Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Chancellery FCh

13. December 2024

Monitoring report on Digital Switzerland Strategy 2024

Reference number: 831-3/9/4

BK-D-D0DA3401/834

Table of contents

1 Introduction

The Digital Switzerland Strategy sets the guidelines for Switzerland's digital transformation. It is binding for the Federal Administration. For other stakeholders such as cantons, communes, business, science and civil society, it serves as a guide on how best to take the opportunities presented by digital change and use them for the benefit of all. The Digital Switzerland Strategy provides a framework in the sense of an umbrella strategy for the Digital Federal Administration Strategy, the Digital Public Services Switzerland Strategy and for sectoral and cantonal strategies.

A key element of the strategy are the focus topics which the Federal Council uses to set political digitalisation priorities each year. On a supplementary basis, five domains are derived from the EU Digital Compass[1]. The monitoring report prepared by the DTI Sector of the Federal Chancellery shows which measures the competent administrative units have implemented in the past year and briefly summarises the status of the digital transformation.

2 Focus topics in 2024

2.1 Focus topic 'Electronic interfaces (APIs)'

Lead administrative unit: Digital Transformation and ICT Steering (DTI)

Electronic interfaces, or APIs (application programming interfaces), serve as the technical connections between digital applications, making data and services electronically accessible. A new application can access existing data and functionalities thanks to these interfaces. APIs are also of major importance to the business sector, since they make it possible to link companies' own applications with federal data. A well-known example is the integration of weather data from MeteoSwiss into numerous applications. APIs were chosen as one of the focus topics of the Digital Switzerland Strategy 2024 in connection with the coming into force of the EMOTA (Federal Act on the Use of Electronic Means to Carry Out Official Tasks), which legally requires the provision of interfaces for the Federal Administration.

2.1.1 Implementation status

In 2024, the emphasis was on the following activities:

- Defining basic principles for interface development: Adaptation of international developer guidelines (for interfaces) to Switzerland. These guidelines were published in the GitHub code repository[2].

- Organising events on the development and use of interfaces: The aim is to increase the number of interfaces so that companies can build innovative and data-based business models and enable Switzerland to make data-based decisions more quickly in all situations, including crises. In two hackathons[3], Switzerland was invited to develop API-related solutions in response to specific challenges.

- Study on API management: A study was conducted to analyse which services the Federal Administration requires for the development and operation of interfaces. The study lays the foundation for establishing overarching infrastructures for APIs and tapping into synergies.

[1] Europe's digital decade: 2030 targets | European Commission

[2] GitHub - swiss/api-guidelines: Federal Administration API Guidelines

[3] [1] GovTech Hackathon organised by the Federal Chancellery GovTech Hackathon 2024 (admin.ch) and [2] SwissHacks organised by the Financial Innovation Desk SwissHacks 2024

- Security guidelines: The National Cyber Security Centre (NCSC), which is responsible for the focus topic of cybersecurity, and the Federal Chancellery have jointly developed security guidelines for electronic interfaces. These Security Guidelines are also published.

2.1.2 Outlook

In the coming years, the defined principles must be utilised by the administration, business and science to design, develop and document interfaces in Switzerland. Only if data and services in Switzerland are accessible electronically via APIs can the potential of digitalisation be fully exploited, e.g. in artificial intelligence (AI).

2.1.3 Conclusion

The first steps have now been taken; important foundations have been laid, particularly with the activities surrounding the federal government's digitalisation strategy and the coming into force of the EMOTA on 1 January 2024. Other challenges remain. These include in particular:

- Legal uncertainties in the context of data use: e.g. how data can be used multiple times under the applicable Data Protection Act, definition of adequate anonymisation of data, data use in the context of AI, etc.
- The insufficient availability of registers for shared (master) data or the lack of data quality.
- The lack of API culture and the non-provision of APIs by organisations under private law.
- The asymmetry of use: the API provider mainly incurs costs for the operation of the API, while the benefit lies mainly with the users.
- The comprehensive documentation of interfaces.

Important challenges have been addressed. For example, the Federal Office of Justice (FOJ) is in the process of developing a legal basis for the secondary use of data (in fulfilment of motion 22.3890 Framework Act for the Secondary Use of Data). The Federal Chancellery is working with the Federal Office of Communications, the Federal Statistical Office and the Directorate of International Law to set up a contact point for data spaces, which is due to commence operations on 1 January 2025. Other topics must be addressed by the individual federal offices and departments, research centres and companies. For example, they themselves must be responsible for building APIs and documenting them. Finally, interfaces are able to realise their full potential only if they can be found and used.

2.1.4 Appraisal

Significant progress was made in the area of electronic interfaces (APIs) in 2024. International guidelines have been adapted for Switzerland, and documentation has been published on GitHub. Events and hackathons promoted the development and use of interfaces. A study analysed the services required to set up and operate interfaces in the Federal Administration. Security guidelines for electronic interfaces were developed and published by the National Cyber Security Centre and the Federal Chancellery. APIs are becoming increasingly relevant, and it is crucial to utilise their potential in making the benefits of data and existing programme functions accessible to others.

The number of available and published APIs must be increased so that the digitalisation of Switzerland can build on them. The growth of available interfaces must therefore be significantly increased. The administration must lead the way, implementing the API-first approach and consistently building accessible specialist applications.

2.2 Focus topic ‘Swiss approach to regulating AI systems’

Lead administrative unit: Federal Office of Communications (OFCOM)

In its decree of 22 November 2023, the Federal Council commissioned the preparation of an overview of possible regulatory approaches for AI in Switzerland. A discussion paper is to be drawn up by the end of 2024; the paper will be accompanied by an overview, i.e. a public report. The work is open-ended. The aim is to create a decision-making basis for the Federal Council so that it can commission regulatory work and define responsibilities as needed starting in 2025.

2.2.1 Implementation status

Detailed baseline analyses are necessary for the overview. The following analyses were prepared by summer 2024:

- Analysis of AI regulation in 18 selected countries: Very different regulatory approaches have been taken around the world. So far, only a few countries have legally binding AI-specific regulatory instruments that have already been adopted. Like Switzerland, most countries are in a phase of discussion or negotiation on how to approach AI regulation.
- Baseline legal analysis: With regard to the Council of Europe's AI Convention, the FOJ's work shows that certain adjustments to Swiss law would be necessary if Switzerland were to ratify the Convention, particularly in the areas of transparency, protection against discrimination, complaints mechanisms and monitoring mechanisms. The EU's AI Act aims to regulate the EU internal market while guaranteeing fundamental rights in the EU. The AI Act takes a product safety approach. If products contain AI, the AI Act is applicable in the EU. It does not currently apply in Switzerland. However, Swiss companies operating in the EU will have to comply with its rules. This will create new trade barriers for exports to the EU.
- Economic and European policy analysis: Switzerland has a mutual recognition agreement (MRA) with the EU on conformity assessments for products in 20 sectors. 12 of the 20 product sectors under the MRA are affected by the EU's AI regulation, given that the AI Act sets out harmonised rules for the placing on the market, putting into service and use of AI systems that are safety components of these products or are themselves such products. In the 12 product sectors affected by the AI Act, the technical regulations of Switzerland and the EU are recognised as equivalent. Conformity assessments for the EU internal market can be carried out by a Swiss conformity assessment body (CAB) recognised by the agreement in accordance with Swiss technical regulations. In order to avoid new technical barriers to trade, Switzerland would have to harmonise its product regulations in these product sectors with those in the AI Act and update the MRA.
- Regulatory activities in the sectors: OFCOM carried out an online survey of 66 administrative offices. The survey revealed that so far, only a few federal agencies have made legal adjustments to their AI responsibilities (FEDRO, FOCBS). In principle, the technology neutrality of existing standards also means that they can be applied to AI. The amendments made to the existing law so far were necessitated in part by the requirements of the new Data Protection Act. As a result, half of the administrative units are planning in-depth clarifications and, if necessary, legal adjustments. Most respondents indicated that a purely sectoral regulatory approach to AI is not sufficient, although they have not examined this in depth.
- Monitoring of AI guidelines: In November 2020, the Federal Council adopted guidelines for the Federal Administration in dealing with AI. The guidelines serve as an orientation aid, especially for the evaluation and use of AI solutions. In March 2024, OFCOM conducted a survey on the current status of the guidelines in the Federal Administration. The survey shows that the AI guidelines are well known and are actively used as a framework for dealing with AI. However, just over a third of respondents see a need for adaptation, given that the general wording of the guidelines is of only limited help in organising specific projects, and an increasing need for guidance exists.

Based on these results, various regulatory approaches for AI in Switzerland will be developed by autumn 2024. The Federal Council aims to discuss these approaches and further work by the end of the year.

2.2.2 Outlook

The work on the overview serves as a basis for further activities on possible AI regulation in Switzerland. As of July 2024, the regulatory approach chosen by the Federal Council is still open.

In order to avoid new technical barriers to trade with the EU, Switzerland would have to harmonise its product regulations in several product sectors with those in the AI Act and update the mutual recognition agreement on conformity assessments (MRA). From today's perspective, extending the MRA to include AI aspects would depend on successful conclusion of the ongoing negotiations with the EU. Ratification of the Council of Europe's AI Convention would also involve amendments to Swiss law.

Within the Federal Administration, strategic considerations on the use of AI in administrative activities and the question of how AI should be coordinated within the Federal Administration will be on the agenda in 2025.

It also appears necessary to update the Federal Council's AI guidelines and make them more specific.

2.2.3 Conclusion

The baseline analyses have laid the foundations for AI regulation in Switzerland. Cooperation between the departments has been valuable. Numerous aspects of AI use, such as transparency requirements and protection against discrimination, are being demanded by various stakeholder groups; what is expected of the Federal Administration is accordingly high. Building on these results, further steps must be taken to protect people's fundamental rights, including economic freedom, and to strengthen Switzerland as an innovation hub.

2.2.4 Appraisal

In 2024, important progress was made on the focus topic of AI, including a baseline legal analysis as a basis for further measures (see implementation status). A discussion on possible regulatory approaches for Switzerland is planned. AI will continue to gain in importance in the coming years. Switzerland must recognise and exploit the opportunities offered by AI without underestimating the risks. This requires a continuation of the discussion about the optimal degree of regulation of AI systems.

2.3 Focus topic ‘Cybersecurity’

Lead administrative unit: National Cyber Security Centre (NCSC)

2.3.1 Implementation status

The focus topic of cybersecurity was implemented through the following measures:

- Drafting of the Cybersecurity Ordinance: On 29 September 2023, Parliament adopted a reporting obligation for cyberattacks on critical infrastructure (e.g. hospitals, energy suppliers and authorities). Amendments to the Information Security Act also define the tasks of the new National Cyber Security Centre (NCSC). In the first quarter of 2024, the implementing provisions for these legislative amendments were drawn up in the Cybersecurity Ordinance. The Federal Council opened consultation proceedings on 22 May 2024.
- Election of the NCS Steering Committee: On 5 April 2023, the Federal Council approved the National Cyberstrategy (NCS) and decided that – as with the first two strategies (2012-18 and 2018-22) – a steering committee (NCS SC) should be set up. As a cross-cutting issue, cybersecurity affects many areas. The NCS should therefore be managed by a committee that brings together a variety of skills and promotes cooperation between the various stakeholders. On 7 June 2023, the DDPS set up the NCS Steering Committee and tasked it with regularly reviewing the NCS and drawing up adjustment proposals for the attention of the Federal Council, defining priorities and timetables together with those responsible for implementation, drawing up proposals for supplementary measures and reporting on NCS implementation.

- Cybersecurity at major events: Major events and international conferences, such as the WEF Annual Meeting or the high-level Summit on Peace in Ukraine on 15-16 June 2024 at the Bürgenstock resort, have an impact on the cyberthreat situation. It is highly likely that events of this kind will increasingly be seen as an opportunity to stage a cyberattack or that participants and their organisations will become the target of such attacks. At both the WEF Annual Meeting and the Bürgenstock Summit, the NCSC ensured the coordination of all participating partner organisations from the cantons, the federal government and the private sector. The deployment plans now in place serve as a basis for future deployments.
- Cyber Europe exercise: From 18 to 20 June 2024, the Cyber Europe 2024 exercise took place with a focus on the energy sector. Switzerland took part as a co-organiser and major partner. Under the leadership of the NCSC, other federal authorities and around 30 organisations from the Swiss energy sector were involved.
- National awareness campaign S-U-P-E-R: Under the slogan 'Improve your digital health', the S-U-P-E-R.ch campaign took place in April 2024 with a focus on updates and virus protection. The campaign echoes the healthy-living trend that has been popular for several years. It was organised by the NCSC, the SCP and the cantonal and communal police forces, supported by the Swiss Internet Security Alliance and EBAS (eBanking – but secure!). On a range of communication channels, the themes of fitness and health were used to illustrate that not only the body must be kept fit, but software too. The S-U-P-E-R.ch campaign website provided further information on the topic, and visitors to the site were able to take a quiz to see how much they had learnt.
- Conclusion of the consultation on the Cybersecurity Ordinance: The consultation on the Cybersecurity Ordinance ends on 13 September 2024. The results of the consultation will be analysed, and the revised ordinance will be submitted to the Federal Council for approval. This will also enable the Federal Council to enact the amendments to the ISA, introducing a reporting obligation for cyberattacks.
- Hosting of the National Cybersecurity Conference: On 26 September 2024, the National Cybersecurity Conference 2024 will take place with a focus on cybersecurity between geopolitics and day-to-day operations. The conference is organised by the NCSC and the Swiss Security Network (SSN).
- Publication of postulate report on ransomware: In the second half of 2024, the report on Postulate 21.4512 Graf-Litscher 'Measures for better protection against ransomware attacks' (lead NCSC) will be published.

2.3.2 Outlook

The need for action in cybersecurity continues to be very high. Cybersecurity remains a crucial prerequisite for successful digitalisation. New technologies (e.g. AI) and increasing geopolitical tensions entail additional challenges for cybersecurity.

2.3.3 Conclusion

With the creation of the National Cyber Security Centre, the National Cyberstrategy and its steering committee, the necessary structures for implementation of cybersecurity measures are in place. Because the topic continues to develop dynamically, ongoing monitoring is crucial. Given that cybersecurity is a cross-cutting issue, the measures must be implemented jointly by all stakeholders from the cantons, the federal government, the private sector and universities.

2.3.4 Appraisal

Important progress was made in cybersecurity in 2024. This includes drafting the Cybersecurity Ordinance, setting up the NCS Steering Committee and organising the Cyber Europe exercise. The development of NCSC expertise in cybersecurity at major events such as the WEF Annual Meeting or the Bürgenstock Summit should also be emphasised, as Switzerland will regularly have to face similar challenges. The ongoing work and measures through the end of the year show that cybersecurity remains a focus and is constantly evolving. This is underscored by the hosting of the National Cybersecurity Conference in September and the response to numerous parliamentary procedural requests, such as the postulate report 21.4512 on ransomware. Switzerland must seize the opportunities offered by consistent cybersecurity at all federal levels, including the Federal Administration, given that the

global risks posed by cyberattacks will continue to increase. Continuing the discussion on optimal protection is essential, especially by raising the awareness of all employees of the administration.

3 Review: Domains for 2024

3.1 Education and skills domain

3.1.1 Indicators

Enhanced digital skills of the population in international comparison

Last updated	2023	42%
Development	Increase (2021: 40%)	
EU comparison	2023	27% (EU-27)

Source: FSO Omnibus Study; Eurostat

Proportion of ICT specialists in Switzerland

Last updated	2023	5.7% total; 4.7% men, 0.9% women
Development	Slight decline (2022: 5.7% total; 4.8% men; 0.9% women)	
EU comparison	2023	4.8% total; 3.85% men, 0.95% women (EU-27)

Source: FSO Omnibus Study and FSO SLFS Survey; Eurostat

Switzerland performs better than the EU in both metrics. The aim is to increase advanced digital skills to over 50% by 2030 and to double the proportion of women from 0.9% to 1.8%.

3.1.2 Measures in the action plan

By the end of August 2024, 9 of the 79 measures in the action plan had been assigned to the education and skills domain. Most of these measures, namely five, are being implemented by the EAER. Two measures come from the FDHA (FSO), and one measure each comes from the DETEC and ETH as an external measure. In particular, important programmes and projects are being continued, such as the 'Simply better!... in the workplace' programme, participation in international comparative studies such as the Programme for International Student Assessment (PISA) and the OECD's Survey of Adult Skills (PIAAC), and the Swiss Internet Governance Forum (IGF).

3.1.3 Conclusion

The aim of the domain is to provide people, businesses and public authorities with sufficient skills to make the most of new technologies and to evaluate them critically. In view of the shortage of skilled labour, this topic continues to be extremely relevant and is still being actively addressed. The proportion of the population with advanced digital skills has improved by 2 percentage points and now amounts to 42% of the population. Switzerland compares favourably with the EU, although it cannot be ruled out that there are certain uncertainties when comparing the indicators.

3.2 Security and trust domain

3.2.1 Indicators

Number of cyber incidents reported to the NCSC

Last updated	2023	49,380 incidents
Development	Increase of 14,853 reported incidents compared to the previous year (2022: 34,527 incidents)	
EU comparison	Not possible	

Source: NCSC

Digital crime; numbers by modus operandi

Last updated	2023	43,839 incidents
Development	Increase of 10,494 reported incidents compared to the previous year (2022: 33,345 incidents)	
EU comparison	Not possible	

Source: FSO Police crime statistics (PCS)

The two metrics in the security and trust domain show a significant increase in reports of cyber incidents (+43%) and digital crime (+30%). This trend has persisted for several years and probably indicates an increase in cyberattacks. At the same time, reporting of such incidents is increasingly becoming less taboo. Although there is no reporting obligation in Switzerland, the public and companies are increasingly recognising the importance of a coordinated fight against cybercrime. This can be seen as a vote of confidence in the public authorities. A comparison with the EU is not possible, however.

3.2.2 Measures in the action plan

By August 2024, 14 of the 79 measures in the action plan had been assigned to the security and trust domain. They come from all departments except the FDHA and the EAER. Two external measures are being implemented by ETH. The DDPS is implementing most of the measures: awareness campaigns on cyberthreats, implementation of mandatory reporting of cyberattacks on critical infrastructures, promotion of ethical hacking and further development of the Cyber-Defence Campus. In 2024, three measures for digital sovereignty were also included in the action plan pursuant to the 2023 focus topic.

3.2.3 Conclusion

The goal of this domain is for people in Switzerland to be able to move around safely in the digital environment and have their privacy protected. People bear primary responsibility for their own digital security, but public institutions must take action in situations where they are unable to protect themselves adequately. On a positive note, the Swiss people consider the authorities to be trustworthy and they report incidents. Investment in cybersecurity must continue unabated, given that threats evolve rapidly and attacks have a potentially devastating impact on the public, businesses and democracy.

3.3 Framework domain

3.3.1 Indicators

Switzerland's position in the digital competitiveness ranking in international comparison

Last updated	2024	Second place
Development	Improvement (2023: Fifth place)	
EU comparison	2024	Denmark: Third place, Denmark: Fifth place

Source: IMD World Digital Competitiveness Ranking

Proportion of new companies in the ICT sector compared to overall figure

Last updated	2022	4.9%
Development	Slight decrease (2021: 5.2%)	
EU comparison	No figures available (different data collected in the EU)	

Source: FSO Business Demography

The two indicators for the framework domain show Switzerland's digital competitiveness and new start-ups in the ICT sector. Switzerland moves up from 5th to 2nd place in digital competitiveness, behind Singapore and ahead of Denmark, the United States and Sweden. Company start-ups in the ICT sector showed a very slight decline of 0.3 percentage points, which lies within normal annual variability. More efforts and incentives are still needed to achieve the desired target of 6% by 2030, however.

3.3.2 Measures in the action plan

By August 2024, 11 of the 79 measures in the action plan had been assigned to the framework domain. They come from all departments except the DDPS and the FDF. AI is receiving the most attention with four projects being carried out as part of the focus topic on the Swiss approach to regulating AI systems. The financial sector is affected by two measures (Swiss Financial Innovation Desk FIND, digitalisation in the World Bank Group). Other measures concern, for example, digitalisation of healthcare and the agriculture and food industry, as well as Switzerland's role in defining international frameworks.

3.3.3 Conclusion

This domain aims to establish a reliable and advantageous framework for the digital environment that Swiss businesses and society can rely on. This is largely guaranteed in Switzerland. The potential need for AI regulation is being analysed carefully from different perspectives. As a small but strongly networked country, Switzerland takes every opportunity to actively shape international frameworks so as to benefit from them in the best possible way.

3.4 Infrastructures domain

3.4.1 Indicators

5G coverage (land area of Switzerland)

Last updated	2022	92%
Development	Strong increase (2021: 74%)	
EU comparison	Not possible: EU countries measure 5G coverage as a percentage of the population, not land area	

Source: OFCOM

Number of data sets available on opendata.swiss

Last updated	06/2024	11,930 data sets
Development	Increase of 2,424 data sets compared to the previous year (June 2023: 9,506 data sets)	
EU comparison	No comparative figures available (different data collection)	

Source: opendata.swiss

The two indicators in the infrastructures domain show that Switzerland is developing well in terms of physical and digital infrastructure. After two years of stagnation at 74% 5G coverage of the country's area, this metric has jumped to 92%. This exceeds expectations and leaves hardly any more room for improvement. Due to Switzerland's topography, it is neither necessary nor desirable to cover 100% of the country's area. Furthermore, the number of available data sets at opendata.swiss increased by 25% between mid-2023 and mid-2024.

3.4.2 Measures in the action plan

In 2024, 19 of the 79 measures in the action plan (around a quarter) have been assigned to the infrastructures domain. DETEC, as the infrastructure department, covers 11 measures in the areas of energy, mobility, construction, media and the internet. Four measures are being implemented by external players, namely relating to rail transport and mobility (SBB, ETH), payment transactions (SIX) and personalised medicine (ETH). The trust infrastructure for the e-ID, the mobility data infrastructure, the federal data science strategy and the DigiSanté programme also fall within this domain.

3.4.3 Conclusion

The objective of this domain is for public authorities to promote and operate reliable and resilient physical as well as digital infrastructures. Switzerland has a very good broadband infrastructure, an indis-

pensable basis for the development of digitalisation in all sectors. In the longer term, the federal government's Gigabit Strategy[4] will further improve the networks by levelling out the gap between central and peripheral regions. The digitalisation of other infrastructures will not be left out, given that strategies and programmes are being introduced and implemented in areas such as mobility, health, energy and construction. The coming years will be crucial for the digitalisation of infrastructures for the benefit of the public and businesses.

3.5 Digital public services domain

3.5.1 Indicators

User access to online public services

Last updated	2023	79%
Development	Slight increase (2022: 78%)	
EU comparison	2023	85%

Source: EU eGovernment Benchmark 2024, Background Report

Digital public services for businesses

Last updated	2023	73%
Development	Significant increase (2021: 62%)	
EU comparison	2023	82%

Source: EU eGovernment Benchmark 2024, Background Report

The EU scores better than Switzerland in both metrics. The Swiss values are considered ‘good’ (51% - 75%) and ‘very good’ (over 76%) according to the scoring grid used. The metric ‘Digital public services for businesses’ shows a significant increase compared to 2021. The aim here would be for Switzerland to achieve a score of very good (over 76 points) for both metrics by 2030. Note that the annual background report is not identical every year. The measure ‘Digital public services for businesses’ is surveyed only every second year.

3.5.2 Measures in the action plan

By August 2024, 25 of the 79 measures in the action plan (around a third) had been assigned to the digital public services domain. All departments are represented. The FDHA reported the most measures (6), e.g. in the area of Open Government Data (OGD), the National Address Service, or with the National Data Management (NaDB) programme. Interoperability and electronic interfaces (focus topic 2024) are the subject of four further measures. Preparatory work is also being carried out for future legislation on data reuse. Other projects for the digitalisation of public services include the ‘Hub consulaire’ and the Travel Admin App (FDFA), digitalisation of the Swiss judiciary, a notarial digitalisation act and the specialist applications eAsyl and eRetour (FDJP). The DDPS reported three measures relating to geoinformation, and the DETEC likewise reported three measures (model project for sustainable spatial development 2020–2024; promotion of digital licences in road traffic; FOEN programme agreements). Also noteworthy is the AGOV project, the authentication service of the Swiss authorities, which in turn will simplify access to many other digital services.

3.5.3 Conclusion

The aim of this domain is for public authorities to offer their services digitally as standard (‘digital first’). The range of digital public services is largely satisfactory and is growing steadily in Switzerland. In particular, the provision of digital public services for businesses has risen sharply from 62% to 74% in the last two years. The development in many other European countries has been faster and better, however. The success of these leading countries is based largely on important basic services such as e-

[4] People across the country should be able to access ultra high-speed Internet. The Federal Council is pursuing this goal with its Gigabit Strategy (Federal Gigabit Strategy (admin.ch))

IDs and centralised portals (one-stop shop solutions) and consistent implementation of the once-only principle (i.e. data is only entered once).

3.6 Overview of the development of the indicators

2020	2021	2022	2023	2024	Entwicklung
Enhanced digital skills of the population					
-	40%	-	42%	-	↗
Proportion of ICT specialists in Switzerland					
5.4%	5.5%	5.7%	5.7%	-	→
Women ICT specialists					
0.9%	0.9%	0.9%	0.9%	-	→
Men ICT specialists					
4.6%	4.6%	4.8%	4.7%	-	↘
Number of cyber incidents reported to the NCSC					
10'833	21'714	34'527	49'380	-	↗
Digital crime; numbers by modus operandi					
24'398	30'351	33'345	43'839	-	↗
Switzerland's position in the digital competitiveness ranking in international comparison					
6	6	5	5	2	↗
Proportion of new companies in the ICT sector compared to overall figure					
5.1%	5.2%	4.9%	-	-	↘
5G coverage (land area of Switzerland)					
74%	74%	92%	-	-	↗
Number of data sets available on opendata.swiss					
-	5886	6'744	9'506	11'930	↗
User access to online public services					
64/100	63/100	78/100	79/100	-	↗
Digital public services for businesses					
-	62%	-	73%	-	↗

4 Overall conclusion of the 2024 Monitoring Report

In 2024, significant progress was made in Switzerland in electronic interfaces (APIs), AI regulation and cybersecurity.

Focus topic ‘APIs’: The first important steps here are the federal digitalisation strategy and the coming into force of the EMOTA. Several challenges remain, however, including [1] legal uncertainties in the context of data use, [2] insufficient availability of registers and [3] asymmetry of use.

Focus topic ‘AI regulation’: The analyses have laid the foundations for AI regulation in Switzerland. Switzerland must recognise and exploit the opportunities offered by AI without underestimating the risks.

Focus topic ‘Cybersecurity’: Important progress was made in the area of cybersecurity, such as [1] drafting the Cybersecurity Ordinance, [2] appointing the NCS Steering Committee, [3] carrying out the Cyber Europe exercise and [4] developing NCSC expertise in cybersecurity at major events.

The increased use of APIs, the drafting of the Cybersecurity Ordinance and the active approach to AI regulation show that Switzerland is proactively tackling the challenges of digital transformation.

Of the five domains, Switzerland still has the greatest need to catch up in terms of digital public services, where it still lags behind the EU. With the upcoming introduction of the e-ID as an essential basic

service and the further development of standardisation and interoperability, however, the gap should soon be closed.

Continuous public awareness-raising and the cooperation of all federal levels are crucial in shaping the digital transformation safely and efficiently. Despite this progress, there is still a need for action, particularly in the implementation and expansion of digital infrastructures and public services (which are in fact in demand). Switzerland remains committed to securing its international competitiveness and making full use of the opportunities offered by digitalisation.

The 2024 Monitoring Report will be published on the Digital Switzerland website (www.digital.swiss).