken.
Empfehlung von Bundesrat und Parlament	Aus all diesen Gründen empfehlen Bundesrat und Parlament, das E-ID-Gesetz anzunehmen. **Ja**

E-ID VOTING PAPER. Source: admin.ch [https://www.admin.ch/gov/de/start/dokumentation/abstimmungen/20250928/e-id-gesetz.html], 2025.

On September 28th, 2025, the Swiss population accepted the Federal Act on having an E-ID to be issued and managed by the State. While 96 % of the population has a smartphone and is therefore directly affected when it comes to data security and privacy policies, the act just barely got accepted by the Swiss population with 50.39 % yes votes and 49.61 % no votes. Refusing the act would have resulted in private actors having to fill the demand of an E-ID. The State would not have been able to account for privacy policies and data security.

However, the acceptance of the Federal Act reassures that the Swiss people want to entrust its E-ID to the state only and maintain sovereignty thereby.

DATA SOVEREIGNTY AND DIGITAL SOVEREIGNTY



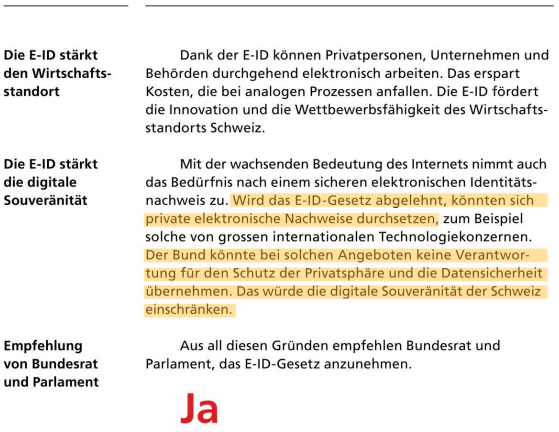
DEFINITION OF DIGITAL SOVEREIGNTY. Source: Swiss Data Alliance [https://static1.squarespace.com/static/643f9805a9dd3137751e41ae/t/666aa87191a3cf03dc9cff38/1718265970892/Digitale+Souveränität+%28Whitepaper%29+final.pdf], 2022. Scheme: Joanna Druey, 2025.

Digital sovereignty is one umbrella term of data sovereignty amongst others. For any topic to enter into the domain of digital sovereignty three areas must be touched: the digital sphere, the territory and the statehood. The term therefore covers digital process operations which have an impact on the territory of Switzerland and its institutions (statehood). Especially, the term statehood foresees that the state as an institution must not be threatened to maintain the states digital sovereignty. If the Swiss government loses data such as the Avalanche Prediction Software, the digital and territorial aspects may be affected. However, Switzerland as an institution is not threatened and therefore its digital sovereignty is also not threatened.

E-ID IN SWITZERLAND



STATISTICS ON E-ID AND IPHONE USAGE IN SWITZERLAND. Source: admin.ch [https://www.admin.ch/gov/de/start/dokumentation/abstimmungen/20250928/e-id-gesetz.html], 2025/statista.ch [https://de.statista.com/themen/3581/smartphone-nutzung-in-der-schweiz/], 2023.



Die E-ID stärkt den Wirtschaftsstandort

Dank der E-ID können Privatpersonen, Unternehmen und Behörden durchgehend elektronisch arbeiten. Das erspart Kosten, die bei analogen Prozessen anfallen. Die E-ID fördert die Innovation und die Wettbewerbsfähigkeit des Wirtschaftsstandorts Schweiz.

Die E-ID stärkt die digitale Souveränität

Mit der wachsenden Bedeutung des Internets nimmt auch das Bedürfnis nach einem sicheren elektronischen Identitätsnachweis zu. Wird das E-ID-Gesetz abgelehnt, könnten sich private elektronische Nachweise durchsetzen, zum Beispiel solche von grossen internationalen Technologiekonzernen. Der Bund könnte bei solchen Angeboten keine Verantwortung für den Schutz der Privatsphäre und die Datensicherheit übernehmen. Das würde die digitale Souveränität der Schweiz einschränken.

Empfehlung von Bundesrat und Parlament

Aus all diesen Gründen empfehlen Bundesrat und Parlament, das E-ID-Gesetz anzunehmen.

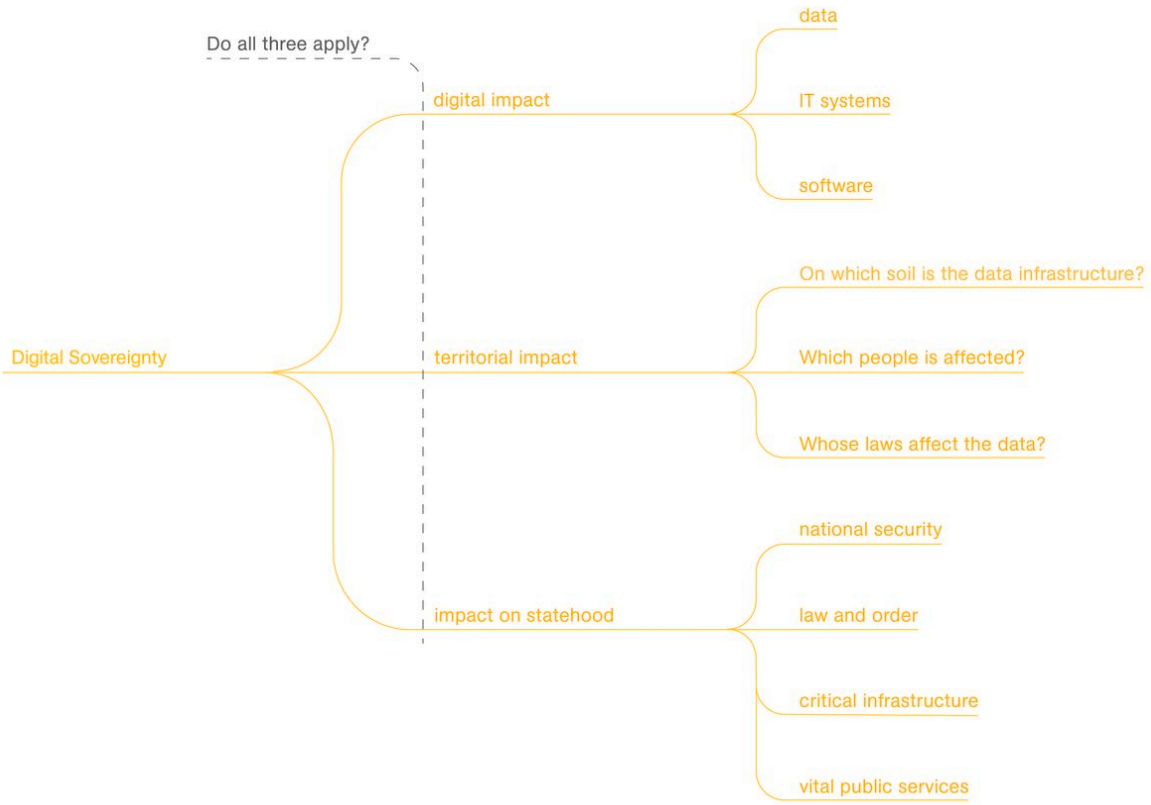
Ja

E-ID VOTING PAPER. Source: admin.ch [https://www.admin.ch/gov/de/start/dokumentation/abstimmungen/20250928/e-id-gesetz.html], 2025.

On September 28th, 2025, the Swiss population accepted the Federal Act on having an E-ID to be issued and managed by the State. While 96 % of the population has a smartphone and is therefore directly affected when it comes to data security and privacy policies, the act just barely got accepted by the Swiss population with 50.39 % yes votes and 49.61 % no votes. Refusing the act would have resulted in private actors having to fill the demand of an E-ID. The State would not have been able to account for privacy policies and data security.

However, the acceptance of the Federal Act reassures that the Swiss people want to entrust its E-ID to the state only and maintain sovereignty thereby.

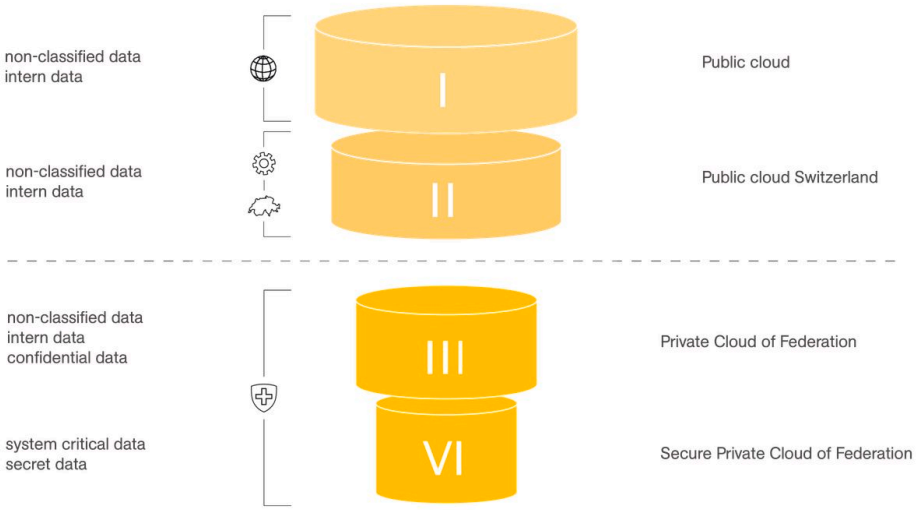
DATA SOVEREIGNTY AND DIGITAL SOVEREIGNTY



DEFINITION OF DIGITAL SOVEREIGNTY. Source: Swiss Data Alliance [https://static1.squarespace.com/static/643f9805a9dd3137751e41ae/t/666aa87191a3cf03dc9cff38/1718265970892/Digitale+Souveränität+%28Whitepaper%29+final.pdf], 2022. Scheme: Joanna Druey, 2025.

Digital sovereignty is one umbrella term of data sovereignty amongst others. For any topic to enter into the domain of digital sovereignty three areas must be touched: the digital sphere, the territory and the statehood. The term therefore covers digital process operations which have an impact on the territory of Switzerland and its institutions (statehood). Especially, the term statehood foresees that the state as an institution must not be threatened to maintain the states digital sovereignty. If the Swiss government loses data such as the Avalanche Prediction Software, the digital and territorial aspects may be affected. However, Switzerland as an institution is not threatened and therefore its digital sovereignty is also not threatened.

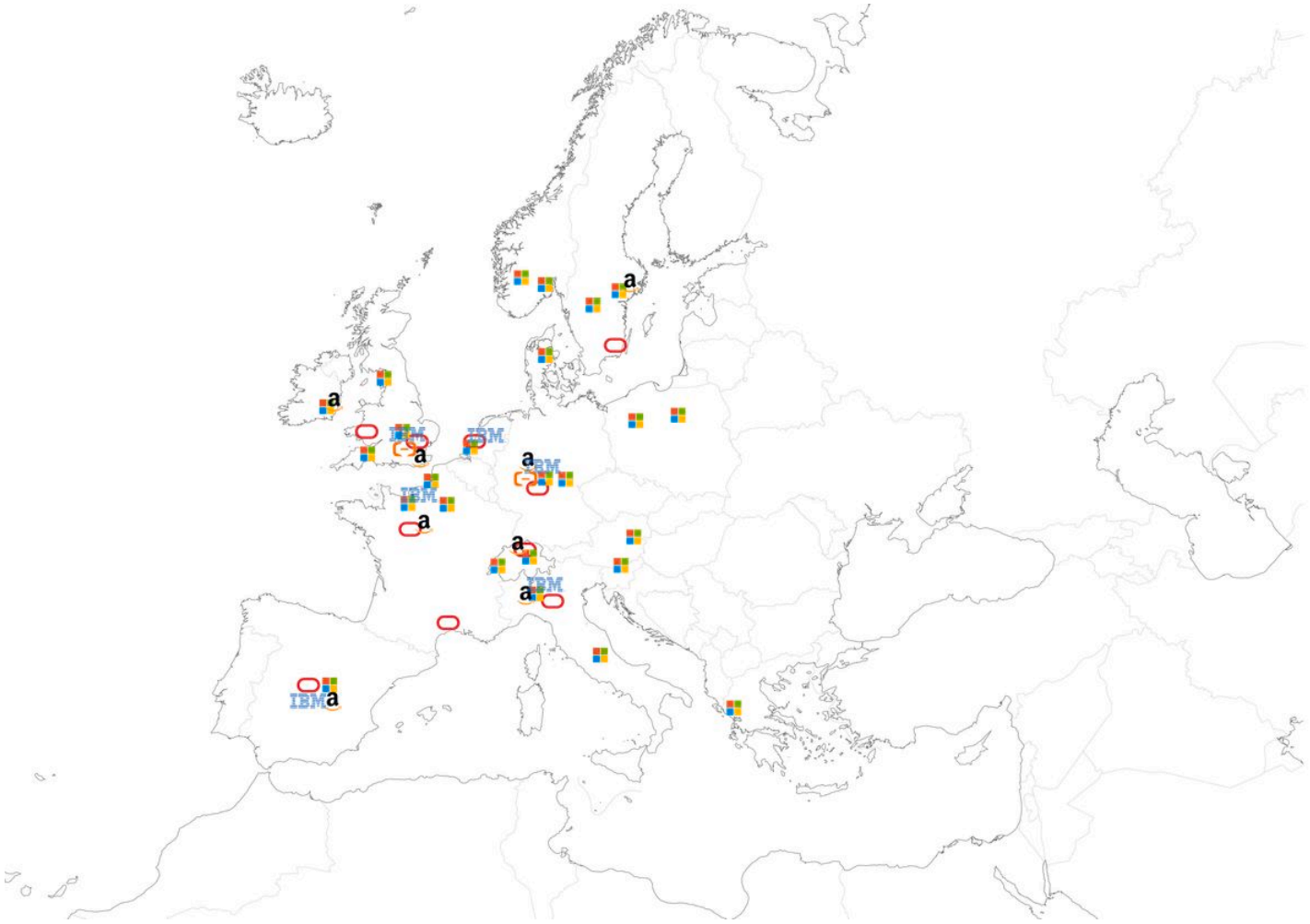
The Inevitable International Part in the Swiss Cloud Strategy



STAGES OF FEDERAL CLOUD STRATEGY. Source: admin.ch [https://www.bk.admin.ch/bk/en/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html], 2025. Modified: Joanna Druey, 2025.

In order to maintain digital sovereignty, the Confederation developed a strategy which classifies data into four stages. They are categorised according to sensitivity and respective level of protection.

STAGE I

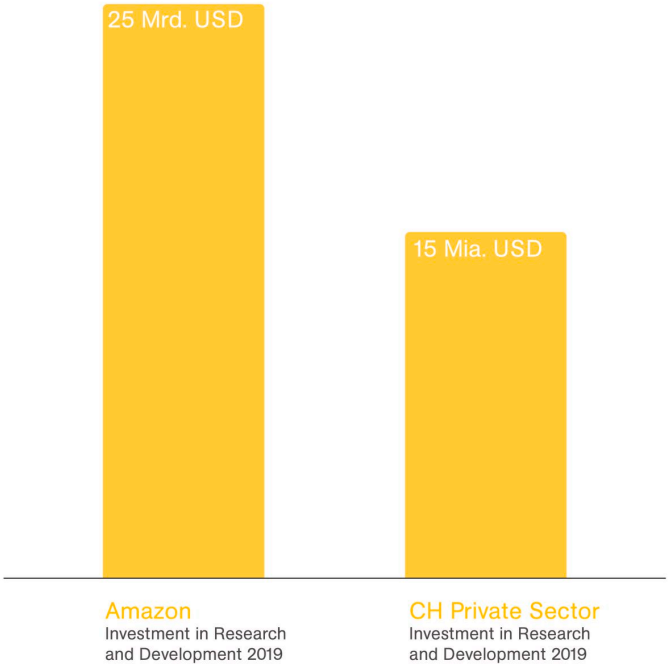


DATA CENTRES IN EUROPE UNDER CONTRACT WITH FEDERATION
The map shows the data centre locations within Europe where the Stage I data may be stored. The locations of the following cloud providers are shown: Oracle, Alibaba Cloud, Microsoft Azure, Amazon Web Services (AWS) and International Business Machines cooperation (IBM). Source: unknown. Scheme: Joanna Druey, 2025.

Oracle Data Region
Alibaba Cloud Data Center
Microsoft Data Region
Amazon Web Services Data Region
IBM Data Region

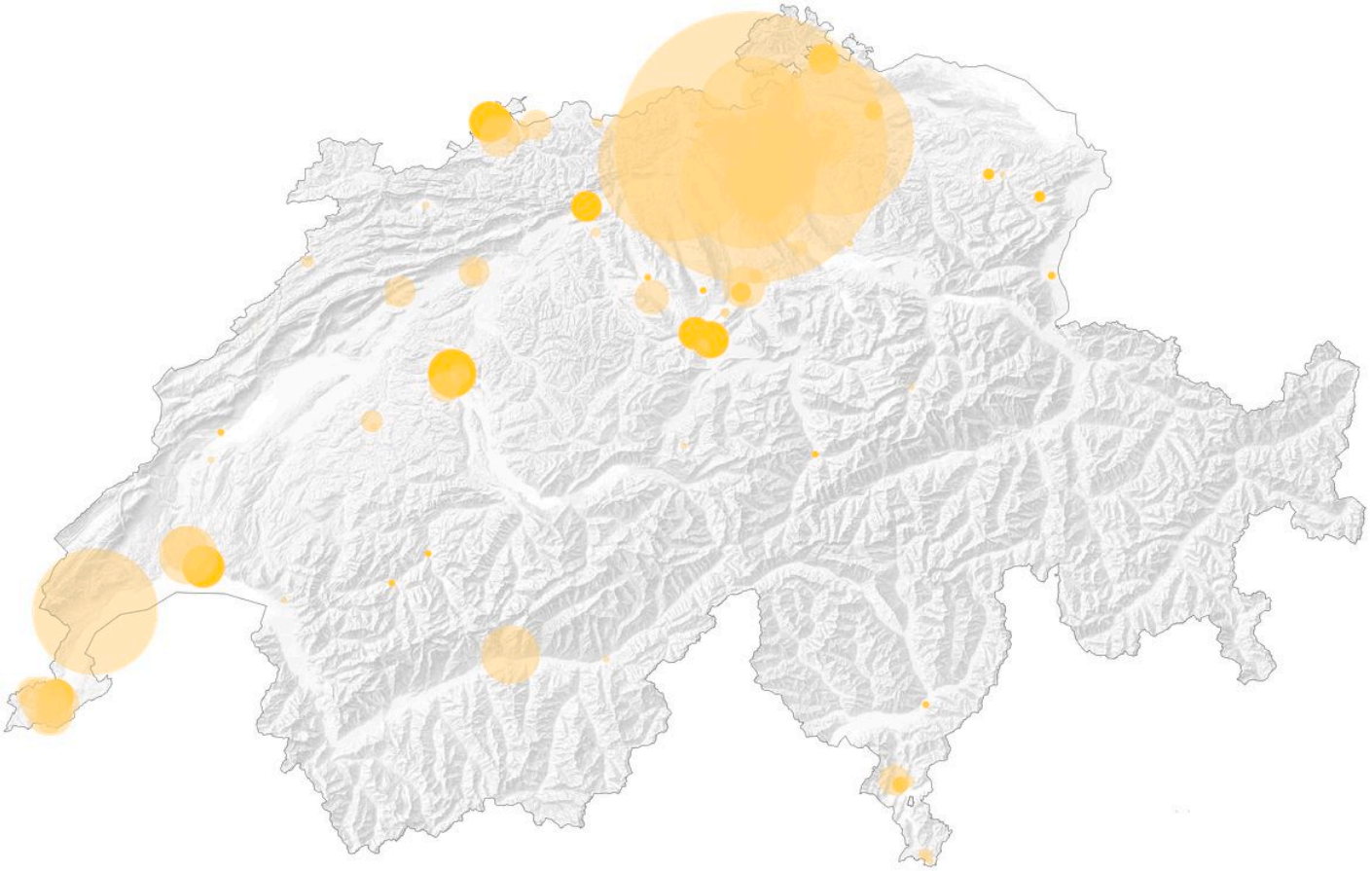
The first stage regards intern and non-classified data such as data from swisstopo Base Maps which will be stored in the public cloud. The Stage I data is purely non-sensitive such as data of weather measurements. These data are stored outside of Switzerland in Ireland but are encrypted as they leave Switzerland. The weather forecast of Switzerland does travel to Ireland, yet nobody can read it without passing through the Swiss data warehouse in Zurich.

The government has made contracts in the year 2023 with five international cloud providers such as Amazon Web Services (AWS), Microsoft Azure, and others. Making these contracts caused media and political outrage. However, having own data centres would be difficult to implement. On one hand, data quantity fluctuates quickly. It would take up to fifteen years to build a data centre while renting as much space as needed with international providers requires only minutes. On the other hand, it would be unreasonable financially for Switzerland to invest in data centres. Amazon Web Services alone invests 25 billions US dollars in research and development. This sum is ten billions more investment in research and development than the whole Swiss private sector across all domains. The financial divergence is clear. The statistics show the capacity of hyperscalers compared to Switzerlands investment capacity.



INVESTMENT IN RESEARCH AND DEVELOPMENT. Source: NZZ.ch [https://www.nzz.ch/wirtschaft/bundesdaten-in-der-cloud-gefaehrliche-abhaengigkeit-vom-ausland-ld.1651398], 2021. Scheme: Joanna Druey, 2025.

STAGE II



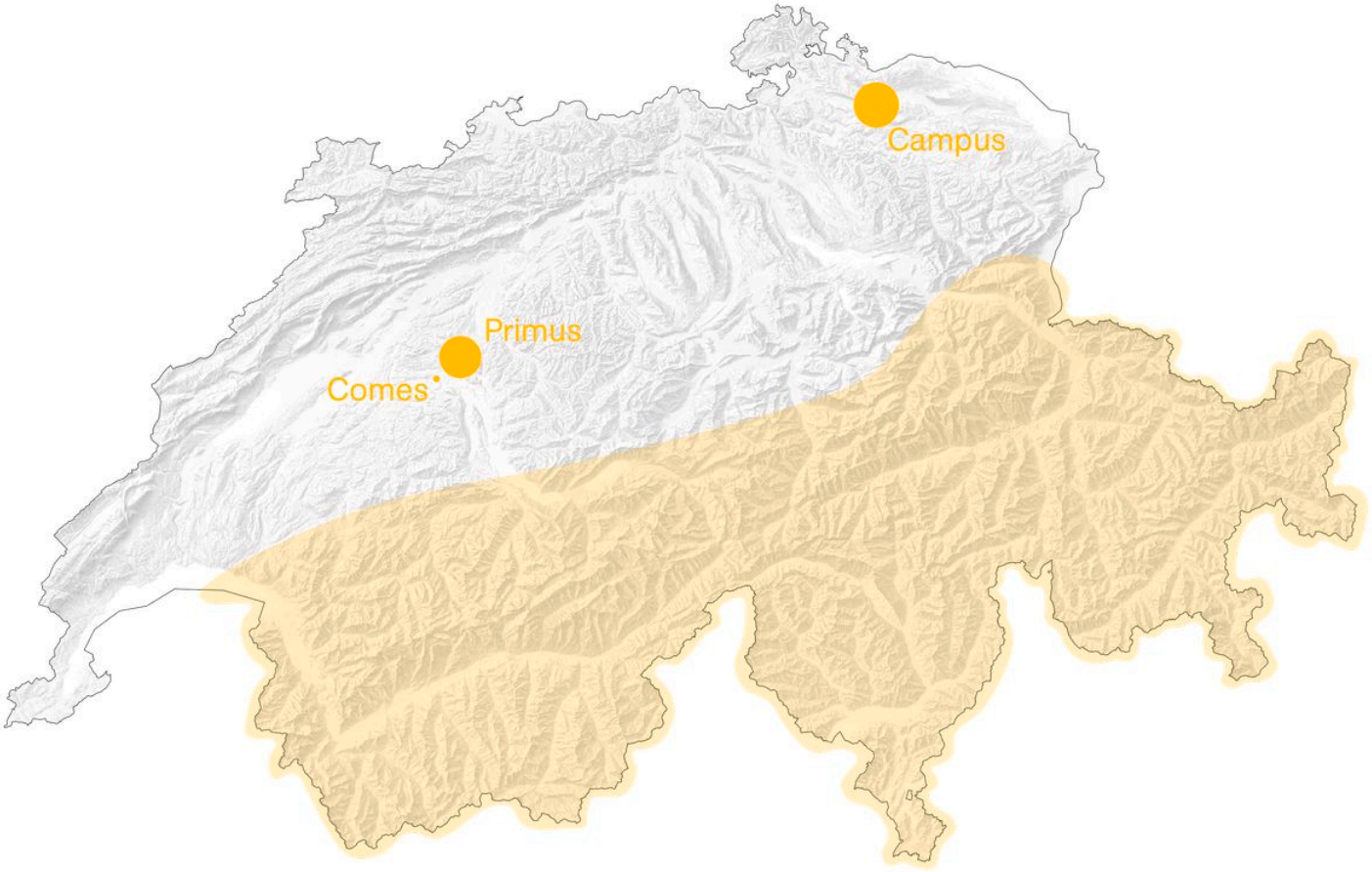
(SEMI-)PUBLIC DATA CENTRES IN SWITZERLAND
The map shows the concentration of data centers in Switzerland. Furthermore, it shows that there is a concentration of data centres in Zurich, where for instance Microsoft Azure data centers are located. Other data centres accumulate throughout the western part of Switzerland such as Geneva or Bern. Source: Modified Studio Resources, 2025. Modification: Joanna Druey, 2025.

Public Data Center

Semi-Public Data Center

Stage II of the cloud strategy regards the non-classified or intern data. The stage II data have specific requirements to be stored within Switzerland, such as certain non-confidential health data. These data will also be stored with Amazon Web Services, Microsoft, or other international providers as mentioned above. In contrast to Stage I, these data will be stored in Switzerland at colocations of the external providers.

STAGE III AND STAGE IV



FEDERAL DATA CENTRES SWITZERLAND
The map shows the locations of Federal data centres in Switzerland. Campus (Frauenfeld, TG), Primus (Bern, BE), Comes (Bern, BE). Furthermore, it visualises the potential locations of other military data centres. As the map showcases, these data centres could be in the alpine territories throughout Switzerland. Source: Studio Resources, 2025. Modified: Joanna Druey, 2025.

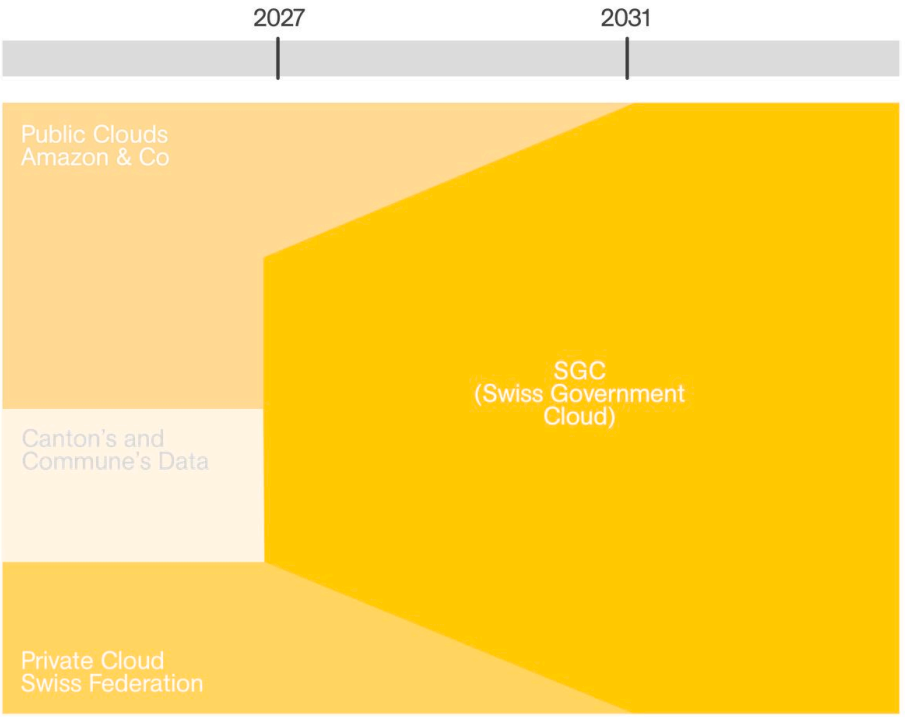
Potential Location of Swiss Military Data Center

Federal Data Center

Stage III and stage IV can contain non-classified data and intern data as well. In addition, they regard confidential, system critical and secret data. These data are stored within federal data centres. Those data centres are utterly secure. Nonetheless, they are vulnerable towards geopolitical threats.

There are potentially three military data centres in bunkers in the Swiss alpine territories. These bunker data centres are most likely built similar to the case study data centre Swiss Fort Knox. Military data centres are of utmost importance to guarantee digital sovereignty in times of conflict as they can provide security even against nuclear threats.

THE SWISS GOVERNMENT CLOUD

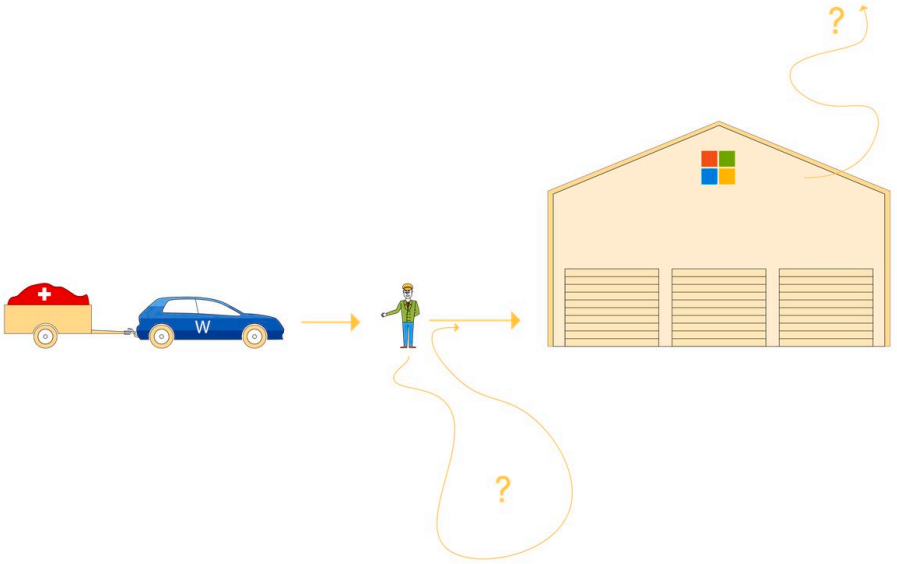


FUTURE SWISS GOVERNMENT CLOUD
Source: admin.ch [https://www.bit.admin.ch/en/sgc-en?utm_source=chatgpt.com], 2025. Modification: Joanna Druey, 2025.

Government data is currently stored in public clouds run by international providers. Switzerland plans to introduce the Swiss Government Cloud (SGC). This would allow Switzerland to regain control over their data and ensure data sovereignty. Moreover and more importantly, the SGC would allow Switzerland to have a unified user platform across all their competencies. The aim is to own and manage the own data. The first data migration is planned to take place in the year 2027. By 2031 the data migration is to be concluded.

The SGC will still use data centres from major hyperscalers but under the principle of colocation. This means that Switzerland wants to use own servers and softwares instead of the ones provided by hyperscalers.

COLOCATION EXPLAINED

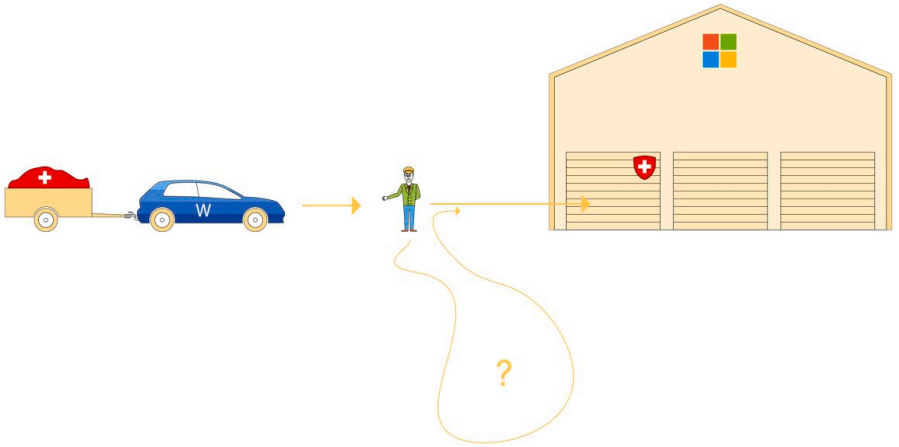


COLOCATION EXPLAINED: SCNENARIO A.
Scheme: Joanna Druey, 2025.

To understand colocation the analogy of a garage will be used.

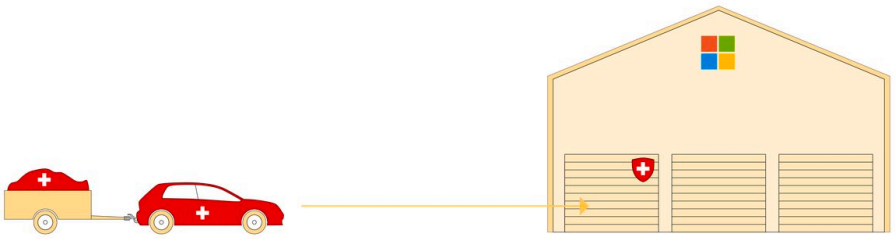
The trailer carries the Swiss data, the car is the software with which the data was created and transferred. In this case the software is Microsoft Word. The cloud provider, or garage, is in this specific case from Microsoft as well, but it could have been any of the above mentioned cloud providers, such as AWS, Oracle, or the like.

Once the trailer is handed over to the parking attendant, the data trailer will be stored at Microsoft's garage. However, it could be that the parking attendant takes the trailer for a spin (giving data to third parties) or looking at what it's carrying. Furthermore, storing the trailer in the garage that Microsoft provides and owns, still leaves the risk that Microsoft may handle it unrightfully, treat and store it unencrypted, or move the contents of it to somewhere else.



COLOCATION EXPLAINED: SCNENARIO B.
Scheme: Joanna Druey, 2025.

In the second scenario Switzerland buys a garage at Microsoft. Thereby, we have to cross through the hallways (in this case fiber connections) to the garage, but we are the only ones having a key and access to it. Yet, the car is a software—in this case Word—which is not created or controlled by Switzerland. The parking attendant would have to park the trailer in the Swiss garage at Microsoft. Still, there could be the possibility to take the car for a stroll or a look inside. Data security, control, and sovereignty would be still at risk.

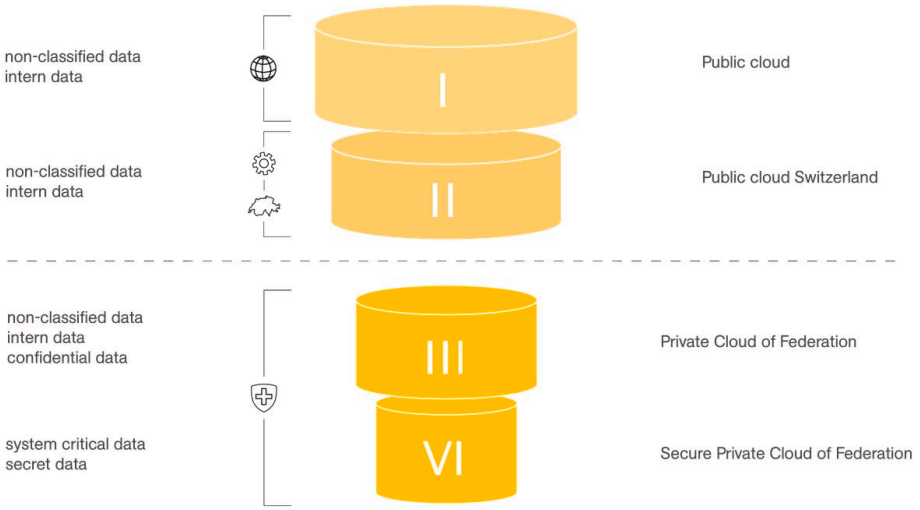


COLOCATION EXPLAINED: SCNENARIO C.
Scheme: Joanna Druey, 2025.

The third and most secure scenario would be that Switzerland not only owns a garage at Microsoft but it also provides a Swiss car which means a Swiss software that carries the trailer safely without the risk that someone else might get involved. The Swiss trailer would be parked directly into the Swiss garage with the Swiss car.

Even though it is the most secure way towards digital sovereignty, the difficulty arises at the level of implementation since people rather use Word than a Swiss software alternative like LibreOffice.

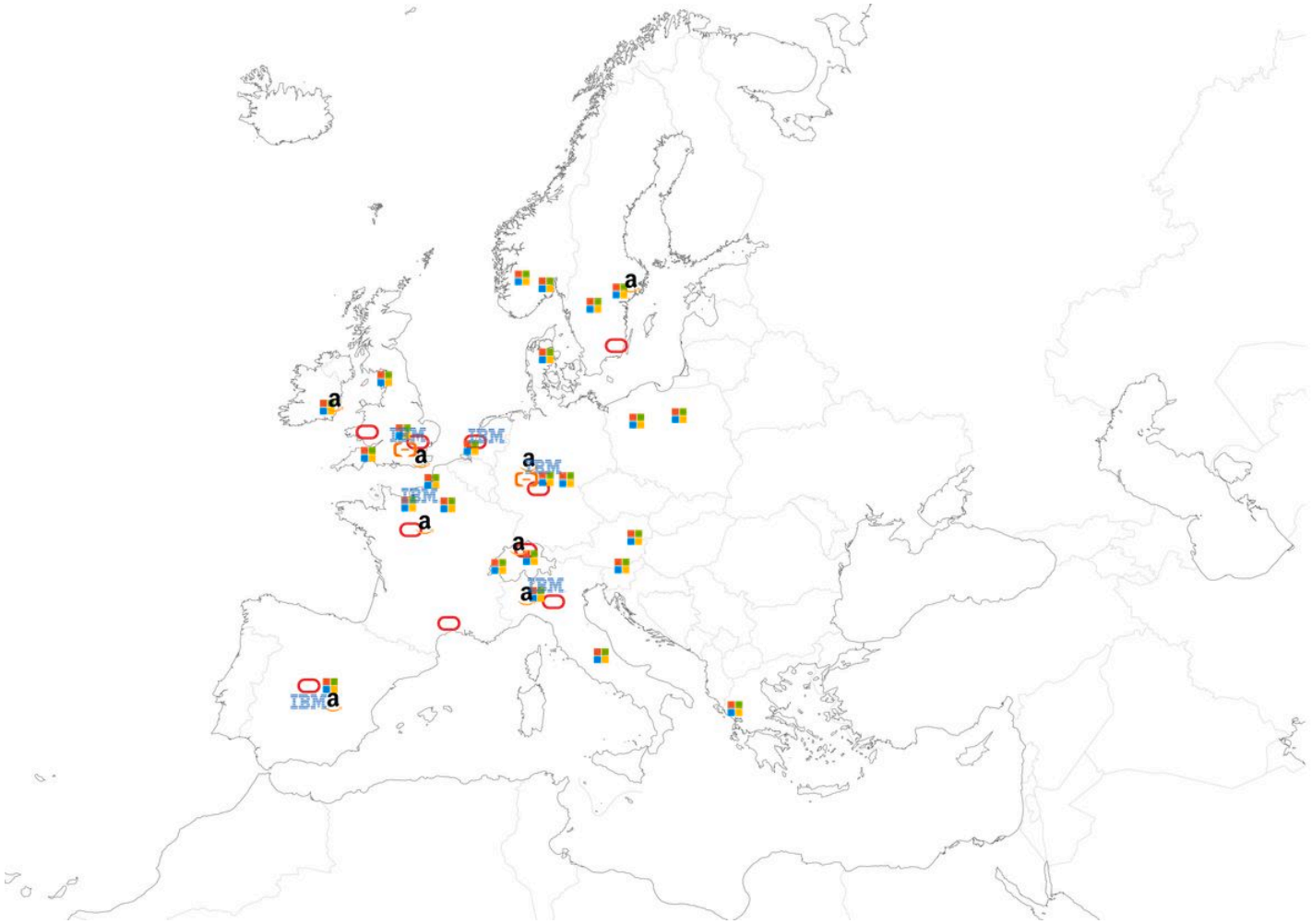
Nevertheless, this strategy has been adopted by numerous institutions worldwide, such as the Austrian Army, as well as other European municipalities and companies such as the German state Schleswig Holstein, the French city Lyon, or the Dutch government through introducing the data sovereignty supporting software LibreOffice.



STAGES OF FEDERAL CLOUD STRATEGY. Source: admin.ch [https://www.bk.admin.ch/bk/en/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html], 2025. Modified: Joanna Druey, 2025.

In order to maintain digital sovereignty, the Confederation developed a strategy which classifies data into four stages. They are categorised according to sensitivity and respective level of protection.

STAGE I

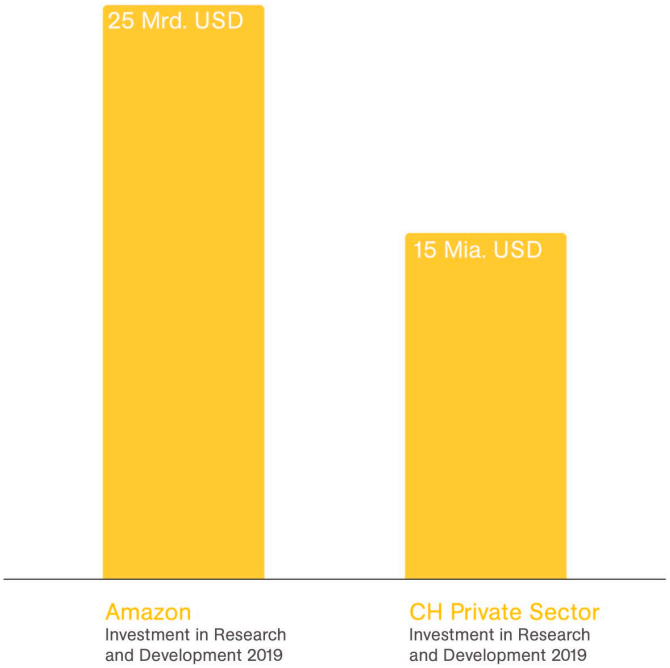


DATA CENTRES IN EUROPE UNDER CONTRACT WITH FEDERATION
The map shows the data centre locations within Europe where the Stage I data may be stored. The locations of the following cloud providers are shown: Oracle, Alibaba Cloud, Microsoft Azure, Amazon Web Services (AWS) and International Business Machines cooperation (IBM). Source: unknown. Scheme: Joanna Druey, 2025.

- Oracle Data Region
- Alibaba Cloud Data Center
- Microsoft Data Region
- Amazon Web Services Data Region
- IBM Data Region

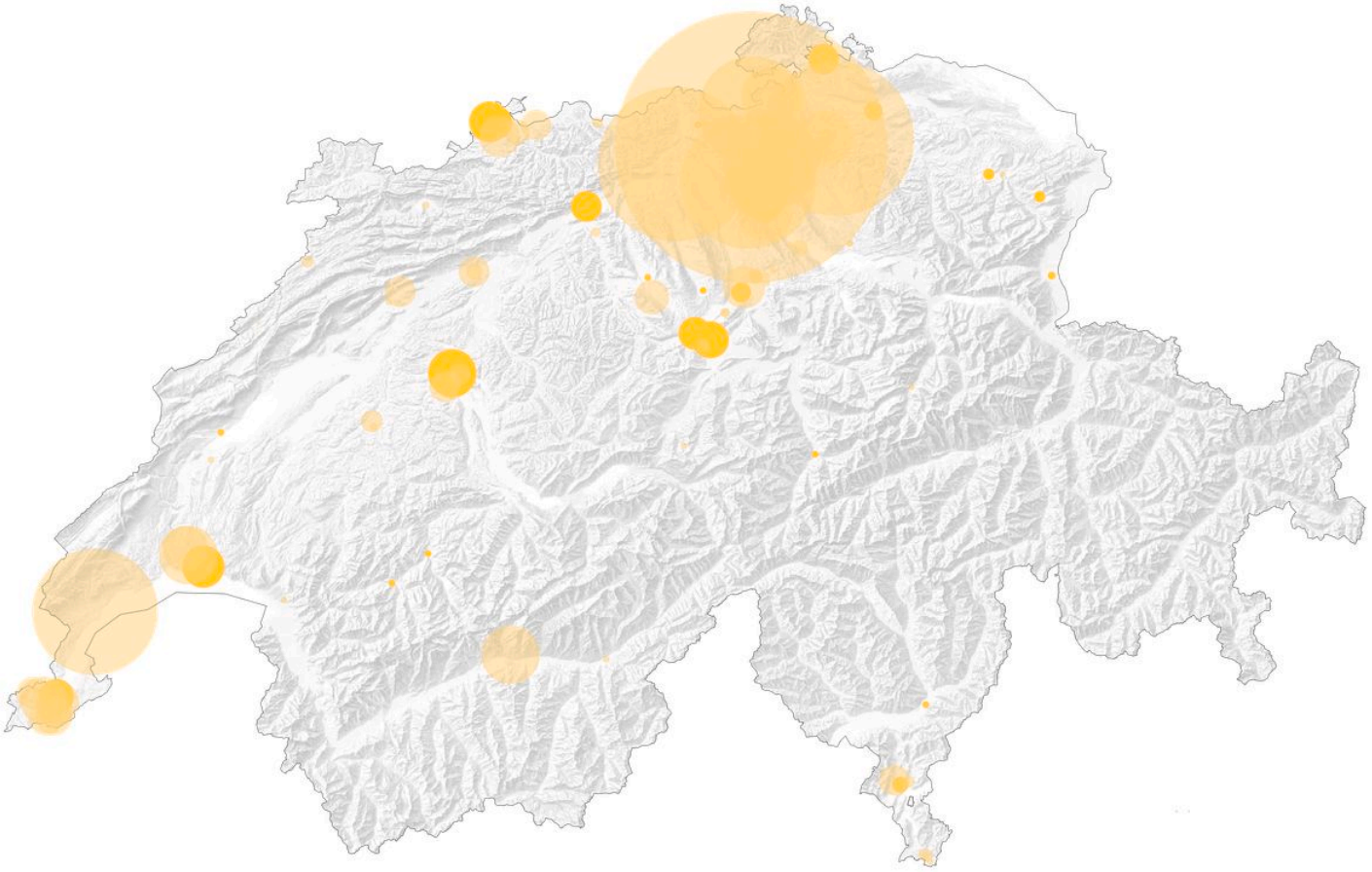
The first stage regards intern and non-classified data such as data from swisstopo Base Maps which will be stored in the public cloud. The Stage I data is purely non-sensitive such as data of weather measurements. These data are stored outside of Switzerland in Ireland but are encrypted as they leave Switzerland. The weather forecast of Switzerland does travel to Ireland, yet nobody can read it without passing through the Swiss data warehouse in Zurich.

The government has made contracts in the year 2023 with five international cloud providers such as Amazon Web Services (AWS), Microsoft Azure, and others. Making these contracts caused media and political outrage. However, having own data centres would be difficult to implement. On one hand, data quantity fluctuates quickly. It would take up to fifteen years to build a data centre while renting as much space as needed with international providers requires only minutes. On the other hand, it would be unreasonable financially for Switzerland to invest in data centres. Amazon Web Services alone invests 25 billions US dollars in research and development. This sum is ten billions more investment in research and development than the whole Swiss private sector across all domains. The financial divergence is clear. The statistics show the capacity of hyperscalers compared to Switzerlands investment capacity.



INVESTMENT IN RESEARCH AND DEVELOPMENT. Source: NZZ.ch [https://www.nzz.ch/wirtschaft/bundesdaten-in-der-cloud-gefaehrliche-abhaengigkeit-vom-ausland-ld.1651398], 2021. Scheme: Joanna Druey, 2025.

STAGE II



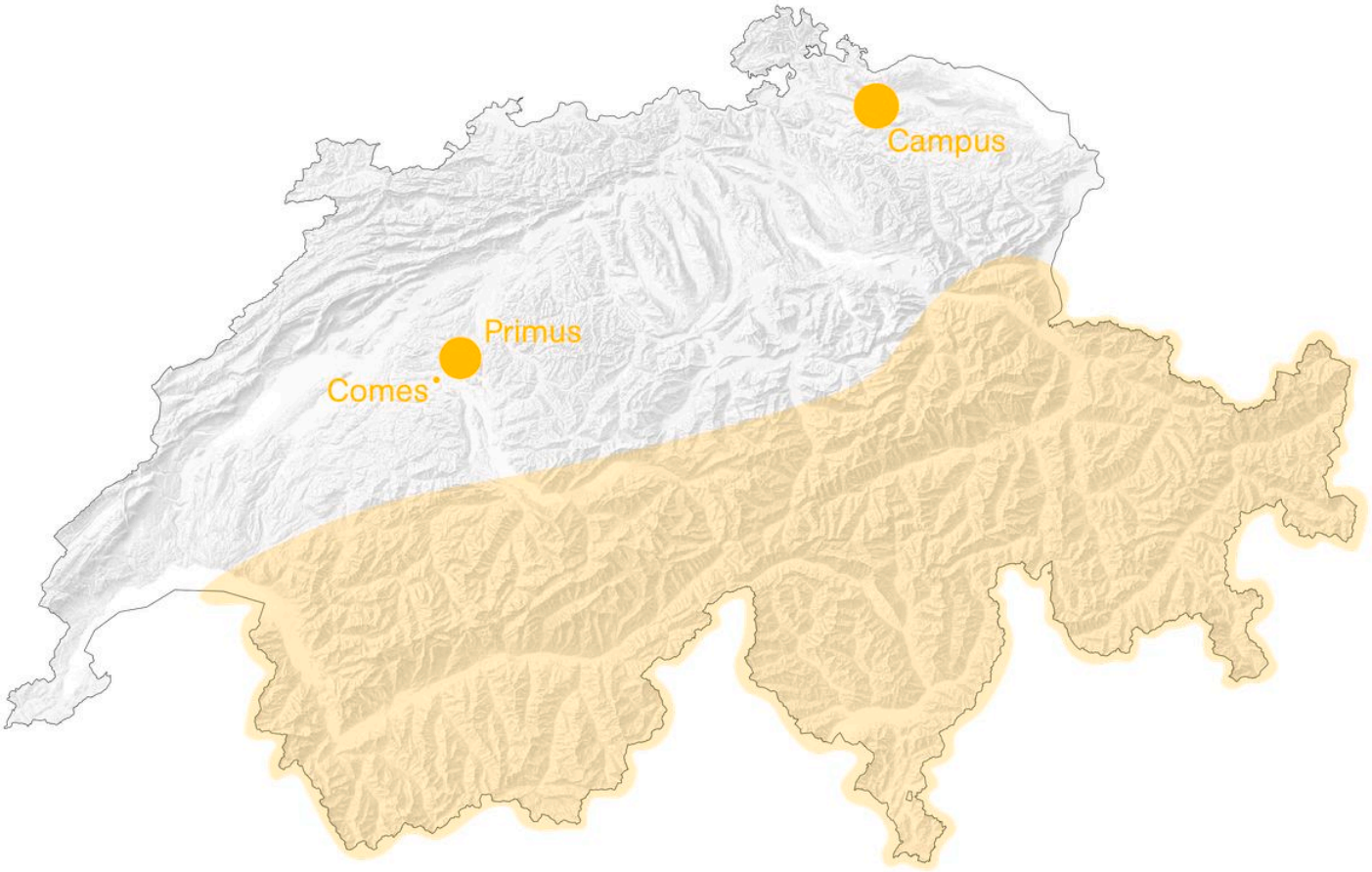
(SEMI-)PUBLIC DATA CENTRES IN SWITZERLAND
The map shows the concentration of data centers in Switzerland. Furthermore, it shows that there is a concentration of data centres in Zurich, where for instance Microsoft Azure data centers are located. Other data centres accumulate throughout the western part of Switzerland such as Geneva or Bern. Source: Modified Studio Resources, 2025. Modification: Joanna Druey, 2025.

Public Data Center

Semi-Public Data Center

Stage II of the cloud strategy regards the non-classified or intern data. The stage II data have specific requirements to be stored within Switzerland, such as certain non-confidential health data. These data will also be stored with Amazon Web Services, Microsoft, or other international providers as mentioned above. In contrast to Stage I, these data will be stored in Switzerland at colocations of the external providers.

STAGE III AND STAGE IV



FEDERAL DATA CENTRES SWITZERLAND
The map shows the locations of Federal data centres in Switzerland. Campus (Frauenfeld, TG), Primus (Bern, BE), Comes (Bern, BE). Furthermore, it visualises the potential locations of other military data centres. As the map showcases, these data centres could be in the alpine territories throughout Switzerland. Source: Studio Resources, 2025. Modified: Joanna Druey, 2025.

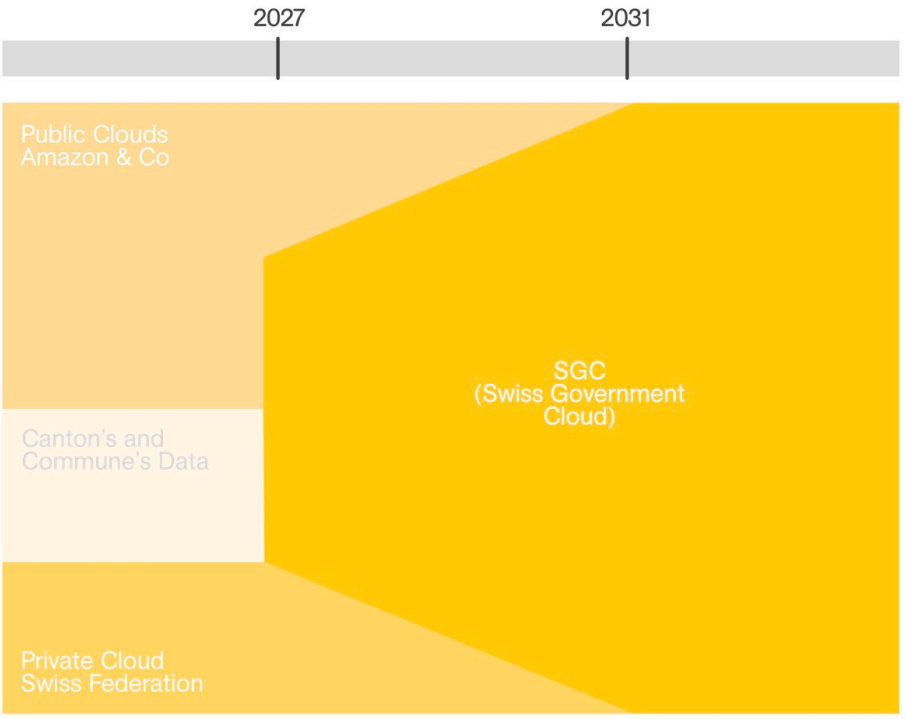
Potential Location of Swiss Military Data Center

Federal Data Center

Stage III and stage IV can contain non-classified data and intern data as well. In addition, they regard confidential, system critical and secret data. These data are stored within federal data centres. Those data centres are utterly secure. Nonetheless, they are vulnerable towards geopolitical threats.

There are potentially three military data centres in bunkers in the Swiss alpine territories. These bunker data centres are most likely built similar to the case study data centre Swiss Fort Knox. Military data centres are of utmost importance to guarantee digital sovereignty in times of conflict as they can provide security even against nuclear threats.

THE SWISS GOVERNMENT CLOUD

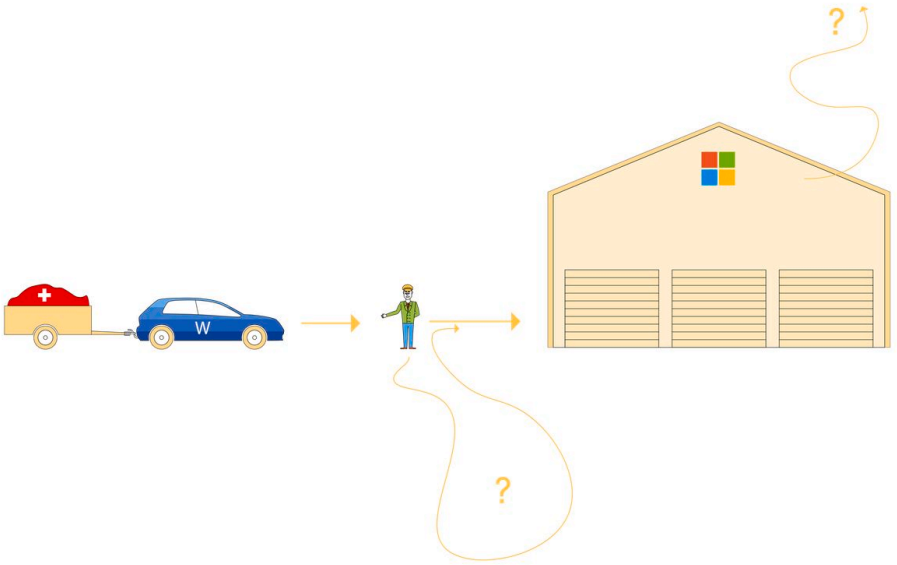


FUTURE SWISS GOVERNMENT CLOUD
Source: admin.ch [https://www.bit.admin.ch/en/sgc-en?utm_source=chatgpt.com], 2025. Modification: Joanna Druey, 2025.

Government data is currently stored in public clouds run by international providers. Switzerland plans to introduce the Swiss Government Cloud (SGC). This would allow Switzerland to regain control over their data and ensure data sovereignty. Moreover and more importantly, the SGC would allow Switzerland to have a unified user platform across all their competencies. The aim is to own and manage the own data. The first data migration is planned to take place in the year 2027. By 2031 the data migration is to be concluded.

The SGC will still use data centres from major hyperscalers but under the principle of colocation. This means that Switzerland wants to use own servers and softwares instead of the ones provided by hyperscalers.

COLOCATION EXPLAINED

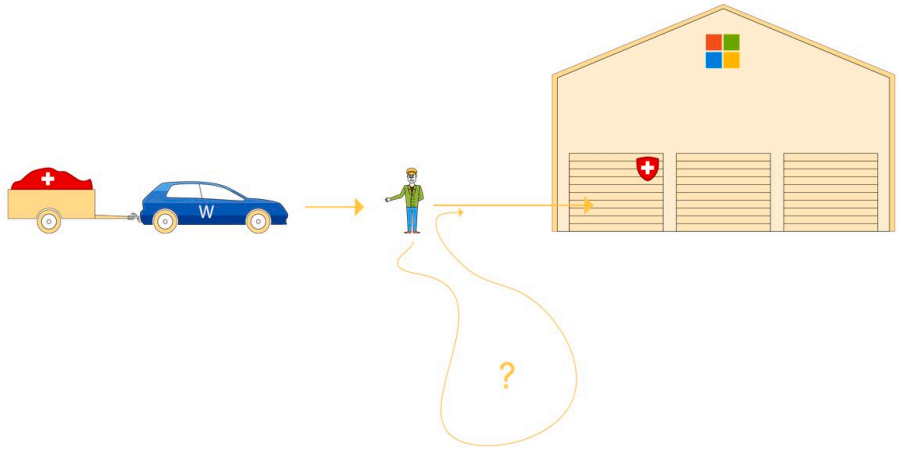


COLOCATION EXPLAINED: SCNENARIO A.
Scheme: Joanna Druey, 2025.

To understand colocation the analogy of a garage will be used.

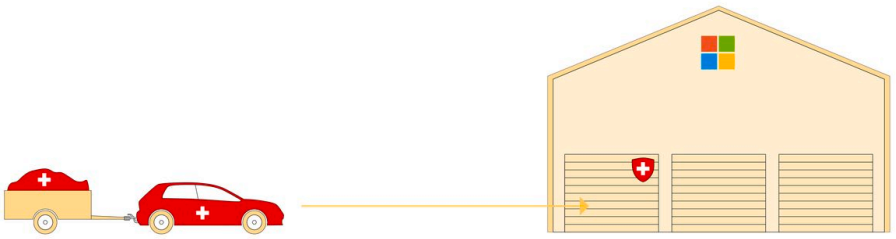
The trailer carries the Swiss data, the car is the software with which the data was created and transferred. In this case the software is Microsoft Word. The cloud provider, or garage, is in this specific case from Microsoft as well, but it could have been any of the above mentioned cloud providers, such as AWS, Oracle, or the like.

Once the trailer is handed over to the parking attendant, the data trailer will be stored at Microsoft's garage. However, it could be that the parking attendant takes the trailer for a spin (giving data to third parties) or looking at what it's carrying. Furthermore, storing the trailer in the garage that Microsoft provides and owns, still leaves the risk that Microsoft may handle it unrightfully, treat and store it unencrypted, or move the contents of it to somewhere else.



COLOCATION EXPLAINED: SCNENARIO B.
Scheme: Joanna Druey, 2025.

In the second scenario Switzerland buys a garage at Microsoft. Thereby, we have to cross through the hallways (in this case fiber connections) to the garage, but we are the only ones having a key and access to it. Yet, the car is a software—in this case Word—which is not created or controlled by Switzerland. The parking attendant would have to park the trailer in the Swiss garage at Microsoft. Still, there could be the possibility to take the car for a stroll or a look inside. Data security, control, and sovereignty would be still at risk.



COLOCATION EXPLAINED: SCNENARIO C.
Scheme: Joanna Druey, 2025.

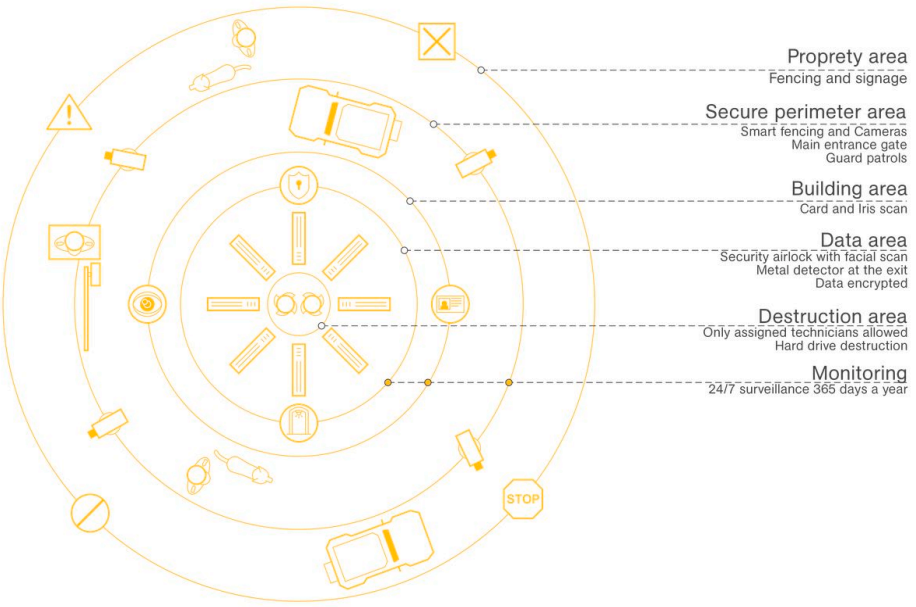
The third and most secure scenario would be that Switzerland not only owns a garage at Microsoft but it also provides a Swiss car which means a Swiss software that carries the trailer safely without the risk that someone else might get involved. The Swiss trailer would be parked directly into the Swiss garage with the Swiss car.

Even though it is the most secure way towards digital sovereignty, the difficulty arises at the level of implementation since people rather use Word than a Swiss software alternative like LibreOffice.

Nevertheless, this strategy has been adopted by numerous institutions worldwide, such as the Austrian Army, as well as other European municipalities and companies such as the German state Schleswig Holstein, the French city Lyon, or the Dutch government through introducing the data sovereignty supporting software LibreOffice.

The Peak of Digital Security

PHYSICAL SECURITY: AN OVERVIEW



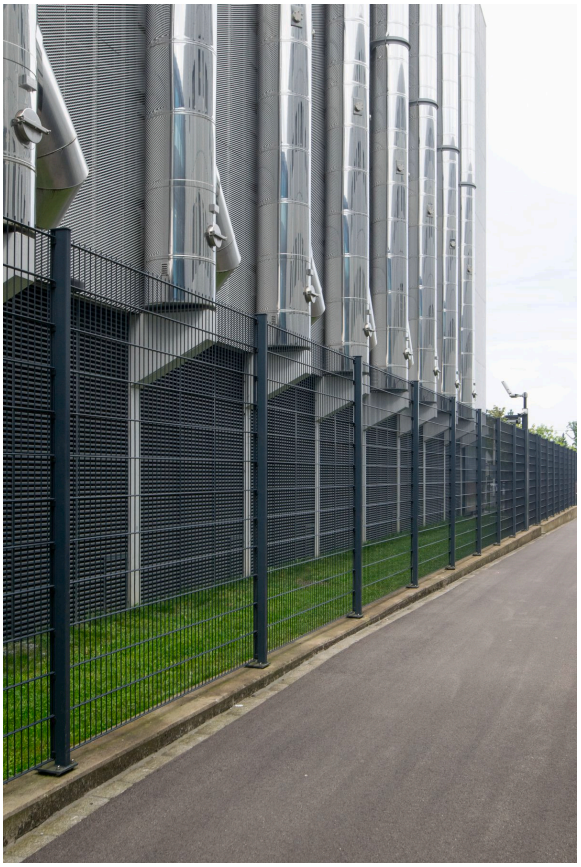
DIGITAL SECURITY.
Scheme: Valentin Egger, 2025.

Physical security concepts for protected buildings, in this case data centres, start with spatial boundaries, separating public from private land through fences and signage to create a securised “inner” space. This inner— and controlled—space, also called the “secure perimeter” is being controlled by patrolling personnel (depending on the object they might be supported by cars, dogs, etc…) supported by hard- and software such as cameras, motion detectors, smart sensors, and so on.

Within these secure perimeters the actual “object of interest,” for example a data centre, resides. Access to these buildings is usually possible through doors (either small ones for personnel or large ones that also allow access by vehicles for deliveries or pickups). These entries are surveilled by cameras and access is only possible with a badge, iris or fingerprint scan and other verification methods (for example a manual search of a car or truck) to authenticate and authorise users. This should also include the verification of a person’s tasks and its access needed for it (this might also include a “bodyguard” to enforce a four-eye principal on what happens within this building or an area of it).

The destruction area refers to the area where the hard disks are destroyed. It is important to acknowledge that data centres offer areas for customers to destroy their hard drives in case they want certain data to disappear without the risk of losing them, having them stolen, or copied. Therefore, the destruction area is only accessible for assigned technicians.

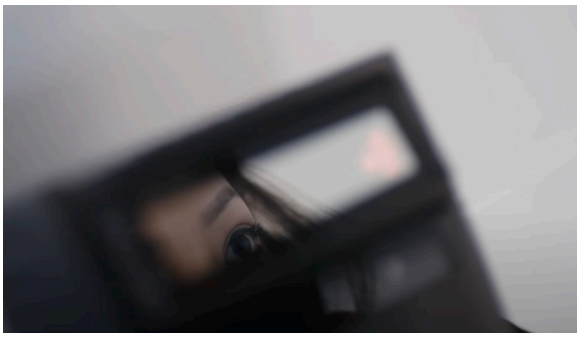
Within the following “entry-area” of a building there is a monitoring area, used for verification and strict surveillance of people. Sometimes this includes airport-like scanners for personnel and baggage to keep out any dangerous devices or software. The final access is then again a door (usually a very thick and secure one) with badge or biometrical readers, a man lock, and other security measures to ensure that only allowed technicians and customers can enter the final “server-area” of the data centres. There might be multiple nested security areas like this one to ensure an even finer separation of customers and employees.



PROPERTY AREA FENCING
Source: Studio Resources, 2025.



SECURE PERIMETER AREA CAMERAS
Source: Studio Resources, 2025.



BUILDING AREA IRIS SCAN
Source: Sicherheit im Google-Rechenzentrum: 6 Ebenen tief. [https://www.youtube.com/watch?v=kd33UVZhnAA]



DATA AREA SECURITY AIRLOCK
AND METAL DETECTOR
Source: Sicherheit im Google-Rechenzentrum: 6 Ebenen tief. [https://www.youtube.com/watch?v=kd33UVZhnAA]

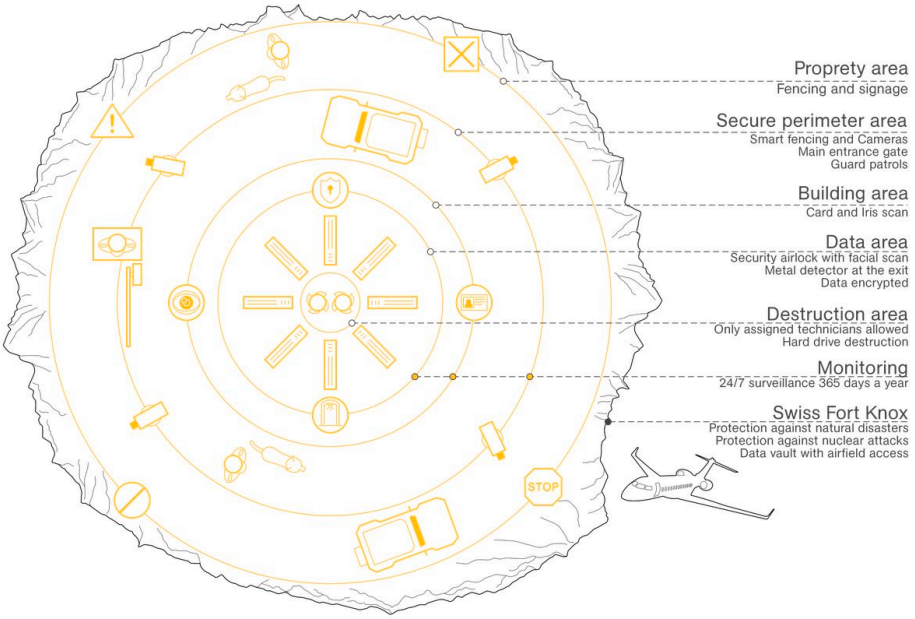


DESTRUCTION AREA FOR
HARDWARE DESTRUCTION
Source: Hunkeler Systeme - Schredder. [https://www.hunkelersysteme.com/produkte/schredder-und-zerkleinerer/]



MONITORING
Source: Sicherheit im Google-Rechenzentrum: 6 Ebenen tief. [https://www.youtube.com/watch?v=kd33UVZhnAA]

SWISS FORT KNOX



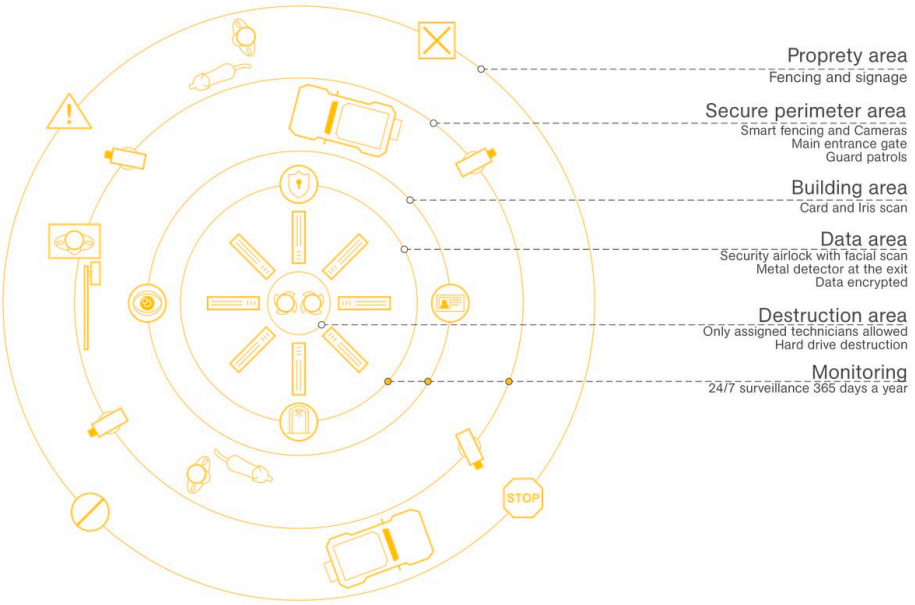
DIGITAL SECURITY: SWISS FORT KNOX
Scheme: Valentin Egger, 2025.

Swiss Fort Knox, owned by Mount10, is located in Saanen, in the Canton of Bern. Due to its territorial conditions this data centre includes even more security measures compared to a classical “above-ground” data centre, by providing direct access via its own airport. Additionally, due to its location within a bunker it is less exposed to aerial and local attacks and is self-supplied with power, water, or other important goods for the data centre for multiple days or weeks. This is comparable to Swiss “Stage IV” data centres which are built and maintained for the Swiss military and government to store and process information also during war times where the physical and digital security of publicly placed data centres cannot be trusted anymore.



SWISS FORT KNOX
Source: Valentin Egger, 2025.

PHYSICAL SECURITY: AN OVERVIEW



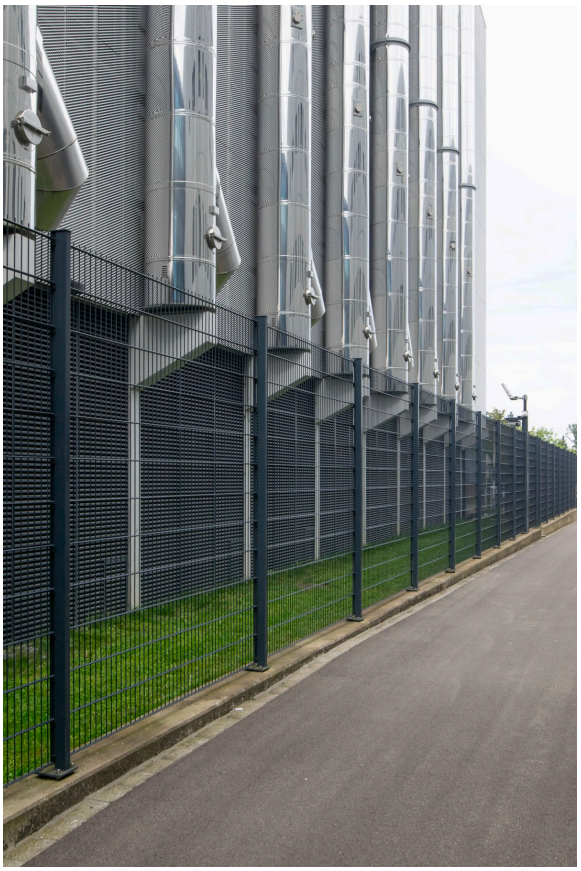
DIGITAL SECURITY.
Scheme: Valentin Egger, 2025.

Physical security concepts for protected buildings, in this case data centres, start with spatial boundaries, separating public from private land through fences and signage to create a securised “inner” space. This inner— and controlled—space, also called the “secure perimeter” is being controlled by patrolling personnel (depending on the object they might be supported by cars, dogs, etc…) supported by hard- and software such as cameras, motion detectors, smart sensors, and so on.

Within these secure perimeters the actual “object of interest,” for example a data centre, resides. Access to these buildings is usually possible through doors (either small ones for personnel or large ones that also allow access by vehicles for deliveries or pickups). These entries are surveilled by cameras and access is only possible with a badge, iris or fingerprint scan and other verification methods (for example a manual search of a car or truck) to authenticate and authorise users. This should also include the verification of a person’s tasks and its access needed for it (this might also include a “bodyguard” to enforce a four-eye principal on what happens within this building or an area of it).

The destruction area refers to the area where the hard disks are destroyed. It is important to acknowledge that data centres offer areas for customers to destroy their hard drives in case they want certain data to disappear without the risk of losing them, having them stolen, or copied. Therefore, the destruction area is only accessible for assigned technicians.

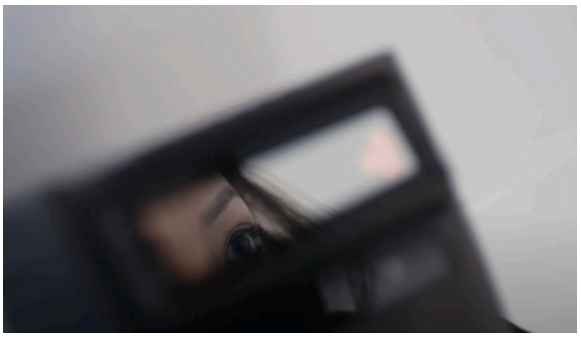
Within the following “entry-area” of a building there is a monitoring area, used for verification and strict surveillance of people. Sometimes this includes airport-like scanners for personnel and baggage to keep out any dangerous devices or software. The final access is then again a door (usually a very thick and secure one) with badge or biometrical readers, a man lock, and other security measures to ensure that only allowed technicians and customers can enter the final “server-area” of the data centres. There might be multiple nested security areas like this one to ensure an even finer separation of customers and employees.



PROPERTY AREA FENCING
Source: Studio Resources, 2025.



SECURE PERIMETER AREA CAMERAS
Source: Studio Resources, 2025.



BUILDING AREA IRIS SCAN
Source: Sicherheit im Google-Rechenzentrum: 6 Ebenen tief. [https://www.youtube.com/watch?v=kd33UVZhnAA]



DATA AREA SECURITY AIRLOCK
AND METAL DETECTOR
Source: Sicherheit im Google-Rechenzentrum: 6 Ebenen tief. [https://www.youtube.com/watch?v=kd33UVZhnAA]

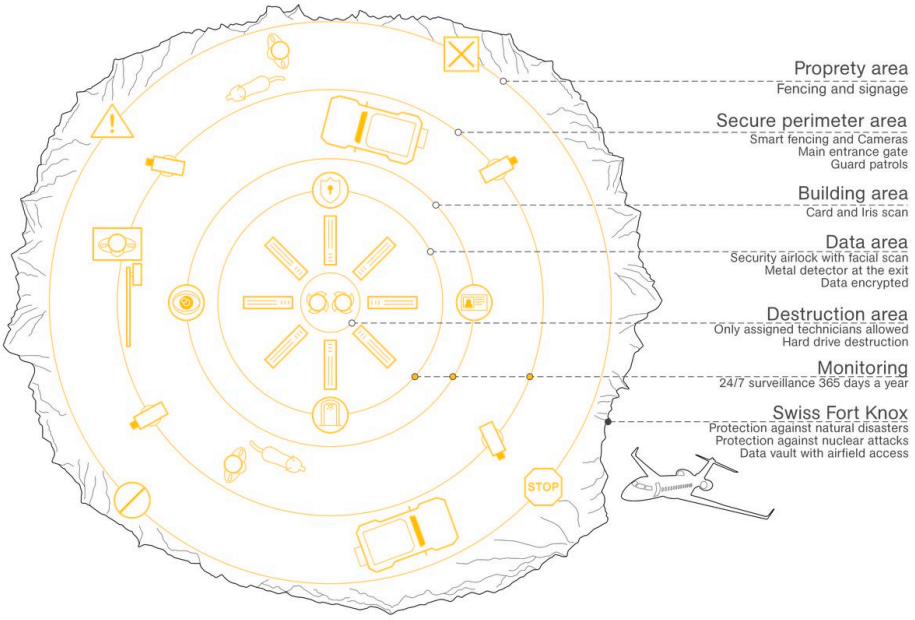


DESTRUCTION AREA FOR
HARDWARE DESTRUCTION
Source: Hunkeler Systeme - Schredder. [https://www.hunkelersysteme.com/produkte/schredder-und-zerkleinerer/]



MONITORING
Source: Sicherheit im Google-Rechenzentrum: 6 Ebenen tief. [https://www.youtube.com/watch?v=kd33UVZhnAA]

SWISS FORT KNOX



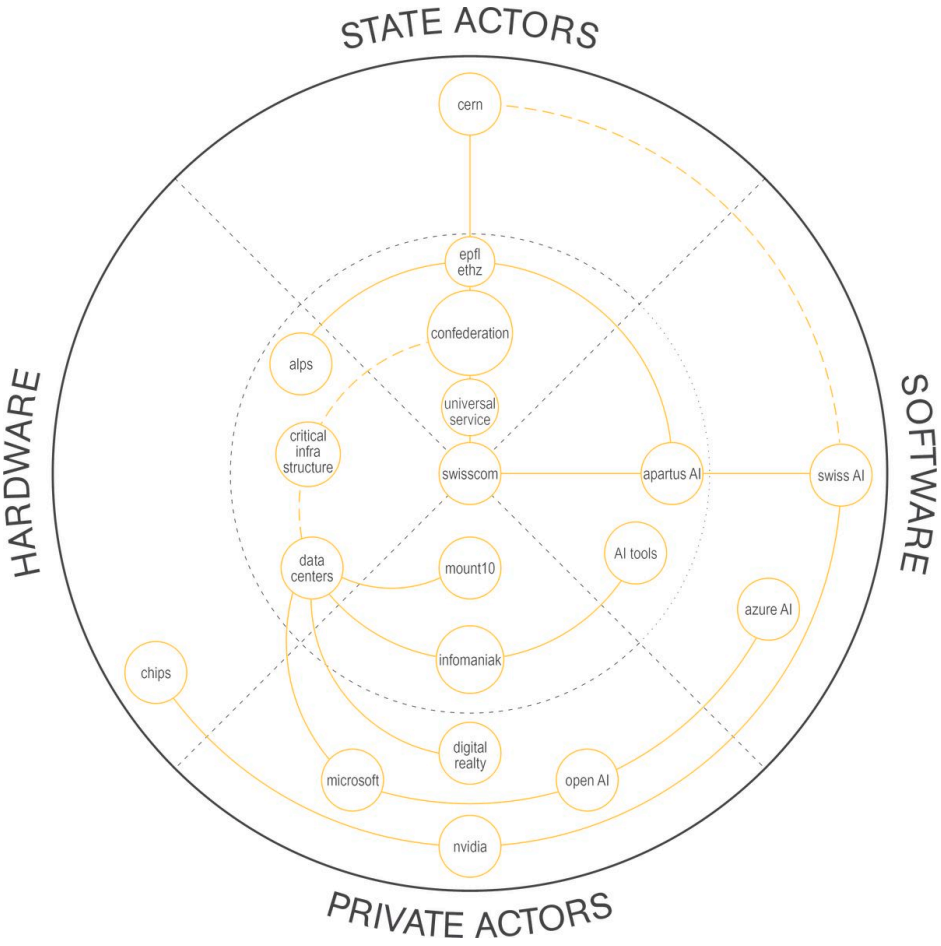
DIGITAL SECURITY: SWISS FORT KNOX
Scheme: Valentin Egger, 2025.

Swiss Fort Knox, owned by Mount10, is located in Saanen, in the Canton of Bern. Due to its territorial conditions this data centre includes even more security measures compared to a classical “above-ground” data centre, by providing direct access via its own airport. Additionally, due to its location within a bunker it is less exposed to aerial and local attacks and is self-supplied with power, water, or other important goods for the data centre for multiple days or weeks. This is comparable to Swiss “Stage IV” data centres which are built and maintained for the Swiss military and government to store and process information also during war times where the physical and digital security of publicly placed data centres cannot be trusted anymore.



SWISS FORT KNOX
Source: Valentin Egger, 2025.

Sovereignty on the Radar



DIFFERENT ACTORS SWISS CLOUD AND SWISS AI. Scheme: Valentin Egger, 2025.

Having gained an understanding of how the Swiss Confederation manages and protects its data, this section focuses on the connections between the various actors that make up the Swiss digital landscape.
It is important to identify the public and private actors and their actions in the software and hardware domains.

PUBLIC ACTORS

First, as the main stakeholder of Swiss sovereignty, the Confederation must ensure that a basic telecommunication service is available to the entire population and in all regions of the country. This universal service was delegated in 2023 to Swisscom, the largest telecommunications operator in Switzerland. The semi-private company has been offering an AI platform that facilitates access to and the use of AI models for Swiss companies since 2024.

To encourage AI innovation and sovereignty, the Confederation supports and funds the Swiss Federal Institute of Technology. For this purpose, EPFL and ETH Zurich have access to public infrastructures such as the Alps supercomputer in Lugano.

The computing power of the supercomputer has allowed these institutions to develop a large-scale open model named Apertus, which is intended to reflect Swiss values of transparency, multilingualism, and responsibility. This model is made available via Swisscom's platform.

Moreover, Swiss public institutions also collaborate with European scientific bodies such as the CERN (Conseil européen pour la recherche nucléaire). While CERN is not a direct partner of the Swiss AI Platform, it partly benefits from it and contributes within the scope of its research.

PRIVATE ACTORS

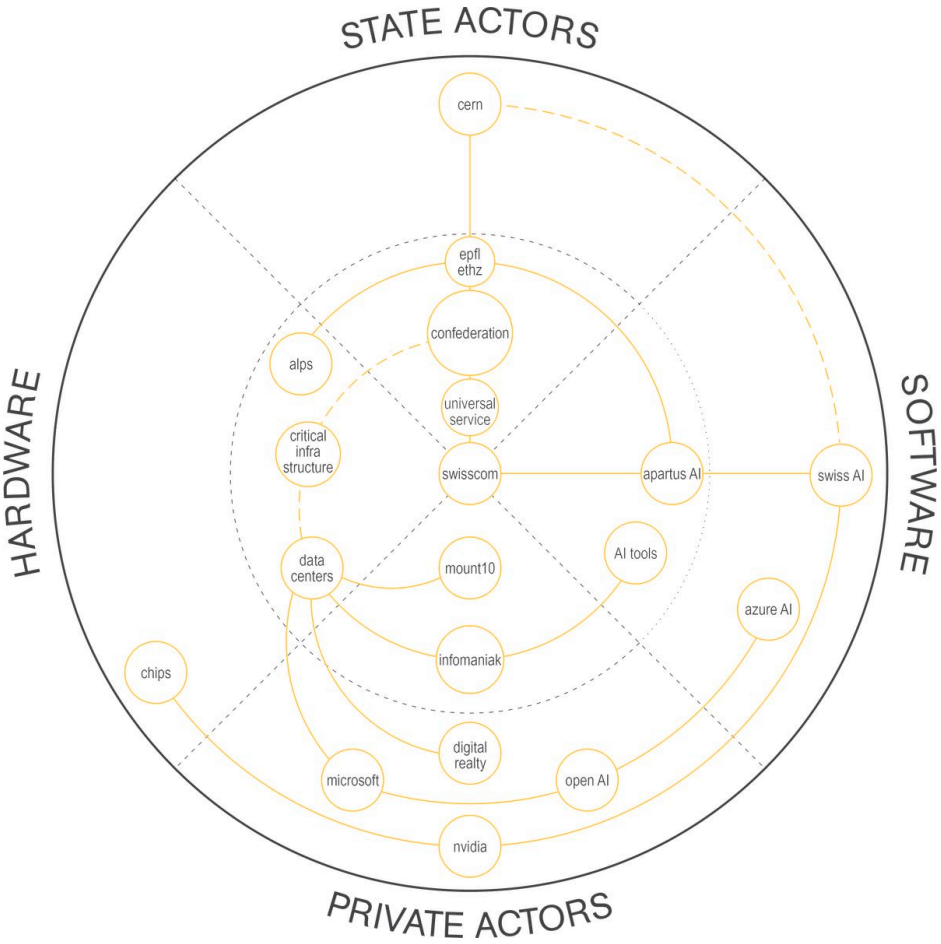
International private actors play an important role in Switzerland's digital ecosystem. Amongst them most important stakeholder remains the company NVIDIA.

NVIDIA is the world leader in making and providing the chips necessary for training and running large artificial intelligence models. The American company is a partner of Swisscom on the AI platform.

Other private actors include Swiss companies which compete with Swisscom such as Infomaniak. The Swiss tech company offers a platform of sovereign AI tools as well, ensuring that data which is produced in Switzerland is also hosted in Swiss data centres.

OpenAI recognised the concern of data sovereignty. Thereupon, it partnered with microsoft for their AI model Azure. That way Swiss data resides in Switzerland as well. The same strategy is adopted by other international and nationwide private actors, such as Digital Realty and Mount10, which is the owner of the alpine bunker data centre Swiss Fort Knox.

The Confederation defines a list of critical infrastructures, considered essential for the proper functioning of Switzerland. Private actors that host sensitive state data or other critical information benefit from logistical and regulatory support from the government.



DIFFERENT ACTORS SWISS CLOUD AND SWISS AI. Scheme: Valentin Egger, 2025.

Having gained an understanding of how the Swiss Confederation manages and protects its data, this section focuses on the connections between the various actors that make up the Swiss digital landscape.
It is important to identify the public and private actors and their actions in the software and hardware domains.

PUBLIC ACTORS

First, as the main stakeholder of Swiss sovereignty, the Confederation must ensure that a basic telecommunication service is available to the entire population and in all regions of the country. This universal service was delegated in 2023 to Swisscom, the largest telecommunications operator in Switzerland. The semi-private company has been offering an AI platform that facilitates access to and the use of AI models for Swiss companies since 2024.

To encourage AI innovation and sovereignty, the Confederation supports and funds the Swiss Federal Institute of Technology. For this purpose, EPFL and ETH Zurich have access to public infrastructures such as the Alps supercomputer in Lugano.

The computing power of the supercomputer has allowed these institutions to develop a large-scale open model named Apertus, which is intended to reflect Swiss values of transparency, multilingualism, and responsibility. This model is made available via Swisscom's platform.

Moreover, Swiss public institutions also collaborate with European scientific bodies such as the CERN (Conseil européen pour la recherche nucléaire). While CERN is not a direct partner of the Swiss AI Platform, it partly benefits from it and contributes within the scope of its research.

PRIVATE ACTORS

International private actors play an important role in Switzerland's digital ecosystem. Amongst them most important stakeholder remains the company NVIDIA.

NVIDIA is the world leader in making and providing the chips necessary for training and running large artificial intelligence models. The American company is a partner of Swisscom on the AI platform.

Other private actors include Swiss companies which compete with Swisscom such as Infomaniak. The Swiss tech company offers a platform of sovereign AI tools as well, ensuring that data which is produced in Switzerland is also hosted in Swiss data centres.

OpenAI recognised the concern of data sovereignty. Thereupon, it partnered with microsoft for their AI model Azure. That way Swiss data resides in Switzerland as well. The same strategy is adopted by other international and nationwide private actors, such as Digital Realty and Mount10, which is the owner of the alpine bunker data centre Swiss Fort Knox.

The Confederation defines a list of critical infrastructures, considered essential for the proper functioning of Switzerland. Private actors that host sensitive state data or other critical information benefit from logistical and regulatory support from the government.

Conclusion

Data sovereignty concerns everyone who has a smartphone. While the majority in Switzerland is affected, the Swiss population narrowly accepted the federal act on having an E-ID. On a governmental level there are strategies that are meant to lead Switzerland towards digital sovereignty. However, a certain interdependency already exists with and within the tech-ecosystem, intertwined between private and public stakeholders. Considering geopolitical tensions, spatial aspects, and Switzerland's reputation and identity as a secure island in the heart of Europe, the country remains unthreatened in the era of intelligence and AI. Mount10 embodies the peak of security with their data centre Swiss Fort Knox being located in a former military bunker in the Swiss alps. Between the love-hate relationship towards the tech-industry, the entanglement of private and public actors and geopolitical tensions, the question remains how much sovereignty can be promised and if the world's most secure data centre Swiss Fort Knox sets an example for future data centre designs or if it is just a seized opportunity in favor of Mount10 and their marketing strategy of Swiss Fort Knox.

Data sovereignty concerns everyone who has a smartphone. While the majority in Switzerland is affected, the Swiss population narrowly accepted the federal act on having an E-ID. On a governmental level there are strategies that are meant to lead Switzerland towards digital sovereignty. However, a certain interdependency already exists with and within the tech-ecosystem, intertwined between private and public stakeholders. Considering geopolitical tensions, spatial aspects, and Switzerland's reputation and identity as a secure island in the heart of Europe, the country remains unthreatened in the era of intelligence and AI. Mount10 embodies the peak of security with their data centre Swiss Fort Knox being located in a former military bunker in the Swiss alps. Between the love-hate relationship towards the tech-industry, the entanglement of private and public actors and geopolitical tensions, the question remains how much sovereignty can be promised and if the world's most secure data centre Swiss Fort Knox sets an example for future data centre designs or if it is just a seized opportunity in favor of Mount10 and their marketing strategy of Swiss Fort Knox.

SOURCES

- “Acceptance of Federal Act on E-ID.” Swiss Federal Administration. Accessed October 18, 2025. https://www.news.admin.ch/de/newnsb/05OCMKFwymouJPy8DLkwm
- Amazon Web Services. “Global Infrastructure.” Accessed October 18, 2025. https://aws.amazon.com/de/about-aws/global-infrastructure/
- “Bundesdaten in der Cloud: Gefährliche Abhängigkeit vom Ausland.” *NZZ* online. Accessed October 18, 2025. https://www.nzz.ch/wirtschaft/bundesdaten-in-der-cloud-gefaehrliche-abhaengigkeit-vom-ausland-ld.1651398
- “Cloud-Auftrag des Bundes: Geheimhaltungs-Daten sollten nicht im Ausland gelagert werden.” *SRF* News. Accessed October 18, 2025. https://www.srf.ch/news/schweiz/cloud-auftrag-des-bundes-geheimhaltungs-daten-sollten-nicht-im-ausland-gelagert-werden
- “Cloud Services and Architecture.” Bundeskanzlei (Swiss Federal Chancellery). Accessed October 18, 2025. https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html
- ETH Zürich. “Apertus: A Fully Open, Transparent, Multilingual Language Model.” October 2, 2025. Accessed October 11, 2025. https://www.apertus.ethz.ch
- Federal Communications Commission. “Universal Service.” January 10, 2024. Accessed October 11, 2025. https://www.bakom.admin.ch/universal-service
- Federal Office for Civil Protection. “Critical Infrastructures.” July 20, 2023. Accessed October 11, 2025. https://www.babs.admin.ch/en/critical-infrastructures.html
- “Global Locations.” Alibaba Cloud. Accessed October 18, 2025. https://www.alibabacloud.com/de/global-locations?_p_lc=1
- Google. “Daten weltweit mit branchenführenden Sicherheitslösungen schützen. Google Rechenzentren.” Accessed October 11, 2025. https://datacenters.google/intl/de_ALL/advancing-security/
- Heath, Nick. “This European Military Just Ditched Microsoft for Open-Source LibreOffice — Here’s Why.” *ZDNet*, September 18, 2025. Accessed October 11, 2025. https://www.zdnet.com/article/this-european-military-just-ditched-microsoft-for-open-source-libreoffice-heres-why/
- Infomaniak. “Sovereign and Open Source AI on Demand.” Accessed October 11, 2025. https://www.infomaniak.com/en/ai-tools
- “Microsoft Data Center Locations.” Microsoft. Accessed October 18, 2025. https://datacenters.microsoft.com/globe/explore?view=map
- Microsoft Switzerland. “Microsoft Announces Availability of Azure OpenAI Service in Swiss Data Center, Accelerating AI Innovation in Switzerland.” September 18, 2023. Accessed October 11, 2025. https://news.microsoft.com/de-ch/2023/09/18/microsoft-announces-availability-of-azure-openai-service-in-swiss-data-center-accelerating-ai-innovation-in-switzerland/?utm_source=chatgpt.com
- “Oracle Public Cloud Regions.” Oracle. Accessed October 18, 2025. https://www.oracle.com/de/cloud/public-cloud-regions/
- “Overview of IBM Cloud Locations.” IBM Cloud. Accessed October 18, 2025 [https://cloud.ibm.com/docs/overview?topic=overview-locations&locale=de
- “Public Clouds des Bundes.” Bundeskanzlei (Swiss Federal Chancellery). Accessed October 18, 2025. https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud/public-clouds-bund.html
- “Ärger um neue Rechenzentren der Schweizer Armee – das musst du wissen.” *Watson*. April 2022. https://www.watson.ch/digital/schweiz/191049306-aerger-um-neue-rechenzentren-der-schweizer-armee-das-musst-du-wissen
- Schweizerische Eidgenossenschaft. “Cloud-Strategie der Bundesverwaltung.” *Informatiksteuerungsorgan des Bundes ISB*. 11 December 2020.
- Schweizerische Eidgenossenschaft. “Strategie Rechenzentren der zivilen Bundesverwaltung.” *Bundeskanzlei BK*. 9 June 2025

- Swisscom. “The Secure Swiss AI Platform with Comprehensive Data Protection.” Accessed October 11, 2025. https://www.swisscom.ch/en/business/ai-platform.html
- “Swiss Fort Knox: Europas sicherstes Datenzentrum.” MOUNT10 AG. Accessed October 18, 2025. https://mount10\.ch/ueber-uns/swiss-fort-knox/
- “Swiss Government Cloud.” Bundeskanzlei (Swiss Federal Chancellery). Accessed October 18, 2025. https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud/swiss-cloud.html

This work by Esma Alili, Timo Feddern, Joanna Druey, and Valentin Egger was created as part of the design studio The Production of Cloud at ETH Zurich in Fall 2025. The PDF is intended for educational purposes only. Its commercial distribution is strictly forbidden.

© 2026, Architecture of Territory

Architecture of Territory
Professor Milica Topalović

TEACHING TEAM
Martin Kohlberger
Yiqiu Liu
Jakob Walter
Jan Westerheide

Prof. Milica Topalović
ETH Zurich
ONA G41
Neunbrunnenstrasse 50
8093 Zurich
Switzerland
+41 (0)44 633 86 88
www.topalovic.arch.ethz.ch