Regulatory Impact Assessment: Revision of the SPTO

Michael Altorfer
Dr. Samuel Rutz
Dr. Michael Funk
Noé Arnold
Lukas Grether

Report commissioned by FONGIT

26.05.2026

ISSN 2235-1868

Meta information

Title:	Regulatory Impact Assessment: Revision of the SPTO
Version:	V1
Date:	26.05.2026
Authors:	Michael Altorfer, Noé Arnold, Michael Funk, Lukas Grether, Samuel Rutz
Contact:	Samuel Rutz, +41 79 204 78 83, samuel.rutz@swiss-economics.ch

Ottikerstrasse 7, 8006 Zürich
www.swiss-economics.ch

Abstract

Switzerland has established itself as a leading location for business models based on digital trust. This is thanks to its political neutrality and stability, its pragmatic regulatory approach, and its access to skilled talent. Even without a comprehensive digital strategy, the existing framework has provided sufficient legal certainty and predictability to foster innovation in areas such as cybersecurity, secure communications, and cloud services.

This report examines the economic implications of the proposed revision of the Ordinance on the Surveillance of Post and Telecommunications (SPTO). Drawing on stakeholder interviews, firm-level cost estimates, and quantitative projections, it finds that the proposed revision constitutes a material departure from established regulatory principles, with economy-wide effects that are particularly pronounced in the digital trust sector. Although formally framed as proportional, the proposed revision would subject most providers of derived communication services to tighter obligations, generating substantial costs and converting Swissness from an asset into a liability.

Full implementation of the proposed revision could result in welfare losses of up to CHF 36 billion and employment losses of up to 219'300 jobs in the digital trust sector by 2035. More fundamentally, the revision risks undermining regulatory coherence and Switzerland's reputation as a trusted jurisdiction—representing a potential tipping point for its role as an international hub for digital trust innovation, with spillovers affecting the broader Swiss economy.

Key findings

Overview of the current situation

Switzerland's digital policy is currently characterised by a fundamental ambiguity that threatens its standing as a trusted business hub.

While the strategy "Digital Switzerland" aims to promote data sovereignty and citizen trust, the proposed revision of the SPTO introduces regulatory uncertainty and causes ultimately strategic incoherence.

A vast majority of the responses in the public consultation oppose the draft of the SPTO revision, reflecting resistance across the entire political and economic spectrum.

The opposition spans the entire political and economic spectrum, from civil society groups referring to unconstitutional mass surveillance to venture capital funds fearing harmful effects for the startup ecosystem.

The revision of the SPTO would markedly extend scope and intrusiveness of surveillance obligations in Switzerland.

The new structure aims for proportionality, but in practice, most PDCS would be subject to significantly tightened surveillance obligations (e.g. metadata retention and encryption removal).

The proposed revision places Swiss firms at a structural disadvantage compared to their peers in the EU and the US.

International comparisons show that both the EU and US have either moved away from or never introduced indiscriminate data retention obligations. By enforcing metadata retention and automatic disclosure, Switzerland would establish a regime that is significantly more intrusive than those of comparable jurisdictions.

Impacts on affected companies

Several thousand companies could be impacted, with projected compliance costs per firm expected to run into the millions.

At this stage, direct cost estimates are inherently uncertain and strongly depend on implementation details and the affected firm's business model. In the long run, indirect costs (e.g. regulatory uncertainty or opportunity costs) may outweigh the direct costs.

The damage is already being done – Swissness is already today transforming from a premium competitive asset into a strategic liability for privacy-centric firms.

Regulatory uncertainty is already being leveraged by international competitors in B2B-tenders to question the reliability of Swiss providers. This reputational erosion is economically significant, given that trust is one of the main reasons why customers choose Swiss services.

Macroeconomic analysis

The digital trust sector is an important growth engine for Switzerland, but its momentum is highly sensitive to regulatory shocks.

With global demand for digital trust services rising, the Swiss digital trust market is positioned for substantial growth over the next decade. However, a "reputational shock" resulting from the SPTO revision could lock Switzerland into an unfavourable development path, hindering the formation of tech clusters.

Negative spillovers could extend far beyond the tech sector, threatening Switzerland's broader trustworthiness.

Trust is all but an irrelevant factor; it affects total factor productivity (TFP), capital accumulation, innovation incentives, and location decisions of globally mobile firms. If the "Swiss trust premium" dissipates, even non-directly affected services in other sectors could see reduced international competitiveness.

Quantitative projections suggest that a full implementation of the revision could result in a welfare loss from the digital trust sector of up to CHF 36 billion in 2035.

The divergence between the status quo and the proposed revision reveals a staggering gap in economic value creation, representing 3 to 4 percent of Swiss GDP. While the lower-bound estimate indicates a welfare loss of CHF 3 billion, the upper bound suggests that the impact of the foregone growth may be much more severe for the Swiss economy.

Cumulative tax revenue losses from the digital trust sector are projected to reach up to CHF 22 billion for the next decade.

The estimated cumulative tax revenue losses of CHF 3 to 22 billion over the period 2025-2035 in comparison to the status quo, are due to foregone receipts from value-added tax (VAT), profit taxes, and income taxes.

The revision of the SPTO risks a massive brain drain, with estimated employment losses of up to 219'300 jobs over the next decade.

While compliance may create some specialised jobs, the net effect of firms downsizing or exiting the market is clearly negative. By 2035, foregone job creation could severely impact the Swiss labour market, with estimated losses ranging from 22'400 to 219'300 jobs.

Contents

Tables

List of Illustrations

Abbreviations

ACN	Alliance for digital trust
AI	Artificial Intelligence
B2B	Business to Business
BKB	Beschaffungskonferenz des Bundes
CCP	Code of Criminal Procedure
CJEU	Court of Justice of the European Union
DACH	Germany (D), Austria (A) and Switzerland (CH)
DBMR	Data Bridge Market Research
DSG	Data Protection Act
DTM	Digital trust market

E-ID	electronic identity
EU	European Union
FDJP	Federal Department of Justice and Police
FTE	Full-time-equivalent
GDP	Gross domestic product
ICT	Information and communications technology
IP	Internet protocol
IPO	Initial public offering
NGO	non-governmental organizations
OP	Obliged parties
OTT	Over-the-Top
PDCS	Providers of derived communication service
PTA	Persons who allow third parties to use their access to a public telecommunications network
PTSS	Postal and Telecommunications Surveillance Service
R&D	Research and development
RIA	Regulatory impact assessment
SaaS	Software as a Service
SECO	State Secretariat for Economic Affairs
SME	Small and medium enterprise
SPTA	Federal Act on the Surveillance of Post and Telecommunications
SPTO	Ordinance on the Surveillance of Post and Telecommunications
TFP	Total factor productivity
TSP	Telecommunication service provider
US	United States
VAT	Value added tax
VoIP	Internet-based communication services equivalent to telecom services
VPN	virtual private network
WEF	World Economic Forum
WMC	Warrant management component

1 Introduction

1.1 Background

On 29 January 2025, the Swiss Federal Council launched the consultation on the proposed revision of the Ordinance on the Surveillance of Post and Telecommunications (SPTO).[1] The consultation process, which concluded on 6 May 2025, received extensive and largely negative feedback from a variety of stakeholders. Companies specialised in trustworthy data and secure communication, including the industry leaders Proton, Threema and Nym, as well as industry associations, political parties, non-governmental organizations (NGO) and consumer organizations, expressed strong concerns about the proposed revision.[2]

The planned revision, under the leadership of the Federal Department of Justice and Police (FDJP), focuses mainly on expanding the surveillance capabilities of the law enforcement authorities. Most noteworthy, it expands surveillance obligations for Providers of Derived Communication Services (PDCS) and introduces new service categories such as PDCS with reduced obligations and PDCS with full obligations, both of which would be subject to stricter requirements. These stricter requirements include extended data retention and identification obligations, mandatory documentation, and reporting duties. In some cases, providers would also need to enable automated responses to requests from law enforcement authorities.[3] Critics argue that such measures would impose disproportionate compliance costs and create a significant security risk. They are concerned that barriers to innovation and market entry could undermine Switzerland's position as a global leader in digital trust and privacy-oriented technologies.

More than 200 responses were submitted during the consultation process, with a majority calling for either a fundamental revision or a complete withdrawal of the proposal. The FDJP has evaluated the consultation results and is preparing a regulatory impact assessment (RIA). After completion of this RIA, the FDJP plans to hold a second consultation.[4]

1.2 Assignment

In this context, FONGIT commissioned an independent RIA for the revision of the SPTO. The assessment focuses on both firm-level and macroeconomic effects of the proposed SPTO revision.

---

[1] Fernmeldeüberwachung und mitwirkungspflichtige Unternehmen: Vernehmlassung eröffnet [21.01.2026]. Note, we always refer to the draft from January 2025 as the proposed revision.

[2] See Completed Consultation Procedures 2025 [20.01.2026].

[3] See Completed Consultation Procedures 2025 [20.01.2026].

[4] Fernmeldeüberwachung und mitwirkungspflichtige Unternehmen: Bundesrat nimmt Ergebnis des Vernehmlassungsverfahrens zur Kenntnis [02.03.2026].

The objective of the assessment is to provide an evidence-based analysis that goes beyond administrative burdens and highlights broader implications for the digital trust sector and Switzerland as a whole.

The RIA compares two regulatory scenarios:

- The **status quo**, representing the current level of regulation; and
- The **Federal Council's consultation proposal** from January 2025.

For each scenario, the RIA assesses both microeconomic and macroeconomic impacts. At the microeconomic level, this includes compliance costs, effects on competition and prices, and broader implications for investment, innovation, tech-clusters and public revenues. At the macroeconomic level, the RIA estimates potential impacts on the gross domestic product (GDP), employment, tax revenues, and Switzerland's international reputation as a digital trust nation.

1.3 Method and structure

This report presents the RIA conducted for the revision of the SPTO and summarises its methodology and key findings. It is structured as follows:

- **Chapter 2** provides an overview of the current situation, covering Switzerland's digital strategy, the proposed SPTO revision, the regulatory options considered, stakeholder responses in the consultation process, and a comparison with the legal frameworks in the European Union (EU) and the United States (US).
- **Chapter 3** analyses the impact on the affected companies. The chapter focuses primarily on PDCS, as the proposed regulatory changes affect these services the most. A separate section also examines the implications for telecommunications service providers (TSPs).
- **Chapter 4** conducts the macroeconomic analysis. First, we explore the relevance of the digital trust sector, second, the consequences of the proposed SPTO revision including potential cross-sectoral spillovers. Lastly, we conduct a quantitative analysis to evaluate the impact on the digital trust market, welfare, employment and tax revenues.

The results are based on desk research, information and analyses provided by FONGIT and wherever possible substantiated with quantitative indicators. The research is complemented by insights of expert interviews that were conducted with representatives of the following organisations:

- Digitale Gesellschaft
- Proton
- SIX
- Threema
- Trust Valley

2 Overview of current situation

This chapter examines the proposed revision of the Ordinance on the Surveillance of Post and Telecommunications (SPTO) in the broader context of Switzerland's digital policy framework. It begins by highlighting the ambiguity of Switzerland's current digital strategy and then outlines the key elements of the proposed SPTO revision before introducing and contrasting the regulatory options analysed in this report. The chapter subsequently reviews the positions expressed by stakeholders during the consultation process. These responses provide initial evidence of the policy ambiguity and of potential adverse effects on Switzerland's digital ecosystem. This initial evidence is substantiated in the firm-level and macroeconomic analyses that follow. Finally, the Swiss proposal is assessed in an international context through a comparison with the legal frameworks in the European Union (EU) and the United States (US), completing the analytical foundation for the subsequent chapters.

2.1 Switzerland's digital regulation at a crossroads

Switzerland's approach to digital regulation currently stands at a crossroads. On the one hand, the Confederation has repeatedly signalled an ambition to position itself as a trusted digital hub, built on strong data protection, citizen trust, and the promotion of innovative, privacy-preserving business models. On the other hand, a recent regulatory development—the proposed revision of the SPTO, which expands indiscriminate surveillance obligations for providers of derived communication services (PDCS, e.g. messengers, e-mail services, or cloud storage providers)—risks undermining this trajectory by introducing legal uncertainty, internal incoherence and ambiguities into the regulatory framework.

A central finding from both the consultation responses and our interviews is that many affected stakeholders struggle to identify a clear and coherent digital strategy in Switzerland, even though the Federal Council annually updates and adopts the strategy "Digital Switzerland".[5] Rather than being guided by a single, overarching regulatory vision, it seems that Switzerland's digital policy has evolved through a series of individual initiatives and legal acts. This has not been inherently problematic so far. Despite the absence of a clearly articulated master strategy, the overall regulatory environment has remained workable and compatible with trust-based digital business models. Interview partners repeatedly emphasised that, from a regulatory perspective, Switzerland has never been perceived as a global frontrunner. However, it is an attractive business location thanks to its reasonable and overall restrained regulatory framework, combined with factors such as the quality of higher education (e.g. ETH, EPFL), neutrality, stability, reputation, and living standards.

Additionally, several other recent policies have directly or indirectly promoted Switzerland as a business location for firms in the digital space. These include the promotion of

[5] Federal Council adopts Digital Switzerland Strategy 2026 [20.01.2026].

trustworthy data spaces and digital self-determination[6], public investment in organisations such as FONGIT or the Trust Valley, and federal digital-innovation funding programmes[7] that aim to foster an innovation-friendly ecosystem for technology startups, including those operating in the field of digital trust.

Switzerland's data protection law (DSG) embeds data minimisation as a core principle, signalling restraint in the use and retention of personal data. Other state-led initiatives, such as the electronic identity (E-ID) or digital sovereignty—two of the focus topics of the digital strategy Switzerland 2026—are explicitly reliant on citizen trust and Swiss based initiatives. Taken together, these elements point towards a regulatory environment that, although fragmented, has so far been broadly aligned in its underlying logic. This environment protects the digital rights of users and fosters business models based on digital trust.

In summary, Switzerland's digital regulation has so far been pragmatic. Despite the absence of a clearly articulated, overarching digital strategy, the regulatory environment has remained broadly compatible with trust-based business models and has provided a sufficient level of predictability for firms to operate. However, the revision of the SPTO risks disrupting this balance. It introduces obligations that conflict with established regulatory principles, lacks clear integration into the broader legal and policy framework. This generates significant uncertainty for those affected. As such, it represents not merely another regulatory adjustment but a tipping point or in the words of one interviewee *"a disaster"*. While this assessment may not yet be fully evident from the facts presented so far, the remainder of the report demonstrates why Switzerland would no longer be a viable location for digital trust firms if the proposed revision were to be introduced.

2.2 Summary of the proposed revision of the SPTO

The partial revision of the SPTO aims to align Swiss surveillance law with modern digital communication technologies. The revision, which underwent consultation in early 2025, is primarily driven by the mandate in the Federal Act on the Surveillance of Post and Telecommunications (SPTA) and the judicial necessity following the Federal Court's "Threema Judgment" in 2021. The latter refers to the landmark ruling by the Swiss Federal Supreme Court (judgment 2C_544/2020), which protected the privacy of the Threema messenger app by ruling that it is not a Telecommunications Service Provider (TSP) under Swiss surveillance law.

The central aim of the proposed revision is to define the categories of Obliged Parties (OP) with greater precision to ensure the imposition of surveillance duties is clear, legally certain,

---

[6] Promotion of trustworthy data spaces and digital self-determination [20.01.2026].

[7] Innosuisse funds 33 projects as part of the Swiss Accelerator as a transitional measure for Horizon Europe [20.01.2026]. It committed CHF 60.4 million, channelling capital toward quantum computing, AI, and cybersecurity.

and—crucially—proportional (Art. 5(2) Federal Constitution).[8] To achieve the required proportionality, the Federal Council introduced a comprehensive re-categorization of OP, structuring duties based on a provider's economic scale and user reach. Figure 1 presents an overview of the obliged parties that are in scope of the proposed revision.

Figure 1: Overview of Obliged Parties in scope of the proposed revision

TSP telecommunication service provider	**PDCS** provider of derived communication services	**PTA** persons who allow third parties to use their access to a public telecommunications network
A TSP provides a network connection and is responsible for the technical transmission of information such as voice, SMS or internet access. Examples include the network providers Sunrise, Swisscom or Salt.	A PDCS offers communication services built on top of existing telecom networks without operating the underlying transmission infrastructure. Services include messaging, email, VPN, or cloud storage. Examples are Proton, Threema or Ricardo.	A PTA may be a person or entity that allows third parties to access a public telecommunications network, such as through public Wi-Fi hotspots. They do not provide services themselves. Examples include hotels, restaurants, or SBB.
Material economic effect on OP due to the proposed revision expected?		
✓	✓	×

Remark: Based on the interviews and consultation material, significant economic effects on PTA appear unlikely. Therefore, this obliged party is not discussed further.

Source: Own representation

New categorisation of Obliged Parties

The new regulation plans to establish distinct tiers for Telecommunications Service Providers (TSP) and Providers of Derived Communication Services (PDCS); see Table 1.

Table 1: Description of categorisation

OP category	Tiers	Threshold for upgrade/full obligations	Key duties of full obligations
TSP	two tiers	▪ Default is "full obligations". ▪ Downgrade to "reduced obligations" requires turnover of less than CHF 100 million *and* participation in less than 10 surveillance targets/year.	Metadata retention (6 months), 24/7 availability/standby duty (*"Pikettpflicht"*), encryption removal, automated data delivery, and real-time surveillance capability.
PDCS	three tiers	▪ Default is "minimal obligations". ▪ Tier 2 ("reduced obligations") is triggered by more than 5'000 users. ▪ Tier 3 ("full obligations") is triggered by: consolidated group turnover of more than CHF 100 million *or* more than 1 million users.	(Almost) same extensive obligations as TSP with "full obligations". "Reduced obligations" are exempt from metadata retention, standby duty and automated data delivery.

Note: See Appendix A.2 for a detailed description of the proposed categorisation and obligations.

[8] Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens: Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) [21.01.2026].

According to the explanatory report[9] on the opening of the consultation procedure this graded approach aims to prevent the disproportionate regulatory leap that previously forced growing PDCS providers to assume the full, costly burden of obligations immediately. However, all PDCS with more than 5'000 participants are automatically part of tier 2 "reduced obligations" and must notify the Postal and Telecommunications Surveillance Service (PTSS) within three months. Thereafter, they have six months to comply with the additional cooperation obligations (*"Mitwirkungspflichten"*) such as identification of users. Note, compliance with the obligations typically requires technical and organisational adjustments, the costs of which are borne entirely by the services (see Chapter 3). However, services are compensated for the costs incurred in specific cooperation operations.[10]

Standardised investigative tools

At the request of law enforcement authorities three types of information gathering and two types of surveillance will be introduced, thereby formalising procedures that were previously treated as ad-hoc requests. The aim is to standardise certain information and retroactive monitoring for user identification (which were previously carried out as special cases) and to enable real-time monitoring of some of the content data.[11] Notably, most requests—both under the new standardised tools and other cooperation obligations—do not require prior judicial authorisation.

2.3 Regulatory options

This section outlines the regulatory differences between the status quo and a full implementation of the revision. Before detailing the specific regulatory differences, we provide a short overview of the regulatory options.

2.3.1 Description of the regulatory options

Retention of the status quo

The reference scenario assumes that the current regulatory framework remains unchanged, including the SPTO as applied since the Federal Court's "Threema Judgment". No changes would be made to the definition, classification, or obligations of firms subject to the SPTO. Both PDCS and TSP would continue to operate under the existing rules, and no additional technical, organisational, or procedural requirements would arise.

A detailed description of the categories and obligations of TSP and PDCS can be found in Appendix A.1.

---

[9] Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens: Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) [21.01.2026].

[10] See Verordnung über die Finanzierung der Überwachung des Post- und Fernmeldeverkehrs (FV-ÜPF) [05.03.2026] and the draft of its revision in the Completed Consultation Procedures 2025 [20.01.2026].

[11] Further details can be found in the Completed Consultation Procedures 2025 [20.01.2026].

Full introduction of the SPTO revision

The regulatory intervention scenario assumes the adoption of the revised SPTO as proposed in early 2025, without incorporating consultation feedback or subsequent amendments. The revised ordinance introduces several significant changes to the structure and content of the legislation, affecting multiple categories of actors.

The most substantial impact concerns PDCS, whose regulatory framework becomes broader and more detailed. Accordingly, this study focuses primarily on assessing the implications of the revised ordinance for PDCS. Other entities, such as TSP, are analysed in less detail. PTA are not examined further, as the proposed revision has only very limited implications for them.

A detailed description of the categories and obligations of TSP and PDCS can be found in Appendix A.2.

2.3.2 Summary of regulatory differences

Regulatory differences for TSP

The core obligations for TSP remain largely unchanged. Nevertheless, the revision introduces some specific adjustments that may have consequences for certain providers. The main novelty is the expansion of the revenue threshold for reduced-obligation status. Under the previous regime, the CHF 100 million threshold was assessed only on the revenues generated by telecommunications services. Under the revised ordinance, the threshold is based on total company-wide Swiss revenues, regardless of whether they stem from telecommunications or other activities. This adjustment has two implications:

- It tightens the threshold, because company-wide revenues are by definition equal to or greater than telecommunications-only revenues;
- It reduces the number of TSP eligible for reduced-obligation status, particularly for diversified companies where telecommunications services represent only a portion of total business activities.

Regulatory differences for PDCS

The proposed revision introduces several changes that materially tighten the regulatory regime for PDCS. Although these providers were already subject to regulation under the previous ordinance and could be designated as providers with extended surveillance or information obligations, the revised framework significantly expands the scope, thresholds and depth of these obligations. While the basic concept of PDCS remains unchanged, the regulatory requirements become substantially more demanding.

The most significant tightening of the regulatory framework for PDCS arises from the introduction of lower and broader thresholds for moving out of the baseline category. Given that 5'000 participants constitute a low threshold in digital markets, a substantially larger proportion of PDCS—in fact, almost all—will fall into higher-obligation categories

compared to the current regime. This has been confirmed by all interview partners and has also been emphasised in the consultation process.

A second source of tightening arises from the expanded and more detailed set of obligations applicable to the higher regulatory tiers. Enhanced surveillance-support duties previously applied only to PDCS with extended obligations, a category into which no provider had ever been placed due to high thresholds.[12] The revised ordinance applies largely the same obligations already at the reduced-obligation level. For PDCS subject to full obligations, the requirements expand further, as summarised in Table 6 of Appendix A.2. As a result, PDCS in the full-obligation tier are regulated in a manner that is substantively equivalent to the regime applied to full-duty TSP. PDCS in the reduced-obligation tier face requirements broadly comparable to those imposed on reduced-duty TSP.

The obligations in the revised SPTO are thus not only more detailed but also apply at much lower thresholds, resulting in a stricter and more comprehensive regulatory regime for PDCS. Obligations that previously applied only to the category of PDCS with extended obligations or to TSPs, will now extend to a far broader set of services.

2.4 Stakeholder response to proposed revision of the SPTO

The consultation process of the SPTO revealed strong and opposing views among key stakeholder groups. Support for the proposed revision mainly comes from cantonal authorities and law enforcement agencies. The strongest opposition originates from the digital trust sector. However, the industry's position is supported by civil society organisations, several non-governmental organisations (NGOs), all political parties, and other actors such as venture capital funds and SIX. Overall, most stakeholders oppose the proposed SPTO revision.[13]

Digital trust industry (firms & associations)

The most forceful opposition comes from the **digital trust sector** (see Box 1). Some of these companies qualify as PDCS and are thus directly affected. Other companies expect negative repercussions due to reputational harm for Swiss firms in the sector. Represented by industry leaders such as **Proton**[14], **Nym**[15], and **Threema**[16], these companies argue that the proposed revision—especially meta data retention and removal of applied encryption obligations—poses an existential threat to their business models. These business models are fundamentally built on minimisation of data collection and maximising security. According to

[12] 800 Schweizer Unternehmen hätten weniger Überwachungspflichten… wenn sie davon wüssten! [28.11.2025]. Note, PDCS with extended obligations is a category in the current SPTO (see Appendix A.1).

[13] Unless otherwise stated, the statements in this section are found in the Completed Consultation Procedures 2025 [20.01.2026].

[14] Proton provides privacy-focused digital services, including secure E-mail, VPN, and cloud storage.

[15] Nym offers a VPN based on noise generating mixnet technology to protect metadata from tracking.

[16] Threema provides a secure messaging service with end-to-end encryption.

these firms, storing additional data and weakening encryption protections would expand the potential attack surface and ultimately reduce user security. Proton has already established server infrastructure abroad and publicly signalled that further investment and expansion may take place outside Switzerland, as the proposed domestic regulatory environment conflicts with the firm's core value proposition.[17]

The major critique points and concerns raised by the sector during the consultation are:

- **Economic relocation risk:** The "full obligations" threshold (1 million users or CHF 100 million turnover) penalises successful, privacy-focused growth. Proton has publicly indicated that the implementation of the revision would necessitate relocation, calling it "economic suicide" for the sector. The "reduced obligations" threshold (5'000 users) covers practically all PDCS, placing regulatory burden on SMEs. The sector argues this low threshold stifles innovation, causes relocation and reduces Switzerland's appeal.
- **Scope over-reach:** The mandated OP definitions are inappropriate for their services. For example, requiring identification duties for Virtual Private Networks (VPNs) fundamentally compromises their core service—anonymity—while the inclusion of personal cloud storage ("*Online-Speicherdienste*") is seen as stretching the PDCS definition beyond its communication-centric legal limit.
- **Fixed cost imbalance:** The current compensation system covers only variable costs (per operation). Firms, especially SME, must bear substantial fixed investment costs to build and maintain the required compliance infrastructure, which disproportionately impairs their competitiveness.

The digital trust industry, supported by a variety of firms like Schweizerische Post, SIX, Redalpine, Founderful, Ronzani Schlauri Anwälte and others, warns that the consequences extend far beyond the direct compliance costs for individual firms. They assert that the proposed measures compromise Switzerland's image as one of the world's leading "digital trust nations". This negative signal would have far reaching consequences as it would threaten Switzerland's competitiveness in the technology sector and its reputation.

[17] E.g., Proton to Expand Infrastructure Beyond Switzerland Over Surveillance Law Fears [20.01.2026], Aus für Anonymität: Schweizer Online-Nutzer sollen sich identifizieren müssen [20.01.2026], Switzerland's New Surveillance Law: A Privacy Crisis for Encrypted Services [20.01.2026].

Box 1: The digital trust sector

The digital trust sector comprises companies whose primary purpose is to establish trust, security, privacy, integrity, and assurance in digital systems, interactions and identities. It can be structured into three interrelated areas:[18]

- **Cybersecurity:** Solutions and services that protect the internal IT environment of organisations and individuals, including breach detection and incident response, digital forensics and auditing, and threat or attack simulation.
- **Digital security:** Technologies and services that establish trust in interactions with the outside world, including identity and access management, biometrics, secure transactions, industrial systems, and networks. This category also covers secure interaction and communication services such as messengers, E-mail providers, VPNs, and cloud solutions.
- **Trustworthy artificial intelligence (AI):** AI designed and deployed under stringent legal, ethical, and technical standards, emphasizing transparency, explainability, robustness, human oversight, and privacy. This includes both generative AI models for content generation and domain-specific AI applications such as fraud detection, predictive maintenance, and cybersecurity tools.

Together, these areas enable secure, reliable digital interactions, safeguard data and personal information, and help maintain confidence in digital systems.

Civil society and NGO

Civil society groups like the "Digitale Gesellschaft" and the "Stiftung für Konsumentenschutz" submitted critical statements, arguing the revision represents a fundamental violation of Swiss law and human rights.

- **Unconstitutional mass surveillance:** The revision is viewed as an "attack on fundamental rights" (Art. 13 Federal Constitution) and establishing a "massive, blanket expansion of surveillance" that is incompatible with the balancing act the SPTA[19] is intended to perform. In an extreme case the revision could mean that law enforcement agencies send an automated request every five seconds to companies with full monitoring obligations, thereby retrieving all registered accesses in real time and building up a complete history.[20]
- **Breach of legality principle:** Critics argue the Federal Council is overstepping its delegated authority by using an ordinance (SPTO) to implement profound restrictions on fundamental rights, a matter that should constitutionally be reserved for an Act of Parliament.

---

[18] See also the Observatory of Digital Trust Sector 2025 [30.01.2026].

[19] Federal Act on the Surveillance of Post and Telecommunications.

[20] Die Schweiz ist drauf und dran, autoritäre Überwachungsstaaten zu kopieren [21.01.2026].

- **Data protection conflict:** The expanded mandatory data retention is deemed incompatible with the principles of data minimisation and purpose limitation under the new DSG, increasing security risks by creating vast, attractive data silos for hackers.
- **Incompatibility with EU Law:** The revision is deemed incompatible with EU law as the Court of Justice of the European Union (CJEU) has established that, in general, indiscriminate and durable retention of data is always incompatible with EU law.

Cantonal authorities and law enforcement

Cantonal governments (including Fribourg, Valais, Nidwalden, Lucerne, Schwyz, and Graubünden) generally supported the revision as necessary and technically sound. However, operational authorities raised critical points concerning speed and effectiveness:

- **Public safety gaps and 24/7 standby duty:** The canton of Aargau critically opposed the exclusion of new identification inquiries (e.g., IR_58_IP_INTERSECT[21]) from the mandatory 24/7 standby duty ("*Pikettpflicht*"). They warn that failure to mandate immediate response capabilities creates "significant surveillance gaps" in high-urgency cases like kidnappings or terrorist threats. Moreover, the canton opposes the exclusion of PDCS with minimal and reduced obligations from the mandatory standby duty.
- **Technical & operational inflexibility:** The cantons of Solothurn and St. Gallen highlighted that the Warrant Management Component (WMC), i.e. the administrative tool used for surveillance currently cannot modify an existing order to include a new device (Multi-Device) or SIM (Extra-SIM), forcing investigators to file a new order.
- **Need for superior law reform:** The "Schweizerische Staatsanwaltschaftskonferenz" (SSK) as well as the cantons of Schwyz and Graubünden stressed that—while the ordinance revisions are necessary technical adjustments—they are insufficient to solve the long-term, systemic challenge of digital evidence collection. They advocate for fundamental reforms of the superior laws, specifically the SPTA and the Code of Criminal Procedure (CCP).

In contrast to these operational concerns, the cantons of Vaud and Geneva placed particular emphasis on the economic and constitutional implications of the revision. Both cantons cautioned that the proposed obligations risk weakening Switzerland's digital economy, especially providers of privacy- and security-oriented communication services. Geneva explicitly referred to the recently enshrined constitutional right to digital integrity and warned that certain surveillance obligations—particularly those affecting end-to-end encryption—could undermine trust in Swiss digital services. Vaud similarly stressed that overly broad or insufficiently differentiated obligations could place Swiss providers at a disadvantage compared to foreign competitors and called for closer alignment with European standards.

[21] IR_58_IP_INTERSECT is a new information type. It could be used for user identification through intersection formation. See Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens: Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) [21.01.2026] for further information.

Box 2: Use of post and telecommunication surveillance

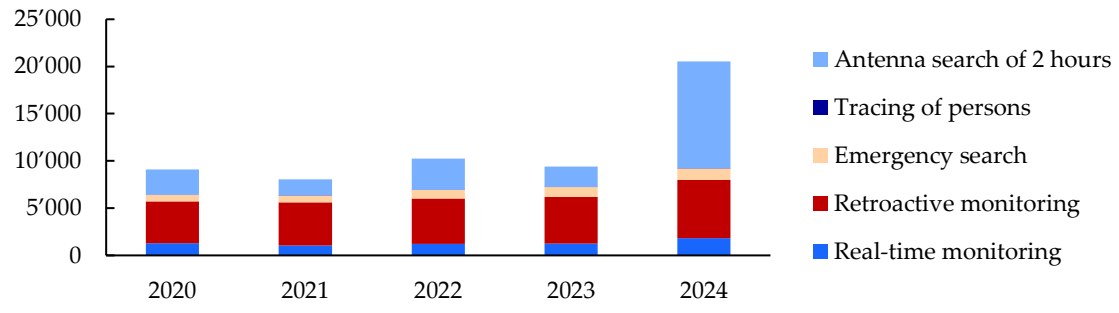
In 2024 Switzerland recorded a significant increase in post and telecommunications surveillance. Law enforcement authorities and the Federal Intelligence Service ordered more than twice as many surveillance measures via the SPTO service as in the previous year (see Figure 2).[22] The main driver behind this development was the sharp rise in antenna searches, which increased fivefold compared to 2023. Antenna search comprises call records of all communications, communication attempts and network accesses that have occurred at a specific location and that have taken place via specific mobile radio cells. The sharp increase in antenna search figures is mainly due to a recent change in the measurement methodology.[23]

Other forms of surveillance also increased notably: real-time monitoring rose by 46 percent to 1'818 cases, while retrospective monitoring measures rose by around a quarter to 6'149 cases. The number of emergency searches in 2024 also grew substantially, reaching 1'223 orders—around 20 percent more than in the previous year—whereas the number of tracing of persons declined slightly to 35.

The surveillance measures focused on several key offence categories. At 43 percent, the largest share related to financial offences, whose surveillance volume more than tripled compared to 2023. Measures related to offences against life and limb also increased sharply, accounting for 19 percent of all orders and more than doubling year-on-year. Around 10 percent of the measures concerned serious violations of the Narcotics Act, where an increase of over 15 percent was recorded. Other categories—such as emergency searches, offences against personal liberty and offences against public order—also saw increases, albeit to a lesser extent.

Overall, the figures for 2024 show a clear expansion of surveillance activity. They indicate that the respective instruments are being used broadly and with increasing intensity by the authorities, particularly in the areas of financial crime, violent offences and narcotics-related crime.

Figure 2: Post and telecommunications surveillance measures by type (2020-2024)



Source: Swiss Economics illustration based on PTSS[24]

[22] Statistics | Post and Telecommunications Surveillance Service PTSS [18.11.2025].

[23] Previously, the count depended on the number of individual cells used in the search, but now the count is simplified to be based only on the service provider and the time period (up to two hours), regardless of the number of cells involved; Beschaffungskonferenz des Bundes (BKB): Statistik zur Fernmeldeüberwachung: Mehr Überwachungsmassnahmen [18.11.2025].

[24] Statistics | Post and Telecommunications Surveillance Service PTSS [18.11.2025].

2.5 International Comparison

Given the potential impact on Switzerland's competitiveness as a technology hub, it is instructive to compare the proposed framework with those of the EU and the US—the world's largest economies and regulators. From a Swiss perspective, alignment with these jurisdictions is relevant for four reasons. First, both the EU and the US set the global regulatory standards in the digital economy. Second, for a small, open economy, regulatory convergence minimises cross-border frictions and compliance costs for internationally active firms. Third, these regions represent credible relocation alternatives for Swiss technology companies, making their legal frameworks benchmarks for competitiveness and innovation. Fourth, users of Swiss PDCS face low switching costs and can readily substitute these services with providers based in the EU or the US.

The following sections summarise and compare the surveillance and data retention regimes in the EU and the US across four dimensions: (i) the scope of affected providers, (ii) data retention obligations, (iii) access to data and available legal recourses, and (iv) the treatment of end-to-end encryption. The analysis shows that the proposed Swiss framework—particularly its broad scope, mandatory retention, and automated data-access requirements—would make Switzerland an outlier among Western democracies and place its digital industry at a significant disadvantage.

2.5.1 Legal situation in the EU

Legal background

The EU's data retention framework originated in Directive 2006/24/EC, was adopted to harmonise national surveillance laws for telecommunication and internet service providers. It required the retention of metadata across a range of services, including telephony, internet services, email, and internet telephony. However, from 2009 onward, the directive faced extensive constitutional and judicial challenges. In successive landmark rulings—*Digital Rights Ireland and Others* (2014, C-293/12 and C-594/12), *Tele2 Sverige and Watson and Others* (2016, C-203/15 and C-698/15), and *La Quadrature du Net and Others* (2020, C-511/18, C-512/18 and C-520/18)—the CJEU held that indiscriminate data retention violates EU fundamental rights. The Court determined that such blanket obligations were disproportionate, lacking a clear link between retained data and specific security threats. It has established that, in general, indiscriminate and durable retention of data is always incompatible with EU law.

As a result, the EU's data retention directive was invalidated, and national implementations diverged. Some member states, notably Germany, the Netherlands, and Romania, fully repealed their frameworks in compliance with the rulings. Others—France, Italy, Spain, and Poland—maintained limited national regimes, though these remain legally vulnerable and only partially enforced. The result is a fragmented landscape in which most EU jurisdictions no longer impose systematic retention obligations.

Scope and obligations

Even where national data retention still exists, the scope remains far narrower than that proposed under the Swiss SPTO revision. EU frameworks generally apply only to network operators, internet service providers, and basic communication providers (e.g. telephony or email). In contrast, the Swiss proposal extends obligations to nearly all "Over-the-Top (OTT)"-services—including messaging platforms, VPNs, proxies, and file-storage providers. This would transform Switzerland into one of the few Western countries imposing surveillance duties on the entire online ecosystem.

Access to data and legal safeguards

Under EU practice, access to retained data is subject to judicial authorization in nearly all cases involving content, traffic, or location data. Providers have standing to challenge disclosure orders on grounds of proportionality, necessity, or legality. No EU legislation mandates automated execution or direct system access by authorities. In contrast, the Swiss proposal would introduce an automated disclosure mechanism requiring certain providers to establish technical interfaces through which law enforcers could query user data directly. Such an obligation is unique among Western democracies and would, inter alia, create systemic cybersecurity vulnerabilities.

End-to-end encryption

The EU has not adopted measures undermining end-to-end encryption. While the European Commission proposed in 2022 a regulation ("Chat Control 2.0") mandating client-side scanning for child sexual abuse material, it has faced overwhelming opposition from member states and remains stalled. Current EU law, grounded in the e-Privacy Directive, still prohibits general monitoring or decryption mandates. The Swiss authorities, by contrast, have not explicitly moved against end-to-end encryption but risk weakening its protection indirectly, as the proposed revision requires services to be able to remove the encryption they applied themselves.

Comparison

Relative to the EU, the Swiss draft stands out for its indiscriminate retention, lack of judicial oversight, and automated enforcement. Most EU jurisdictions have shifted toward targeted, proportional surveillance subject to court control. The Swiss proposed framework reverses this trend, combining the most intrusive elements of EU member states (e.g. the French retention obligations[25]) with weaker procedural safeguards, i.e. limited judicial authorisation requirements. Its adoption would isolate Switzerland from European privacy standards and jeopardise its position as a trusted data jurisdiction.

[25] Telecoms, Media and Internet Laws and Regulations France 2026 [10.03.2026].

2.5.2 Legal situation in the US

Legal background

The US has never implemented blanket data retention laws. The Patriot Act of 2001 expanded access to existing data but stopped short of mandating pre-emptive retention. A later attempt—the 2009 SAFETY Act—proposed requiring service providers to retain user-identifying data for two years but was rejected by Congress. Consequently, US providers retain only the data necessary for business operations and produce it upon lawful request. This minimal-regulation approach has inter alia supported the rise of the US as a global technology leader.

Access to data and legal safeguards

Law enforcement access in the US follows a clear hierarchy:

- **Subpoenas** for non-content data (e.g. subscriber details) may be issued but can be challenged for overbreadth, irrelevance, or undue burden.
- **Warrants**, required for content data, must be issued by a judge based on probable cause and can be contested under the Fourth Amendment.

US law thus provides multiple procedural safeguards and explicit avenues for providers to challenge data requests. Unlike the proposed Swiss model, there are no obligations for automated or direct system access. The legal framework emphasises targeted collection and judicial oversight, maintaining a balance between security and privacy.

End-to-end encryption

Efforts to mandate decryption have failed. The 2020 *Lawful Access to Encrypted Data Act*—which would have required providers to deliver unencrypted data on request—was abandoned due to lack of political support. As a result, end-to-end encryption remains protected and widely used in US digital services.

Comparison

Compared with the United States, Switzerland's proposed framework involves significantly more indiscriminate surveillance. Whereas the US relies on post-facto, targeted access subject to judicial review, Switzerland's system would impose pre-emptive, indiscriminate data collection coupled with mandatory technical backdoors (e.g. encryption removal). The US approach offers stronger protection for providers and users alike, preserving both privacy and competitiveness. Switzerland's revision, by contrast, would erode both, positioning the country among the most intrusive surveillance regimes in the Western world.

2.6 Summary

Switzerland's digital policy stands at a crossroads. On the one hand, the country has positioned itself as a trusted digital hub, emphasising strong data protection, innovation-friendly framework conditions, and initiatives aimed at digital sovereignty and trusted data

spaces. On the other hand, the proposed revision of the SPTO moves in the opposite direction by substantially expanding surveillance obligations. Rather than reinforcing Switzerland's positioning as a trusted digital hub, it risks undermining regulatory coherence and generating uncertainty for firms whose business models rely on privacy and security.

This tension is reflected in the consultation process, which reveals broad resistance to the proposed approach. While cantonal authorities partially and law enforcement agencies generally support the revision, a vast majority of consultation responses oppose it. The strongest criticism comes from the digital trust industry, supported by civil society organisations, political parties and investors. These stakeholders argue that the proposed obligations directly conflict with business models based on data minimisation, strong encryption and user anonymity, create disproportionate compliance costs, and generate strong incentives for relocation. Civil society groups further highlight constitutional concerns, including violations of proportionality, the legality principle and data protection law.

Against this background, the report develops and compares the differences of two alternative regulatory scenarios: retention of the status quo and full introduction of the SPTO revision. Although the new structure is intended to improve proportionality, the chosen thresholds—particularly the low entry point of 5'000 users for PDCS with reduced obligations—mean that in practice most services would be subject to surveillance obligations. Combined with the significantly expanded duties imposed on the tier PDCS with reduced obligations, a full introduction of the revision would markedly extend both the scope and the intrusiveness of surveillance in Switzerland compared to the status quo.

The international comparison further reinforces these concerns. Both the EU and the US have moved away from indiscriminate data retention and broad surveillance obligations. In the EU, blanket retention has largely been ruled incompatible with fundamental rights by the CJEU, and remaining national regimes are narrow, contested and weakly enforced. In other words, the envisaged approach would be incompatible with the regulation in the EU. The US has never introduced mandatory data retention and relies on targeted, ex post access subject to judicial oversight. The Swiss proposal would introduce a significantly stricter framework than in comparable jurisdictions.

Table 2 illustrates this divergence. It shows that key obligations such as metadata retention, identification duties, last-IP retention and automatic disclosure would apply more broadly under the proposed Swiss framework than under current Swiss practice and as in the EU or the US. Note, large international technology firms operating under EU or US law are not subject to the Swiss obligations. The table thus highlights the risk that the revision would place Swiss-based PDCS at a structural disadvantage relative to foreign competitors due to the additional obligations, that only apply to Swiss-based firms.

Table 2: Summary of obligations for PDCS

	Current state CH	SPTO draft "full obligations"	SPTO draft "reduced obligations"	EU	US	Int. Firms (Google, Meta)
Metadata retention obligation	×	✓	×	×	×	×
Identification obligation	×	✓	✓	×	×	×
Last-IP retention obligation	×	✓	✓	×	×	×
Automatic disclosure	×	✓	×	×	×	×
Last-IP without court order	×	✓	✓	×	×	×

Note: Automatic disclosure, metadata retention and identification obligation are existing in the current state in Switzerland for services with more than CHF 100 million revenues but not enforced.

Source: Swiss Economics based on Proton

Overall, Chapter 2 demonstrates that the proposed SPTO revision would not merely modernise Swiss surveillance law but would fundamentally tighten the regulatory framework. In doing so, it would contradict Switzerland's broader digital policy objectives and establish a regime that is markedly more intrusive than those of the EU and the US. Several interview partners warned that the proposed SPTO revision might be a tipping point, negatively affecting Switzerland's international reputation as a trusted and predictable digital jurisdiction, especially since the regulation is to be introduced through the back door by means of an ordinance.

3 Impacts on affected companies

This chapter examines the impact of the planned revision on companies that would be directly affected by the proposed measures. Building on the previous chapter, it identifies the relevant types of firms and outlines the channels through which the revised SPTO would influence their operations and cost structures. The analysis focuses on the regulatory option of a full implementation of the SPTO revision.

This chapter does not cover potential indirect effects, such as second-round impacts arising from reputational considerations or implications for Switzerland's attractiveness as a business location. These effects are addressed separately in Chapter 4. Furthermore, this report does not provide a detailed analysis of the impacts on end users and other stakeholders. However, illustrative examples are presented in Box 3.

3.1 Impact on Telecommunication Service Providers

Telecommunications Service Providers (TSP) constitute a sizeable and heterogeneous group within the scope of the SPTO. According to the definition used in the ordinance, there are currently around 1'000 entities in Switzerland that qualify as TSP. Of these, only a small subset—currently six providers—are subject to the full set of obligations under the existing regime. The vast majority of TSP can therefore operate under a reduced regulatory burden, often because their services or scale do not meet the thresholds that trigger full compliance requirements. Evidence suggests, however, that only 200 of the approximately 1'000 eligible firms have requested and been granted a downgrade, indicating a certain lack of transparency, understanding of the current framework or simply unaffectedness by the SPTO so far.[26]

As discussed in Section 2.3.2, the main regulatory change introduced by the SPTO revision for TSP lies in the potential expansion of the group subject to full obligations. Interview partners were unable to provide precise estimates of how many firms would be affected by such an upgrade. This reflects the diversity of business models within the TSP category, as well as the uncertainty created by the proposed revision. However, only those firms that are reclassified and upgraded would face materially higher compliance requirements.

For providers subject to the full obligations, the resulting additional costs are expected to vary significantly. Interview partners emphasised that the costs would depend strongly on firm-specific factors, such as existing technical infrastructure, the types of data already processed and stored, and whether organisational measures—such as a 24/7 standby duty—are already in place due to other regulatory requirements or operational needs. For firms that are not yet subject to comparable obligations, it is plausible to assume that the additional costs would be similar to those for PDCS that would be upgraded to full obligations.

[26] 800 Schweizer Unternehmen hätten weniger Überwachungspflichten… wenn sie davon wüssten! [28.11.2025].

As Section 3.2.3 shows, initial costs of CHF 2 to 3 million and running costs of CHF 1.5 million per year are expected for PDCS.[27]

Importantly, interview partners did not expect the SPTO revision to create a significant competitive disadvantage within the national TSP sector. Since TSP offer comparable services, they would all be subject to the same regulatory framework and any cost increases would apply symmetrically. Moreover, unlike PDCS, TSP primarily operate in a domestic, tightly regulated market and are not exposed to the same degree of international competition as PDCS. As a result, the regulatory changes are not expected to materially distort competitive dynamics, even if they lead to higher compliance costs for a subset of providers. These additional costs would most likely be passed on to customers, such that the services of TSP would become more expensive.

In summary, the SPTO revision would affect the TSP sector primarily through the potential reclassification and upgrading of certain providers to full obligations. While this would entail additional costs for affected firms, the magnitude of these costs is expected to vary considerably depending on existing structures and regulatory exposure. At the same time, the revision is unlikely to alter competition within the national TSP market significantly, as regulatory requirements would apply uniformly to all comparable providers and international competitive pressure remains limited. Consequently, this study does not further elaborate on the effects on TSP, as the expected impacts are limited and the available data do not allow for a meaningful differentiation or robust quantification across firms. A more thorough and systematic market analysis would be required to draw conclusive evidence on the number of affected providers and the magnitude of the associated compliance costs.

3.2 Impact on Providers of Derived Communication Services

Providers of Derived Communication Services (PDCS) are likely to be most affected by the proposed measures. This section provides a detailed analysis in four steps. First, it defines which company-types fall within the scope of PDCS. Second, it estimates the number of companies directly impacted. Third, it presents the associated direct and indirect costs. Finally, it examines the broader operational and strategic consequences for these firms.

3.2.1 Affected companies

PDCS offer a heterogeneous set of online services that **mediate communication** between users without being traditional telecom operators. Based on the explanatory report of the

[27] These estimates remain uncertain, as firms currently lack clarity on the precise form and scope of the future requirements. In particular, the required data to comply with the identification obligation could substantially affect implementation complexity, given that compliance hinges on stringent data security standards that must be put in place to safeguard the data. It is, e.g., obvious that an IP-address would require less protection than saved passport copies.

FDJP, interviews, and desk research, the following groups clearly fall under the PDCS concept in the Federal Council's draft revision:[28]

- **Indirect internet access services (VPN and proxy services):** These services redirect internet traffic independently of the user's internet access service and typically modify the source IP address under which users appear online. They are commonly used for encryption, anonymisation, or bypassing geo-blocking restrictions. Swiss-based examples include **ProtonVPN** and **Nym**, both of which explicitly market privacy and security as core features.
- **Applications for data transmission between users (apps and software):** This category includes applications and programs that enable the transmission of text, voice, images, video, or other data between users, provided they are not bundled with internet access. The definition is technology-neutral and covers both mobile and desktop software. Swiss examples include **Infomaniak** and **Swissdotnet**, both of which provide user-to-user data transmission over the internet.
- **Internet-based communication services equivalent to telecom services (VoIP):** These services functionally replace traditional telecommunications offerings, such as voice calls, but are provided entirely over the internet and independently of network operators. Typical examples are internet-based telephony and video calling services. Examples of Swiss-based VoIP are services such as **Chorus Call** or **Virtual-Call**.
- **E-mail services for third parties:** E-mail services include webmail, professional mail hosting, and secure or encrypted E-mail solutions offered to users or organisations. They represent one of the most established forms of derived communication services. Examples of Swiss based providers include **Proton Mail** and **Swissmail**, both of which provide E-mail services to private and business customers.
- **Internet-based messaging and notification services:** Messaging services enable real-time or asynchronous communication between users via text, images, voice messages, or multimedia content. This includes instant messaging apps, chat platforms, and messaging components embedded in larger platforms. Swiss-based examples include **Threema** and **Session**, as well as messaging functionalities within Swiss platforms such as **Digitec** or **Ricardo**.
- **Online storage, hosting and content-sharing services:** These services allow users to store, share, and collaboratively work on digital content such as documents or files. Although their primary purpose is data storage, communication occurs through sharing links, access rights, comments, and collaborative editing. Swiss examples include **Exoscale**, **Hostpoint, nine** and **Tresorit**, all of which offer hosting or cloud-based storage features. The communicative element arises from enabling interaction between multiple

[28] A sample of the companies mentioned were contacted to provide an assessment of the impact of the SPTO on their business. Only a few companies responded to this request.

users around shared content. As such, these services are considered PDCS even if communication is not their primary advertised function.

This list represents illustrative examples based on the explanatory report and the interviews conducted for this study. The PDCS definition is broad and technology-neutral, meaning that **additional service types and/or hybrid business models** may also fall within scope. At present, interview partners did not identify further concrete examples beyond the categories outlined above, however, they emphasised the prevailing legal uncertainty for potentially affected firms.

3.2.2 Number of affected companies

There are no reliable figures regarding the number of companies that would fall under the PDCS-category. The consultation responses, desk research and expert interviews conducted in preparation for this study, did not yield a reliable range or total count of such firms. Nevertheless, the available evidence indicates that a substantial number of companies operating in Switzerland may potentially fall within scope. Several data points illustrate the breadth of potentially affected service providers:

- CompanyData.com lists 456 communication companies in Switzerland, covering a broad range of digital and telecommunication service offerings.[29] While not all of these firms necessarily qualify as PDCS, their communication offering may bring them within the PDCS definition.
- A study on online dating platforms in the DACH-area finds approximately 400 dating platforms serving the Swiss market.[30] It remains unclear how many of these companies are legally established in Switzerland and would therefore be directly affected by the SPTO revision. Swiss-based examples include DuoLivo and swissfriends. Dating platforms typically rely on user-to-user messaging and notification functionalities, which may bring them within the PDCS definition.
- The FHNW annual online retailer survey covers 581 Swiss online retailers.[31] Some of these platforms provide integrated messaging or notification services enabling communication between users, such as Ricardo or tutti.ch. However, no systematic data exist on how many surveyed retailers offer such features in a way that would qualify them as PDCS.
- PoiData.io lists 1090 web hosting companies in Switzerland as of December 2025.[32] Based on the explanatory report it appears likely that many of these companies qualify as PDCS.

---

[29] List of Communication Companies in Switzerland [20.01.2026].

[30] Der Online-Dating-Markt in der Schweiz 2018/2019 [20.01.2026].

[31] Zumstein, Dörner & Schüler (2025). Onlinehändlerbefragung 2025. Onlinehändlerbefragung 2025 [11.03.2026].

[32] List of Web hosting companies in Switzerland? [20.01.2026].

- Swiss made software, a label for Swiss software companies, has more than 1'100 members.[33] It is unclear how many of these members qualify as PDCS, but illustrative examples potentially falling under the definition include Threema, Infomaniak, and Cloudpartner.
- According to Tracxn the Swiss Software as a Service (SaaS) sector comprises 2'280 companies. Some of these companies, e.g. Proton, clearly qualify as PDCS but no systematic data exists on the total number of PDCS in the SaaS sector.[34]

Taken together, these figures suggest that the number of potentially affected companies is likely to be significant, even if only a subset of firms within each category ultimately qualifies as PDCS under the revised legal framework. The lack of a precise count reflects the absence of robust statistical classifications aligned with providers of derived communication services. This uncertainty was repeatedly highlighted by interview partners and in the consultations and illustrates the need for greater clarity of the number of affected firms to assess economic effects more precisely.

3.2.3 Implementation costs

The SECO guidelines for regulatory impact assessments[35] as well as the guidelines to estimate regulatory costs for enterprises[36] both explicitly state that direct and indirect costs should be considered in the impact analysis of firms.

Direct costs

The interview partners emphasised that any cost estimates are inherently uncertain at this stage due to ongoing regulatory refinement and the yet-to-be-finalised implementation details. They also depend heavily on each PDCS's business model, scale, technology stack, and existing compliance maturity. The proposed revision could require a complete overhaul of the security architecture for some firms while for other firms, the additional costs may be negligible, as their existing systems and processes already largely meet the anticipated requirements. Generally speaking, the more privacy-centric a firm's business model is, the greater the cost.

Nevertheless, the interview partners provided order-of-magnitude cost ranges that illustrate the scale of expected direct monetary impact:

- **PDCS with reduced obligations:** Interviewees estimate annual compliance costs in the region of CHF 1 million per company, driven by the need for additional IT specialists, expanded server capacity, and the development of systems to support new information-

[33] swiss made software – uniting quality and digital sovereignty [20.01.2026].

[34] SaaS Sector in Switzerland [20.01.2026].

[35] Handbuch Regulierungsfolgenabschätzung (RFA) [20.01.2026].

[36] Leitfaden zur Schätzung der Regulierungskosten [20.01.2026]. This guideline is based on the *Unternehmensentlastungsgesetz*.

readiness and reporting duties. Should a provider need to outsource retention infrastructure or use hyperscaler services to meet data-retention demands, these costs could escalate into the multiple-million-franc range, contingent on user volumes and the exact nature and duration of the retention obligations.

- **PDCS with full obligations:** For larger providers subject to full surveillance duties, the estimated development costs are approximately CHF 2 to 3 million, with ongoing annual expenditures of around CHF 1.5 million to cover staffing (security engineers, compliance personnel), data storage, and operational support for 24/7 availability and automated interfaces.

A central driver of the direct costs is the need for qualified personnel. Implementation requires detailed analysis of internal data structures, the identification and mapping of legally relevant data fields to required output formats, and the development of automated or semi-automated query mechanisms. In addition, organisations must define internal validation and approval workflows, build out extensive documentation, and conduct rigorous testing. This phase requires specialised technical expertise, supported by legal and compliance resources—a combination that significantly increases personnel cost burden. Operationalising these systems can also require ongoing training, retention of specialists, and added overhead for security and audit processes.

Among PDCS, cloud storage providers face a particularly high regulatory risk under the proposed revision. Although the precise scope of potential metadata retention obligations remains undefined, industry assessments suggest that providers could be required to implement extensive retention capabilities. One provider estimates the additional costs could reach 10 percent of revenues for small providers, compared to approximately 1 percent for large domestic cloud providers.

The cloud storage market is characterised by low margins and intense competition from global hyperscalers such as AWS and Azure. Swiss-based providers typically operate on thin margins and have limited scope to pass through significant additional compliance costs without eroding their competitive position. If retention requirements were to prove extensive, the associated investment, storage, and operational expenditures would likely exceed operating margins on a sustained basis. In that case, the business model of offering cloud storage services from Switzerland would no longer be economically viable. Market exit or relocation of activities to jurisdictions with lower regulatory burdens would then represent rational and potentially unavoidable responses.

Intangible and indirect costs

In addition to quantifiable direct costs, affected firms may also incur less easily quantifiable but potentially significant costs:

- **Strategic disruption**: Roadmaps, product development cycles, and innovation efforts may be paused, delayed, or reprioritised as technical and compliance resources are diverted toward surveillance-related build-outs.

- **Regulatory uncertainty**: The mere process of adapting to an evolving regulatory regime creates costs — for instance, in scenario planning, legal assessment, and negotiations with customers or investors — as firms hedge against ambiguous future obligations that may be detrimental to their business model.
- **Opportunity costs**: Time and capital allocated to compliance, scenario planning and other additional tasks due to the proposed revision cannot be deployed elsewhere, potentially slowing market growth or product enhancements.

These indirect impacts rarely appear as explicit budget items but have tangible effects on organisational capacity, strategic flexibility, and competitive positioning. In the longer term, the importance of these indirect costs may exceed that of the direct costs. The costs outlined above therefore capture only part of the overall economic burden; the broader consequences are discussed in the following section.

3.2.4 Consequences

The proposed expansion of surveillance obligations for PDCS is likely to generate material competitive, strategic, and market impacts, particularly for companies whose value propositions are tied to trust, privacy, security and Swissness.

Competitive disadvantage and reputation effects

A central concern for Swiss PDCS is that the revised obligations would undermine their competitive position relative to foreign competitors. Unlike traditional TSP, PDCS typically operate in global markets. Swiss PDCS therefore compete directly with services headquartered in jurisdictions where no comparable surveillance obligations apply, notably in the US and the EU. Prominent examples include messaging services such as WhatsApp and Signal, or E-mail providers such as Microsoft Outlook and Gmail.

Where foreign competitors face lighter or no equivalent requirements, Swiss PDCS would incur higher compliance costs and operational constraints. These may translate into higher prices, slower innovation cycles, reduced product functionality, or the need to redesign core features. More fundamentally, the additional compliance, retention, and operational expenditures may erode already thin margins in internationally competitive segments. In markets characterised by high price transparency and limited scope for cost pass-through (e.g. cloud storage), sustained cost increases can render Swiss-based provision economically unviable. In such cases, market exit or relocation to jurisdictions with lower regulatory burdens becomes a rational economic response.

Beyond pure cost pressures, the revision poses a direct threat to the unique selling proposition (USP) of providers. These effects are particularly pronounced for privacy-centric firms whose business models are explicitly built on data minimisation and strong confidentiality guarantees. For these providers, the identification and data-retention obligations introduced by the SPTO revision are structurally incompatible with their core value proposition.

The competitive disadvantage is already evident today. According to interview partners, regulatory uncertainty surrounding the revision is increasingly being leveraged by international competitors in tender processes, particularly in B2B markets, to question the suitability of Swiss providers. Combined with the international visibility of the revision,[37] this dynamic contributes to a deterioration in the perceived trustworthiness of Swiss privacy-centric services even before the rules enter into force. This reputational channel is economically relevant: according to a customer survey conducted by an interview partner, reputation is the second most important reason for customers choosing its service over competitors.

Several interview partners further emphasised that Swissness, currently a competitive asset, risks turning into a disadvantage—especially for privacy-centric firms—under the revised framework. This concern is not purely theoretical. Proton, the largest Swiss privacy-technology firm, has already begun relocating parts of its infrastructure to Germany and Norway, explicitly citing legal uncertainty and concerns that the revised surveillance obligations would conflict with its privacy commitments. Proton has also publicly stated that adoption of the SPTO revision in its proposed form would necessitate further relocation.[38] Interview partners expect that other privacy-focused providers would follow, as their USP would no longer be compatible with Swiss regulation.

Looking ahead, international competitors not subject to equivalent surveillance regimes are likely to capture market shares from Swiss providers as users prioritise credible privacy guarantees. From an economic perspective, this outcome will weaken not only domestic firms but also the effectiveness of the regulatory objective itself: given the high substitutability of digital communication services across borders, criminal activity is likely to shift towards foreign platforms. This would negate the intended surveillance benefits while reducing domestic value creation.

Strategic disruption and opportunity costs

Adapting to expanded and uncertain obligations requires the reallocation of scarce resources away from product development and innovation toward compliance and risk mitigation. For many firms, this may imply delayed product launches, postponed investments and a strategic reprioritisation. Consequently, affected firms risk losing ground to foreign competitors that do not face comparable obligations.

Regulatory uncertainty further affects firms' strategic positioning vis-à-vis investors and capital markets. Unclear or evolving obligations increase perceived regulatory risk, which can depress valuations, raise financing costs and deter investment, particularly for scaleups

[37] E.g., Proton to Expand Infrastructure Beyond Switzerland Over Surveillance Law Fears [20.01.2026], Aus für Anonymität: Schweizer Online-Nutzer sollen sich identifizieren müssen [20.01.2026], Switzerland's New Surveillance Law: A Privacy Crisis for Encrypted Services [20.01.2026].

[38] Proton Says It'll Leave Switzerland if This Controversial Law Is Passed [20.01.2026], Proton-CEO Andy Yen: «Wer Gesetzgebung der Polizei überlässt, sollte sich nicht wundern, wenn er eines Tages in einem Polizeistaat aufwacht» [21.01.2026].

and late-stage startups. Several interview partners noted that for firms considering initial public offerings (IPO) or major growth financing rounds, uncertainty surrounding the SPTO revision acts as a negative signal, constraining strategic options well beyond the immediate scope of surveillance compliance.

Labour market and employment consequences

The regulatory shift may also affect firm-level employment, with broader macroeconomic employment implications (see also Chapter 4). On the one hand, expanded compliance obligations require additional specialised personnel, such as IT-security experts, compliance officers and data engineers. This may lead to some job creation by firms. However, industry evidence suggests that such demand may coincide with skills shortages and rising wage pressures, limiting the extent of net employment gains.[39] Moreover, these additional positions are primarily compliance-oriented and do not directly contribute to value creation or innovation. On the other hand, if a meaningful share of firms relocate, downscale or exit the Swiss market, job losses are likely to outweigh compliance-related hiring. Early-stage ventures with limited resources are particularly exposed, as such small businesses are unable to absorb largely fixed compliance costs and specialised staffing requirements. Interview partners consistently assessed the net employment effect as negative, especially in the medium to long term.

Impacts on value creation and tax revenues

The effects on value creation and public finances follow directly from the competitive and strategic dynamics described above. Firms that reduce their Swiss footprint—by relocating infrastructure, legal entities, intellectual property or headquarters abroad—contribute less to domestic GDP, corporate tax revenues and local supply chains. If high-skilled employees relocate alongside these activities, the impact extends to income tax revenues and social security contributions, amplifying fiscal losses.

Beyond direct tax effects, such relocations weaken knowledge spillovers, clustering and agglomeration effects as well as ecosystem dynamics that are critical for innovation-driven sectors. A sustained outflow of firms and talent risks triggering a form of brain drain, reducing Switzerland's attractiveness as a location for trust-, security and privacy-oriented technologies. These sector-wide effects are further analysed in Section 4.1.

[39] Switzerland Cybersecurity Market Size & Share Analysis - Growth Trends and Forecast (2026 - 2031) [20.01.2026].

3.3 Summary

This chapter analysed the economic effects of the proposed SPTO revision on companies that are **directly** subject to the regulation, especially traditional Telecommunications Service Providers (TSP) and Providers of Derived Communication Services (PDCS).

For **TSP**, the main regulatory change arises from the potential reclassification of some providers to full obligations. While this would increase compliance costs for affected firms, the magnitude of these costs is expected to vary considerably depending on existing infrastructure and regulatory exposure. Importantly, competition within the Swiss TSP market is unlikely to be materially affected, as comparable providers would face similar obligations and international competitive pressure remains limited. As a result, higher costs would most likely be passed on to customers.

The situation is fundamentally different for **PDCS**. The definition of derived communication services is broad and technology-neutral, covering a wide range of digital business models, including messaging, E-mail, hosting, cloud services, and communication functionalities embedded in platforms. While the precise number of affected firms cannot be robustly quantified due to data limitations and legal uncertainty, available evidence suggests that a substantial number of Swiss-based companies may fall within scope.

For these firms, particularly for those within the cloud storage sector or with privacy-centric business models, **direct compliance costs** are expected to be significant. Depending on whether firms are subject to reduced or full obligations, interview evidence points to annual compliance costs in the order of CHF 1 million for reduced obligations and initial investments of CHF 2 to 3 million plus recurring costs of around CHF 1.5 million per year for full obligations. These costs are driven primarily by specialised personnel requirements, data-retention infrastructure, security architecture adjustments, and 24/7 operational readiness. Beyond these direct expenditures, firms also face serious **indirect costs** related to regulatory uncertainty, opportunity costs, and internal resource reallocation.

The revision has particularly pronounced consequences at firm-level for PDCS with privacy-centric business models. Firstly, Swiss PDCS face a competitive disadvantage and reputational risks compared with foreign competitors. Secondly, firms must divert resources from innovation to compliance, delaying product development, constraining strategic flexibility, and reducing investment attractiveness, especially for startups. Thirdly, labour market effects include increased demand for specialised compliance roles, but net job losses are likely if firms downsize, relocate, or exit the market, particularly in high-skilled positions. Finally, domestic value creation and tax revenues may decline as firms move infrastructure, legal entities, or employees abroad, thereby reducing their GDP contributions, tax payments, and knowledge spillovers. The broader macroeconomic and international implications are analysed in the following chapter.

Box 3: Impact on other stakeholders: private users and public institutions

The consequences affect not only companies, but also other stakeholders. The obligation to store metadata increases both the availability and the concentration of sensitive information at companies affected by the SPTO revision. The mere presence of such data on servers expands the potential attack surface for cyberattacks, as highlighted particularly by the Internet Society[40] and Konsumentenforum Switzerland[41]. Firms that previously operated with data-minimising architectures are required to retain information that would otherwise not be stored, as it has no technical value. This creates additional targets for hacking, since the expected value of a successful breach increases.

The revision also affects consumers by reducing the overall security of their personal data. The potential harm resulting from a single security breach increases as larger volumes of metadata are stored for longer periods. These risks arise independently of any unlawful behaviour by the affected users and apply to the general population.

At the same time, the accumulation of metadata also affects the usability, flexibility, and effective service quality providers can offer. A substantial share of these services' value is derived from data minimisation and confidentiality. Requirements that mandate broader data collection or retention directly undermine these core product attributes, leading to a deterioration in perceived service quality from the user perspective.

The SPTO revision also affects public institutions, which increasingly rely on secure digital communication services. For example, the Swiss government and its public authorities, including the Swiss Army, have adopted the encrypted messaging services by Threema as a primary channel for communication, largely in response to concerns about confidentiality and data protection.

The proposed revision may alter the security properties of these services by introducing mandatory metadata retention. As with private users, the increased availability and concentration of metadata could expand potential security vulnerabilities for federal institutions and state employees. This risk may be further amplified if regulatory pressure leads Swiss-based providers to relocate infrastructure, such as data servers, abroad. In such cases, sensitive communications involving federal employees or military personnel could be stored under different security standards or outside the direct control of Swiss authorities.

As a result, the revision may increase the exposure of governmental and military communications to data breaches or unauthorised access. While this does not imply an immediate loss of confidentiality, it raises the expected risks associated with handling sensitive state-related information and may affect the long-term digital resilience of public institutions.

[40] Internet Society Switzerland Chapter. (2025). *Geplante VÜPF-Revision bedroht Grundrechte und kompromittiert Verschlüsselungen.* Geplante VÜPF-Revision bedroht Grundrechte und kompromittiert Verschlüsselung - ISOC Switzerland Chapter [02.03.2026].

[41] Konsumentenforum Switzerland. (2025). *Stellungnahme zur VÜPF-Revision*. https://konsum.ch/wp-content/uploads/2025/05/VL-Stellungnahme-Konsumentenforum.pdf [11.03.2026].

4 Macroeconomic analysis

This chapter analyses the macroeconomic impacts of a full implementation of the revised SPTO relative to a continuation of the status quo. PDCS and TSP are not confined to a single sector but are embedded in a wide range of economic activities—for example in finance (e.g. SIX), e-commerce (e.g. Digitec), and the digital trust sector (e.g. Threema). Consequently, the effects of the SPTO revision are expected to be heterogeneous across sectors. The strongest negative impact is anticipated in the digital trust sector, which fundamentally depends on credibility, confidentiality, and secure data handling (see Section 3.2). Measures such as removable encryption and extended data retention periods (see Section 2.3.2 and Appendix A.2) risk undermining this trust, increasing attack surfaces and the probability of data breaches, with potentially rapid and disproportionate losses in confidence.

4.1 Relevance of the digital trust sector

Switzerland offers exceptional conditions for the development of digital trust. Historic political neutrality, strong and independent institutions, legal certainty, and political stability create a uniquely reliable environment for data-intensive industries. The country's data-protection standards—combined with a workable regulation—are seen as key locational advantages. This is reflected in the presence of international corporations such as Kaspersky, Acronis, or SWIFT, which operate data centres in Switzerland to benefit from its high-quality infrastructure and robust privacy regime.[42]

To institutionalise and accelerate this momentum, the cantons of Vaud and Geneva founded the "Trust Valley" in 2020, a competence centre dedicated to cybersecurity, digital trust, and emerging technologies. The region currently hosts more than 300 specialised companies and over 500 experts, forming a dense and fast-growing digital trust ecosystem.[43] Complementary initiatives, such as the Swiss Digital Initiative and its globally pioneering Digital Trust Label, reinforce Switzerland's position by providing internationally recognised standards for trustworthy digital services. These efforts are underpinned by robust public-private collaboration. For example, over 50 partners from government and academia (including EPFL) meet annually at the "Trust Valley Day" to coordinate their industry's strategic priorities and to network and explore opportunities illustrating the vibrancy of the tech cluster.

Beyond these institutional developments, the sector's economic importance is becoming more measurable. According to different market analyses the global digital trust market is projected to reach between CHF 92 and 386 billion in 2025 of which CHF 3.2 to 6.4 billion can be—based on calculations by Swiss Economics—attributed to the Swiss digital trust

[42] Factsheet: Die Schweiz als Standort für Cybersicherheit [20.01.2026].

[43] See the website of Trust Valley.

sector.[44] The Swiss market is projected to grow at an annual rate of between 10.1 and 21.6 percent in the coming years. This implies a projected market size of between CHF 5.2 and 17.1 billion by 2030 and between CHF 8.5 and 45.5 billion by 2035. This growth is driven by the rapid digitalization of core industries (finance, healthcare, manufacturing), high per capita R&D expenditure supported by favourable federal digital-innovation funding programs and Switzerland's long-standing emphasis on data sovereignty and privacy protection.[45]

Switzerland's digital trust sector extends beyond the Lake Geneva region. The country also hosts one of the world's most recognised blockchain clusters: Zug's "Crypto Valley".[46] Over the past decade, favourable corporate tax policies, legal clarity and a highly tech-literate investor base enabled blockchain and Web3 firms to scale globally from Switzerland. The region attracted hundreds of startups, global foundations (e.g. Ethereum Foundation) and significant venture capital, thus consolidating Switzerland's reputation as a neutral, secure and innovation-friendly environment for decentralised technologies.

[44] The calculations are presented in **Appendix B**. The reason for the wide range is an imprecise definition of the digital trust market and limited data availability.

[45] See e.g. Digital Trust Market Size & Share Analysis - Growth Trends and Forecast (2026 - 2031) [20.01.2026], Switzerland Cybersecurity Market Size & Share Analysis - Growth Trends and Forecast (2026 - 2031) [20.01.2026].

[46] See the website of Crypto Valley.

Box 4: Towards a "Stockholm-Style" Innovation Cluster?

A compelling European reference point for cluster dynamics is Stockholm, which has established itself as one of the continent's most successful tech ecosystems.[47] It produces a high number of globally scaled firms from a relatively small domestic market. Stockholm's ecosystem—valued at approximately USD 250 billion with more than 2'500 startups and 30+ unicorns[48]—has grown through sustained capital mobilisation, deep integration between research institutions, investors and corporate partners, and a culture of international ambition and collaboration. The presence of world-renowned success stories (e.g., Spotify, Klarna) has generated significant founder-operator recycling and reinvestment into new ventures, creating a self-reinforcing cycle of experience, capital and leadership that lowers growth frictions for subsequent generations of firms.[49]

Switzerland exhibits several structural similarities that could support a comparable trajectory:

- high concentration of deep-tech talent and strong academic anchors (EPFL, ETH Zurich),
- policy frameworks favouring legal certainty and low regulatory risk,
- an established venture capital ecosystem (e.g. Redalpine, Founderful),
- emerging, internationally visible clusters (Trust Valley, Crypto Valley), and
- steady market expansion of the relevant sectors.

Together, these factors position Switzerland well to emerge as a counterpart to Stockholm's innovation cluster. Achieving this potential would depend on replicating the mechanisms that enabled Sweden's early successes, including strong capital formation, internationalisation from inception, and a feedback loop of successful exits generating experienced entrepreneurs and investors.

Sweden's experience suggests that success breeds success: unicorn exits and scaleups not only generate capital but also produce a pool of experienced founders, executives and angel investors who actively seed and mentor the next generation of companies, reinforcing cluster dynamics and lowering barriers to scaling.

Whether such a development ultimately materialises in Switzerland is, of course, uncertain. However, several interview partners emphasised that the digital trust sector is at a critical inflection point, where a new cluster is likely to emerge. At present, Switzerland appears well positioned to compete in this race. However, a full implementation of the proposed SPTO revision would, in the view of the interviewees, effectively end this race before it has truly begun for Switzerland.

---

[47] Similar cluster dynamics have also been observed in other leading innovation hubs, such as Tel Aviv. There, decades of targeted public support, strong venture capital mobilisation (e.g. through the Yozma initiative), and close integration between academia, startups, and multinational firms have produced a globally significant ecosystem—particularly in cybersecurity, AI, and life sciences. Like Stockholm, Tel Aviv illustrates how early scaleups, exits, and internationalisation can trigger self-reinforcing cycles of capital formation, talent recycling, and entrepreneurial experience. See e.g. "Start-up Nation": An incomplete history and profile of Israel's rise in Cybersecurity [20.01.2026], Tel Aviv Ranks #4 Global Startup Ecosystem in 2025 Global Startup Ecosystem Report by Startup Genome [20.01.2026].

[48] STOCKHOLMS EKOSYSTEM FÖR STARTUPS 2025 [27.02.2026].

[49] Stockholm - Europe's Unicorn Factory [27.02.2026].

Role of data sovereignty, privacy protection and reputation in the digital trust sector

A growing body of research on data governance and the economics of privacy highlights that strong data-protection regimes and clear data-sovereignty arrangements are key factors in the location of digital trust industries. The OECD shows that trusted, well-governed data environments both reinforce trust across the data ecosystem and stimulate investment and data sharing. Conversely, weak governance and loss of control over data undermine innovation and digital value creation.[50]

Similarly, empirical research in the field of the economics of privacy has found that the willingness of users and firms to adopt digital services depends critically on the provision of credible privacy guarantees. When these guarantees are undermined, usage, innovation and market growth decline.[51] The Digital Trust report by CEBR quantifies this relationship, showing that higher levels of digital trust are associated with significantly stronger economic growth and that trust deficits translate into missed GDP and revenue potential. The report finds that a 5 percentage-point increase in digital trust is associated with an average increase in GDP per capita of USD 3'000.[52]

Recent policy and industry analyses take this one step further by framing data sovereignty as a "strategic design imperative" for building and maintaining digital trust.[53] If data-sovereignty and privacy protections are weakened, firms may withhold sensitive data, relocate critical infrastructure or reduce investment. This could lead to the stagnation or even erosion of digital trust clusters.[54]

A loss of trust has, thus, a direct and significant economic impact. The World Economic Forum (WEF) warns that a lasting breach of trust in technology and data protection endangers innovation and economic strength: *"If trust in technology is lost forever, then so too might be the possibility of a future of innovation and opportunity."* A survey by Mc Kinsey[55] shows that more than half of consumers only buy from companies known for protecting customer data. As soon as reports of data breaches or questionable handling of privacy emerge, customers switch to competitors (40 percent of respondents ended their business relationship due to

---

[50] Going Digital to Advance Data Governance for Growth and Well-being [20.01.2026], Data governance | OECD [20.01.2026], Privacy and data protection [20.01.2026].

[51] Acquisti, Tayolor & Wagman (2016). The Economics of Privacy.

[52] The digital trust index [20.01.2026].

[53] See e.g. Cybersecurity as Switzerland's Strategic Imperative [22.01.2026], Data Sovereignty: The Driving Force Behind Europe's Sovereign Cloud Strategy [20.01.2026], Digital trust: Why it matters for businesses [20.01.2026], SAP's Sovereignty Commitment: "Building a Secure and Sovereign Future, Together" [20.01.2026], Why data sovereignty is now a dealbreaker in cybersecurity [21.01.2026].

[54] Concrete examples are the relocation of infrastructure of Proton (see Section 3.2.4) or the relocation of Session to Switzerland (see Introducing the Session Technology Foundation [20.01.2026]). Note, Session relocated to Switzerland before the proposal of the SPTO revision became public.

[55] Digital trust: Why it matters for businesses [20.01.2026].

a data protection violation).[56] The survey further establishes that a strong reputation for data protection attracts not only customers but also investors and skilled workers. Some parts of the literature even regard digital trust as intangible capital: once trust has been shaken, it is difficult to regain.[57]

This effect can also be observed at the firm-level. According to a Gartner survey of CIOs in Western Europe, 61 percent report increased concerns about digital sovereignty and control over data and infrastructure due to geopolitical developments. This has led to a higher reliance on local or regional cloud solutions.[58] An analysis by Proton found that approximately 75 percent of public firms in Europe use US-based tech services.[59] Consequently a shift to European tech would require the European market—including the digital trust sector—to grow significantly. In line with these findings, Gartner forecasts a significant rise in spending on sovereign cloud infrastructure and predicts that spending on sovereign cloud in Europe will increase by over 80 percent year on year in 2026.[60] This suggests that concerns about sovereignty are becoming a key factor in investment decisions. In this broader context, it seems that firms are placing greater importance on the legal and regulatory environment in which their data is hosted.

In addition, the recent discussions within the EU regarding a European preference in public procurement suggest that not only firms but also the governments are adapting their behaviour. Especially in the areas defence and digital sovereignty, concerns regarding over-reliance on the US as well as security concerns over US providers are raised in Switzerland.[61] While these developments are still in an early stage, they suggest that European solutions could have significant growth opportunities in the public sector.

Against this backdrop, the growth prospects for Swiss digital trust providers are structurally strong. Demand for data sovereignty, secure cloud infrastructure, and credible privacy guarantees is expanding rapidly, thereby increasing the overall size of the digital trust

---

[56] This phenomenon is currently playing out in the AI sector following the Department of Defense (DoD) contract shift. After the DoD terminated its agreement with Anthropic—reportedly over the latter's refusal to facilitate domestic mass surveillance—and signed a direct contract with OpenAI, market data showed a surge of Anthropic's Claude in the App Store ranking (see Claude just beat ChatGPT on the App Store, and the reason is surprising [09.03.2026]). The impact was significant enough that OpenAI CEO Sam Altman publicly clarified on X [09.03.2026] that OpenAI would not engage in mass surveillance, in an attempt to restore consumer trust.

[57] Paliszkiewicz, Chen, Launer (2022). Trust and Digital Business., Digital trust: Why it matters for businesses [20.01.2026], Why data sovereignty is now a dealbreaker in cybersecurity [21.01.2026].

[58] Gartner Survey Reveals Geopolitics Will Drive 61% of CIOs and IT Leaders in Western Europe to Increase Reliance on Local Cloud Providers [13.02.2026].

[59] US tech rules the European market [18.02.2026].

[60] Gartner Says Worldwide Sovereign Cloud IaaS Spending Will Total $80 Billion in 2026 [13.02.2026].

[61] See for instance Von der Abhängigkeit zur Selbstbestimmung: Die digitale Zukunft der Schweiz [18.02.2026], Können wir uns bei unserer Verteidigung noch auf die USA verlassen? [18.02.2026], How tenaciously Palantir courted Switzerland [24.02.2026].

market. At the same time, firms are reassessing hosting locations and regulatory environments, creating scope for trusted jurisdictions to capture a larger relative share of this growing market. Switzerland, with its reputation for legal stability, trust, neutrality, and institutional credibility, is well positioned to benefit from this double dynamic—an expanding market and the potential to increase its share of it. However, the proposed SPTO revision introduces a significant downside risk: it weakens Switzerland's regulatory landscape and the perception of the Swiss brand, thereby undermining precisely the trust advantage on which this growth opportunity relies, thereby constraining or even reversing the sector's expansion trajectory.

4.2 Consequences of the proposed SPTO revision

Building on the analysis of the digital trust sector, this section examines the economic consequences of a full implementation of the revised SPTO. The analysis proceeds from the most directly affected sector to the broader macroeconomic consequences, reflecting how regulatory and reputational effects can spread from decisions made by individual firms to the wider economy.

Immediate effects on the digital trust sector

Interview evidence consistently indicates that the SPTO revision would fundamentally impair the growth prospects of Switzerland's digital trust sector. Although only a subset of digital trust firms are directly subject to the revised obligations, interview partners emphasised that the measures would undermine the viability of any privacy-centric business model by eroding perceived trustworthiness thus negatively affecting the entire Swiss digital trust sector.

Adjustments are already observable. Proton has established server infrastructure abroad and has publicly signalled that further investment and expansion in Switzerland are on hold as long as the implementation of the revised SPTO remains imminent. According to Proton, the Swiss regulatory environment is no longer compatible with its core value proposition.

Interviewees further indicated that similar considerations apply to a broad range of startups and scaleups active in privacy-enhancing technologies, secure communications, cybersecurity and cloud services, as well as to other internationally oriented providers.

Another example of this trend is the VPN provider PrivadoVPN. In early 2026, the company announced its relocation to Iceland, explicitly linking this decision to concerns regarding the proposed SPTO revision.[62]

As a result, the dynamic growth of the Swiss Trust Valley ecosystem is likely to be hampered. Rather than evolving into a dynamic cluster, the ecosystem risks stagnation or fragmentation, as anchor firms scale abroad and startups either relocate early in their life cycle

[62] 'Our users deserve better' – PrivadoVPN set to leave Switzerland on privacy grounds | TechRadar [13.02.2026].

or are founded outside Switzerland from the outset. Given the significant influence of network effects, mentorship, and signalling in cluster formation, the departure or failure to expand of just a few prominent players can be sufficient to prevent the development of a viable international hub.

Reputational effects and trust loss as a transmission channel

Beyond direct sectoral effects, all interview partners stressed the importance of reputational spillovers. Switzerland's international reputation as a trusted, neutral, and discreet jurisdiction is widely regarded as a shared asset that can benefit a wide range of economic activities. Trust, however, is asymmetrically fragile: it is costly and time-consuming to build but can be lost rapidly and is difficult to restore once damaged.

Trust affects total factor productivity (TFP), capital accumulation, innovation incentives, and location decisions of globally mobile firms.[63] Regulatory interventions that alter perceptions of trustworthiness can therefore have an overwhelming effect on sectors beyond those directly affected. The SPTO revision risks triggering precisely such a reputational shock.

Spillovers to other trust-based sectors

The economic consequences of the SPTO revision are unlikely to remain confined to the digital trust sector. Negative perceptions may spill over to other trust-intensive industries, including finance, insurance, healthcare-related data services, advanced research collaborations, and parts of the export-oriented services sector.

In these industries, Switzerland does not compete internationally on price or scale, but on credibility, stability, and institutional quality. A weakening of the "trusted Switzerland" narrative could reduce competitiveness even if products and services themselves remain unchanged. This mechanism mirrors recent international developments, where shifts in the perceived trustworthiness of jurisdictions (especially the US) –rather than changes in technology—have led firms and governments to reassess data location, supplier choices, and strategic dependencies.[64]

From a macroeconomic perspective, such spillovers amplify the initial shock. The relocation decisions of digital trust firms may have secondary effects on banking relationships, financing structures, professional services, and capital market activity. Over time, this can weaken the broader innovation ecosystem and reduce Switzerland's attractiveness as a location for high value-added activities.

---

[63] See e.g. Smith (2020). Trust and Total Factor Productivity: What Do We Know About Effect Size and Causal Pathways?, de Bliek & Burger (2015). Regional Trust, Liabilities of Foreignness and the Location Decision of Multinational Firms in Europe.

[64] E.g. Should Europe wean itself off US tech? [20.01.2026], Get over your X: A European plan to escape American technology [20.01.2026].

Figure 3 summarises the sector-specific impact channels of the revision. It highlights that PDCS within the digital trust sector are most directly and severely affected, facing both higher costs and a deterioration in trustworthiness. However, the figure also illustrates that even sectors outside the trust economy may still be affected, reflecting the broad, economy-wide relevance of trust and reputation. These secondary effects on other sectors can arise through several channels. For example, declining household income in the digital trust sector may reduce consumption, with negative repercussions for sectors such as tourism or construction.

Figure 3: Heatmap of sector-specific impact channels

	Other sectors (e.g., tourism, construction)	Other trust sectors (e.g,. finance, insurance)	Digital trust sector
Non-PDCS	Secondary effects	Reputational spillovers	Perceived trustworthiness
PDCS	Costs ↑ Secondary effects	Costs ↑ Reputational spillovers	Costs ↑ Trustworthiness

Source: Own representation

Path-dependency and aggregate implications for growth and investment

The proposed revision of the SPTO could undermine Switzerland's competitive advantages based on trust and reputation, which are structural rather than cyclical. If trust were to erode over a sustained period, this would weaken investment incentives, slow innovation, and dampen productivity growth, affecting long-term growth trajectories. Once trust-based clusters fail to emerge or existing activities relocate, it becomes difficult to recover the momentum and foregone investment, even if the regulatory framework is adjusted at a later stage.

In this context, path dependency is a key consideration. The regulatory decisions taken today will not only shape the immediate legal environment but also the long-term location choices and ecosystem development.[65] Once firms have shifted investment abroad, relocated parts of their operations, or deprioritised Switzerland in their growth strategies, it is costly and time-consuming to reverse these decisions. Interview partners consistently emphasised that subsequent regulatory corrections are not sufficient to reverse the damage caused by an extended period of uncertainty. From this perspective, the SPTO revision entails the risk of locking Switzerland into an unfavourable development path by weakening the very sectors that are built on its traditional strengths of trust, stability, and institutional credibility.

[65] See e.g. Martin & Sunley (2006). Path dependence and regional economic evolution. Journal of Economic Geography., Dixit & Pindyck (1994). Investment Under Uncertainty. Princeton U. Press., Antonelli (1997). The economics of path-dependence in industrial organization. International Journal of Industrial Organization.

From a structural growth perspective, the development of trust-based digital activities can be understood as an S-curve dynamic. Switzerland appears to be positioned at the beginning of the expansion phase, where network effects, cluster formation, and increasing returns to scale can generate accelerating growth. In such a phase, early momentum is critical: if regulatory uncertainty prevents the ecosystem from reaching critical mass, the economy risks remaining on the lower, flat segment of the curve instead of transitioning to sustained expansion. Locking in a non-expansion path at this stage would imply not only foregone short-term gains but the loss of an entire high-growth trajectory that, once missed, is difficult to recreate.[66]

4.3 Impact on the digital trust sector

This section develops a forward-looking assessment of the Swiss digital trust sector under the two described regulatory options (see Section 2.3): retention of the status quo and full introduction of SPTO revision. The objective is not to produce point estimates, but to illustrate how different regulatory paths could shape the sector's medium- to long-term development. Given the inherent uncertainty surrounding both regulatory implementation and how firms will respond, the quantification is intentionally presented as a range of estimates.

4.3.1 Assumptions

Retention of the status quo

Assuming the current regulatory framework continues, the Swiss economy and the digital trust sector are assumed to grow broadly in line with existing projections. Switzerland would retain its established positioning as a trusted jurisdiction for data-intensive and security-critical digital services and the "Swiss trust premium" would still be intact. Firms could continue to scale within Switzerland, new entrants would consider Switzerland an attractive location. Furthermore, network effects within the Digital Trust Valley would support growth. In this scenario, uncertainty mainly relates to the pace of growth, not its direction, which is why we present a relatively wide but strictly positive range of estimates.

Crucially, the status quo scenario assumes regulatory clarity. It is assumed that all actors consider a revision of the SPTO obligations for PDCS to be off the political agenda and do not expect renewed legislative attempts to reintroduce comparable provisions in the foreseeable future. In other words, the baseline reflects not only a continuation of the current regime, but also the absence of renewed regulatory uncertainty that could otherwise delay investment, scaling decisions, or market entry.

[66] See e.g., Porter, M. E. (1998). Clusters and the New Economics of Competition. Harvard Business Review., Arthur, W. B. (1989). Competing Technologies, Increasing Returns, and Lock-In by Historical Events. The Economic Journal, *99(394).*, Rogers, E. M. (2003). Diffusion of Innovations (Fifth edition). Free Press.

The remaining uncertainty surrounding future growth is twofold.[67] First, the trajectory of the Swiss digital trust sector is closely linked to global dynamics and will depend on how strongly international demand expands. Second, uncertainty remains regarding the evolution of Switzerland's relative market share. However, the evidence presented suggests that, given rising demand for data sovereignty and trusted jurisdictions, Switzerland is well positioned to increase its share within the growing global market.

Full introduction of the SPTO revision

The second option reflects the implementation of the revised SPTO. We assume that the Swiss economy will grow broadly in line with existing projections and that the digital trust sector will continue to exist in Switzerland. However, we assume that its aggregate size will remain broadly unchanged over a five- respectively ten-year period, implying zero net growth. As we explain below, these assumptions are conservative for several reasons.

First, PDCS would be directly and disproportionately affected. Higher compliance costs, operational constraints, and legal uncertainty would force many existing providers to substantially adapt their business models or relocate activities abroad. Second, and critically, the impact would not be confined to PDCS alone. The digital trust sector is highly integrated. Switzerland's appeal lies in its collective reputation as a reliable and predictable jurisdiction for trusted digital services. A regulatory shift perceived internationally as undermining confidentiality and legal certainty would therefore spill over to firms that are not formally subject to the regulation. The would result in a deterioration of their positioning in the international market, as the "Swiss trust premium" erodes. This could potentially lead to downsizing, relocation or foreclosure of firms in the Swiss digital trust sector that do not qualify as PDCS. Furthermore, the evidence presented in section 4.2 indicates that other trust-based sectors —and potentially the Swiss economy as a whole—may be affected, implying lower growth than currently projected.

Taken together, these effects very likely result in a slowdown in Swiss economic growth and a (partial) collapse of the digital trust sector. They also imply a loss of the sector's growth engine. While the digital trust sector may persist, its current vibrant expansion and clustering dynamics would almost certainly dissipate. Our assumption that the aggregate size of the digital sector remains the same is therefore conservative.

[67] If regulatory clarity were combined with a structurally improved and innovation-enhancing framework, growth could exceed the upper bound of the status quo baseline. This upside case is not incorporated into the present scenario.

4.3.2 Quantification of the economic impact

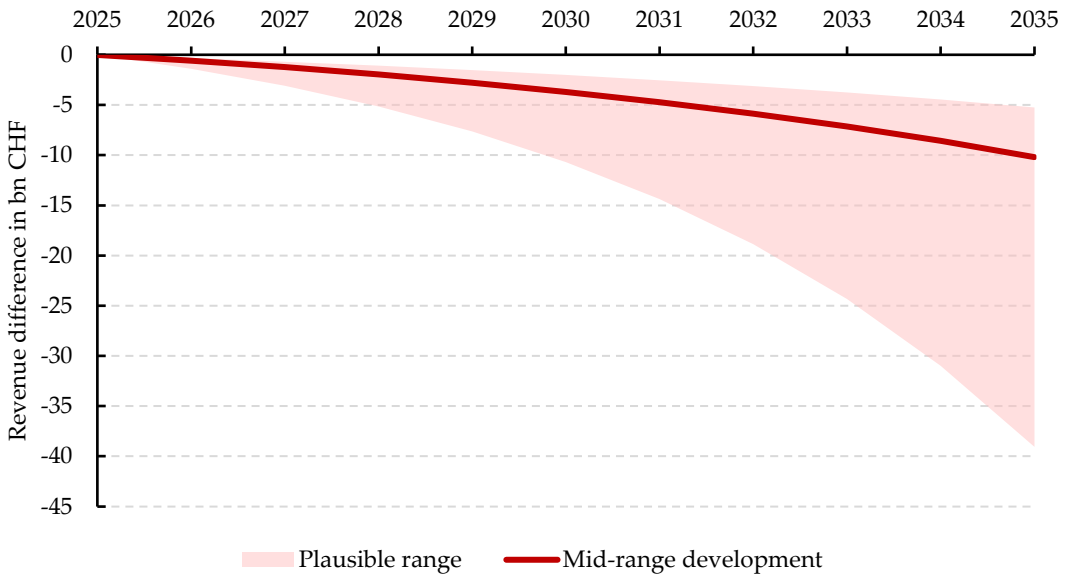
This section quantifies the economic effects, focusing on revenues, welfare, employment, and tax impacts. It presents the difference between a trajectory based on the status quo and a full implementation of the SPTO revision.[68]

Impact on revenues

It is currently estimated that the digital trust sector in Switzerland is worth between CHF 3.2 billion and 6.4 billion. However, projected growth differs markedly across trajectories.

Under the status quo, the sector is projected to expand at an average annual rate of 12 percent over the next decade (with a range of 10.1 to 21.6 percent). If the SPTO revision is introduced, the sector is expected to experience zero growth over the same period. The impact of the proposed SPTO revision on the digital trust sector is calculated as the difference between these two trajectories over the next ten years, as illustrated in Figure 4.

Figure 4: Revenue differences



Source: Own representation

Figure 4 shows the exponentially increasing negative impact of persistent growth differentials over time. The widening range illustrates that uncertainty increases with the projection horizon. By 2030, potential yearly revenue losses range from CHF 2 to 10.7 billion, increasing to CHF 5.2 to 39.1 billion by 2035. While short-term effects may appear moderate, this trajectory indicates that long-term consequences will become increasingly significant due to the compounding nature of the sector's growth. It is also notable that the potential downward negative effects are asymmetrically higher, as the outcome depends heavily on the

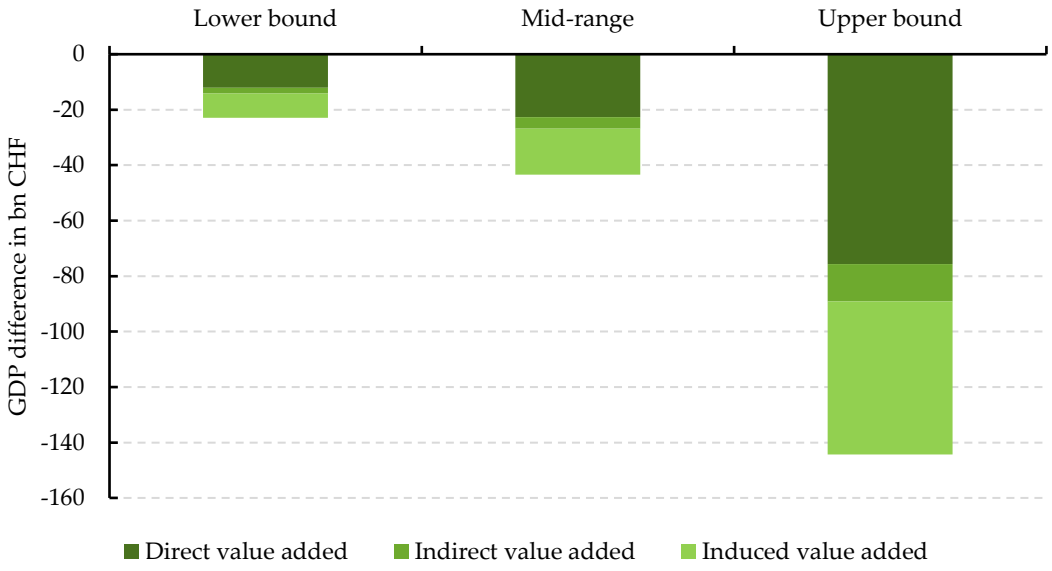
[68] The methodological approach, underlying assumptions, detailed calculations, and data sources are documented in Appendix B.

strength of sustained growth dynamics over a full decade. Our mid-range estimate suggests potential cumulative losses of approximately CHF 46.8 billion by 2035.

Impact on Welfare

The welfare analysis focuses on order-of-magnitude estimates of cumulative welfare losses over the period 2025-2035. Welfare impacts are derived using input-output-tables, which allow the decomposition of effects into direct, indirect, and induced components. Direct welfare losses reflect value added foregone within the digital trust sector itself; indirect effects capture spillovers along upstream supply chains, while induced effects arise from reduced household income and consumption. These estimates are aggregated over the full projection horizon to provide a cumulative assessment of welfare implications. Figure 5 presents the results for the lower bound, mid-range, and upper bound development.

Figure 5: Cumulative welfare differences (2025-2035)



Source: Own representation

The results indicate a lower-bound cumulative welfare loss of around CHF 14 billion when only direct and indirect effects are considered. Depending on assumptions regarding sectoral growth, the upper bound of these direct and indirect losses could reach approximately CHF 89 billion. If induced effects are also included, the cumulative upper-bound impact could rise to as much as CHF 144 billion. However, because induced effects are highly sensitive to modelling assumptions, these figures should be interpreted as indicative ranges rather than precise estimates, with the upper bounds reflecting substantial uncertainty.

Box 5: Quantification of cross-sectoral spillovers

Beyond the direct effects in the digital trust sector, negative spillovers to the broader Swiss economy are likely (see section 4.2). While these effects are potentially substantial, they are inherently difficult to quantify and subject to considerable uncertainty.

One way to illustrate the potential severity of such spillovers is the CEBR Trust Index.[69] Switzerland currently scores 73 index points, reflecting high levels of confidence in digital services, governance, and data protection. A decline in trust—for instance, triggered by the proposed SPTO revision—would be expected to lower this score.

If Switzerland's trust levels were to fall to those observed in countries such as Germany or the United States (roughly 20 index points lower), GDP per capita could decline over time by about USD 12'000—around 10 percent of its current level.[70] While these estimates should be interpreted with caution, they indicate that such a development would imply a substantial loss in welfare for the Swiss population.

Most interview partners were unable to quantify the negative impact on the Swiss economy. Nevertheless, they highlighted an important asymmetry: The direct economic effects are most pronounced for firms operating within the digital trust sector—with welfare losses including induced effects reaching up to CHF 36 billion or 3 to 4 percent of GDP in 2035.[71] However, the largest costs are likely to arise from cross-sectoral spillovers and economy-wide losses in trust.

[69] The digital trust index [20.01.2026]. We obtained the figure for Switzerland upon request from CEBR.

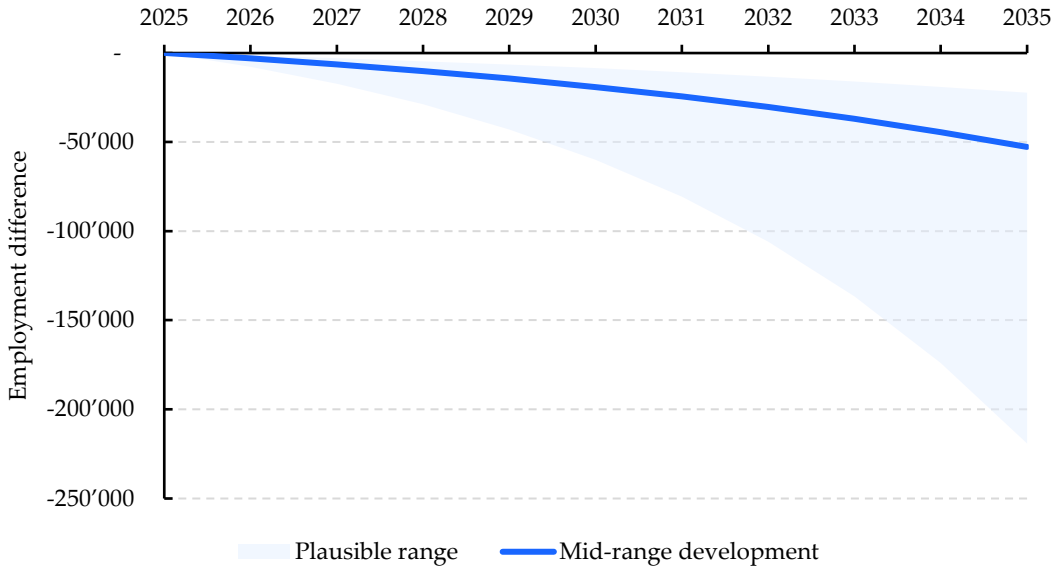
[70] THE CEBR analysis finds that one index point increase in digital trust is associated with an average increase in GDP per capita of USD 596 (The digital trust index [20.01.2026]). Accordingly, a 20 index point decline is associated with an average decrease in GDP per capita of approximately USD 12'000. In addition, the IMF estimates GDP per capita in Switzerland in 2025 at USD 111'050 (IMF Switzerland Country Data [06.03.2026]). Hence, the decline of approximately USD 12'000 corresponds to around 10 percent of the current level of GDP per capita.

[71] CHF 36 billion corresponds to 3 to 4 percent of Swiss GDP in 2035 if the nominal GDP growth rate were to lie between 0.75 and 3.25 percent on average. It is expected that the actual growth rate will fall within this range (see e.g. Energieperspektiven 2050+ Volkswirtschafltiche Auswirkungen [06.03.2026] published by the Federal Council).

Impact on employment

Employment in the digital trust sector is estimated to range between 13’800 and 36’200 jobs in 2025. As described in Appendix B, employment is projected using the same range of growth rates as applied to revenues, ensuring a consistency across economic indicators. The impact of the proposed SPTO revision is, as before, quantified as the deviation between the status quo and a full implementation of the SPTO revision. Figure 6 illustrates the resulting employment trajectories over the next ten years.

Figure 6: Employment differences



Source: Own representation

The figure illustrates a rapidly intensifying negative impact. The widening spread of outcomes reflects growing uncertainty as the projection horizon extends. By 2030, estimated employment losses in the digital trust sector range between 8’500 and 60’000 jobs, rising to between 22’400 and 219’300 by 2035. This pattern suggests that while the short-term impact remains relatively contained, the longer-term effects will become increasingly severe. Under the mid-range development scenario, employment losses are estimated at around 52’700 jobs by 2035. Taken together, these figures suggest a significant risk of a large-scale exodus of highly skilled workers from Switzerland’s digital trust sector, implying that the revision of the SPTO could trigger a major brain drain.

Impact on taxes

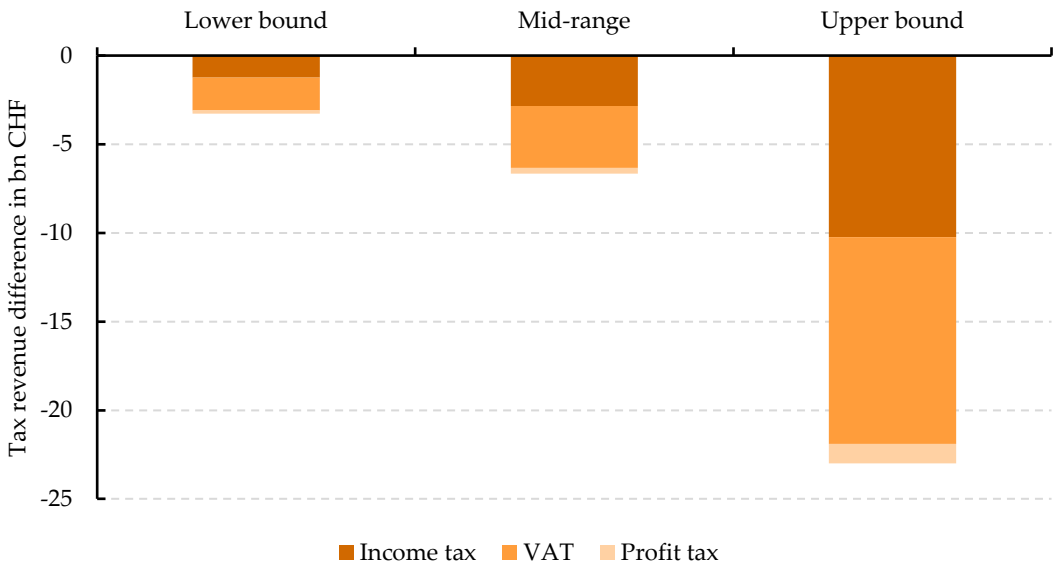
Given the substantial uncertainty surrounding the estimation of foregone tax revenues, we limit the analysis to order-of-magnitude estimates of cumulative tax losses over the period 2025-2035. The calculation focuses on tax revenues from

- value added taxes (VAT),
- profit taxes and,
- income taxes, including communal, cantonal, and direct federal taxes.

Appendix B.4 provides a detailed description of the underlying assumptions and methodological choices used in the calculation for each tax category.

The results are presented in Figure 7. The wide range reflects uncertainty regarding future sectoral dynamics. Against this background, the results should—again—be interpreted as indicative. Overall, the estimated cumulative tax revenue losses over the projection horizon range from approximately CHF 3 to 22 billion.

Figure 7: Cumulative tax revenue differences (2025-2035)



Source: Own representation

4.4 Summary

This chapter evaluates the macroeconomic consequences of a full implementation of the revised SPTO compared with maintaining the status quo. As PDCS and TSP are embedded across a wide range of economic activities, the effects of the revision will be heterogeneous across sectors. The most significant impacts are expected in the digital trust sector, where business models fundamentally rely on credibility, confidentiality, and secure data handling. Given this central role and its strong growth dynamics, the digital trust sector is analysed as the primary transmission channel through which broader macroeconomic effects materialise.

The analysis shows that a full implementation of the SPTO revision would substantially weaken the growth prospects of the Swiss digital trust sector. While only a subset of firms would be directly affected, the perceived erosion of Switzerland's trustworthiness would affect the entire ecosystem. Interview evidence and observed firm behaviour indicate a high risk of stalled investment, relocation of activities abroad, and the dissipation of cluster dynamics. The sector would at best stagnate in the medium to long term.

Quantitatively, the divergence between the two regulatory options is substantial. Relative to the status quo, annual revenue losses in the digital trust sector are estimated to reach between CHF 5.2 and 39.1 billion by 2035. Cumulative revenue losses amount to approximately CHF 47 billion by 2035 in the mid-range estimate, reflecting the compounding effects of foregone growth. Welfare losses, measured using input–output analysis, are estimated at CHF 14 to 89 billion for direct and indirect effects over the period 2025-2035.

This dynamic is mirrored in the employment effects as well: By 2035 employment losses relative to the status quo are estimated to range between 22'400 and 219'300 jobs, with a mid-range estimate of around 47'200 foregone jobs. Foregone tax revenues over the same period are estimated at between CHF 3 billion to 22 billion in cumulative terms, including VAT, profit taxes, and income taxes.

Beyond these quantifiable effects, the chapter highlights the risk of a broader macroeconomic impact, driven by reputational factors. A weakening of Switzerland's international standing as a trusted jurisdiction would likely affect other trust-intensive sectors, amplifying the initial shock. While these spillovers are difficult to quantify, they may ultimately represent the largest economic cost. Overall, the results indicate that the SPTO revision poses a significant structural risk to growth, employment, welfare, and public finances, due to the loss of a key trust-based growth engine of the Swiss economy.

A Categories and obligations of TSP and PDCS

A.1 Retention of the status quo

Table 3 summarises the categories and obligations of TSP, and Table 4 provides the same overview for PDCS. Both summaries are based on the current version of the SPTO. The detailed obligations are set out in the SPTO as of 26 March 2024.

Table 3: TSP categories and their respective obligations

Category	Classification criteria	Obligations
TSP with reduced obligations (Art. 51)	Downgrading upon request to the PTSS if the legal conditions are met. Main criteria: (a) the provider offers telecommunications services **exclusively in the field of education and research**, *or* (b) in the last 12 months it has received **no more than 10 surveillance orders relating to 10 different surveillance targets**, *and* (c) the **total domestic revenue of the transmission and derived communication service is less than CHF 100 million** in each of the last two business years. The assessment is based on **transmission and derived communication service revenue**, not on total corporate revenue.	Fundamental obligations include: ▪ identify users using appropriate means[72] ▪ retain subscriber information required for information requests ▪ provide standardised information responses and special information ▪ demonstrate information-readiness ▪ permit surveillance measures, grant access to systems where require and remove provider-applied encryption ▪ transmit available traffic metadata upon request without any retention obligation
TSP with full obligations	Standard category: every TSP is initially considered as a TSP with full obligations. A downgrading becomes effective only once the PTSS formally approves it. If the criteria of Art. 51 cease to be fulfilled, the TSP must notify the PTSS, who then declares the re-upgrade to the full-obligations category.	All obligations from the reduced category plus: ▪ 24/7 on-call service ▪ retention of traffic metadata needed for certain information requests and retroactive surveillance ▪ provision of information through the automated information-request interface of the PTSS and demonstration of readiness to use it ▪ automated information provision and mandatory use of the information-request interface ▪ technical capability to deliver both content and metadata for real-time and retroactive surveillance. Newly upgraded TSP benefit from transition periods of 2 or 12 months, depending on the complexity of the obligations.

[72] The explanatory report mentions some examples that could qualify as appropriate means under Art. 19. For instance, Identification via credit card and saving the authorization data or identification via the SIM-card and saving the International Mobile Subscriber Identity (IMSI).

Table 4: PDCS categories and their respective obligations

Category	Classification criteria	Obligations
PDCS without more extensive duties	**Default category**, applicable as long as neither the criteria to meet the more extensive duties to provide information (Art. 22) nor the more extensive surveillance duties (Art. 52) are met	Only basic cooperation and information duties: ▪ provide information in a formless manner ▪ permit surveillance measures and grant access to systems where required ▪ provide any information necessary for surveillance ▪ transmit available traffic metadata upon request without any retention obligation
PDCS with more extensive duties to provide information (Art. 22)	**PTSS declares** a PDCS to be a provider with more extensive duties when, as of the reference date 30 June: **more than 100 requests for information** (12-month average across all derived communication services) *or* **domestic turnover of more than CHF 100 million** in the previous two business years if a large part of its business operations provides derived communication services *and* **more than 5'000 subscribers**.	Similar obligations as TSP with full obligations regarding **information duties**. However, some exceptions and downgrades apply: ▪ instead of 24/7 on-call service, provide contact information of internal on-call service (if existing) for particularly urgent cases. ▪ not required to provide information in accordance with Art. 48a–48c Transition periods: 2 months for simpler obligations, 12 months for technically complex ones.
PDCS with more extensive surveillance duties (Art. 52)	**PTSS declares** a PDCS to be a provider with more extensive duties when, as of the reference date 30 June: **10 or more different surveillance targets** (12-month average across all derived communication services) *or* **domestic turnover of more than CHF 100 million** in the previous two business years, provided a large part of its business operations provides derived communication services *and* **more than 5'000 subscribers**.	Similar obligations as TSP with full obligations regarding **surveillance duties**. However, some exceptions and downgrades apply: ▪ not required to conduct the type of surveillance in Art. 56a, 56b, 67 letters b and c and 68 paragraph 1 letters b and c ▪ not required to provide information in accordance with Art. 48a–48c Transition periods: 2 to 12 months depending on the obligation

A.2 Full introduction of the SPTO revision

Definition and obligations of TSP

A TSP—corresponding to the legal category "*Fernmeldedienstanbieterinnen (FDA)*"—is a provider that is responsible for the technical transmission of information. Unlike service providers that operate on top of another network, TSP offer access or transport services directly to end users and bear contractual responsibility for ensuring the delivery of communications. This includes providers that operate a public telecommunications network, offer direct access to such a network (e.g., internet access), provide public mobile communications services, or supply public telephony services together with network access.

Because TSP operate at the transmission layer and may hold traffic metadata and communication content relevant for surveillance, the ordinance assigns them a graduated set of obligations. These are divided into two categories: TSP with reduced obligations and TSP

with full obligations. The latter constitutes the default case under the revised ordinance. Table 5 summarises the two categories and their respective obligations.

Table 5: TSP categories and their respective obligations

Category	Classification criteria	Obligations
TSP with reduced obligations (Art. 16b)	Downgrading upon request to the PTSS if the legal conditions are met. Main criteria: (a) the provider offers telecommunications services **exclusively in the field of education and research**, *or* (b) in the last 12 months it has received **no more than 10 surveillance orders relating to 10 different surveillance targets**, *and* (c) the **total domestic revenue of the company is less than CHF 100 million** in each of the last two business years. The assessment is based on **total corporate revenue**, i.e., not only telecommunications-related revenue.	Fundamental obligations include: ▪ identify users by appropriate means ▪ retain subscriber information required for information requests ▪ provide standardised information responses and special information ▪ demonstrate information-readiness ▪ permit surveillance measures, grant access to systems where require and remove provider-applied encryption ▪ transmit available traffic metadata upon request without any retention obligation
TSP with full obligations (Art. 16c)	Standard category: every TSP is initially considered as a TSP with full obligations. A downgrading becomes effective only once the PTSS formally approves it. If the criteria of Art. 16b cease to be fulfilled, the TSP must notify the PTSS, who then declares the re-upgrade to the full-obligations category.	All obligations from the reduced category plus: ▪ 24/7 on-call service ▪ retention of traffic metadata needed for certain information requests and retroactive surveillance ▪ provision of information through the automated information-request interface of the PTSS and demonstration of readiness to use it ▪ automated information provision and mandatory use of the information-request interface ▪ technical capability to deliver both content and metadata for real-time and retroactive surveillance. Newly upgraded TSP benefit from transition periods of 6 or 12 months, depending on the complexity of the obligations.

Definition and obligations of PDCS

A PDCS (as introduced by the revision and corresponding to the legal category "*Anbieterinnen abgeleiteter Kommunikationsdienste, AAKD*") is a provider that enables interpersonal communication between users but does so on the basis of the communication infrastructure of another telecommunications service. PDCS do not operate their own access or transport networks; instead, they offer communication functionality "over the top" of a primary communication service. This includes, for example, messaging, calling, or other interpersonal-communication features integrated into online platforms, apps, or digital services. PDCS may be independent providers or may offer communication features as part of a broader digital service ecosystem.

What characterises PDCS legally is not the business model, but the technical fact that they rely on another provider's underlying communication infrastructure while still enabling direct interpersonal communication. Because they act as intermediaries in the communication process and may hold user- or message-related information relevant to surveillance, the ordinance subjects them to tiered obligations depending on their scale. An important result of the consultation process is that the definition of PDCS is not even for professionals in the field entirely clear and thus there exists considerable uncertainty on which firms—on top of the named examples—could also be PDCS.

The obligations of PDCS are categorised into three categories. PDCS with minimal obligations, PDCS with reduced obligations and PDCS with full obligation. Table 6 summarises the three categories and their respective obligations.

Table 6: PDCS categories and their respective obligations

Category	Classification criteria	Obligations
PDCS with minimal obligations (Art. 16e)	**Default category**, applicable as long as neither the criteria of reduced obligations nor full obligations are met. Concretely: **less than 5'000 participants** (12-month average) **and less than CHF 100 million** in domestic revenues in each of the previous two business years.	Only basic cooperation and information duties: ▪ provide information in a formless manner ▪ permit surveillance measures and grant access to systems where required ▪ provide any information necessary for surveillance ▪ transmit available traffic metadata upon request without any retention obligation
PDCS with reduced obligations (Art. 16f)	**Automatic upgrade** when, as of the reference date 30 June: **more than 5'000 but less than 1 million participants** (12-month average across all derived communication services) *and* **domestic revenues of less than CHF 100 million** in the previous two business years.	Obligations aligned with reduced-duty TSP: ▪ identify users by appropriate means ▪ retain subscriber information required for information requests ▪ provide standardised information responses and special information ▪ demonstrate information-readiness ▪ remove encryption applied by the provider Additional obligations must be implemented within 6 months after 30 June.
PDCS with full obligations (Art. 16g)	**Second upgrade** for providers of significant economic or user relevance. Criteria: (a) at least **1 million participants** (12-month average, reference date 30 June), *or* (b) **domestic revenues of more than CHF 100 million** in the previous two business years.	Obligations aligned with full-duty TSP. All obligations from the reduced category plus: ▪ 24/7 on-call service ▪ retention of traffic metadata needed for certain information requests and retroactive surveillance (6-month retention) ▪ automated information provision and mandatory use of the information-request interface ▪ technical capability to deliver both content and metadata for real-time and retroactive surveillance. Transition periods: 6 months for simpler obligations, 12 months for technically complex ones.

B Quantification of the Swiss digital trust market

This Appendix details the quantification of the economic impacts considered in this study. Appendix B.1 describes the methodology used to estimate revenues, Appendix B.2 covers the assessment of welfare effects, Appendix B.3 outlines the approach to quantifying employment, and Appendix B.4 presents the estimation of tax effects. All data sources and key references underlying these quantifications are summarised in Appendix B.5.

B.1 Revenues

Two complementary approaches are used to estimate the size of the Swiss digital trust market (DTM) in 2025:

- **Top-down allocation of the global DTM** to Switzerland based on Switzerland's share of global GDP, as well as its share of the global information and communications technology (ICT) and cybersecurity markets.
- **Extrapolation from France**, using published revenue data for the French digital trust market and scaling it to Switzerland based on relative market sizes.

The two approaches are first described in detail, after which the resulting estimates for the Swiss DTM are presented.

Breakdown of the global DTM 2025

The Swiss share of the global digital trust market is calculated using the following formula:

$$\boldsymbol{DTM_{CH} = DTM_{Global} * Share_{CHF/Global} * FX_{USD/CHF}} \quad (1)$$

where DTM_{Global} denotes the estimated global digital trust market, $Share_{CH/Global}$ represents Switzerland's share of the global economy or relevant markets, and $FX_{USD/CHF}$ is the USD/CHF exchange rate.

Estimates of the global DTM from six market studies range from USD 110 to 482 billion. The Swiss share is approximated using Switzerland's share of global GDP as well as its share of the global ICT and cybersecurity markets. Across five different indicators, the resulting shares range from 0.4 to 2.5 percent.[73] The exchange rate is based on the Federal Tax Administration's annual average USD/CHF rate for 2025, set at 0.83.

Extrapolation of the French DTM 2025

As a second approach, a market observatory published by the French Alliance for digital trust (*Alliance pour la Confiance Numérique*, ACN) is used. In its 2025 observatory, ACN reports revenues of EUR 21.3 billion for the French digital trust sector in 2024, compared to total global revenues of EUR 33.5 billion of French companies.

[73] GDP share from IMF, ICT share from Mordor Intelligence and Cybersecurity share from Mordor Intelligence, Data Bridge Market Research and Ken Research.

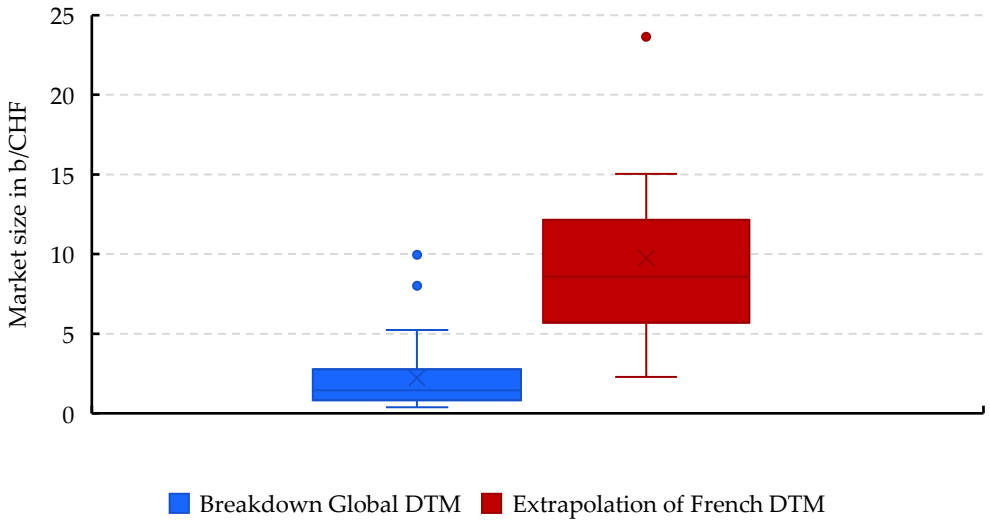
To obtain figures for 2025, the revenues are extrapolated, assuming a constant annual growth rate of 7.6 percent, corresponding to the average annual growth rate observed between 2018 and 2024 in France. This yields French digital trust revenues of EUR 22.9 to 36.0 billion in 2025.

The Swiss DTM is then derived by adapting equation (1) to the French revenue figures and scaling them according to Switzerland's share relative to France. Five alternative estimates of this share are considered, ranging from 11 to 70 percent.[74] The EUR/CHF exchange rate is set at 0.94.

Swiss DTM in 2025

Given the wide dispersion of input parameters, the estimated size of the Swiss digital trust market is subject to substantial uncertainty (see Figure 8).

Figure 8: Market size of the Swiss DTM in 2025



Source: Own representation

The estimates suggest that the Swiss DTM in 2025 ranges from CHF 0.4 to 23.6 billion. This wide range is driven by three main factors: First, projections of the global DTM differ substantially across sources, with estimates from Precedence Research being more than four times smaller than those of Mordor Intelligence. Second, the top-down breakdown of the global market generally yields lower estimates than the extrapolation based on French data. Third, the assumed Swiss market shares vary considerably across indicators: cybersecurity figures from Ken Research imply a Swiss DTM more than six times larger than estimates based on cybersecurity data from Mordor Intelligence.

To derive a more plausible central corridor, greater weight is assigned to the French-based estimates, as they rely on observed, sector-specific revenues from a clearly defined domestic

[74] GDP share from IMF, ICT share from Mordor Intelligence and Cybersecurity share from Mordor Intelligence, Data Bridge Market Research and Ken Research.

digital trust market instead of rough global market estimates. The analysis consequently focuses on French domestic revenues, excluding international revenues, to eliminate the possibility of a clear upward outlier. On this basis, both the lowest global estimates and the upper-end outcomes implied by extrapolating French international revenues are excluded. Moreover, the Swiss market shares implied by Mordor Intelligence and Ken Research appear inconsistent with Switzerland's GDP and ICT shares, which are instead well reflected in the estimates reported by Data Bridge Market Research. As a result, a Swiss share of 1 percent of the global DTM and 30 percent of the French domestic market are assumed as most likely values. Based on these considerations, the Swiss DTM in 2025 is assessed to lie in the range of approximately CHF 3.2 to 6.4 billion.

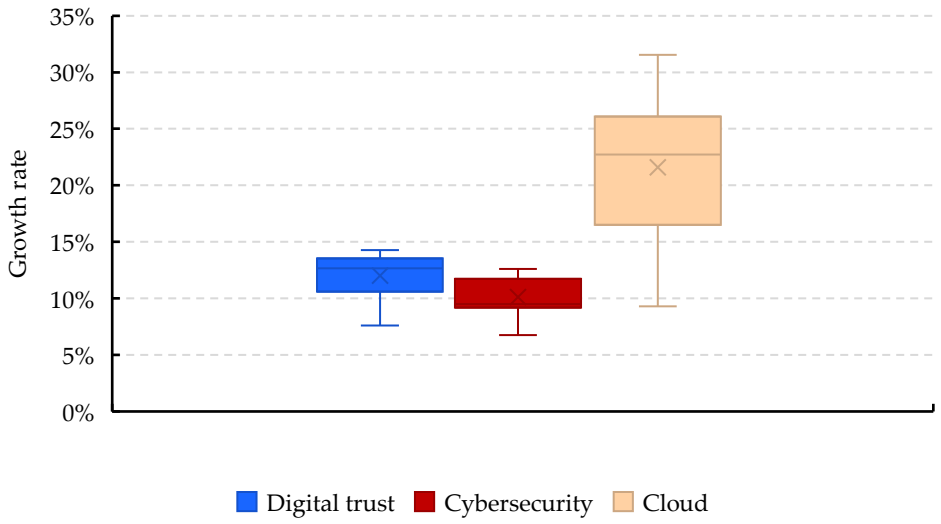
We exclude indirect revenue losses related to upstream activities from the quantitative analysis. However, a high-level assessment based on input-output-tables indicates that accounting for these indirect effects would imply additional revenue losses in the order of 60 percent.

Market growth

Several growth rates were identified that provide a plausible range for the development of the Swiss DTM over the next 5 to 10 years.

- **Digital trust**: This category includes available growth estimates for the global and French digital trust markets. No dedicated projections for the Swiss DTM were identified, underscoring the uncertainty surrounding its standalone trajectory.
- **Cybersecurity**: This category comprises growth estimates for the global, French, and Swiss cybersecurity markets. As cybersecurity constitutes a core segment of the DTM, these figures provide a relevant proxy for expected market dynamics.
- **Cloud**: This category contains estimates for global and Swiss cloud markets (e.g. cloud storage, public cloud). Cloud is part of digital security and thus represents a relevant area of the DTM.

Figure 9: Growth rate estimates



Note: Although evidence suggests that the Swiss cloud market has recently outpaced global growth, global benchmarks are retained without upward adjustment to ensure a conservative assessment framework.[75]

Source: Own representation

The figure shows that the estimated growth rates of all areas vary considerably. However, on average cybersecurity grow the least at 10.13 percent and cloud the most at 21.59 percent. This divergence is consistent with industry lifecycles: while cybersecurity represents a more mature, established market, the cloud sector is still in its early expansion phase, characterised by more dynamic growth. This range provides a structured corridor for scenario calibration. Cybersecurity represents the most mature core segment of the DTM and therefore constitutes a lower bound. Cloud markets, by contrast, capture the most dynamic and innovation-driven components of digital trust ecosystem and thus define an economically plausible upper bound. The DTM average estimate serves as a central benchmark.

Relying on these three sectoral averages ensures consistency, avoids cherry-picking individual outliers, and anchors the Swiss DTM projection within market dynamics of closely related segments. Accordingly, 10.13 percent is applied as a conservative lower bound, 21.59 percent as an upper bound reflecting high-growth dynamics, and 12.01 percent as a plausible central growth rate for the Swiss DTM over the next 5 to 10 years.

B.2 Welfare

The GDP impact is estimated using input-output-tables for NOGA 62 and 63 (IT and information services), which serve as a proxy for the digital trust sector. This framework allows the derivation of direct, indirect, and induced value added effects based on the revenue estimates presented above. Direct value added reflects the contribution generated within the digital trust sector itself. The resulting estimate for Switzerland, based on NOGA 62 and 63, is broadly consistent with ACN's corresponding estimates for the French digital trust

[75] Cloud Computing 2022 [17.02.2026].

sector. Indirect value added captures upstream spillover effects along the supply chain and is derived using established sectoral input coefficients from the input-output framework.

While the estimation of direct and indirect effects is relatively robust and well-grounded in the underlying data, the induced value added–primarily driven by additional consumption financed through higher household incomes–is subject to substantially greater uncertainty. As it depends on behavioural assumptions and multiplier effects, the induced component should therefore be interpreted as an upper bound of the welfare effects rather than a central estimate.

B.3 Employment

Employment in the Swiss DTM in 2025 is estimated using two approaches.

- **Extrapolation from France**: This approach relies on published employment figures for the French digital trust sector and scales them to Switzerland based on relative market sizes.
- **Revenues per employee ratio:** This method relies on the published revenues per full-time-equivalents (FTE) ratio[76] in the input-output-tables for the NOGA Codes 62 and 63 in Switzerland and scales it with the average employment rate. This ratio is then applied to the estimated mid-range revenues.

A top-down allocation from the global DTM is not feasible due to the absence of reliable data on global employment. The extrapolation therefore follows the same methodology as outlined in Appendix B.1; we also exclude indirect EMPLOYMENT losses related to upstream activities from the quantitative analysis.

First, according to ACN, the French digital trust sector employed around 107'000 people in 2024. Applying the scaling approach (see Appendix B.1) yields a range of 12'900 to 84'400 employees for the Swiss digital trust sector in 2025. Using the previously identified plausible market share of 30 percent results in a point estimate of approximately 36'200 employees.

Second, we apply the revenues per employee ratio of CHF 352 thousand per employee[77] to the mid-range revenues in 2025 in the Swiss DTM to calculate the employment in the Swiss DTM. It yields an estimate of 13'800 employees. Our client estimates current employment at around 25'000. Accordingly, we use the client estimate as the mid-range estimate, the revenues per employee ratio as lower bound and the extrapolated figure as the upper bound for the employment projections.

[76] Intuitively, this ratio describes how much revenue a firm in this sector generates on average for each full-time employee. If the revenues-per-FTE ratio is then scaled by the average employment rate it then describes how much revenue is generated on average per employee.

[77] Calculated as CHF 420 thousand per FTE times the employment rate of 83.5 percent. For simplification purposes it is assumed that the resulting ratio stays constant over the next ten years.

Employment growth

Employment growth is calibrated using historical data for the French digital trust sector. According to ACN, employment increased from 52'300 employees in 2018 to 107'000 in 2024, corresponding to an average annual growth rate of 12.67 percent over the period 2018 to 2024. Growth was particularly strong between 2023 and 2024, when employment rose from 89'000 to 107'000 (an increase of 20 percent).

This most recent growth rate substantially exceeds the growth rates reported for the overall market in France and is therefore treated as an outlier and excluded from the baseline analysis. To remain conservative, we apply the same range of growth rates to employment as to revenues, despite the fact that historical evidence for France suggests that employment growth has on average exceeded revenue growth by around five percentage points.

B.4 Taxes

The estimation of foregone tax revenues is subject to increasing uncertainty, particularly over longer time horizons. Nevertheless, in line with the methodological guidelines[78], we provide order-of-magnitude estimates, as presenting a plausible range of outcomes offers greater analytical value than refraining from quantification altogether. The estimation covers effects on value-added tax (VAT), income and profit tax revenues.

VAT

The VAT impact is derived from the estimated revenue losses and applies a constant VAT rate of 8.1 percent.[79] To remain conservative, VAT is assumed to be deducted from the reported revenue figures rather than added on top, thereby avoiding an overstatement of tax revenue losses.

Income taxes

The income tax estimation assumes an annual gross income of CHF 108'000, corresponding to the lowest median income observed in 2024 across the relevant sectors, i.e. telecommunications (NOGA 61), IT services (NOGA 62), and information service activities (NOGA 63). Taking the median instead of the average and assuming a constant income level over time reflects a conservative approach. The average effective tax rate is set at 13 percent, based on the Swiss tax calculator[80] and corresponding to a 35-year-old single individual residing in Zurich in 2025. It should be noted that the digital trust sector is currently concentrated in the cantons of Geneva and Vaud, where the effective tax rate for the same

[78] Leitfaden zur Schätzung der Regulierungskosten [20.01.2026]. This guideline is based on the *Unternehmensentlastungsgesetz*.

[79] Also, likely a conservative assumption as the VAT has gradually increased over the past decades and currently two items are discussed in parliament that might lead to further increases.

[80] Tax calculator [28.01.2026].

income level would range between 15 and 18 percent. The chosen assumption therefore understates, rather than overstates, potential income tax losses.

Profit taxes

The estimated impact on profit taxes is derived from cumulative revenues over the period 2025 to 2035. Given that the digital trust sector is still in a high-growth phase and characterised by a large share of startups, a conservative profit margin of 5 percent is assumed. This assumption lies well below the Software Industry's reported average profit margin of 8.8 percent in 2022 as documented in the Swiss Software Industry Survey 2023. For taxation, we apply the prevailing effective profit tax rate of 14 percent for profits up to CHF 10 million of the canton Vaud.

B.5 Data sources

Value	Meaning	Source name	Source link
EUR 21.3 bn	Revenue in FR by French digital trust companies 2024	ACN	https://www.confiance-numerique.fr/wp-content/uploads/2025/06/acn-observatory-of-digital trust-2025.pdf
EUR 33.5 bn	Global revenues by French digital trust companies 2024	ACN	https://www.confiance-numerique.fr/wp-content/uploads/2025/06/acn-observatory-of-digital trust-2025.pdf
7.6 %	Avg. growth rate of digital trust sector in France 2016-24	ACN	https://www.confiance-numerique.fr/wp-content/uploads/2025/06/acn-observatory-of-digital trust-2025.pdf
107'000	Employees in French digital trust sector 2024	ACN	https://www.decision.eu/wp-content/uploads/2024/06/Observatory-of-digital trust-sector-2024.pdf
89'000	Employees in French digital trust sector 2023	ACN	https://www.confiance-numerique.fr/wp-content/uploads/2025/06/acn-observatory-of-digital trust-2025.pdf
52'300	Employees in French digital trust sector 2018	ACN	https://www.confiance-numerique.fr/wp-content/uploads/2023/11/Observatoire-ACN-de-la-Confiance-numerique-2019.pdf
USD 3'360 bn USD 1'000 bn USD 117'170 bn	GDP of FR GDP of CH GDP World	IMF	https://www.imf.org/external/datamapper/NGDPD@WEO/OEMDC/ADVEC/WEOWORLD
0.831 0.937	FX USD/CHF FX EUR/CHF	FTA	https://www.estv.admin.ch/estv/de/home/bundesabgaben/wehrpflichtersatzabgabe/wpe-jahresmittelkurse.html
USD 482 bn 14.28 %	Global DTM 2025 CAGR	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/digital trust-market
USD 135 bn 13.3 %	Global DTM 2025 CAGR	FMI	https://www.futuremarketinsights.com/reports/digital trust-market
USD 133 bn 13.3 %	Global DTM 2025 CAGR	GVR	https://www.grandviewresearch.com/industry-analysis/digital trust-market-report
USD 110.47 bn 11.6 %	Global DTM 2025 CAGR	Presedence research	https://www.precedenceresearch.com/digital trust-market
USD 388.54 bn 12 %	Global DTM 2025 CAGR	Market Research Future	https://www.marketresearchfuture.com/reports/digital trust-market-21989
USD 118 bn	Global DTM 2024	Ken Research	https://www.kenresearch.com/global-digital trust-market

USD 44.7 bn	ICT market CH	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/switzerland-ict-market
USD 135 bn	ICT market FR	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/france-ict-market
USD 6'030 bn	ICT market global	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/information-and-communications-technology-market
USD 0.97 bn 6.75 %	Cybersecurity CH Market size 2025 CAGR	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/switzerland-cybersecurity-market
USD 2.66 bn 9.3 %	Cybersecurity CH Market size 2024 CAGR	Data Bridge Market Research (DBMR)	https://www.databridgemarketresearch.com/nucleus/switzerland-cybersecurity-market
USD 3.5 bn	Cybersecurity CH Market size 2024	Ken Research	https://www.kenresearch.com/switzerland-cyber-security-market
USD 3.5 bn 9.4 %	Cybersecurity CH Market size 2024 CAGR	Trend Tracker Analytics	https://www.linkedin.com/pulse/north-america-switzerland-cybersecurity-market-cnwxc/
USD 235.5 bn 12.28 %	Cybersecurity Global Market size 2025 CAGR	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/cyber-security-market
USD 301.92 bn 12.6 %	Cybersecurity Global Market size 2025 CAGR	Presedence Research	https://www.precedenceresearch.com/cyber-security-market
USD 227.59 bn 9.1 %	Cybersecurity Global Market size 2025 CAGR	Markets & Markets	https://www.marketsandmarkets.com/PressReleases/cyber-security.asp
USD 203.9 bn 9.5 %	Cybersecurity Global Market size 2024 CAGR	DBMR	https://www.databridgemarketresearch.com/reports/global-cybersecurity-market
USD 141 bn	Cybersecurity Global Market size 2024	Ken Research	https://www.kenresearch.com/global-cybersecurity-software-market
USD 9.1 bn 11.08 %	Cybersecurity FR Market size 2025 CAGR	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/france-cybersecurity-market
USD 8.09 bn 11.2 %	Cybersecurity FR Market size 2024 CAGR	DBMR	https://www.databridgemarketresearch.com/nucleus/france-cybersecurity-market
USD 5.0 bn	Cybersecurity FR Market size 2024	Ken Research	https://www.kenresearch.com/france-cybersecurity-for-critical-infrastructure-market
8.1 %	VAT	FTA	https://www.estv.admin.ch/de/mwst-steuersaetze-schweiz

CHF per month 9'380 9'874 9'014	Med. income 2024 Telecommunications IT Services Information Services	FSA	https://www.bfs.admin.ch/bfs/de/home/statistiken/arbeit-erwerb/loehne-erwerbseinkommen-arbeitskosten.html
48.62 % 57.32 % 92.72 % CHF 420'000	Direct value added Indirect value added Induced value added revenues per FTE	FSA	https://www.bfs.admin.ch/bfs/de/home/statistiken/volkswirtschaft/input-output.html
5.362 m 4.480 m	Employees FTE	FSA	https://www.bfs.admin.ch/bfs/de/home/statistiken/arbeit-erwerb/erwerbstaetigkeit-arbeitszeit/erwerbsbevoelkerung/arbeitsmarktstatus.html
14 %	Profit taxes Vaud	KPMG	https://kpmg.com/ch/de/medien/medienmitteilungen/2025/05/clarity-swiss-taxes.html
8.8 %	EBIT Software Industry 2022	Swiss Software Industry Survey 2023	https://www.swico.ch/media/filer_public/93/d4/93d4ad40-8986-4eb5-9fc6-6e632871faac/ssis_report_2023.pdf
23.45%	Cloud Storage Market global CAGR	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/cloud-storage-market
24.41%	Cloud Storage Market global CAGR	DBMR	https://www.databridgemarketresearch.com/reports/global-cloud-storage-market
31.1%	Cloud AI Market global CAGR	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/cloud-ai-market
31.53%	Cloud AI Market global CAGR	DBMR	https://www.databridgemarketresearch.com/reports/global-cloud-ai-market
9.31%	Cloud Managed Services Market CAGR	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/cloud-managed-services-market
17.69%	Public Cloud Market global CAGR	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/public-cloud-market
22.95%	Public Cloud Migration Market global CAGR	DBMR	https://www.databridgemarketresearch.com/reports/global-public-cloud-migration-market
22.5%	Public Cloud CH CAGR	PWC	https://www.pwc.ch/en/insights/fs/how-swiss-banks-and-insurers-can-leverage-the-cloud-for-value-creation.html
12.97%	Cloud Service Market CH CAGR	DBMR	https://www.databridgemarketresearch.com/nucleus/switzerland-cloud-service-market
20%	IaaS & SaaS CH growth rate	Kellerhals Carrard	https://kellerhals-carrard.ch/download/204/2022_cloud_computing_switzerland.pdf