swiss economics

Regulierungsfolgenabschätzung: Revision der VÜPF

Michael Altorfer

Dr. Samuel Rutz

Dr. Michael Funk

Noé Arnold

Lukas Grether

Bericht im Auftrag von FONGIT

26.05.2026

ISSN 2235-1868

Metainformationen

Titel:	Regulierungsfolgenabschätzung: Revision der VÜPF
Version:	V1
Datum:	26.05.2026
Autoren:	Michael Altorfer, Noé Arnold, Michael Funk, Lukas Grether, Samuel Rutz
Kontakt:	Samuel Rutz, +41 79 204 78 83, samuel.rutz@swiss-economics.ch

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

Abstract

Die Schweiz hat sich als führender Standort für Geschäftsmodelle im Bereich «Digital Trust» etabliert. Dies ist u.a. auf ihre politische Neutralität und Stabilität, den pragmatischen Regulierungsrahmen sowie den Zugang zu qualifizierten Fachkräften zurückzuführen. Auch ohne eine umfassende Digitalstrategie hat der bestehende Rahmen bislang ausreichend Rechtssicherheit und Vorhersehbarkeit geboten, um Innovationen in Bereichen wie Cybersicherheit, sichere Kommunikation und Cloud-Dienste zu fördern.

Vorliegender Bericht untersucht die ökonomischen Auswirkungen der Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF). Auf Basis von Expertengesprächen, Kostenschätzungen auf Unternehmensebene sowie quantitativen Projektionen wird gezeigt, dass die geplante Revision eine Abkehr von etablierten regulatorischen Grundsätzen darstellt und mit gesamtwirtschaftlichen Effekten einhergeht, die sich insbesondere im Digital Trust-Sektor deutlich bemerkbar machen. Obwohl die Revision formal als verhältnismässig dargestellt wird, würde sie die meisten Anbieter abgeleiteter Kommunikationsdienste strengeren Pflichten unterwerfen, erhebliche Kosten verursachen und «Swissness» von einem Wettbewerbsvorteil in einen -nachteil verwandeln.

Eine vollständige Umsetzung der vorgeschlagenen Revision könnte bis 2035 zu Wohlfahrtsverlusten von bis zu CHF 36 Mrd. und zu Beschäftigungsverlusten von bis zu 219'300 Arbeitsplätzen im Digital Trust-Sektor führen. Grundsätzlicher noch besteht das Risiko, dass die Revision die regulatorische Kohärenz sowie den Ruf der Schweiz als vertrauenswürdiger Rechtsraum untergräbt – ein potenzieller Kipppunkt für ihre Rolle als internationaler Innovationshub für digitales Vertrauen, mit Ausstrahlungseffekten auf die gesamte Schweizer Volkswirtschaft.

Zentrale Ergebnisse

Überblick über die aktuelle Situation

Die digitale Politik der Schweiz ist derzeit von einer grundlegenden Ambivalenz geprägt, die ihre Stellung als vertrauenswürdiger Wirtschaftsstandort gefährdet.

Während die Strategie «Digitale Schweiz» darauf abzielt, Datensouveränität und Vertrauen der Bevölkerung zu stärken, schafft die vorgeschlagene Revision der VÜPF regulatorische Unsicherheit und führt letztlich zu strategischer Inkohärenz.

Die Mehrheit der Stellungnahmen in der Vernehmlassung lehnt den Entwurf der VÜPF-Revision ab, was den breiten politischen und wirtschaftlichen Widerstand spiegelt.

Die Ablehnung reicht von zivilgesellschaftlichen Organisationen, die auf verfassungswidrige Massenüberwachung hinweisen, bis hin zu Risikokapitalfonds, die negative Auswirkungen auf das Startup-Ökosystem befürchten.

Die Revision der SPTO würde Umfang und Intensität der Überwachungspflichten in der Schweiz deutlich ausweiten.

Die neue Regelung zielt auf Verhältnismässigkeit ab, doch in der Praxis würden für die meisten Anbieter abgeleiteter Kommunikationsdienste (AAKD) deutlich verschärfte Überwachungspflichten gelten (z. B. Vorratsspeicherung und Aufhebung von Verschlüsselung).

Die vorgeschlagene Revision benachteiligt Schweizer Unternehmen strukturell gegenüber ihren Wettbewerbern in der EU und den USA.

Internationale Vergleiche zeigen, dass die EU und die USA von pauschaler Vorratsdatenspeicherung abgerückt sind oder diese nie eingeführt haben. Mit der Durchsetzung von Vorratsdatenspeicherung und automatischer Herausgabe würde in der Schweiz ein Regime etabliert, das deutlich eingriffsintensiver ist als jenes in vergleichbaren Rechtsordnungen.

Auswirkungen auf betroffene Unternehmen

Mehrere tausend Unternehmen könnten von der geplanten VÜPF-Revision betroffen sein; die Compliance-Kosten pro Unternehmen dürften in die Millionen gehen.

Wie hoch die Compliance-Kosten ausfallen werden, hängt stark von Umsetzung der Vorlage und dem Geschäftsmodell der einzelnen AAKD ab. Langfristig könnten die indirekten Kosten (z.B. regulatorische Unsicherheit oder Opportunitätskosten) die direkten Kosten jedoch klar übersteigen.

Der Schaden entsteht schon heute: «Swissness» wandelt sich bereits heute von einem Wettbewerbsvorteil zu einer strategischen Belastung für datenschutzorientierte Firmen.

Die regulatorische Unsicherheit wird von internationalen Wettbewerbern bereits heute in B2B-Ausschreibungen genutzt, um die Verlässlichkeit von Schweizer Anbieter in Frage zu stellen. Der Reputationsverlust ist ökonomisch bedeutsam, da Vertrauen einer der Hauptgründe ist, weshalb Kunden Schweizer Dienste wählen.

Makroökonomische Analyse

Der Digital Trust-Sektor ist ein wichtiger Wachstumsmotor für die Schweiz, reagiert jedoch äusserst sensibel auf regulatorische Änderungen.

Angesichts der weltweit steigenden Nachfrage nach digitalen Vertrauensdiensten ist der Schweizer Markt gut für Wachstum im kommenden Jahrzehnt positioniert. Ein durch die VÜPF-Revision ausgelöster «Reputationsschock» könnte die Schweiz jedoch auf einen ungünstigen Entwicklungspfad bringen und die Bildung von Technologieclustern hemmen.

Negative Spillover-Effekte könnten weit über den Technologiesektor hinausreichen und das allgemeine Vertrauen in den Standort Schweiz gefährden.

Vertrauen ist keineswegs ein vernachlässigbarer Faktor; es beeinflusst die totale Faktorproduktivität, die Kapitalakkumulation, Innovationsanreize sowie Standortentscheidungen global mobiler Unternehmen. Sollte der «Schweizer Vertrauensbonus» erodieren, könnten auch nicht direkt betroffene Dienstleistungen in anderen Sektoren an internationaler Wettbewerbsfähigkeit einbüssen.

Quantitative Prognosen deuten darauf hin, dass eine vollständige Umsetzung der Revision bis 2035 kumulierte Wohlfahrtsverluste von bis zu CHF 36 Mrd. im Digital Trust-Sektor verursachen könnte.

Die Diskrepanz zwischen dem Status quo und der vorgeschlagenen Revision offenbart mögliche Wertschöpfungsverluste von bis zu 3-4 Prozent des Schweizer BIP. Während die Untergrenze der Schätzung auf Wohlfahrtsverluste von rund CHF 3 Mrd. hindeutet, könnte die Obergrenze jedoch auch ein Vielfaches hiervon betragen; die Auswirkungen des entgangenen Wachstums für die Schweizer Wirtschaft könnte somit gravierend ausfallen.

Die kumulierten Steuerausfälle aus dem Digital Trust-Sektor könnten sich im kommenden Jahrzehnt kumulativ auf bis zu CHF 22 Mrd. belaufen.

Die geschätzten kumulierten Steuerausfälle von CHF 3 bis 22 Mrd. im Zeitraum 2025-2035 gegenüber dem Status quo setzten sich aus entgangenen Einnahmen aus der Mehrwertsteuer, Gewinnsteuern und Einkommenssteuern zusammen.

Die Revision der VÜPF birgt das Risiko eines massiven Braindrains, mit geschätzten Beschäftigungsverlusten von bis zu 219'300 Arbeitsplätzen im nächsten Jahrzehnt.

Zwar könnten durch Compliance-Anforderungen einzelne spezialisierte Arbeitsplätze entstehen, der Nettoeffekt aus Unternehmensverlagerungen, Marktaustritten etc. ist jedoch eindeutig negativ. Bis 2035 könnte die verhinderte Schaffung von Arbeitsplätzen den Schweizer Arbeitsmarkt erheblich belasten, mit geschätzten Verlusten zwischen 22'400 und 219'300 Stellen.

Inhaltsverzeichnis

Tabellen

Abbildungen

Abkürzungen

AAKD	Anbieter abgeleiteter Kommunikationsdienste
ACN	Allianz für Digital Trust
B2B	Business to Business
BIP	Bruttoinlandprodukt
BKB	Beschaffungskonferenz des Bundes
BÜPF	Bundesgesetz über die Überwachung des Post- und Fernmeldeverkehrs
DACH	Deutschland (D), Österreich (A) und Schweiz (CH)
DBMR	Data Bridge Market Research
Dienst ÜPF	Dienst Überwachung des Post- und Fernmeldeverkehrs
DSG	Datenschutzgesetz

DTM	Digital Trust Markt
E-ID	Elektronische Identität
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EU	Europäische Union
EuGH	Europäischer Gerichtshof
FDA	Fernmeldedienstanbieterin
IKT	Informations und Kommunikationstechnologie
IP	Internet Protokoll
KI	Künstliche Intelligenz
KMU	Kleine und mittlere Unternehmen
MWP	Mitwirkungspflichtige
MWST	Mehrwertsteuer
NGO	Nichtregierungsorganisation
OTT	Over The Top
PZD	Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen
RFA	Regulierungsfolgenabschätzung
SaaS	Software as a Service
SECO	Staatssekretariat für Wirtschaft
StPO	Strafprozessordnung
USA	Vereinigte Staaten
VoIP	Internetbasierte Kommunikationsdienste, die Telekommunikationsdiensten entsprechen
VÜPF	Verordnung über die Überwachung des Post- und Fernmeldeverkehrs
VZÄ	Vollzeitäquivalent
VPN	Virtuelles privates Netzwerk
WEF	Weltwirtschaftsforum
WMC	Warrant Management Component

1 Einleitung

1.1 Ausgangslage

Am 29. Januar 2025 eröffnete der Bundesrat die Vernehmlassung zur vorgeschlagenen Revision der *Verordnung über die Überwachung des Post- und Fernmeldeverkehrs* (VÜPF).[1] Im Rahmen des Vernehmlassungsverfahren, das am 6. Mai 2025 endete, äusserte sich eine Vielzahl von interessierten Kreisen, und zwar überwiegend negativ. Insbesondere auf Datenschutz und sichere Kommunikation spezialisierte Unternehmen – darunter die Branchenführer Proton, Threema und Nym –, aber auch Branchenverbände, politische Parteien, Nichtregierungsorganisationen (NGO) und Verbraucherorganisationen äusserten starke Bedenken hinsichtlich der Revisionsvorschläge des Bundesrates.[2]

Die unter der Leitung des Eidgenössischen Justiz- und Polizeidepartements (EJPD) geplante Revision konzentriert sich primär auf den Ausbau der Überwachungsmöglichkeiten der Strafverfolgungsbehörden. Hervorzuheben ist dabei, dass die Überwachungspflichten für Anbieter von abgeleiteten Kommunikationsdiensten (AAKD) erweitert und neue Unterkategorien eingeführt werden sollen – etwa AAKD mit reduzierten Pflichten und AAKD mit vollen Pflichten, die künftig beide strengeren Anforderungen unterliegen würden. Dazu gehören u.a. erweiterte Überwachungs- und Auskunftspflichten. Teilweise müssten Anbieter zudem automatisierte Antworten auf Anfragen von Strafverfolgungsbehörden ermöglichen.[3] Kritiker argumentieren deshalb, dass solche Massnahmen unverhältnismässige Compliance-Kosten verursachen und ein erhebliches Sicherheitsrisiko darstellen würden. Sie befürchten überdies, dass Innovations- und Markteintrittsbarrieren die Position der Schweiz als weltweit führender Anbieter von Technologien im «Digital Trust»-Bereich und Datenschutz untergraben könnten.

Im Rahmen der Vernehmlassung gingen mehr als 200 Stellungnahmen ein, wobei die Mehrheit entweder eine grundlegende Überarbeitung oder eine vollständige Rücknahme des Revisionsvorschlags forderte. Das EJPD hat die Vernehmlassungsergebnisse ausgewertet und eine externe Regulierungsfolgenabschätzung (RFA) in Auftrag gegeben. Nach Abschluss dieser RFA plant das EJPD eine zweite Vernehmlassungsrunde.[4]

1.2 Auftrag

In diesem Zusammenhang hat FONGIT eine unabhängige RFA zur Revision der VÜPF in Auftrag gegeben. Diese konzentriert sich sowohl auf die Auswirkungen auf

---

[1] Fernmeldeüberwachung und mitwirkungspflichtige Unternehmen: Vernehmlassung eröffnet [21.01.2026]. Beachte, dass wir stets den Entwurf vom Januar 2025 als «Revisionsvorschlag» bezeichnen.

[2] Siehe Vernehmlassung 2022/21 [20.01.2026].

[3] Siehe Vernehmlassung 2022/21 [20.01.2026].

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

Unternehmensebene als auch auf die makroökonomischen Auswirkungen der vorgeschlagenen Revision.

Ziel der unabhängigen RFA ist es, eine faktenbasierte Analyse zu erstellen, die nicht nur auf den administrativen Aufwand, der mit einer allfälligen Revision der VÜPF einhergeht, fokussiert, sondern auch die weiterreichenden potenziellen Auswirkungen auf den Digital Trust-Sektor sowie auf die Schweiz insgesamt aufzeigt.

Die unabhängige RFA vergleicht zwei Regulierungsszenarien:

- Den **Status quo**, der das derzeitige Regulierungsniveau darstellt; und
- die **Vernehmlassungsvorlage des Bundesrats** vom Januar 2025.

Für jedes Szenario bewertet die unabhängige RFA sowohl die mikroökonomischen als auch makroökonomischen Auswirkungen. Auf mikroökonomischer Ebene umfasst dies Compliance-Kosten, Auswirkungen auf Wettbewerb und Preise sowie Folgen für Investitionen, Innovation, Technologiecluster und öffentliche Einnahmen. Auf makroökonomischer Ebene schätzt die unabhängige RFA die potenziellen Auswirkungen auf das Bruttoinlandsprodukt (BIP), die Beschäftigung, die Steuereinnahmen und den internationalen Ruf der Schweiz als Digital Trust-Nation.

1.3 Methoden und Struktur

Die unabhängige RFA ist wie folgt strukturiert:

- **Kapitel 2** bietet einen Überblick über die aktuelle Situation und erläutert die digitale Strategie der Schweiz, die vorgeschlagene VÜPF-Revision, die geprüften Regulierungsoptionen sowie die Stellungnahmen der betroffenen Stakeholder in der Vernehmlassung. Zudem enthält Kapitel 2 einen Vergleich mit den rechtlichen Rahmenbedingungen in der Europäischen Union (EU) sowie den Vereinigten Staaten (USA).
- **Kapitel 3** analysiert die Auswirkungen auf die betroffenen Unternehmen. Das Kapitel konzentriert sich in erster Linie auf AAKD, da diese von den vorgeschlagenen regulatorischen Änderungen voraussichtlich am stärksten betroffen wären. Ein separater Abschnitt untersucht überdies die Auswirkungen der VÜPF-Revision auf die Fernmeldedienstanbieter (FDA).
- **Kapitel 4** enthält eine makroökonomische Analyse: Es beleuchtet die Bedeutung des Digital Trust-Sektors für die Schweiz, erörtert die potenziellen Auswirkungen der VÜPF-Revision einschliesslich sektorübergreifender Spillover-Effekte und präsentiert eine quantitative Abschätzung der Folgen für den Digital Trust-Markt, die gesamtwirtschaftliche Wohlfahrt, die Beschäftigung sowie die Steuereinnahmen.

Die Ergebnisse vorliegender unabhängiger RFA basieren auf «Desk Research», Informationen und internen Analysen von FONGIT und werden, soweit möglich, mit empirischer Evidenz untermauert. Zudem wurden Experteninterviews mit Vertretern der folgenden Organisationen durchgeführt: Digitale Gesellschaft, Proton, SIX, Threema und Trust Valley.

2 Überblick über die aktuelle Situation

Dieses Kapitel untersucht die vorgeschlagene Revision der *Verordnung über die Überwachung von Post und Fernmeldeverkehrs* (VÜPF) im Kontext der digitalen Strategie der Schweiz. Zunächst wird die Ambivalenz der aktuellen digitalen Strategie der Schweiz aufgezeigt, anschliessend werden die Kernelemente der vorgeschlagenen VÜPF-Revision umrissen und die möglichen Regulierungsoptionen vorgestellt. In einem weiteren Schritt werden sodann die Stellungnahmen der interessierten Kreise aus dem Vernehmlassungsverfahren diskutiert. Die entsprechenden Antworten liefern Hinweise auf eine drohende Inkohärenz der digitalen Strategie der Schweiz und sprechen mögliche negative Auswirkungen der VÜPF-Revision auf das hiesige digitale Ökosystem an, denen in den nachfolgenden Kapiteln dann vertieft nachgegangen wird. Schliesslich wird der Schweizer Revisionsvorschlag einem Vergleich mit den rechtlichen Rahmenbedingungen in der Europäischen Union (EU) und den Vereinigten Staaten (USA) unterzogen.

2.1 Die digitale Regulierung in der Schweiz am Scheideweg

Die digitale Regulierung in der Schweiz steht derzeit an einem Scheideweg. Einerseits hat der Bund wiederholt seine Ambitionen bekundet, die Schweiz als vertrauenswürdiger digitaler Hub zu positionieren, der auf einem starken Datenschutz, dem Vertrauen der Bürger und der Förderung innovativer Geschäftsmodelle basiert. Andererseits droht die vorgeschlagene VÜPF-Revision, welche die Überwachungspflichten für Anbieter abgeleiteter Kommunikationsdienste (AAKD) – also Anbietern von Messenger-Services, E-Mail-Diensten, Cloud-Diensten etc. – pauschal ausweiten will, diesen Kurs zu untergraben. Es drohen Rechtsunsicherheit sowie regulatorische Inkohärenzen und Unklarheiten.

Eine zentrale Erkenntnis aus den Rückmeldungen zur Vernehmlassung und den von uns geführten Expertengesprächen ist, dass es vielen betroffenen Akteuren schwerfällt, eine klare und schlüssige digitale Strategie in der Schweiz zu erkennen. Dies, obwohl der Bundesrat die Strategie «Digitale Schweiz» jährlich aktualisiert und verabschiedet.[5] Anstatt sich an einer übergreifenden regulatorischen Vision zu orientieren, scheint sich die Digitalpolitik der Schweiz durch eine Reihe einzelner Initiativen und Rechtsakte zu entwickeln. Dies wurde bislang als unproblematisch eingeschätzt – trotz fehlender klar definierter Gesamtstrategie erwies sich das regulatorische Umfeld insgesamt als funktionsfähig und mit vertrauensbasierten digitalen Geschäftsmodellen vereinbar. Die Interviewpartner betonten dann auch wiederholt, dass die Schweiz aus regulatorischer Sicht nie als globaler Vorreiter wahrgenommen wurde. Vielmehr stellte sie bis anhin dank ihres angemessenen und insgesamt zurückhaltenden regulatorischen Rahmens – kombiniert mit Faktoren wie Qualität der schweizerischen Hochschulen (z.B. ETH, EPFL), Neutralität und Stabilität, Reputation sowie dem gehobenen Lebensstandard – ein attraktiver Wirtschaftsstandort dar.

[5] Bundesrat verabschiedet Strategie Digitale Schweiz 2026 [20.01.2026].

Darüber hinaus haben mehrere andere kürzlich ergriffene Massnahmen die Schweiz als Wirtschaftsstandort für Unternehmen im digitalen Bereich direkt oder indirekt gefördert. Dazu gehören etwa die Förderung vertrauenswürdiger Datenräume und der digitalen Selbstbestimmung[6] oder öffentliche Investitionen in Organisationen wie FONGIT oder das «Trust Valley». Zu nennen sind zudem die Förderprogramme des Bundes für digitale Innovation[7], die darauf abzielen, ein innovationsfreundliches Ökosystem für Technologie-Startups zu schaffen – darunter auch solche, die im «Digital Trust»-Bereich tätig sind. Im Bereich des Datenschutzes verankert das *Schweizer Datenschutzgesetz* (DSG) ferner die Datenminimierung als Kernprinzip und damit eine zurückhaltende Nutzung und Speicherung personenbezogener Daten. Auch andere staatliche Initiativen, wie die elektronische Identität (E-ID) oder die digitale Souveränität – zwei Schwerpunkte der «Digitalen Strategie Schweiz 2026» –, stützen sich explizit auf das Vertrauen der Bürger.

Insgesamt kann das regulatorische Umfeld im digitalen Bereich der Schweiz zwar als fragmentiert charakterisiert werden, die zugrundeliegende Logik wies bislang jedoch trotzdem eine gewisse Kohärenz auf: Es schützt die digitalen Rechte der Nutzer und fördert Geschäftsmodelle, die auf digitalem Vertrauen basieren. Auch wenn eine klar formulierte, übergreifende digitale Strategie fehlte, blieb das regulatorische Umfeld mit vertrauensbasierten Geschäftsmodellen vereinbar und bot den Unternehmen ein ausreichendes Mass an Vorhersehbarkeit für ihre Geschäftstätigkeit.

Die geplante VÜPF-Revision birgt jedoch die Gefahr, dieses fragile Gleichgewicht zu stören. Sie will Verpflichtungen einführen, die im Widerspruch zu international etablierten Regulierungsgrundsätzen stehen, und lässt eine klare Einbindung in den übergeordneten rechtlichen und politischen Rahmen vermissen. Dies führt zu erheblicher Unsicherheit für die betroffenen Unternehmen. Damit stellt sie nicht einfach eine kosmetische regulatorische Anpassung dar, sondern ein eigentlicher Wendepunkt – oder in den Worten eines Interviewpartners «*eine Katastrophe*». Wird die vorgeschlagene Revision wie vom Bundesrat vorgeschlagen umgesetzt, besteht das Risiko, dass die Schweiz für Digital Trust-Unternehmen künftig kein tragfähiger Standort mehr ist.

2.2 Zusammenfassung der geplanten VÜPF-Revision

Die Teilrevision des VÜPF zielt darauf ab, das Schweizer Überwachungsrecht den modernen digitalen Kommunikationstechnologien anzupassen. Die Revision, die Anfang 2025 in die Vernehmlassung ging, hat ihren Ursprung einerseits im entsprechenden Auftrag im *Bundesgesetz über die Überwachung des Post- und Fernmeldeverkehrs* (BÜPF). Andererseits schuf das «Threema-Urteil» des Bundesgerichts aus dem Jahr 2021 (Urteil 2C_544/2020) einen Revisionsbedarf. Es schützte die Privatsphäre der Messenger-App Threema, indem es

[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]. Innosuisse stellte CHF 60.4 Millionen bereit und steuerte Kapital in die Bereiche Quantencomputing, KI und Cybersicherheit.

entschied, dass Threema nach dem Schweizer Überwachungsrecht kein Fernmeldedienstanbieter (FDA) sei.

Das zentrale Ziel der vorgeschlagenen Revision besteht darin, die Kategorien der Mitwirkungspflichtigen (MWP) genauer zu definieren, um sicherzustellen, dass die Auferlegung von Überwachungspflichten klar, rechtssicher und – was entscheidend ist – verhältnismässig ausfällt (Art. 5 Abs. 2 BV).[8] Um die Verhältnismässigkeit zu gewährleisten, hat der Bundesrat eine umfassende Neukategorisierung der MWP vorgenommen, wobei die Pflichten auf Grundlage der wirtschaftlichen Grösse und Nutzerreichweite eines Anbieters festgelegt werden. Abbildung 1 gibt einen Überblick über die neu geplanten MWP.

Abbildung 1: Überblick über die neu geplanten Mitwirkungspflichten

FDA Anbieterinnen von Fernmeldediensten	**AAKD** Anbieterinnen abgeleiteter Kommunikationsdienste	**PZD** Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen
Eine FDA stellt eine Netzwerkverbindung bereit und ist für die technische Übertragung von Informationen wie Sprache, SMS oder Internetzugang zuständig. Beispiele hierfür sind die Netzbetreiber Sunrise, Swisscom oder Salt.	Eine AAKD bietet Kommunikationsdienste an, die auf bestehenden Telekommunikationsnetzen aufbauen, ohne die zugrunde liegende Übertragungsinfrastruktur selbst zu betreiben. Zu den Diensten gehören Messaging, E-Mail, VPN oder Cloud-Speicher. Beispiele hierfür sind Proton, Threema oder Ricardo.	Eine PZD kann eine Person oder Organisation sein, die Dritten den Zugang zu einem öffentlichen Telekommunikationsnetz ermöglicht, beispielsweise über öffentliche WLAN-Hotspots. Sie erbringt selbst keine Dienste. Beispiele hierfür sind Hotels, Restaurants oder die SBB.
Sind aufgrund der geplanten Revision wesentliche wirtschaftliche Folgen auf den MWP zu erwarten?		
✓	✓	×

Anmerkung: Gemäss Expertengesprächen und Vernehmlassungsantworten erscheinen (nennenswerte) wirtschaftliche Auswirkungen auf die PZD unwahrscheinlich. Daher wird auf die PZD nachfolgend nicht weiter eingegangen.

Quelle: Eigene Darstellung

Neue Kategorisierung der Mitwirkungspflichtigen

Die revidierte VÜPF sieht vor, unterschiedliche Unterkategorien für FDA und AAKD einzuführen (vgl. Tabelle 1). Gemäss dem erläuternden Bericht zur Eröffnung des Vernehmlassungsverfahrens[9] zielt dieser abgestufte Ansatz darauf ab, besser differenzierte Hochstufungskategorien zu schaffen. So sollen insbesondere Hochstufungen vermieden werden, die wachsende AAKD unmittelbar neue, kostspielige Verpflichtungen auferlegen. Hervorzuheben ist, dass neu alle AAKD mit mehr als 5'000 Teilnehmenden automatisch in die Unterkategorie 2 mit reduzierten Pflichten fallen sollen. Erreichen sie diese Teilnehmerzahl

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

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

müssen sie dies dem *Dienst Überwachung Post- und Fernmeldeverkehr* (Dienst ÜPF) innerhalb von drei Monaten melden. Danach haben sie sechs Monate Zeit, um den neuen Mitwirkungspflichten – etwa der Identifizierung von Nutzern – nachzukommen. Zu beachten ist, dass die Erfüllung der Mitwirkungspflichten in der Regel technische und organisatorische Anpassungen erfordert, deren Kosten vollständig von den AAKD zu tragen sind (vgl. hierzu auch Kapitel 3). Die AAKD erhalten jedoch eine Entschädigung für die Kosten, die bei bestimmten Kooperationsmassnahmen anfallen.[10]

Tabelle 1: Beschreibung der neuen Kategorisierung

MWP	Unterkategorien	Voraussetzungen für eine Hochstufung	Wesentliche Anforderungen bei vollen Pflichten
FDA	zwei	▪ Standardmässig: volle Pflichten ▪ Herunterstufung zu reduzierten Pflichten bei weniger als CHF 100 Mio. Jahresumsatz *und* weniger als 10 Überwachungsziele pro Jahr	Aufbewahrung von Randdaten[11] (6 Monate), 24/7 Pikettpflicht, Aufhebung der Verschlüsselung, automatisierte Datenübermittlung und Echtzeitüberwachung
AAKD	drei	▪ Standardmässig: minimale Pflichten ▪ Unterkategorie 2 der reduzierten Pflichten ab 5'000 Teilnehmende ▪ Unterkategorie 3 der vollen Pflichten ab konsolidiertem Konzernumsatz von mehr als CHF 100 Mio. oder mehr als 1 Mio. Teilnehmende	(Fast) dieselben Pflichten wie bei FDA mit vollen Pflichten. Bei reduzierten Pflichten entfallen die Aufbewahrung von Randdaten, die Pikettpflicht und die automatisierte Datenübermittlung.

Anmerkung: Eine ausführliche Beschreibung der geplanten Kategorisierung und der damit verbundenen Pflichten befindet sich in Anhang A.2.

Standardisierte Ermittlungsinstrumente

Auf Wunsch der Strafverfolgungsbehörden werden neu drei Auskunfts- und zwei Überwachungstypen neu geschaffen, wodurch gewisse Verfahren formalisiert werden. Ziel ist es, bestimmte Informationen und die rückwirkende Überwachung zur Nutzeridentifizierung (die bisher als besondere Verfahren gehandhabt wurden) zu standardisieren und die Echtzeitüberwachung gewisser Inhaltsdaten zu ermöglichen.[12] Hervorzuheben ist in diesem Zusammenhang, dass die meisten Anfragen – sowohl im Rahmen der neuen standardisierten Instrumente als auch anderer Kooperationspflichten – keiner vorherigen richterlichen Genehmigung bedürfen.

2.3 Regulierungsoptionen

In diesem Abschnitt werden die regulatorischen Unterschiede zwischen der derzeitigen Situation und einer Umsetzung der Revision, wie sie vom Bundesrat vorgeschlagen wurde,

[10] Siehe Verordnung über die Finanzierung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF) [05.03.2026] und den Entwurf der Revision Vernehmlassung 2022/21 [20.01.2026].

[11] Im internationalen Sprachgebrauch häufig als Metadaten bezeichnet.

[12] Siehe Vernehmlassung 2022/21 [20.01.2026] für weitere Details.

dargelegt. Bevor auf die konkreten regulatorischen Unterschiede eingegangen wird, erfolgt ein kurzer Überblick über die regulatorischen Optionen.

2.3.1 Beschreibung der Regulierungsoptionen

Das **Referenzszenario (Status quo)** geht davon aus, dass der derzeitige Rechtsrahmen unverändert bleibt, einschliesslich der VÜPF, wie sie seit dem «Threema-Urteil» des Bundesgerichts angewendet wird. Es würden somit keine Änderungen an der Definition, der Einstufung oder den Verpflichtungen der der VÜPF unterliegenden Unternehmen vorgenommen. Sowohl AAKD als auch FDA würden weiterhin den bestehenden Vorschriften unterliegen, und es würden keine zusätzlichen technischen, organisatorischen oder verfahrenstechnischen Anforderungen geschaffen.

Das **Szenario einer vollständigen Umsetzung der VÜPF-Revision** geht hingegen davon aus, dass die überarbeitete VÜPF wie Anfang 2025 vom Bundesrat vorgeschlagen verabschiedet wird. Allfällige Anpassungen an der VÜPF-Revision aufgrund von Rückmeldungen aus der Konsultation oder spätere mögliche Änderungen werden somit in diesem Szenario nicht berücksichtigt. Die Revision sieht mehrere wesentliche Änderungen an Struktur und Inhalt der VÜPF vor, die sich auf verschiedene Gruppen von Akteuren auswirken. Die grössten Auswirkungen betreffen AAKD, für die der regulatorische Rahmen umfassender und detaillierter wird. Dementsprechend konzentrieren wir uns nachfolgend in erster Linie auf die Bewertung der möglichen Auswirkungen auf AAKD. Auf die FDA wird zwar eingegangen, die Analyse fällt aber weniger detailliert aus.[13] Nicht weiter thematisiert werden hingegen die PZD, da die vorgeschlagene Revision sehr begrenzte Auswirkungen auf sie hat.

2.3.2 Zusammenfassung der regulatorischen Unterschiede

Die **Kernverpflichtungen für FDA** bleiben weitgehend unverändert. Dennoch bringt die Revision einige spezifische Anpassungen mit sich, die für bestimmte Anbieter Konsequenzen haben können. Die wichtigste Neuerung ist die Ausweitung der Umsatzschwelle für die Unterkategorie der reduzierten Pflichten. Unter der bisherigen Regelung wurde die Schwelle von CHF 100 Mio. nur auf die mit Fernmeldediensten erzielten Umsätze bezogen. Neu soll die Schwelle auf den gesamten Schweizer Umsätzen des Unternehmens basieren, unabhängig davon, ob diese aus Fernmeldedienstleistungen oder anderen Aktivitäten stammen. Diese Anpassung hat zwei Wirkungen:

- Sie verschärft die Schwelle, da die unternehmensweiten Umsätze per Definition mindestens so hoch sind wie die reinen Fernmeldedienstumsätze.

[13] Eine detaillierte Beschreibung der Kategorien und Pflichten von FDA und AAKD im Status quo sowie im Falle einer Umsetzung der VÜPF-Revision findet sich in Anhang A.1 respektive Anhang A.2.

- Sie verringert die Anzahl der FDA, die für die Unterkategorie mit reduzierten Pflichten in Frage kommt. Betroffen hiervon sind insbesondere diversifizierte Unternehmen, bei denen die Fernmeldedienste nur einen Teil der Geschäftstätigkeit ausmachen.

Die vorgeschlagene Revision der VÜPF sieht mehrere Änderungen vor, welche die **Regulierung für AAKD** erheblich verschärfen. Obwohl die AAKD bereits bisher der Regulierung durch die VÜPF unterstanden und sie entsprechend als Anbieter mit erweiterten Überwachungs- oder Auskunftspflichten eingestuft werden konnten, erweitert die überarbeitete Verordnung den Umfang, die Schwellenwerte und die Tiefe der Pflichten erheblich. Während das Grundkonzept der AAKD unverändert bleibt, werden die regulatorischen Anforderungen deutlich strenger.

Die bedeutendste Verschärfung für AAKD ergibt sich aus der Einführung niedrigerer und weiter gefasster Schwellenwerte für eine Hochstufung aus der Basiskategorie der minimalen Pflichten. In Anbetracht der Tatsache, dass 5'000 Teilnehmer auf digitalen Märkten einen äusserst niedrigen Schwellenwert darstellen, wird – im Vergleich zu heute – künftig wohl der allergrösste Teil der AAKD in eine Kategorie mit höheren Verpflichtungen fallen. Dies wurde von allen Interviewpartnern bestätigt und auch im Konsultationsprozess immer wieder hervorgehoben.

Eine zweite Verschärfung ergibt sich aus dem erweiterten und detaillierteren Katalog von Mitwirkungspflichten, die für die Unterkategorien mit reduzierten und vollen Pflichten gelten. Diese galten zuvor nur für AAKD mit weitergehenden Überwachungs- oder Auskunftspflichten – eine Kategorie, in die aufgrund der hohen Schwellenwerte bisher noch kein Anbieter hochgestuft wurde.[14] Die überarbeitete Verordnung sieht zwar weitgehend dieselben Verpflichtungen wie bisher vor, diese sollen jedoch bereits für die Unterkategorie mit reduzierten Pflichten zur Anwendung kommen. Für AAKD, die den vollen Pflichten unterliegen, sollen die Anforderungen zudem ausgeweitet werden, wie in Tabelle 6 in Anhang A.2 aufgezeigt. Künftig sollen AAKD mit vollen Pflichten in einer Weise reguliert werden, wie dies heute im Wesentlichen für FDA mit vollen Pflichten der Fall ist. AAKD in der Unterkategorie mit reduzierten Pflichten sollen hingegen in Zukunft Anforderungen unterliegen, die mit denen vergleichbar sind, die heute für FDA mit reduzierten Pflichten gelten.

Die vorgesehenen Pflichten in der überarbeiteten VÜPF sind somit nicht nur detaillierter, sondern gelten auch bereits ab wesentlich niedrigeren Schwellenwerten, was insgesamt zu einer spürbar strengeren und umfassenderen Regulierung für AAKD führt. Pflichten, die zuvor nur für die Kategorie der AAKD mit weitergehenden Pflichten oder für FDA galten, sollen sich künftig auf ein weitaus breiteres Spektrum von Dienstleistern erstrecken.

[14] 800 Schweizer Unternehmen hätten weniger Überwachungspflichten… wenn sie davon wüssten! [28.11.2025]. AAKD mit weitergehenden Verpflichtungen ist eine Kategorie in der geltenden VÜPF (siehe Anhang A.1).

2.4 Reaktionen der Stakeholder

Die Vernehmlassung brachte gegensätzliche Standpunkte unter den wichtigsten Stakeholder zu Tage. Unterstützung für die vorgeschlagene Revision der VÜPF kam hauptsächlich von kantonalen Behörden und Strafverfolgungsbehörden. Der stärkste Widerstand geht hingegen vom Digital Trust-Sektor aus. Letzterer wird von zivilgesellschaftlichen Organisationen, mehreren Nichtregierungsorganisationen (NGO), allen politischen Parteien sowie anderen Akteuren (etwa Risikokapitalfonds oder SIX) unterstützt. Insgesamt lehnen die meisten Interessengruppen die vorgeschlagene VÜPF-Revision klar ab.[15]

Digital Trust-Branche – Unternehmen und Verbände

Der stärkste Widerstand kommt aus der **Digital Trust-Branche** (vgl. Box 1). Einige dieser Unternehmen gelten als AAKD; sie sind somit direkt von den Revisionsplänen betroffen. Sie rechnen unter anderem mit gravierenden Reputationsschäden für den Schweizer Digital Trust-Sektor. Vertreten durch Branchenführer wie Proton[16], Nym[17] und Threema[18], argumentieren diese Unternehmen, dass die geplante Revision – insbesondere die Vorratsdatenspeicherung und die Aufhebung der Verschlüsselungspflichten – eine existenzielle Bedrohung für ihre Geschäftsmodelle darstellt, da diese grundsätzlich auf der Minimierung der Datenerhebung und der Maximierung der Sicherheit basieren. So würde die Speicherung zusätzlicher Daten und die drohende Schwächung der Verschlüsselung die potenzielle Angriffsfläche vergrössern und letztlich die Sicherheit der Nutzer beeinträchtigen. Proton hat aufgrund der Revisionspläne des Bundes bereits Serverinfrastruktur im Ausland aufgebaut und öffentlich signalisiert, dass weitere Investitionen ausserhalb der Schweiz stattfinden könnten, da sich das inländische Regulierungsumfeld in eine Richtung entwickle, die im Widerspruch zum Wertversprechen des Unternehmens stehe.[19]

Die wichtigsten Kritikpunkte und Bedenken, die von der Branche während der Vernehmlassung vorgebracht wurden, sind die nachfolgenden:

- **Risiko von Standortverlagerungen:** Die Schwelle für die vollen Pflichten (1 Mio. Teilnehmende oder CHF 100 Mio. Umsatz) benachteiligt erfolgreiches, datenschutzorientiertes Wachstum. Proton hat öffentlich darüber gesprochen, dass die Umsetzung des Revisionsvorschlags eine Standortverlagerung erforderlich machen würde – die Revision wird als «wirtschaftlichen Selbstmord» für die Branche bezeichnet. Die Schwelle für

[15] Sofern nicht anders angegeben, finden sich die Aussagen in diesem Abschnitt in der Vernehmlassung 2022/21 [20.01.2026].

[16] Proton bietet datenschutzorientierte digitale Dienste an, darunter sichere E-Mail, VPN und Cloud-Speicher.

[17] Nym bietet ein VPN an, das auf der Mixnet-Technologie zur Rauschgenerierung basiert, um Metadaten vor Nachverfolgung zu schützen.

[18] Threema ist ein sicherer Messaging-Dienst mit End-to-End-Verschlüsselung.

[19] Siehe z. B., 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].

die reduzierten Pflichten (5'000 Teilnehmende) erfasst praktisch alle AAKD in der Schweiz und belastet KMU mit unverhältnismässigem regulatorischem Aufwand. Die Branche ist insgesamt der Ansicht, dass die niedrige Schwelle Innovationen behindert, Standortverlagerungen verursacht und die Standortattraktivität der Schweiz mindert.

- **Zu umfassender Geltungsbereich:** Die Definitionen der MWP stehen für viele AAKD in direktem Gegenspruch zu ihren Geschäftsmodellen. So untergräbt etwa die Auferlegung von Identifizierungspflichten die Kerndienstleistung von Anbietern virtueller privater Netzwerke (VPN) – nämlich Anonymität – grundlegend. Zugleich stellt der Einbezug von Online-Speicherdiensten als AAKD eine Ausweitung dar, die deutlich über die bislang auf Kommunikationsinhalte ausgerichteten rechtlichen Grenzen hinausgeht.
- **Ungleichgewicht bei den Fixkosten:** Das derzeitige Vergütungssystem der Akteure im Digital Trust-Sektor deckt typischerweise nur die variablen Kosten (pro Auftrag). Unternehmen, insbesondere KMU, müssen deshalb erhebliche fixe Investitionskosten tragen, um die erforderliche Compliance-Infrastruktur aufzubauen und zu unterhalten, was ihre Wettbewerbsfähigkeit unverhältnismässig beeinträchtigt.

Box 1: Die Digital Trust-Branche

Der Digital Trust-Sektor umfasst Unternehmen, deren primärer Zweck darin besteht, Vertrauen, Sicherheit, Datenschutz, Integrität und Zuverlässigkeit in digitalen Systemen, Interaktionen und Identitäten zu gewährleisten. Er lässt sich in drei miteinander verbundene Bereiche unterteilen:[20]

- **Cybersicherheit:** Lösungen und Dienste zum Schutz der internen IT-Umgebung von Unternehmen und Privatpersonen, darunter die Erkennung von Sicherheitsverletzungen und die Reaktion auf Vorfälle, digitale Forensik und Audits sowie die Simulation von Bedrohungen oder Angriffen.
- **Digitale Sicherheit:** Technologien und Dienste, die Vertrauen in die Interaktion mit der Aussenwelt schaffen, darunter Identitäts- und Zugriffsmanagement, Biometrie, sichere Transaktionen, industrielle Systeme und Netzwerke. Diese Kategorie umfasst auch Dienste für sichere Interaktion und Kommunikation wie Messenger Services, E-Mail-Anbieter, VPN und Cloud-Lösungen.
- **Vertrauenswürdige künstliche Intelligenz (KI):** KI, die unter Einhaltung strenger rechtlicher, ethischer und technischer Standards entwickelt und eingesetzt wird, wobei Transparenz, Nachvollziehbarkeit, Robustheit, menschliche Kontrolle und Datenschutz im Vordergrund stehen. Dies umfasst sowohl generative KI-Modelle zur Erstellung von Inhalten als auch fachspezifische KI-Anwendungen wie Betrugserkennung, vorausschauende Wartung und Werkzeuge für die Cybersicherheit.

Zusammen ermöglichen diese Bereiche sichere und zuverlässige digitale Interaktionen, schützen Daten und personenbezogene Informationen und tragen dazu bei, das Vertrauen in digitale Systeme zu wahren.

[20] Siehe auch Observatory of Digital Trust Sector 2025 [30.01.2026].

Die Digital Trust-Branche, unterstützt von einer Vielzahl von Unternehmen wie etwa der Schweizerischen Post, SIX, Redalpine, Founderful, Ronzani Schlauri Anwälte und anderen, warnt davor, dass die Folgen der VÜPF-Revision weit über die direkten Compliance-Kosten für einzelne Unternehmen hinausreichen. Sie macht geltend, dass die vorgeschlagenen Massnahmen das Image der Schweiz als eine der weltweit führenden Digital Trust-Nationen gefährden. Dieses negative Signal hätte weitreichende Folgen, da es die Wettbewerbsfähigkeit der Schweiz im Technologiesektor gefährden würde.

Zivilgesellschaft und NGO

Auch zivilgesellschaftliche Organisationen wie die «Digitale Gesellschaft» und die «Stiftung für Konsumentenschutz» reichten kritische Stellungnahmen ein. Sie argumentieren, die Revision stelle einen grundlegenden Verstoss gegen das Schweizer Recht und die Menschenrechte dar.

- **Verfassungswidrige Massenüberwachung:** Die Revision wird als «*Angriff auf die Grundrechte*» (Art. 13 BV) und als Einführung einer «*massiven, flächendeckenden Ausweitung der Überwachung*» angesehen, die mit der von der BÜPF[21] angestrebten Ausgewogenheit unvereinbar ist. Im Extremfall könnte als Folge der Revision eine Strafverfolgungsbehörden alle fünf Sekunden eine automatisierte Anfrage an Unternehmen mit vollen Pflichten senden und so alle registrierten Zugriffe in Echtzeit abrufen und eine lückenlose Historie erstellen.[22]
- **Verstoss gegen das Legalitätsprinzip:** Argumentiert wird überdies, dass der Bundesrat seine Befugnisse überschreite, indem er mittels einer Verordnung (VÜPF) tiefgreifende Einschränkungen der Grundrechte vornehme – eine Angelegenheit, die verfassungsrechtlich einem Gesetz des Parlaments vorbehalten sein sollte.
- **Konflikt mit dem Datenschutzgesetz:** Die erweiterte obligatorische Vorratsdatenspeicherung wird als unvereinbar mit den Grundsätzen der Datenminimierung und der Zweckbindung gemäss dem neuen DSG gesehen; sie erhöhe die Sicherheitsrisiken, indem riesige, für Hacker attraktive Datensilos geschaffen werden.
- **Unvereinbarkeit mit dem EU-Recht:** Die geplante Revision der VÜPF wird letztlich auch als unvereinbar mit dem europäischen Recht bezeichnet, da der Gerichtshof der Europäischen Union (EuGH) festgestellt hat, dass eine anlasslose und dauerhafte Vorratsspeicherung von Daten grundsätzlich immer gegen mit EU-Recht verstosse.

Kantonale Behörden und Strafverfolgungsbehörden

Die Kantonsregierungen (darunter Freiburg, Wallis, Nidwalden, Luzern, Schwyz und Graubünden) unterstützten die Revision im Allgemeinen und erachten sie als notwendig

[21] Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs.

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

und fachlich korrekt. Kritisiert wird jedoch die Geschwindigkeit und die Wirksamkeit der Massnahmen:

- **Lücken in der öffentlichen Sicherheit und 24/7-Pikettdienst:** Der Kanton Aargau lehnt den Ausschluss neuer Auskunftstypen (z. B., IR_58_IP_INTERSECT[23]) und von AAKD mit minimalen und reduzierten Pflichten von der 24/7-Pikettpflicht ab. Er warnt davor, dass dies in Fällen hoher Dringlichkeit wie Entführungen oder terroristischen Bedrohungen zu «erheblichen Überwachungslücken» führe.
- **Technische und operative Inflexibilität:** Die Kantone Solothurn und St. Gallen weisen darauf hin, dass die «Warrant Management Component (WMC)» – d.h. das für die Überwachung eingesetzte administrative Verwaltungstool des Diensts ÜPF – eine bestehende Anordnung derzeit nicht so anpassen könne, dass ein neues Endgerät (Multi-Device) oder eine neue SIM (Extra-SIM) hinzugefügt werden kann. Die Strafverfolgungsbehörden sind deshalb gezwungen, jeweils eine neue Anordnung einzureichen.
- **Notwendigkeit einer Reform auf übergeordneter Gesetzesstufe:** Die Schweizerische Staatsanwaltschaftskonferenz (SSK) sowie die Kantone Schwyz und Graubünden betonten, dass die Revision der VÜPF zwar eine notwendige technische Anpassungen darstelle, diese langfristig jedoch nicht ausreiche, um die systemische Herausforderung der digitalen Beweiserhebung zu bewältigen. Sie sprechen sich deshalb für grundlegende Reformen auf der übergeordneter Gesetzesstufe aus, namentlich des BÜPF und der Schweizerischen Strafprozessordnung (StPO).

Im Gegensatz zu diesen eher operativen Anliegen betonen die Kantone Waadt und Genf die wirtschaftlichen und verfassungsrechtlichen Implikationen der VÜPF-Revision. Beide Kantone warnen davor, dass die geplanten Pflichten die digitale Wirtschaft in der Schweiz schwächen könnten, insbesondere die AAKD. Genf verweist zudem ausdrücklich auf das kürzlich in der Kantonsverfassung verankerte Recht auf digitale Unversehrtheit und warnt, dass bestimmte Mitwirkungspflichten – namentlich jene, die die Ende-zu-Ende-Verschlüsselung betreffen – das Vertrauen in Schweizer digitale Dienste untergraben könnten. Die Waadt betonte ihrerseits, dass zu weit gefasste oder unzureichend differenzierte Pflichten Schweizer Anbieterinnen gegenüber ausländischen Mitbewerbern benachteiligen könnten, und forderte eine stärkere Anlehnung an die europäische Regulierung.

Box 2: Verwendung von Massnahmen bei der Post- und Fernmeldeüberwachung

Im Jahr 2024 verzeichnete die Schweiz einen markanten Anstieg bei den Post- und Fernmeldeüberwachungen. Die Strafverfolgungsbehörden und der Nachrichtendienst des Bundes (NDB) ordneten beim Dienst ÜPF mehr als doppelt so viele Überwachungsmassnahmen an wie im

[23] IR_58_IP_INTERSECT ist ein neuer Auskunftstyp. Er kann für die Benutzeridentifikation durch Schnittmengenbildung eingesetzt werden. Siehe Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens: Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF) [21.01.2026] für weitere Informationen.

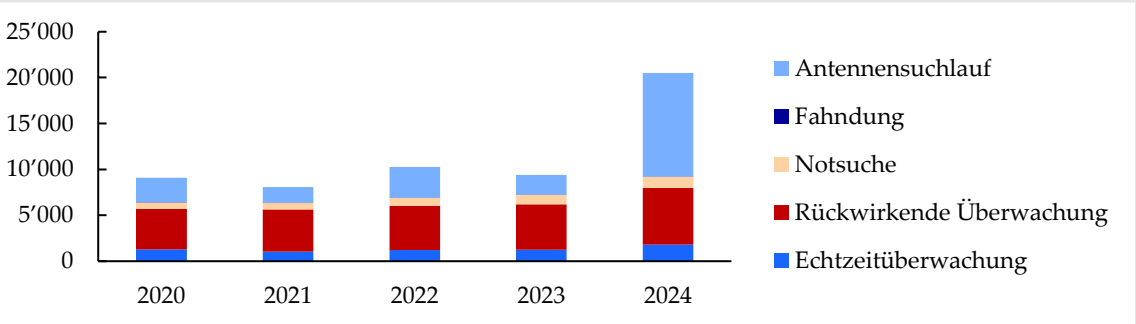
Vorjahr (vgl. Abbildung 2).[24] Haupttreiber dieser Entwicklung war der starke Anstieg beim Antennensuchlauf, der sich gegenüber 2023 verfünffachte. Zum Antennensuchlauf gehört die rückwirkende Überwachung aller an einem bestimmten Standort angefallenen Kommunikationen, Kommunikationsversuche und Netzzugänge, die über bestimmte Mobilfunkzellen stattgefunden haben. Der signifikante Anstieg bei den Antennensuchläufen ist hauptsächlich auf eine kürzliche Änderung der Erhebungsmethodik zurückzuführen.[25]

Auch andere Massnahmen haben deutlich zugenommen: Die Echtzeitüberwachungen stiegen um 46 Prozent auf 1'818 Fälle, während die rückwirkenden Überwachungen um rund ein Viertel auf 6'149 Fälle zunahmen. Die Anzahl der Notsuchen erhöhte sich 2024 ebenfalls substanziell auf 1'223 Anordnungen – rund 20 Prozent mehr als im Vorjahr –, während die Anzahl der Fahndungen leicht zurückging.

Die Überwachungsmassnahmen konzentrierten sich auf mehrere Deliktskategorien. Den grössten Anteil bildeten mit 43 Prozent Vermögensdelikte, deren Überwachungsvolumen sich gegenüber 2023 mehr als verdreifacht hat. Stark zugenommen haben auch die Massnahmen betreffend strafbare Handlungen gegen Leib und Leben, die 19 Prozent aller Anordnungen ausmachten und sich gegenüber dem Vorjahr mehr als verdoppelten. Rund 10 Prozent der Massnahmen betrafen schwere Zuwiderhandlungen gegen das Betäubungsmittelgesetz, wo ein Anstieg von über 15 Prozent verzeichnet wurde. Weitere Kategorien – wie Notsuchen, Delikte gegen die persönliche Freiheit und Delikte gegen den öffentlichen Frieden – verzeichneten ebenfalls Zuwächse, wenn auch in geringerem Ausmass.

Gesamthaft zeigen die Zahlen für 2024 eine klare Ausweitung der Überwachungstätigkeit. Sie belegen, dass die entsprechenden Instrumente von den Behörden breit und mit zunehmender Intensität eingesetzt werden, insbesondere in den Bereichen Wirtschaftskriminalität, Gewaltdelikte und Betäubungsmittelkriminalität.

Abbildung 2: Massnahmen nach Auftragsart (2020-2024)



Source: Swiss Economics basierend auf Dienst ÜPF[26]

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

[25] Bisher hing die Zählung von der Anzahl der einzelnen Mobilfunkzellen ab, die bei der Suche herangezogen wurden. Neu wurde diese Zählung vereinfacht: Sie richtet sich nur noch nach dem Netzbetreiber und dem Zeitraum (bis zu zwei Stunden), unabhängig von der Anzahl der beteiligten Mobilfunkzellen; Beschaffungskonferenz des Bundes (BKB): Statistik zur Fernmeldeüberwachung: Mehr Überwachungsmassnahmen [18.11.2025].

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

2.5 Internationaler Vergleich

Angesichts der potenziellen Auswirkungen auf die Wettbewerbsfähigkeit der Schweiz als Technologiestandort ist es aufschlussreich, den vorgeschlagenen Rechtsrahmen mit jenem der EU und der USA – den weltgrössten Volkswirtschaften und Regulatoren – zu vergleichen. Aus Schweizer Perspektive ist die Angleichung an diese Rechtsordnungen aus vier Gründen relevant. Erstens setzen sowohl die EU als auch die USA die globalen Regulierungsstandards in der digitalen Wirtschaft. Zweitens minimiert regulatorische Konvergenz in einer kleinen, offenen Volkswirtschaft Friktions- und Compliance-Kosten für international tätige Unternehmen. Drittens stellen diese Regionen glaubwürdige Abwanderungsalternativen für Schweizer Technologieunternehmen dar, womit ihr Rechtsrahmen zum Massstab für Wettbewerbsfähigkeit und Innovation wird. Viertens haben die Kunden von Schweizer AAKD tiefe Wechselkosten und können die entsprechenden Dienste ohne Weiteres auch von Anbieterinnen mit Sitz in der EU oder den USA beziehen.

Nachfolgend werden die Überwachungs- und Vorratsdatenspeicherungsregimes der EU und der USA in vier Dimensionen verglichen: (i) Anwendungsbereich, (ii) Vorratsdatenspeicherungspflichten, (iii) Datenzugang und rechtliche Vorschriften sowie (iv) der Umgang mit der Ende-zu-Ende-Verschlüsselung. Die Analyse zeigt, dass der vom Bundesrat vorgeschlagene Rechtsrahmen die Schweiz im internationalen Vergleich zu einem Aussenseiter machen und die hiesige Digitalwirtschaft erheblich benachteiligen würde.

2.5.1 Rechtslage in der EU

Der rechtliche Rahmen der EU zur Vorratsdatenspeicherung wurde ursprünglich in Richtlinie 2006/24/EG geregelt, die zum Zweck der Harmonisierung der nationalen Überwachungsvorschriften für Telekommunikations- und Internetdienstanbieterinnen erlassen wurde. Sie wollte die Unternehmen zur Speicherung von Metadaten bei verschiedensten Diensten, darunter Telefonie, E-Mail, Internetdienste und -telefonie verpflichten. Ab 2009 sah sich die Richtlinie jedoch verfassungsrechtlichen und gerichtlichen Anfechtungen ausgesetzt. In den Grundsatzentscheiden *Digital Rights Ireland und andere* (2014, C-293/12 und C-594/12), *Tele2 Sverige und Watson und andere* (2016, C-203/15 und C-698/15) und *La Quadrature du Net und andere* (2020, C-511/18, C-512/18 und C-520/18) stellte der EuGH fest, dass eine anlasslose Vorratsdatenspeicherung gegen EU-Grundrechte verstosse. Das Gericht befand, dass derartige pauschale Verpflichtungen unverhältnismässig seien und keinen hinreichenden Zusammenhang zwischen den gespeicherten Daten und konkreten Sicherheitsbedrohungen aufweisen.

In der Folge wurde die EU-Richtlinie zur Vorratsdatenspeicherung für ungültig erklärt und die nationalen Umsetzungen entwickelten sich auseinander. Einige Mitgliedstaaten – namentlich Deutschland, die Niederlande und Rumänien – hoben ihre Regelwerke in Umsetzung der erwähnten Urteile vollständig auf. Andere – Frankreich, Italien, Spanien und Polen – behielten begrenzte nationale Überwachungsvorschriften bei, die jedoch rechtlich angreifbar bleiben und auch nur teilweise vollzogen werden. Das Ergebnis ist eine

fragmentierte Rechtslage, in der die meisten EU-Mitgliedstaaten keine systematischen Vorratsdatenspeicherungspflichten mehr kennen.

Selbst dort, wo auf nationaler Ebene noch eine Vorratsdatenspeicherungen verlangt wird, ist ihr Anwendungsbereich deutlich enger gefasst als dies der VÜPF-Revisionsvorschlag vorsieht. Die nationalen Regelwerke in der EU erfassen meist nur Netzbetreiber, Internetdienstanbieterinnen und Grundkommunikationsanbieter (z.B. Telefonie oder E-Mail). Demgegenüber dehnt der Schweizer Vorschlag die Pflichten auf nahezu alle «Over the Top (OTT)»-Dienste aus – darunter Messaging-Plattformen, VPN, Proxy-Server und Dateispeicherdienste. Damit würde die Schweiz zu einem der wenigen westlichen Länder, das die Überwachungspflichten auf das gesamte digitale Ökosystem ausdehnt.

Nach EU-Regeln unterliegt der Zugang zu gespeicherten Daten ferner in nahezu allen Fällen, die Inhalts-, Verkehrs- oder Standortdaten betreffen, einer richterlichen Genehmigung. Die entsprechenden Anbieterinnen sind somit befugt, Herausgabeanordnungen wegen Unverhältnismässigkeit, fehlender Erforderlichkeit oder Rechtswidrigkeit anzufechten. Keine Rechtsvorschrift in der EU sieht hingegen einen automatischen Vollzug oder einen direkten Systemzugang durch die Behörden vor. Demgegenüber würde in der Schweiz ein automatischer Herausgabemechanismus eingeführt, der einen Teil der Anbieter verpflichtet, technische Schnittstellen einzurichten, über die Strafverfolgungsbehörden Nutzerdaten direkt abfragen könnten. Eine solche Verpflichtung wäre in westlichen Demokratien einzigartig und würde überdies auch systemische Cybersicherheits-Schwachstellen schaffen.

Auf EU-Ebene wurden bislang keine Massnahmen ergriffen, die direkt in die Ende-zu-Ende-Verschlüsselung eingreifen. Zwar schlug die Europäische Kommission im Jahr 2022 mit der sogenannten «Chatkontrolle 2.0» eine Verordnung vor, die ein Scannen von Inhalten auf Darstellungen sexuellen Kindesmissbrauchs ermöglichen würde; der Vorschlag stiess jedoch auf erheblichen Widerstand der Mitgliedstaaten und ist derzeit blockiert. Das geltende EU-Recht auf Grundlage der «ePrivacy-Richtlinie» (2002/58/EG) untersagt weiterhin eine allgemeine Überwachung sowie Verpflichtungen zur Entschlüsselung. Auch der Bundesrat beabsichtigt zwar im Rahmen der VÜPF-Revision nicht, die Ende-zu-Ende-Verschlüsselung direkt anzugreifen, nimmt jedoch deren faktische Schwächung in Kauf: Der Revisionsvorschlag verlangt, dass AAKD in der Lage sein müssen, von ihnen selbst implementierte Verschlüsselung zu entfernen.

Im Vergleich zum geltenden Rechtsrahmen in der EU zeichnet sich die geplante Revision der VÜPF somit durch eine exzessive Vorratsdatenspeicherung, fehlende gerichtliche Kontrollen und einen automatisierten Vollzug aus. Die meisten EU-Mitgliedstaaten kennen demgegenüber heute eine gezielte, verhältnismässige, richterlich kontrollierte Überwachung. Die vom Bundesrat vorgeschlagene Revision geht somit diametral in eine andere Richtung: Sie kombiniert eingriffsintensive Elemente einzelner EU-Mitgliedstaaten (etwa die französischen Vorratsdatenspeicherungspflichten[27]) mit schwächeren

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

Verfahrensgarantien, also eingeschränkten Anforderungen an eine richterliche Genehmigung. Die Umsetzung der VÜPF-Revision würde die Schweiz folglich von den europäischen Datenschutzstandards abkoppeln und ihre Stellung als vertrauenswürdiger Datenstandort gefährden.

2.5.2 Rechtslage in den USA

Die USA haben nie ein flächendeckendes Vorratsdatenspeicherungsgesetz erlassen. Der Patriot Act von 2001 erweiterte den Zugang zu bestehenden Daten, schrieb jedoch keine präventive Vorratsspeicherung vor. Ein späterer Versuch – der SAFETY Act von 2009 – hätte Anbieterinnen verpflichtet, nutzeridentifizierende Daten während zwei Jahren zu speichern; er wurde jedoch vom Kongress abgelehnt. US-amerikanische Anbieterinnen speichern folglich nur die für den Geschäftsbetrieb erforderlichen Daten und geben diese auf rechtmässiges Ersuchen hin heraus. Dieser auf Minimalregulierung ausgerichtete Ansatz hat unter anderem zum Aufstieg der USA als globaler Technologieführer beigetragen.

Der Zugang von Strafverfolgungsbehörden zu Daten folgt in den USA einer klaren Hierarchie:

- **Vorladung** («Subpoenas») für Nicht-Inhaltsdaten – z.B. Metadaten, sprich Informationen über eine Kommunikation – können ausgestellt, jedoch wegen übermässiger Reichweite, Irrelevanz oder unverhältnismässiger Belastung angefochten werden.
- **Durchsuchungsbefehle** («Warrants») sind für Inhaltsdaten – also Daten über den eigentlichen Inhalt einer Kommunikation – erforderlich und müssen von einem Gericht auf der Grundlage eines hinreichenden Tatverdachts ausgestellt werden. Sie können gestützt auf den Vierten Zusatzartikel zur US-Verfassung angefochten werden.

Das US-amerikanische Recht sieht damit mehrere Verfahrensgarantien und ausdrückliche Anfechtungsmöglichkeiten für Anbieterinnen gegenüber staatlichen Datenersuchen vor. Anders als im vorgeschlagenen Schweizer Modell bestehen keine Pflichten für einen automatischen oder direkten Systemzugang. Der Rechtsrahmen setzt auf eine gezielte Datenerhebung und richterliche Kontrolle und wahrt so die Balance zwischen Sicherheit und Privatsphäre.

Auch versuche, eine Entschlüsselungspflicht einzuführen, sind in den USA gescheitert. Der *Lawful Access to Encrypted Data Act* von 2020 – der Anbieterinnen verpflichtet hätte, Daten auf Verlangen unverschlüsselt herauszugeben – wurde mangels politischer Unterstützung aufgegeben. Die Ende-zu-Ende-Verschlüsselung ist daher geschützt und in US-amerikanischen Digitaldiensten weit verbreitet. Im Vergleich zu den USA sieht die Revision des VÜPF somit eine weitgehend anlasslose Überwachung vor. Während die USA auf einen nachträglichen, gezielten Datenzugang unter richterlicher Kontrolle setzen, würde das neue Schweizer System eine präventive, anlasslose Datenerhebung einführen und mit der Pflicht zur Entfernung von Verschlüsselungen sogar noch einen bedeutenden Schritt weitergehen als die USA. Der US-amerikanische Ansatz ist insgesamt durch einen starken Schutz der Anbieter und Nutzer gekennzeichnet und wahrt sowohl die Privatsphäre als

auch die Wettbewerbsfähigkeit. Mit der Schweizer Revision der VÜPF würde demgegenüber sowohl die Privatsphäre als auch die Wettbewerbsfähigkeit untergraben und das Land mit einem der am weitestgehenden Überwachungsregimes der westlichen Welt ausgestattet.

2.6 Zusammenfassung

Die digitale Politik der Schweiz steht an einem Scheideweg. Einerseits hat sich das Land als vertrauenswürdiger Digitalstandort positioniert, der auf einen starken Datenschutz, innovationsfreundliche Rahmenbedingungen sowie Initiativen zur digitalen Souveränität und zu vertrauenswürdigen Datenräumen setzt. Andererseits wirkt jedoch der VÜPF-Revisionsvorschlag in die entgegengesetzte Richtung, indem er die Überwachungspflichten erheblich ausweitet. Anstatt die Positionierung der Schweiz als Digitalstandort zu stärken, besteht das Risiko, die regulatorische Kohärenz zu untergraben und Rechtsunsicherheit für Unternehmen, deren Geschäftsmodelle auf Datenschutz und -sicherheit beruhen, zu schaffen.

Diese Spannung zeigt sich auch im Vernehmlassungsverfahren, das breiten Widerstand gegenüber der geplanten VÜPF-Revision aufzeigt. Nur die Kantone und Strafverfolgungsbehörden befürworten die Revision teilweise. Von der grossen Mehrheit der Vernehmlassungsteilnehmer wird die Revision jedoch entschieden abgelehnt. Die schärfste Kritik kommt aus der Digital Trust-Branche, unterstützt von zivilgesellschaftlichen Organisationen, politischen Parteien und Investoren. Diese Akteure machen insbesondere darauf aufmerksam, dass die neu geplanten Pflichten direkt im Widerspruch zu Geschäftsmodellen stehen, die auf Datenminimierung, starker Verschlüsselung und Nutzeranonymität beruhen, unverhältnismässige Compliance-Kosten verursachen und starke Anreize zu Standortverlagerungen schaffen. Zivilgesellschaftliche Organisationen heben zudem verfassungsrechtliche Bedenken hervor, darunter Verstösse gegen den Grundsatz der Verhältnismässigkeit, das Legalitätsprinzip und das Datenschutzrecht.

Vor diesem Hintergrund wurden zwei Regulierungsszenarien verglichen: die Beibehaltung des Status quo und eine vollständige Umsetzung der VÜPF-Revision. Obschon mit dem Revisionsvorschlag die Verhältnismässigkeit verbessert werden soll, führen die gewählten Schwellenwerte – insbesondere der tiefe Wert von 5'000 Teilnehmenden für AAKD mit reduzierten Pflichten – dazu, dass in der Praxis die meisten AAKD künftig einschneidenden Überwachungspflichten unterliegen würden. In Verbindung mit den erheblich ausgeweiteten Mitwirkungspflichten, die AAKD in der Kategorie mit reduzierten Pflichten auferlegt werden sollen, würde sowohl der Anwendungsbereich als auch die Eingriffsintensität der Überwachung in der Schweiz gegenüber dem Status quo massiv ausgedehnt.

Der internationale Vergleich stützt und verstärkt diese Schlussfolgerung: Sowohl die EU als auch die USA haben sich von der anlasslosen Vorratsdatenspeicherung und weit gefassten Überwachungspflichten abgewandt. In der EU hat der EuGH eine flächendeckende Vorratsdatenspeicherung als mit den Grundrechten unvereinbar eingestuft; die verbleibenden nationalen Regime sind eng gefasst, bleiben rechtlich angreifbar und werden nur zum

Teil vollzogen. Auch die USA haben nie eine obligatorische Vorratsdatenspeicherung eingeführt und setzen auf einen gezielten, nachträglichen Datenzugang unter richterlicher Kontrolle. Der Schweizer Revisionsvorschlag sieht somit einen deutlich strengeren Regulierungsrahmen vor als ihn vergleichbare Rechtsordnungen kennen.

Tabelle 2 veranschaulicht diese Divergenz. Sie zeigt, dass als Folge der Revision der VÜPF zentrale Pflichten für AAKD wie Metadaten-Vorratsspeicherung, Identifikationspflichten, Speicherung der letzten IP-Adresse und automatische Herausgabe von Daten eingeführt würden, die heute so weder in der Schweiz noch in der EU oder den USA bestehen. Pikant ist dabei, dass grosse internationale Technologieunternehmen wie etwa Google oder Meta, die dem EU- oder US-Recht unterstehen, den Schweizer Pflichten nicht unterworfen wären. Die Revision würde somit Schweizer AAKD strukturell gegenüber ausländischen Mitbewerbern benachteiligen, da die zusätzlichen Pflichten ausschliesslich für in der Schweiz ansässige Unternehmen gelten.

Tabelle 2: Zusammenfassung der Verpflichtungen für AAKD

	Status quo CH	VÜPF-Revision: volle Pflichten	VÜPF-Revision: reduzierte Pflichten	EU	US	Int. Firmen (Google, Meta)
Metadaten-Speicherung	×	✓	×	×	×	×
Identifizierungs-pflichten	×	✓	✓	×	×	×
Speicherung letzte IP	×	✓	✓	×	×	×
Automatische Herausgabe	×	✓	×	×	×	×
Letzte IP ohne Gerichtsbeschluss	×	✓	✓	×	×	×

Anmerkung: In der Schweiz bestehen derzeit zwar die Pflichten zur automatischen Herausgabe, zur Aufbewahrung von Metadaten und zur Identifizierung für AAKD mit weitergehenden Pflichten. Bisher wurde jedoch keine AAKD in diese Kategorie hochgestuft.

Source: Swiss Economics basierend auf Proton

Insgesamt zeigt Kapitel 2, dass die vorgeschlagene VÜPF-Revision nicht einfach das Schweizer Überwachungsrecht modernisieren, sondern die regulatorischen Rahmenbedingungen grundlegend verschärfen würde. Damit würde sie den übergeordneten Zielen im Bereich der digitalen Politik der Schweiz zuwiderlaufen und einem Regime Vorschub leisten, das deutlich weiter geht als dasjenige der EU und der USA. Mehrere Interviewpartner warnten dann auch, dass die vorgeschlagene VÜPF-Revision ein eigentlicher Wendepunkt darstelle und den internationalen Ruf der Schweiz als Jurisdiktion mit einer vertrauenswürdigen und berechenbaren digitale Rechtsordnung beschädigen könnte; zumal die neuen Regeln auf Verordnungsstufe – also quasi durch die Hintertür – eingeführt werden sollen.

3 Auswirkungen auf betroffene Unternehmen

Dieses Kapitel untersucht die Auswirkungen der geplanten VÜPF-Revision auf Unternehmen, die von den vorgeschlagenen Massnahmen direkt betroffen wären. Aufbauend auf dem vorherigen Kapitel werden die relevanten Unternehmenstypen identifiziert und die Kanäle skizziert, über die die revidierte VÜPF deren Betrieb und Kostenstrukturen beeinflussen würde. Nicht behandelt werden in diesem Kapitel hingegen allfällige indirekte Effekte, wie etwa nachgelagerte Auswirkungen aufgrund von Reputationsschäden oder Implikationen für die Attraktivität der Schweiz als Unternehmensstandort. Auf diese Effekte wird gesondert in Kapitel 4 eingegangen. Auch die Auswirkungen auf Endnutzer und andere Stakeholder werden nachfolgend nicht detailliert analysiert; illustrative Beispiele werden jedoch in Box 3 diskutiert.

3.1 Auswirkungen auf Fernmeldedienstanbieter

Fernmeldedienstanbieterinnen (FDA) bilden eine zahlenmässig bedeutende und heterogene Gruppe im Anwendungsbereich der VÜPF. Gemäss der in der Verordnung verwendeten Definition gibt es in der Schweiz derzeit ca. 1'000 Unternehmen, die als FDA qualifizieren. Von diesen unterliegt nur eine kleine Gruppe – derzeit sechs Anbieterinnen – dem vollständigen Pflichtenkatalog der VÜPF. Die grosse Mehrheit der FDA könnte daher aktuell von reduzierten Mitwirkungspflichten profitieren, häufig weil ihre Dienste oder ihre Grösse die festgelegten Schwellenwerte nicht erreichen, um in die Kategorie der vollen Pflichten zu fallen. Gleichzeitig hat sich jedoch gezeigt, dass nur 200 der rund 1'000 anspruchsberechtigten Unternehmen eine Herabstufung beantragt und erhalten haben, was auf fehlende Transparenz, ein unzureichendes Verständnis des geltenden rechtlichen Rahmens oder schlicht Nichtbetroffenheit durch die VÜPF hindeutet.[28]

Wie in Abschnitt 2.3.2 erläutert, liegt die hauptsächliche regulatorische Änderung der VÜPF-Revision für FDA in der voraussichtlichen Erweiterung der Gruppe, die den vollständigen Pflichten unterliegt. Die Interviewpartner waren nicht in der Lage, genaue Schätzungen darüber abzugeben, wie viele Unternehmen von einer solchen Heraufstufung betroffen sein könnten. Dies ist auf die Vielfalt der Geschäftsmodelle innerhalb der FDA-Kategorie zurückzuführen und ist illustrativ, für die durch den Revisionsvorschlag geschaffene Rechtsunsicherheit. Klar ist jedoch, dass die gesteigerten Mitwirkungspflichten nur jene Unternehmen treffen würden, die neu ein- bzw. heraufgestuft werden.

Für FDA, die den vollständigen Pflichten unterliegen, dürften die daraus resultierenden Mehrkosten erheblich variieren. Die Interviewpartnerinnen betonten, dass die Kosten stark von unternehmensspezifischen Faktoren abhängen, etwa der bereits bestehenden technischen Infrastruktur oder den aktuell verarbeiteten und gespeicherten Daten. Entscheidend dürfte überdies sein, ob organisatorische Massnahmen wie ein 24/7-Pikettdienst heute

[28] 800 Schweizer Unternehmen hätten weniger Überwachungspflichten… wenn sie davon wüssten! [28.11.2025].

schon – z.B. aufgrund anderer regulatorischer Anforderungen oder betrieblicher Notwendigkeiten – bestehen. Für Unternehmen, die heute keinen vergleichbaren Pflichten unterliegen, ist es plausibel anzunehmen, dass die Mehrkosten jenen der AAKD ähneln würden, die in die Kategorie der vollen Pflichten heraufgestuft würden. Wie nachfolgend in Abschnitt 3.2.3 aufgezeigt, sind für solche AAKD Initialkosten von CHF 2 bis 3 Mio. und laufende Kosten von CHF 1.5 Mio. pro Jahr zu erwarten.[29]

Die Interviewpartner gehen nicht davon aus, dass die VÜPF-Revision mit erheblichen Wettbewerbsverzerrungen für die FDA einhergehen würde. Da FDA vergleichbare Dienste anbieten, würden sie alle demselben Regulierungsrahmen unterliegen, und allfällige Kostenerhöhungen hätten symmetrische Auswirkungen. Anders als AAKD sind FDA zudem primär auf einem nationalen, stark regulierten Markt tätig und somit dem internationalen Wettbewerb nicht im gleichen Masse ausgesetzt wie AAKD. Daher wird nicht erwartet, dass die regulatorischen Änderungen die Wettbewerbsdynamik wesentlich beeinflussen würde, auch wenn sie für gewisse FDA mit höheren Compliance-Kosten einhergingen. Diese Mehrkosten würden mit grösster Wahrscheinlichkeit an die Kundinnen weitergegeben, sodass im Resultat einfach die Dienste der FDA im Inland teurer würden.

Zusammenfassend würde die VÜPF-Revision den FDA-Sektor primär durch die potenzielle Neueinstufung bzw. Heraufstufung bestimmter Anbieterinnen in die Kategorie mit vollständigen Pflichten betreffen. Obschon dies für betroffene Unternehmen Mehrkosten mit sich brächte, dürfte die Höhe dieser Kosten je nach bestehenden Strukturen und Betroffenheit von der neuen Regulierung erheblich variieren. Gleichzeitig ist nicht davon auszugehen, dass die Revision den Wettbewerb im nationalen FDA-Markt wesentlich verändern würde, da die Regulierungsanforderungen einheitlich für alle FDA gelten und der internationale Wettbewerbsdruck begrenzt ist. Aufgrund dieser Einschätzung wird im Folgenden auf eine Vertiefung der Auswirkungen auf FDA verzichtet – die zu erwartenden Effekte sind begrenzt und die verfügbaren Daten erlauben keine robusten Quantifizierungen.

3.2 Auswirkungen auf Anbieter abgeleiteter Kommunikationsdienste

Anbieterinnen abgeleiteter Kommunikationsdienste (AAKD) sind von den vorgeschlagenen Massnahmen am stärksten betroffen. Um die erwarteten Auswirkungen der Revision der VÜPF auf die AAKD aufzuzeigen, wird zunächst abgeklärt, welche Anbieterinnen überhaupt in den Anwendungsbereich der VÜPF fallen, um anschliessend die Anzahl der direkt betroffenen Unternehmen zu abzuschätzen. Danach werden die direkten und

[29] Diese Schätzungen sind mit Unsicherheiten behaftet, da den Unternehmen derzeit Klarheit über die genaue Ausgestaltung und den Umfang der geplanten Anforderungen fehlt. Insbesondere könnten die zur Erfüllung der Identifizierungspflicht zu speichernden Daten die Komplexität der Umsetzung für die AAKD erheblich beeinflussen, denn die Einhaltung der Vorschriften könnte strengere Sicherheitsstandards zum Schutz der Daten notwendig machen. So liegt es beispielsweise auf der Hand, dass die Speicherung einer IP-Adresse weniger Schutz erfordert als gespeicherte Kopien von Reisepässen.

indirekten Regulierungskosten sowie die weitergehenden operativen und strategischen Konsequenzen für die betroffenen AAKD dargestellt.

3.2.1 Betroffene Unternehmen

AAKD bieten eine heterogene Palette von Online-Diensten an, die Kommunikation zwischen Nutzern ermöglichen, ohne jedoch die Rolle traditioneller FDA einzunehmen. Gestützt auf den Erläuterungsbericht des EJPD, Interviews und Desk Research fallen unter anderem folgende Gruppen unter den AAKD-Begriff, wie ihn der Bundesrat verwendet:[30]

- **Indirekte Internetzugangsdienste (VPN und Proxy-Dienste):** Diese Dienste leiten den Internetverkehr unabhängig vom Internetzugangsdienst der Nutzerinnen um und ändern in der Regel die Quell-IP-Adresse, unter welcher die Nutzer online erscheinen. Sie werden häufig zur Verschlüsselung, Anonymisierung oder zur Umgehung von «Geo Blocking»-Beschränkungen eingesetzt. Schweizerische Beispiele sind **ProtonVPN** und **Nym**, die beide Datenschutz und Sicherheit explizit als Kernelemente ihres Geschäftsmodells vermarkten.
- **Anwendungen zur Datenübertragung zwischen Nutzern (Apps und Software):** Darunter fallen Programme und Apps, mit denen Nutzer untereinander Daten austauschen können – etwa Texte, Sprache, Bilder oder Videos. Entscheidend ist, dass diese Anwendungen nicht zusammen mit einem Internetzugang angeboten werden, sondern eigenständig funktionieren. Die Definition ist bewusst technologieneutral und umfasst sowohl Apps auf dem Smartphone als auch Programme auf dem Computer. Beispiele aus der Schweiz sind **Infomaniak** und **Swissdotnet**, die beide den Datenaustausch zwischen Nutzern über das Internet ermöglichen.
- **Internetbasierte Kommunikationsdienste für Dritte (VoIP):** Diese Dienste ersetzen herkömmliche Telekommunikationsangebote wie Sprachanrufe, werden jedoch vollständig über das Internet und unabhängig vom Netzzugang erbracht. Typische Beispiele sind internetbasierte Telefonie- und Videokonferenzdienste. Schweizerische VoIP-Anbieterinnen sind etwa **Chorus Call** oder **Virtual-Call**.
- **E-Mail-Dienste für Dritte:** E-Mail-Dienste umfassen Webmail, professionelles Mail-Hosting sowie sichere oder verschlüsselte E-Mail-Lösungen, die Nutzern oder Organisationen angeboten werden. Sie stellen eine der etabliertesten Formen abgeleiteter Kommunikationsdienste dar. Schweizerische Anbieterinnen sind beispielsweise **Proton Mail** und **Swissmail,** die beide E-Mail-Dienste für Privat- und Geschäftskunden anbieten.
- **Internetbasierte Messaging- und Benachrichtigungsdienste für Dritte:** Messaging-Dienste ermöglichen Echtzeit- oder asynchrone Kommunikation zwischen Nutzern über Text, Bilder, Sprachnachrichten oder multimediale Inhalte. Dazu gehören Instant-

[30] Eine Auswahl der genannten Unternehmen wurde kontaktiert, um eine Einschätzung der Auswirkungen der VÜPF-Revision auf ihre Geschäftstätigkeit abzugeben. Nur wenige Unternehmen haben auf die Anfrage reagiert.

Messaging-Apps, Chat-Plattformen und Messaging-Funktionalitäten, die in grössere Plattformen eingebettet sind. Schweizerische Beispiele für diese Art von AAKD sind **Threema** und **Session**, aber auch – aufgrund der Messaging-Funktionalitäten innerhalb der Plattformen – **Digitec** oder **Ricardo**.

- **Onlinespeicher-, Hosting- und Content-Sharing-Dienste**: Diese Dienste ermöglichen es Nutzerinnen, digitale Inhalte wie Dokumente oder Dateien zu speichern, zu teilen und gemeinsam zu bearbeiten. Obschon ihr primärer Zweck die Datenspeicherung ist, kann Kommunikation durch das Teilen von Links, Zugriffsrechten, Kommentaren und kollaboratives Bearbeiten stattfinden. Beispiele von Schweizer Anbietern umfassen **Exoscale**, **Hostpoint**, **nine** oder **Tresorit**, die alle Hosting- oder cloudbasierte Speicherlösungen anbieten.

Die angeführten Beispiele sind illustrativ; sie basieren auf dem Erläuterungsbericht und den im Rahmen dieser Studie durchgeführten Interviews. Da die Definition von AAKD sehr weit und technologieneutral gefasst ist, lässt sich nicht ausschliessen, dass **weitere Arten von Diensten und/oder hybride Geschäftsmodelle** in den Anwendungsbereich der VÜPF fallen. Auch in diesem Zusammenhang wurde deshalb von den Interviewpartnern verschiedentlich die Rechtsunsicherheit erwähnt, die die geplante Revision der VÜPF für die Unternehmen schafft.

3.2.2 Anzahl betroffener Unternehmen

Es gibt keine zuverlässigen Schätzungen zu den Unternehmen, die von der Revision der VÜPF betroffen sein könnten. Weder aufgrund der Vernehmlassungsantworten noch allgemeiner Recherchen oder der für diese Studie durchgeführten Experteninterviews lässt sich eine zuverlässige Bandbreite oder eine Gesamtzahl der potenziell betroffenen Unternehmen eruieren. Es deutet jedoch vieles darauf, dass eine erhebliche Anzahl von in der Schweiz tätigen Unternehmen in den Anwendungsbereich der revidierten VÜPF fallen könnte:

- CompanyData.com listet 456 **Kommunikationsunternehmen** in der Schweiz auf, die eine breite Palette digitaler und telekommunikationsbezogener Dienste anbieten.[31] Obschon es sich nicht bei all diesen Unternehmen um AAKD handelt, könnten sie aufgrund ihres Kommunikationsangebots unter die AAKD-Definition fallen.
- Eine Studie im DACH-Raum findet rund 400 **Online-Dating-Plattformen**, die den Schweizer Markt bedienen.[32] Es bleibt unklar, wie viele dieser Unternehmen in der Schweiz ansässig und damit von der VÜPF-Revision betroffen wären (schweizerische Beispiele sind etwa DuoLivo oder swissfriends). Dating-Plattformen stützen sich in der Regel auf Nutzer-zu-Nutzer-Messaging- und Benachrichtigungsfunktionalitäten, die die Kriterien für die Einstufung als AAKD erfüllen können.

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

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

- Die jährliche **Online-Händler**-Umfrage der FHNW erfasst 581 Schweizer Händler.[33] Einige dieser Plattformen bieten integrierte Messaging- oder Benachrichtigungsdienste an, die die Kommunikation zwischen Nutzern ermöglichen, wie etwa Ricardo oder tutti.ch. Es gibt jedoch keine systematischen Daten darüber, wie viele der befragten Händler solche Funktionen in einer Weise anbieten, die sie als AAKD qualifizieren würde.
- PoiData.io listet per Dezember 2025 1'090 **Webhosting-Unternehmen** in der Schweiz auf.[34] Gestützt auf die Ausführungen im Erläuterungsbericht erscheint es wahrscheinlich, dass viele dieser Unternehmen die Kriterien für die Einstufung als AAKD erfüllen.
- Swiss Made Software, ein Label für Schweizer **Softwareunternehmen**, zählt mehr als 1'100 Mitglieder.[35] Es ist unklar, wie viele dieser Mitglieder als AAKD qualifizieren, doch Beispiele, die vermutlich unter die Definition fallen, sind Threema, Infomaniak und Cloudpartner.
- Gemäss Tracxn umfasst der Schweizer «**Software as a Service (SaaS)»-Sektor** 2'280 Unternehmen. Einige dieser Unternehmen, etwa Proton, qualifizieren eindeutig als AAKD. Systematische Daten zur Gesamtzahl der AAKD im SaaS-Sektor gibt es jedoch keine.[36]

Insgesamt legen diese Zahlen nahe, dass die Anzahl der von der VÜPF-Revision potenziell betroffenen Unternehmen erheblich sein dürfte, selbst wenn letztlich nur ein Teil der obigen Unternehmen unter dem revidierten Rechtsrahmen als AAKD qualifizieren. Die Unsicherheit über das Ausmass der Betroffenheit von Unternehmen spiegelt insbesondere das Fehlen robuster, auf AAKD ausgerichteter statistischer Klassifikationen wider. Der Bedarf nach grösserer Klarheit über die Anzahl betroffener Unternehmen um die wirtschaftlichen Auswirkungen der geplanten VÜPF-Revision (besser) abschätzten zu können, wurde auch von den Interviewpartnerinnen wiederholt hervorgehoben.

3.2.3 Implementierungskosten

Sowohl die SECO-Leitlinien zur Regulierungsfolgenabschätzung[37] als auch der Leitfaden zur Schätzung der Regulierungskosten[38] halten ausdrücklich fest, dass bei der Folgenabschätzung für Unternehmen direkte und indirekte Kosten zu berücksichtigen sind.

---

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

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

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

[36] SaaS Sector in Switzerland [20.01.2026].

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

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

Direkte Kosten

Die Interviewpartner betonten, dass Kostenschätzungen aufgrund der fehlenden regulatorischen Konkretisierung und der noch nicht finalisierten Umsetzungsdetails in diesem Stadium grundsätzlich mit Unsicherheit behaftet sind. Sie hängen zudem stark vom Geschäftsmodell, der Grösse, der eingesetzten Technologie und den bereits bestehenden Compliance-Strukturen der jeweiligen AAKD ab. So könnte der Revisionsvorschlag bei einigen Unternehmen eine vollständige Überarbeitung der Sicherheitsarchitektur erfordern, während bei anderen die Mehrkosten voraussichtlich vernachlässigbar sind, da ihre bestehenden Systeme und Prozesse die absehbaren Anforderungen bereits weitgehend erfüllen. Generell gilt: Je datenschutzzentrierter das Geschäftsmodell eines Unternehmens ist, desto grösser sind die Kosten.

Dennoch nannten die Interviewpartner Grössenordnungen, die das Ausmass der erwarteten direkten monetären Auswirkungen veranschaulichen:

- **AAKD mit reduzierten Pflichten:** Die Befragten schätzen die jährlichen Compliance-Kosten auf rund CHF 1 Mio. pro Unternehmen, bedingt durch den Bedarf an zusätzlichen IT-Spezialisten, erweiterter Serverkapazitäten und der Entwicklung von Systemen zur Unterstützung der neuen Auskunftsbereitschafts- und Meldepflichten. Sollte eine Anbieterin gezwungen sein, die Speicherinfrastruktur auszulagern oder Hyperscaler-Dienste zur Erfüllung der Vorratsdatenspeicherungsanforderungen zu nutzen, könnten diese Kosten – je nach Nutzervolumen sowie Art und Dauer der Speicherpflichten – in den mehrstelligen Millionenbereich steigen.
- **AAKD mit vollständigen Pflichten:** Für grössere Anbieterinnen, die vollständigen Mitwirkungspflichten unterliegen, werden die Entwicklungskosten auf rund CHF 2 bis 3 Mio. geschätzt, mit laufenden jährlichen Ausgaben von rund CHF 1.5 Mio. für Personal (Sicherheitsingenieure, Compliance-Personal etc.), Datenspeicherung sowie Betriebsunterstützung für den 24/7-Pikettdienst und automatisierte Schnittstellen.

Ein zentraler Treiber der direkten Kosten ist der Bedarf an qualifiziertem Personal. Die Implementierung erfordert eine detaillierte Analyse interner Datenstrukturen, die Identifikation und Zuordnung rechtlich relevanter Datenfelder zu den geforderten Ausgabeformaten sowie die Entwicklung automatisierter oder halbautomatisierter Abfragemechanismen. Zudem müssen die betroffenen AAKD interne Validierungs- und Genehmigungsprozesse definieren, umfassende Dokumentationen erstellen und rigorose Tests durchführen. Dies erfordert spezialisiertes technisches Fachwissen, unterstützt durch juristische Ressourcen – eine Kombination, die den Personalaufwand erheblich erhöht. Der Betrieb dieser Systeme erfordert zudem voraussichtlich laufende Schulungen, bindet Spezialistinnen und verursacht zusätzlichen Aufwand für Sicherheits- und Auditprozesse.

Unter den AAKD sind besonders Anbieter von Cloud-Speicherdiensten einem hohen regulatorischen Risiko ausgesetzt. Obschon der genaue Umfang der angedachten Randdaten-Vorratsspeicherungspflichten noch nicht abschliessend definiert ist, legen brancheninterne Einschätzungen nahe, dass die entsprechenden Anbieterinnen zusätzlich umfangreiche

Speicherkapazitäten bereitstellen müssten. Ein Interviewpartner schätzte, dass die Mehrkosten bei kleinen Anbieterinnen bis zu 10 Prozent des Umsatzes erreichen könnten, verglichen mit rund 1 Prozent für grosse inländische Anbieter von Cloud-Speicherdiensten.

Der Markt für Cloud-Speicherdienste ist durch intensiven Wettbewerb von globalen Hyperscalern wie AWS und Azure gekennzeichnet. Schweizerische Anbieter operieren in der Regel mit knappen Margen und haben begrenzten Spielraum, zusätzliche Compliance-Kosten an die Kunden weiterzugeben, ohne ihre Wettbewerbsposition zu gefährden. Sollten sich die Speicherpflichten im Rahmen der VÜPF-Revision als umfangreich erweisen, würden die damit verbundenen Investitions-, Speicher- und Betriebskosten die Betriebsmargen mit hoher Wahrscheinlichkeit dauerhaft übersteigen. In diesem Fall wäre das Geschäftsmodell von Schweizer Anbieterinnen von Cloud-Speicherdiensten wirtschaftlich nicht mehr tragfähig. Marktaustritte oder Verlagerung der Aktivitäten in Länder mit geringerer Regulierungslast wären dann rationale und zu erwartende Reaktionen.

Indirekte Kosten

Neben quantifizierbaren direkten Kosten können den betroffenen Unternehmen auch schwerer quantifizierbare, aber potenziell erhebliche Kosten entstehen:

- **Strategische Disruption:** Roadmaps, Produktentwicklungszyklen und Innovationsbemühungen könnten pausiert, verzögert oder neu priorisiert werden, wenn Ressourcen für den Aufbau überwachungsbezogener Infrastrukturen umgeleitet werden.
- **Regulatorische Unsicherheit:** Bereits der Prozess der Anpassung an ein sich veränderndes Regulierungsregime verursacht Kosten – etwa für Szenarioplanung, rechtliche Einschätzungen und Verhandlungen mit Kunden oder Investoren –, da sich Unternehmen gegen unklare künftige Pflichten, die ihrem Geschäftsmodell schaden könnten, absichern müssen.
- **Opportunitätskosten:** Zeit und Kapital bzw. generell Produktionsfaktoren, die aufgrund des Revisionsvorschlags für Compliance, Szenarioplanung und andere zusätzliche Aufgaben aufgewendet werden müssen, können nicht anderweitig eingesetzt werden, was das Marktwachstum oder Produktverbesserungen potenziell verlangsamt.

Diese indirekten Auswirkungen erscheinen in der Regel nicht als explizite Budgetpositionen, haben aber spürbare Auswirkungen auf die organisatorischen Kapazitäten, die strategische Flexibilität und die Positionierung im Wettbewerb. Langfristig kann die Bedeutung dieser indirekten Kosten jene der direkten Kosten um ein Vielfaches übersteigen. Die oben aufgeführten Kosten erfassen daher nur einen Teil der gesamten wirtschaftlichen Belastung. Weitergehende Konsequenzen werden im folgenden Abschnitt erörtert.

3.2.4 Konsequenzen

Die vorgeschlagene Ausweitung der Überwachungspflichten für AAKD dürfte erhebliche wettbewerbs-, strategie- und marktbezogene Auswirkungen zeitigen, insbesondere für Unternehmen, deren Wertversprechen an Vertrauen, Datenschutz, Sicherheit und Swissness geknüpft ist.

Wettbewerbsnachteile und Reputationseffekte

Eine zentrale Sorge Schweizer AAKD ist, dass die revidierten Pflichten ihre Wettbewerbsposition gegenüber ausländischen Mitbewerbern untergraben würden. Anders als herkömmliche FDA sind Schweizer AAKD typischerweise auf globalen Märkten tätig. Sie stehen in direktem Wettbewerb mit Anbieterinnen, die ihren Sitz in Ländern haben, in denen keine vergleichbaren Überwachungspflichten gelten (namentlich in den USA und der EU). Prominente Beispiele sind Messaging-Dienste wie WhatsApp und Signal oder E-Mail-Anbieterinnen wie Microsoft Outlook und Gmail.

Wo ausländische Mitbewerber weniger oder gar keine gleichwertigen Anforderungen erfüllen müssen, hätten Schweizer AAKD höhere Compliance-Kosten und operative Einschränkungen zu tragen. Diese können sich in höheren Preisen, langsameren Innovationszyklen, eingeschränkter Produktfunktionalität oder der Notwendigkeit, Kernfunktionen neuzugestalten, niederschlagen. Aufgrund der zusätzlichen Compliance-, Speicher- und Betriebskosten könnten überdies die ohnehin knappen Margen in international wettbewerbsintensiven Segmenten (weiter) erodieren. In Märkten, die durch hohe Preistransparenz und begrenzten Spielraum zur Kostenweitergabe gekennzeichnet sind (z.B. Cloud-Dienste), besteht das Risiko, dass anhaltende Kostensteigerungen den Schweizer Standort unrentabel machen. In solchen Fällen wird der Marktaustritt bzw. die Verlagerung in Länder mit geringeren Regulierungsanforderungen zur rationalen wirtschaftlichen Reaktion.

Über den Kostendruck hinaus stellt die Revision eine direkte Bedrohung für das Alleinstellungsmerkmal der Schweizer AAKD dar. Besonders ausgeprägt bei datenschutzzentrierten Unternehmen, deren Geschäftsmodell explizit auf Datenminimierung und starken Vertraulichkeitsgarantien aufbaut. Für diese Anbieterinnen sind die durch die VÜPF-Revision eingeführten Identifikations- und Vorratsdatenspeicherungspflichten unvereinbar mit ihrem Wertversprechen.

Der Wettbewerbsnachteil für Schweizer AAKD materialisiert sich bereits heute. Laut Interviewpartnern wird die regulatorische Unsicherheit rund um die VÜPF-Revision zunehmend von internationalen Mitbewerbern in Ausschreibungsverfahren, insbesondere im B2B-Bereich, genutzt, um die Eignung Schweizer AAKD in Frage zu stellen. In Verbindung mit der internationalen Sichtbarkeit der Revision[39] trägt diese Dynamik zu einer Verschlechterung der wahrgenommenen Vertrauenswürdigkeit Schweizer datenschutzzentrierter Dienste bei, noch bevor die Revision überhaupt in Kraft getreten ist. Dieser Reputationsverlust ist wirtschaftlich relevant: Gemäss einer von einem Interviewpartner durchgeführten Kundenbefragung ist die Reputation der zweitwichtigste Grund, weshalb Kunden deren Dienste gegenüber denjenigen von Mitbewerbern bevorzugen.

[39] Z. B., 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].

Mehrere Interviewpartnerinnen betonten zudem, dass «Swissness» – derzeit ein Wettbewerbsvorteil – unter dem revidierten Rechtsrahmen insbesondere für datenschutzzentrierte Unternehmen zum Nachteil werden könnte. Diese Befürchtungen sind nicht rein theoretischer Natur: Proton, das grösste Schweizer Datenschutztechnologieunternehmen, hat bereits begonnen, Teile seiner Infrastruktur nach Deutschland und Norwegen zu verlagern, unter ausdrücklicher Berufung auf Rechtsunsicherheit und Bedenken, dass die revidierten Überwachungspflichten mit bestehenden Datenschutzverpflichtungen kollidieren würden. Proton hat zudem öffentlich erklärt, dass eine Umsetzung der VÜPF-Revision in der vorgeschlagenen Form weitere Verlagerungen erforderlich machen würde.[40] Die Interviewpartnerinnen erwarten, dass andere datenschutzorientierte Anbieterinnen folgen würden, da ihr Wertversprechen nicht mehr mit der Schweizer Regulierung vereinbar wäre.

Mit Blick auf die Zukunft dürften internationale Mitbewerber, die keinen gleichwertigen Überwachungsregimes unterliegen, Marktanteile von Schweizer Anbieterinnen übernehmen, da Nutzer glaubwürdigen Datenschutzgarantien Vorrang einräumen. Aus wirtschaftlicher Sicht schwächt dieses Ergebnis nicht nur inländische Unternehmen, sondern auch die Wirksamkeit des Regulierungsziels selbst: Angesichts der hohen Substituierbarkeit digitaler Kommunikationsdienste über die Grenzen hinweg dürfte kriminelle Aktivitäten einfach vermehrt über ausländische Plattformen abgewickelt werden. Dies würde den angestrebten Nutzen einer verstärkten Überwachung grundlegend in Frage stellen und gleichzeitig die inländische Wertschöpfung schwächen.

Strategische Disruption und Opportunitätskosten

Die Anpassung an ausgeweitete und unklare Pflichten erfordert – wie bereits erwähnt – die Umverteilung knapper Ressourcen weg von Produktentwicklung und Innovation hin zu Compliance und Risikominimierung. Für viele Unternehmen kann dies verzögerte Produktlancierungen, aufgeschobene Investitionen und strategische Neupriorisierungen bedeuten. Betroffene Unternehmen riskieren dadurch, gegenüber ausländischen Mitbewerbern, die keinen vergleichbaren Pflichten unterliegen, ins Hintertreffen zu geraten.

Die regulatorische Unsicherheit beeinträchtigt zudem die strategische Positionierung der betroffenen Unternehmen gegenüber Investoren und Kapitalmärkten. Unklare oder sich verändernde Pflichten erhöhen das wahrgenommene regulatorische Risiko, was Bewertungen drücken, Finanzierungskosten erhöhen und Investitionen abschrecken kann; insbesondere bei Scale-ups und Startups. Mehrere Interviewpartner wiesen darauf hin, dass die Unsicherheit rund um die VÜPF-Revision für Unternehmen, die einen Börsengang oder grössere Finanzierungsrunden erwägen, als negatives Signal wirkt und strategische Optionen einschränkt.

[40] 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].

Arbeitsmarkt- und Beschäftigungsfolgen

Die neuen regulatorischen Rahmenbedingungen können sich auch auf die Beschäftigung auf Unternehmensebene auswirken, mit weitergehenden makroökonomischen Implikationen für die Beschäftigung (vgl. Kapitel 4). Einerseits erfordern ausgeweitete Mitwirkungspflichten zusätzliches spezialisiertes Personal, etwa IT-Sicherheitsexperten, Compliance-Beauftragte und Dateningenieurinnen. Dies kann bei Unternehmen zwar zu einer gewissen Schaffung von neuen Stellen führen. Branchenbefunde legen jedoch nahe, dass eine solche Nachfragesteigerung mit Fachkräftemangel und steigendem Lohndruck zusammenfallen, was den Umfang der Nettobeschäftigungsgewinne begrenzt. Zudem werden diese zusätzlichen Stellen primär im Compliance-Bereich geschaffen und tragen somit nicht direkt zu Wertschöpfung oder Innovation bei. Andererseits dürften Stellenverluste die Neueinstellung überwiegen, wenn ein Teil der Unternehmen Ressourcen verlagert, die Präsenz in der Schweiz reduziert oder aus dem Markt austritt. Gerade junge Startups mit begrenzten Ressourcen sind besonders exponiert, da solche Kleinunternehmen die weitgehend fixen Compliance-Kosten und spezialisierten Personalanforderungen oft nicht absorbieren können. Die Interviewpartner beurteilten den Nettobeschäftigungseffekt mittel- bis langfristig dann auch durchgängig als negativ.

Auswirkungen auf Wertschöpfung und Steuereinnahmen

Die Auswirkungen auf Wertschöpfung und öffentliche Finanzen ergeben sich direkt aus der oben beschriebenen Wettbewerbs- und Strategiedynamik. Unternehmen, die ihre Schweizer Präsenz reduzieren – durch Verlagerung von Infrastruktur, juristischen Personen, geistigem Eigentum oder Hauptsitzen ins Ausland –, leisten einen geringeren Beitrag zur inländischen Wertschöpfung, zu den Unternehmenssteuereinnahmen sowie zu den lokalen Lieferketten. Wenn sich diese Effekte auf die Präsenz von qualifizierten Mitarbeitenden in der Schweiz erstrecken, sind überdies auch Auswirkungen auf die Einnahmen aus Einkommenssteuern und die Sozialversicherungsbeiträge zu erwarten.

Über die direkten fiskalischen Effekte hinaus schwächen solche Verlagerungen Wissens-Spillovers, Clustering- und Agglomerationseffekte sowie Ökosystemdynamiken, die für innovationsgetriebene Sektoren entscheidend sind. Ein anhaltender Abfluss von Unternehmen und Talenten birgt das Risiko, einen «Brain Drain» auszulösen, der die Attraktivität der Schweiz als Standort für vertrauens-, sicherheits- und datenschutzorientierte Technologien mindert. Diese sektorübergreifenden Effekte werden in Abschnitt 4.1 weiter analysiert.

Box 3: Effekte auf weitere Stakeholder: Endnutzer und öffentliche Institutionen

Die möglichen Konsequenzen der VÜPF-Revision betreffen nicht nur Unternehmen, sondern auch weitere Stakeholder. So erhöht etwa die Pflicht zur Speicherung von Metadaten sowohl die Verfügbarkeit als auch die Konzentration sensibler Informationen bei den AAKD. Bereits die blosse Existenz solcher Daten auf Servern vergrössert die potenzielle **Angriffsfläche für Cyberangriffe**,

wie insbesondere die Internet Society[41] und das Konsumentenforum Schweiz[42] hervorheben. Unternehmen, die bisher mit datenminimierenden Architekturen arbeiteten, sind verpflichtet, Informationen vorzuhalten, die andernfalls nicht gespeichert würden, da sie keinen technischen Mehrwert haben. Dies schafft zusätzliche Angriffsziele, da der erwartete Wert eines erfolgreichen Einbruchs steigt.

Die Revision betrifft auch direkt die **Endkonsumenten**, indem sie die Sicherheit ihrer persönlichen Daten mindert. Der potenzielle Schaden aus einem einzelnen Sicherheitsvorfall steigt, da grössere Mengen an Metadaten über längere Zeiträume gespeichert werden. Gleichzeitig beeinträchtigt die Anhäufung von Metadaten auch die Benutzerfreundlichkeit, die Flexibilität und die Servicequalität der AAKD. Da sich ein erheblicher Teil des Wertes der angebotenen Dienste zudem aus Datenminimierung und Vertraulichkeit ableitet, untergraben Anforderungen, die eine umfangreichere Datenerhebung oder -speicherung vorschreiben, direkt diese Produktmerkmale. Sie führen aus Nutzerperspektive zu einer Verschlechterung der angebotenen Qualität der Dienste.

Die VÜPF-Revision betrifft im Übrigen auch **öffentliche Institutionen**, die zunehmend auf sichere digitale Kommunikationsdienste angewiesen sind. So benutzten die Schweizer Bundesbehörden – einschliesslich der Schweizer Armee – den verschlüsselten Messaging-Dienst von Threema als primären Kommunikationskanal, grösstenteils als Reaktion auf Bedenken hinsichtlich Vertraulichkeit und Datenschutz. Der Revisionsvorschlag könnte die Sicherheitseigenschaften dieser Dienste durch die Einführung einer obligatorischen Metadaten-Vorratsspeicherung verändern. Wie bei Privatnutzern könnte die erhöhte Verfügbarkeit und Konzentration von Metadaten potenzielle Sicherheitsschwachstellen für Bund und Kantone vergrössern. Dieses Risiko könnte sich weiter verstärken, wenn regulatorischer Druck Schweizer Anbieterinnen dazu veranlasst, Infrastruktur – etwa Datenserver – ins Ausland zu verlagern. In solchen Fällen könnte sensible Korrespondenz von Bundesangestellten oder Militärpersonal unter anderen Sicherheitsstandards oder ausserhalb der direkten Kontrolle Schweizer Behörden gespeichert werden. Die Revision der VÜPF birgt damit die Gefahr, die Exposition von Regierungs- und Militärkommunikation gegenüber Datenpannen oder unbefugten Zugriffen zu erhöhen. Obschon dies keinen unmittelbaren Verlust der Vertraulichkeit impliziert, erhöht es die erwarteten Risiken im Umgang mit sensiblen staatsbezogenen Informationen und kann die langfristige digitale Resilienz öffentlicher Institutionen beeinträchtigen.

3.3 Zusammenfassung

Dieses Kapitel analysiert die wirtschaftlichen Auswirkungen der vorgeschlagenen VÜPF-Revision auf Unternehmen, die direkt von der neuen Regulierung betroffen wären, insbesondere die herkömmlichen Fernmeldedienstanbieterinnen (FDA) und Anbieterinnen abgeleiteter Kommunikationsdienste (AAKD). Dabei ist für **FDA** die hauptsächliche Konsequenz aus der geplanten Revision, dass bestimmte Anbieterinnen neu in die Kategorie der

[41] 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].

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

vollen Pflichten eingestuft würden. Obschon dies für alle betroffenen Unternehmen mit höheren Compliance-Kosten einhergeht, dürften die konkreten Kosten der einzelnen FDA – je nach bestehender Infrastruktur und Regulierungsexposition – erheblich variieren. Letztlich ist davon auszugehen, dass der Wettbewerb im Schweizer FDA-Markt aufgrund der VÜPF-Revision nicht wesentlich beeinträchtigt würde, da die Anbieterinnen ähnlichen Pflichten gegenüberstehen und der internationale Wettbewerbsdruck begrenzt ist. Infolgedessen würden die höheren Kosten mit grosser Wahrscheinlichkeit einfach an die Kunden weitergegeben.

Grundlegend anders präsentiert sich die Situation für **AAKD**. Die Definition der abgeleiteten Kommunikationsdienste ist weit gefasst und technologieneutral; sie umfasst eine breite Palette digitaler Geschäftsmodelle, darunter Messaging, E-Mail, Hosting, Cloud-Dienste und in Plattformen eingebettete Kommunikationsfunktionalitäten. Obschon die genaue Anzahl der betroffenen Unternehmen nicht robust quantifiziert werden kann, legen die verfügbaren Quellen nahe, dass eine erhebliche Anzahl in der Schweiz ansässiger Unternehmen in den Anwendungsbereich der revidierten VÜPF fallen könnte.

Für diese Unternehmen, insbesondere jene im Cloud-Speichersektor oder mit datenschutzzentrierten Geschäftsmodellen, sind die **direkten Compliance-Kosten** voraussichtlich erheblich. Je nachdem, ob Unternehmen reduzierten oder vollen Pflichten unterliegen, lassen die Interviewergebnisse auf jährliche Compliance-Kosten in der Grössenordnung von CHF 1 Mio. (reduzierte Pflichten) bzw. auf Initialinvestitionen von CHF 2 bis 3 Mio. zuzüglich laufender Kosten von rund CHF 1.5 Mio. pro Jahr (volle Pflichten) schliessen. Diese Kosten werden primär durch spezialisierte Personalanforderungen, Vorratsdatenspeicherungsinfrastruktur, Anpassungen der Sicherheitsarchitektur und eine 24/7-Betriebsbereitschaft verursacht. Über diese direkten Ausgaben hinaus erwachsen den Unternehmen auch erhebliche **indirekten Kosten**, die sich mit regulatorischer Unsicherheit, Opportunitätskosten und interner Ressourcenumverteilung begründen lassen.

Die Revision hat besonders ausgeprägte Konsequenzen für AAKD mit datenschutzzentrierten Geschäftsmodellen. Erstens erleiden Schweizer AAKD gegenüber ausländischen Mitbewerbern einen Wettbewerbsnachteil und Reputationsrisiken. Zweitens müssen Unternehmen Ressourcen von Innovation auf Compliance umlenken, was die Produktentwicklung verzögert, die strategische Flexibilität einschränkt und die Investitionsattraktivität mindert, insbesondere für Startups. Drittens ist eine erhöhte Nachfrage nach spezialisierten Compliance-Experten zu erwarten, dennoch dürften aufgrund von Verlagerungen insgesamt Nettobeschäftigungsverluste wahrscheinlich sein. Schliesslich können inländische Wertschöpfung und Steuereinnahmen sinken, wenn Unternehmen Infrastruktur, juristische Personen oder Mitarbeitende ins Ausland verlagern.

4 Makroökonomische Analyse

Dieses Kapitel analysiert die makroökonomischen Auswirkungen einer vollständigen Umsetzung der revidierten VÜPF im Vergleich zu einer Fortführung des Status quo. Die Dienste der AAKD und FDA sind dabei nicht auf einen spezifischen Sektor beschränkt, sondern in ein breites Spektrum wirtschaftlicher Aktivitäten eingebettet – etwa in den Finanzsektor (z.B. SIX), den E-Commerce (z.B. Digitec) und die Digital Trust-Branche (z.B. Threema). Folglich sind die Auswirkungen der VÜPF-Revision sektorübergreifend und heterogen. Die stärksten negativen Auswirkungen werden jedoch offensichtlich in der Digital Trust-Branche erwartet, die grundlegend von Glaubwürdigkeit, Vertraulichkeit und sicherem Datenumgang abhängt (vgl. Abschnitt 3.2). Massnahmen wie aufhebbare Verschlüsselung und verlängerte Vorratsdatenspeicherungsfristen (vgl. Abschnitt 2.3.2 und Anhang A.2) riskieren, dieses Vertrauen zu untergraben, Angriffsflächen für Cyberattacken zu vergrössern und die Wahrscheinlichkeit von Datenpannen zu erhöhen.

4.1 Relevanz des Digital Trust-Sektors

Die Schweiz bietet aussergewöhnliche Rahmenbedingungen für die Entwicklung von Digital Trust-Diensten. Politische Neutralität und Stabilität, starke und unabhängige Institutionen sowie hohe Rechtssicherheit schaffen ein einzigartiges Umfeld für datenintensive Industrien. Die Datenschutzstandards des Landes – kombiniert mit einer praxistauglichen Regulierung – gelten als zentrale Standortvorteile. Dies zeitigt sich in der Präsenz internationaler Unternehmen wie Kaspersky, Acronis oder SWIFT, die in der Schweiz Rechenzentren betreiben, um von der hochwertigen Infrastruktur und dem robusten Datenschutzregime zu profitieren.[43]

Um diese Standortvorteile zu festigen, gründeten die Kantone Waadt und Genf im Jahr 2020 das «Trust Valley», ein Kompetenzzentrum für Cybersicherheit, digitales Vertrauen und Zukunftstechnologien. Das «Trust Valley» beherbergt derzeit mehr als 300 spezialisierte Unternehmen und über 500 Experten. Es bildet ein dichtes und schnell wachsendes Ökosystem.[44] Ergänzende Initiativen wie die «Swiss Digital Initiative» und ihr global wegweisendes «Digital Trust Label» stärken die Positionierung der Schweiz durch international anerkannte Standards für vertrauenswürdige digitale Dienste. Diese Bemühungen werden durch eine institutionalisierte Zusammenarbeit zwischen öffentlichen und privaten Institutionen unterstützt. So treffen sich beispielsweise jährlich über 50 Partner aus Verwaltung und Wissenschaft (darunter die EPFL) am «Trust Valley Day», um die strategischen Prioritäten zu koordinieren, sich zu vernetzen und Chancen zu erkunden.

Über die institutionellen Entwicklungen hinaus ist die wirtschaftliche Bedeutung des Digital Trust-Sektors zunehmend messbar: Gemäss verschiedenen Marktanalysen wird der globale Markt für Digital Trust bis 2025 voraussichtlich zwischen CHF 92 und 386 Mrd.

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

[44] Siehe die Webseite vom Trust Valley.

erreichen, wovon – basierend auf Berechnungen von Swiss Economics – CHF 3.2 bis 6.4 Mrd. auf die Schweiz entfallen.[45] Es wird erwartet, dass der Schweizer Markt in den kommenden Jahren mit einer jährlichen Rate von ca. 10 bis 21 Prozent wächst. Dies impliziert eine prognostizierte Marktgrösse von CHF 5.2 bis 17.1 Mrd. bis 2030 und CHF 8.5 bis 45.5 Mrd. bis 2035. Dieses Wachstum wird durch die rasch fortschreitende Digitalisierung von Kernindustrien wie dem Finanzensektor und dem Gesundheitswesen, hohen Pro-Kopf-Ausgaben für Forschung und Entwicklung – unterstützt durch Förderprogramme des Bundes für digitale Innovation – sowie der gelebten Datensouveränität und dem fortschrittlichen Datenschutz in der Schweiz vorangetrieben.[46]

Räumlich erstreckt sich die Schweizer Digital Trust-Industrie über die Genferseeregion hinaus und umfasst etwa auch den weltweit bekannten Blockchain-Cluster des «Crypto Valley» in Zug.[47] So ermöglichten günstige Unternehmenssteuerregelungen, Rechtssicherheit und eine technologieaffine Investorenbasis Blockchain- und Web3-Unternehmen, von der Schweiz aus global zu skalieren. Die Region zog Hunderte von Startups, globale Stiftungen (z.B. die Ethereum Foundation) und Risikokapital an und festigte damit den Ruf der Schweiz als neutrales, sicheres und innovationsfreundliches Umfeld für dezentralisierte Technologien.

Box 4: Auf dem Weg zu einem Innovationscluster nach Stockholmer Vorbild?

Ein europäisches Referenzbeispiel für Cluster-Dynamiken ist Stockholm, wo sich eines der erfolgreichsten Tech-Ökosysteme des Kontinents etabliert hat.[48] Trotz des kleinen Heimmarkts hat es zahlreiche global agierende Unternehmen hervorgebracht. Das Stockholmer Ökosystem – mit einem Wert von rund USD 250 Mrd., mehr als 2'500 Startups und über 30 Unicorns[49] – wächst durch anhaltende Kapitalmobilisierung, enge Integration zwischen Forschungseinrichtungen, Investoren

[45] Die grosse Bandbreite der Schätzungen ist der ungenauen Definition des «Digital Trust»-Marktes und der begrenzten Verfügbarkeit von Daten geschuldet; die genauen Berechnungen können Anhang B entnommen werden.

[46] Siehe z. B. 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].

[47] Siehe die Webseite von Crypto Valley.

[48] Ähnliche Clusterdynamiken wurden auch in anderen führenden Innovationszentren wie Tel Aviv beobachtet. Dort haben jahrzehntelange gezielte staatliche Förderung, eine starke Mobilisierung von Risikokapital (z.B. durch die Yozma-Initiative) und eine enge Verzahnung von Wissenschaft, Startups und multinationalen Unternehmen ein weltweit bedeutendes Tech-Ökosystem hervorgebracht – insbesondere in den Bereichen Cybersicherheit, KI und Biowissenschaften. Wie Stockholm veranschaulicht auch Tel Aviv, wie frühe Scale-ups, Exits und Internationalisierung sich selbst verstärkende Zyklen aus Kapitalbildung, Talentrecycling und unternehmerischer Erfahrung befördern können. Vgl. z.B. "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].

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

und Unternehmenspartnern sowie einer Kultur internationaler Ambitionen und Kollaborationen. Erfolgsgeschichten wie Spotify oder Klarna haben dazu geführt, dass Gründer und Führungskräfte ihre Erfahrungen, Netzwerke und Mittel in neue Unternehmen einbringen. Dadurch ist ein Kreislauf aus Wissen, Kapital und Führungskompetenz entstanden, der den Markteintritt und das Wachstum nachfolgender Unternehmensgenerationen erleichtert.[50]

Die Schweiz weist Gemeinsamkeiten mit Schweden auf, die eine vergleichbare Entwicklung begünstigen könnten:

- Hohe Konzentration von Deep-Tech-Talenten und akademische Anker (EPFL, ETH Zürich);
- stabile politische Rahmenbedingungen, die eine hohe Rechtssicherheit garantieren;
- ein etabliertes Risikokapital-Ökosystem (z.B. Redalpine, Founderful);
- aufstrebende, international sichtbare Cluster («Trust Valley», «Crypto Valley») und
- eine stetige Marktausweitung in den relevanten Sektoren.

Diese Faktoren sprechen dafür, dass die Schweiz grundsätzlich gut positioniert ist, um Innovationscluster zu entwickeln. Um das Potenzial auszuschöpfen, erscheint es dabei vielversprechend, die Mechanismen nachzubilden, die zu den frühen Erfolgen Schwedens beigetragen haben. Dazu zählen insbesondere eine solide Kapitalbildung, eine starke internationale Ausrichtung sowie der Aufbau eines Kreislaufs, der erfahrene Unternehmerinnen sowie Investoren hervorbringt. Denn die Erfahrungen Schwedens zeigen, dass unternehmerischer Erfolg sich selbst verstärken kann: Exits von Unicorns und die Entwicklung von Scale-ups setzen nicht nur Kapital frei, sondern vergrössern auch den Pool erfahrener Gründerinnen, Führungskräfte und Business Angels. Diese investieren in neue Unternehmen, bringen ihr Know-how ein und begleiten deren Aufbau. Dadurch werden Cluster-Dynamiken gestärkt und Hürden bei der Skalierung für nachfolgende Unternehmen gesenkt.

Ob sich eine solche Entwicklung in der Schweiz tatsächlich einstellt, bleibt naturgemäss offen. Mehrere Interviewpartner betonten jedoch, dass die Digital Trust-Branche in Europa an einem kritischen Punkt steht, an dem die Entstehung eines neuen Clusters wahrscheinlich ist. Derzeit erscheint die Schweiz im internationalen Wettbewerb als Standort für ein solch neues Cluster gut positioniert. Nach Einschätzung der Befragten würde die Umsetzung der vorgeschlagenen VÜPF-Revision die Ausgangslage für die Schweiz jedoch erheblich verschlechtern und die Wettbewerbsvorteile weitgehend zunichtemachen; dies nota bene noch bevor sich ein solcher Cluster überhaupt bilden könnte.

Rolle von Datensouveränität, Datenschutz und Reputation im Digital Trust-Sektor

Eine wachsende Literatur zu «Data Governance» und der Ökonomie des Datenschutzes zeigt, dass starke Datenschutzregime und klare Datensouveränitätsregeln zentrale Faktoren für die Ansiedlung einer Digital Trust-Industrie darstellen. Die OECD weist nach, dass vertrauenswürdige, gut regulierte Datenumgebungen sowohl das Vertrauen im gesamten Datenökosystem stärken als auch Investitionen und Datenaustausch stimulieren.

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

Umgekehrt untergräbt eine schwache Governance und der Kontrollverlust über Daten Innovation und digitale Wertschöpfung.[51]

Ebenso hat die empirische Forschung im Bereich der Datenschutzökonomie gezeigt, dass die Bereitschaft von Nutzerinnen und Unternehmen, digitale Dienste zu nutzen, entscheidend von der Bereitstellung glaubwürdiger Datenschutzgarantien abhängt. Werden diese Garantien untergraben, gehen Nutzung, Innovation und Marktwachstum zurück. [52] Der «Digital Trust Report» von CEBR quantifiziert diese Beziehung und zeigt, dass ein höheres Mass an digitalem Vertrauen mit deutlich stärkerem Wirtschaftswachstum verbunden ist und dass Vertrauensdefizite in entgangenem BIP- und Umsatzpotenzial münden. CEBR kommt zum Schluss, dass ein Anstieg des digitalen Vertrauens um 5 Prozentpunkte mit einer durchschnittlichen Zunahme des BIP pro Kopf von USD 3'000 einhergeht.[53]

Jüngere politische und brancheninterne Analysen gehen noch einen Schritt weiter. Sie bezeichnen Datensouveränität als «strategischen Gestaltungsimperativ» für den Aufbau und die Aufrechterhaltung von digitalem Vertrauen.[54] Werden Datensouveränität und Datenschutz geschwächt, besteht die Gefahr, dass Unternehmen sensible Daten zurückhalten, kritische Infrastruktur verlagern oder Investitionen reduzieren. Dies könnte zur Stagnation oder gar Erosion von Digital Trust-Clustern führen.[55]

Ein Vertrauensverlust hat damit direkte und potenziell erhebliche wirtschaftliche Auswirkungen. Auch das Weltwirtschaftsforum (WEF) warnt, dass ein dauerhafter Vertrauensverlust in Technologie und Datenschutz Innovation und Wirtschaftskraft gefährdet: «*If trust in technology is lost forever, then so too might be the possibility of a future of innovation and opportunity*.» Eine Umfrage von McKinsey[56] zeigt überdies, dass mehr als die Hälfte der Konsumenten ausschliesslich bei Unternehmen kauft, die für den Schutz von Kundendaten bekannt sind. Sobald Berichte über Datenpannen oder einen fragwürdigen Umgang mit dem Datenschutz bekannt werden, wechseln Kunden zu Mitbewerbern (40 Prozent der

---

[51] 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].

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

[53] The digital trust index [20.01.2026].

[54] Siehe z. B. 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].

[55] Konkrete Beispiele sind die Verlagerung der Infrastruktur von Proton (siehe Abschnitt 3.2.4) oder die Verlagerung von Session im Jahr 2024 – also vor der Veröffentlichung des Revisionsvorschlags – in die Schweiz (Siehe Introducing the Session Technology Foundation [20.01.2026]).

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

Befragten beendeten eine Geschäftsbeziehung aufgrund einer Datenschutzverletzung).[57] Die Umfrage stellt weiter fest, dass ein starker Datenschutz nicht nur Kunden, sondern auch Investorinnen und Fachkräfte anzieht. Teile der Literatur betrachten digitales Vertrauen sogar als immaterielles Kapital: Einmal erschüttert, ist Vertrauen nur schwer zurückzugewinnen.[58]

Dieser Effekt lässt sich auch auf Unternehmensebene beobachten. Gemäss einer Gartner-Umfrage unter CIO in Westeuropa berichten 61 Prozent von gestiegenen Bedenken hinsichtlich digitaler Souveränität und Kontrolle über Daten und Infrastruktur aufgrund geopolitischer Entwicklungen. Dies hat zu einer stärkeren Nutzung lokaler oder regionaler Cloud-Lösungen geführt.[59] Eine Analyse von Proton ergab in diesem Zusammenhang, dass derzeit rund 75 Prozent der börsenkotierten Unternehmen in Europa US-amerikanische Technologiedienste nutzen.[60] Eine Verlagerung hin zu europäischen Technologien würde daher mit erheblichem Wachstum des europäischen Marktes – einschliesslich des Digital Trust-Sektors – einhergehen. In Übereinstimmung mit diesen Befunden prognostiziert Gartner einen deutlichen Anstieg der Nachfrage nach souveräner Cloud-Infrastruktur und sagt voraus, dass die Ausgaben hierfür in Europa im Jahr 2026 gegenüber dem Vorjahr um über 80 Prozent steigen werden.[61] Dies deutet darauf hin, dass Bedenken hinsichtlich digitaler Souveränität zunehmend zu einem zentralen Faktor bei Investitionsentscheidungen werden. Insgesamt scheinen Unternehmen dem rechtlichen und regulatorischen Umfeld, in dem ihre Daten gehostet werden, eine immer grössere Bedeutung beizumessen.

Darüber hinaus legen auch die jüngsten Diskussionen innerhalb der EU über eine europäische Präferenz im öffentlichen Beschaffungswesen nahe, dass nicht nur Unternehmen, sondern auch der öffentliche Sektor sein Verhalten zusehends anpasst. Auch in der Schweiz werden in den Bereichen Verteidigung und digitale Souveränität Bedenken hinsichtlich einer übermässigen Abhängigkeit von den USA sowie Sicherheitsbedenken gegenüber US-

---

[57] Dieses Phänomen zeigt sich derzeit im KI-Sektor infolge der Konflikte des US-Verteidigungsministeriums mit Anthropic. Nachdem das Pentagon seinen Vertrag mit Anthropic gekündigt hatte – angeblich wegen dessen Weigerung, die Massenüberwachung im Inland zu ermöglichen – und einen Direktvertrag mit OpenAI unterzeichnet hatte, zeigten Marktdaten einen sprunghaften Anstieg von Anthropics Claude im App-Store-Ranking (vgl. Claude just beat ChatGPT on the App Store, and the reason is surprising [09.03.2026]). Die Auswirkungen waren so erheblich, dass OpenAI-CEO Sam Altman auf X [09.03.2026] öffentlich klarstellte, dass OpenAI keine Massenüberwachung betreiben werde, um das Vertrauen der Verbraucher wiederherzustellen.

[58] 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].

[59] 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].

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

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

amerikanischen Anbieterinnen geäussert.[62] Obschon diese Entwicklungen noch in einem frühen Stadium sind, deuten sie darauf hin, dass europäische Lösungen im öffentlichen Sektor erhebliche Wachstumschancen aufweisen.

Vor diesem Hintergrund sind die Wachstumsaussichten für Schweizer Digital Trust-Anbieterinnen grundsätzlich intakt. Die Nachfrage nach Datensouveränität, sicherer Cloud-Infrastruktur und glaubwürdigen Datenschutzgarantien wächst rasch und vergrössert damit den Gesamtmarkt für Digital Trust-Dienste. Die Tatsache, dass aktuell viele Unternehmen ihre Hosting-Standorte sowie die regulatorische Umgebung überprüfen, eröffnet vertrauenswürdigen Rechtsordnungen die Möglichkeit, einen Teil dieses wachsenden Marktes dazu zu gewinnen. Die Schweiz ist mit ihrem Ruf für Rechtssicherheit, Vertrauen, Neutralität und institutionelle Glaubwürdigkeit gut positioniert, von dieser doppelten Dynamik – einem wachsenden Markt und dem Potenzial, ihren Anteil daran zu steigern – zu profitieren. Die geplante VÜPF-Revision droht jedoch dieses Potenzial zu gefährden: Sie verschlechtert die regulatorischen Rahmenbedingungen und die positive Reputation der Marke Schweiz. Letztlich werden damit genau die Vertrauensvorteile, auf dem diese Wachstumschance beruht, untergraben.

4.2 Konsequenzen der geplanten VÜPF-Revision

Aufbauend auf der Analyse des Digital Trust-Sektors werden nachfolgend die wirtschaftlichen Konsequenzen einer vollständigen Umsetzung der revidierten VÜPF untersucht. Die Analyse geht vom am direktesten betroffenen Sektor zu weitergehenden makroökonomischen Konsequenzen über und zeigt auf, wie regulatorische und reputationsbezogene Effekte sich von Entscheidungen einzelner Unternehmen auf die gesamte Wirtschaft ausweiten können.

Unmittelbare Auswirkungen auf den Digital Trust-Sektor

Die Interviewergebnisse deuten durchgängig darauf hin, dass die geplante VÜPF-Revision die Wachstumsaussichten der Schweizer Digital Trust-Branche substanziell beeinträchtigen würde. Obschon nur ein Teil der Unternehmen im Digital Trust-Sektor direkt den revidierten Pflichten unterliegt, betonten die Interviewpartner, dass die Revision die Tragfähigkeit aller datenschutzzentrierten Geschäftsmodelle tangieren würde; sie erodiert die wahrgenommene Vertrauenswürdigkeit und beeinflusst damit die gesamte Schweizer Digital Trust-Industrie negativ.

Erste Auswirkungen lassen sich bereits beobachten. So hat Proton Serverinfrastruktur im Ausland aufgebaut und öffentlich kommuniziert, dass weitere Investitionen in der Schweiz auf Eis liegen, solange die Einführung der revidierten VÜPF im Raume steht. Nach Angaben von Proton wäre das Schweizer Regulierungsumfeld bei einer Umsetzung der VÜPF-

[62] Siehe z. B. 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].

Revision nicht mehr mit ihrem Wertversprechen vereinbar. Ein weiteres konkretes Beispiel ist der VPN-Anbieter PrivadoVPN. Anfang 2026 gab das Unternehmen seine Verlagerung nach Island bekannt und begründete diese Entscheidung ausdrücklich auch mit Bedenken hinsichtlich des VÜPF-Revisionsvorschlags.[63] Die Befragten weisen weiter darauf hin, dass ein breites Spektrum von Startups und Scale-ups, die in datenschutzfördernden Technologien, sicherer Kommunikation, Cybersicherheit und Cloud-Diensten tätig sind, vor vergleichbaren Abwägungen steht.

Die Revision der VÜPF, wie vom Bundesrat vorgeschlagen, dürfte somit das dynamische Wachstum des Schweizer Ökosystems im Digital Trust-Sektor stark bremsen. Anstatt sich zu einem dynamischen Cluster zu entwickeln, droht dem Ökosystem Stagnation und Fragmentierung, da Ankerunternehmen im Ausland skalieren und Startups entweder frühzeitig in ihrem Lebenszyklus abwandern oder von vornherein ausserhalb der Schweiz gegründet werden. Angesichts des erheblichen Einflusses von Netzwerkeffekten, Mentoring und Signalwirkung bei der Clusterbildung kann schon der Abgang oder die ausbleibende Expansion weniger prominenter Akteure ausreichen, um die Entstehung eines tragfähigen internationalen Hubs zu verhindern.

Allgemeine Effekte von Reputations- und Vertrauensverlust

Über die direkten sektoralen Auswirkungen hinaus heben alle Interviewpartner die Bedeutung von Reputationseffekten hervor. Der internationale Ruf der Schweiz als vertrauenswürdige, neutrale und diskrete Rechtsordnung gilt weithin als entscheidender Faktor, der einem breiten Spektrum wirtschaftlicher Aktivitäten zugutekommt. Vertrauen ist jedoch asymmetrisch fragil: Es ist kostspielig und zeitaufwendig aufzubauen, kann jedoch rasch verloren gehen und ist – einmal beschädigt – schwer wiederherzustellen.

Vertrauen beeinflusst die Faktorproduktivität, die Kapitalakkumulation, Innovationsanreize und Standortentscheidungen global mobiler Unternehmen.[64] Regulatorische Eingriffe, welche die Wahrnehmung der Vertrauenswürdigkeit eins Landes verändern, können daher grosse Auswirkungen auf Sektoren jenseits der direkt betroffenen haben. Der VÜPF-Revisionsvorschlag riskiert, genau einen solchen Reputationsverlust auszulösen.

Spillover auf andere vertrauensbasierte Sektoren

Die wirtschaftlichen Konsequenzen der geplanten VÜPF-Revision dürften sich somit nicht auf die Digital Trust-Branche beschränken. Insbesondere ist es wahrscheinlich, dass die befürchteten negativen Effekte auf andere vertrauensbasierte Sektoren übergreifen würden, darunter Finanz- und Versicherungsdienstleistungen, datenbezogene Dienstleistungen im

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

[64] Vgl. z. B. 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.

Gesundheitswesen, Kooperationen in der Spitzenforschung und Teile des exportorientierten Dienstleistungssektors.

In diesen Bereichen konkurriert die Schweiz international nicht nur über die Preise, sondern vor allem auch über Glaubwürdigkeit, Stabilität und institutionelle Qualität. Eine Schwächung des Narrativs der «vertrauenswürdigen Schweiz» könnte deshalb die Wettbewerbsfähigkeit mindern, selbst wenn Produkte und Dienstleistungen an sich gleichbleiben. Dieser Mechanismus zeigte sich etwa jüngst in den USA, wo die Veränderung der wahrgenommenen Vertrauenswürdigkeit der Rechtsordnung – und nicht etwa technologische Änderungen – Unternehmen und Regierungen dazu veranlasst haben, Datenspeicherorte, Lieferantenauswahl und strategische Abhängigkeiten neu zu bewerten.[65]

Aus makroökonomischer Sicht verstärken solche Spillover-Effekte den ursprünglichen Schock. Verlagerungsentscheidungen von Digital Trust-Unternehmen können dabei weitreichende Folgewirkungen entfalten – etwa auf Bankbeziehungen, Finanzierungsstrukturen, professionelle Dienstleistungen und Kapitalmarktaktivitäten. Mittel- bis langfristig besteht die Gefahr, dass dadurch das gesamte Innovationsökosystem geschwächt und die Attraktivität der Schweiz als Standort für wertschöpfungsschaffende Aktivitäten beeinträchtigt wird.

Abbildung 3 fasst die sektorspezifischen Wirkungskanäle der geplanten VÜPF-Revision zusammen. Sie verdeutlicht, dass AAKD im Digital Trust-Sektor am unmittelbarsten und stärksten von den Revisionsplänen betroffen sind – sie sind direkt mit steigenden Kosten und einem potenziellen Vertrauensverlust konfrontiert. Die Abbildung zeigt jedoch auch, dass selbst nicht-vertrauensbasierte Sektoren betroffen sein können, was die breite, gesamtwirtschaftliche Relevanz von Vertrauen und Reputation widerspiegelt. Diese sekundären Effekte auf andere Sektoren können über mehrere Kanäle entstehen. So können beispielsweise sinkende Ausgaben in der Digital Trust-Industrie mit negativen Auswirkungen auf den Tourismus oder die Bauwirtschaft einhergehen.

Abbildung 3: Heatmap der branchenspezifischen Wirkungskanäle

	Andere Sektoren (z. B. Tourismus, Bau)	**Andere vertrauensbasierte Sektoren (z. B. Finanzen, Versicherungen)**	**«Digital Trust» Sektor**
Nicht-AAKD	Sekundäre Effekte	Reputationsspillover	Wahrgenommene Vertrauenswürdigkeit
AAKD	Kosten ↑ Sekundäre Effekte	Kosten ↑ Reputationsspillover	Costs ↑ Vertrauenswürdigkeit

Quelle: Eigene Darstellung

[65] Siehe z. B. Should Europe wean itself off US tech? [20.01.2026], Get over your X: A European plan to escape American technology [20.01.2026].

Pfadabhängigkeiten und Implikationen für Wachstum und Investitionen

Sollte der Ruf der Schweiz als Nation mit einer vertrauenswürdigen Rechtsordnung nachhaltig beschädigt werden, könnte dies Investitionsanreize schwächen, Innovation verlangsamen und das Produktivitätswachstum dämpfen, was den langfristigen Wachstumspfad beeinflussen würde. Wenn vertrauensbasierte Cluster nicht entstehen oder bestehende Aktivitäten abwandern, wird es selbst bei einer späteren Anpassung des regulatorischen Rahmens schwierig, die unterdrückte Dynamik wiederherzustellen und entgangene Investitionen zu kompensieren.

In diesem Zusammenhang spielen Pfadabhängigkeiten eine zentrale Rolle. Die heute getroffenen Regulierungsentscheidungen prägen nicht nur das unmittelbare rechtliche Umfeld, sondern beeinflussen auch die langfristige Standortattraktivität und somit die Entwicklung des Ökosystems.[66] Haben Unternehmen einmal Investitionen oder Teile ihres Geschäfts ins Ausland verlagert und die Schweiz in ihrer Wachstumsstrategie depriorisiert, ist eine Umkehr dieser Entscheidungen kostspielig und zeitaufwendig. Die Interviewpartner betonten dann auch durchgängig, dass nachträgliche regulatorische Korrekturen nicht ausreichen, um einen durch eine längere Phase der Unsicherheit verursachten Schaden rückgängig zu machen. Aus dieser Perspektive birgt der VÜPF-Revisionsvorschlag das Risiko, dass die Schweiz auf einen ungünstigen Entwicklungspfad geraten könnte, indem genau jene Sektoren geschwächt werden, die auf ihren traditionellen Stärken von Vertrauen, Stabilität und institutioneller Glaubwürdigkeit beruhen.

Aus einer strukturellen Wachstumsperspektive kann die Entwicklung vertrauensbasierter digitaler Aktivitäten mittels der sogenannten S-Kurve beschrieben werden: Die Schweiz befindet sich aktuell am Beginn der Expansionsphase, in der Netzwerkeffekte, Clusterbildung und steigende Skalenerträge in der Regel beschleunigtes Wachstum erzeugen. In diesem Stadium ist entscheidend, dass das Momentum nicht durch regulatorische Unsicherheit behindert wird. Ansonsten droht ein Verharren auf dem unteren, flachen Abschnitt der S-Kurve, anstatt in die Phase nachhaltiger Expansion überzugehen. Ein Verharren auf dem Nicht-Expansionspfad würde dabei nicht nur kurzfristig die Erträge mindern, sondern die gesamte Wachstumsentwicklung behindern, was später kaum mehr aufzuholen ist.[67]

---

[66] Siehe z. B. 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.

[67] Siehe z. B. 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.

4.3 Auswirkungen auf die Digital Trust-Branche

Dieser Abschnitt präsentiert eine vorausschauende Beurteilung der Entwicklung der Schweizer Digital Trust-Branche unter den zwei beschriebenen Regulierungsoptionen (vgl. Abschnitt 2.3): Beibehaltung des Status quo und vollständige Umsetzung der VÜPF-Revision. Dabei sollen keine Punktschätzungen präsentiert werden. Vielmehr soll es darum gehen, aufzuzeigen, wie unterschiedliche regulatorische Pfade die mittel- bis langfristige Entwicklung des Sektors prägen könnten. Angesichts der inhärenten Unsicherheit hinsichtlich der regulatorischen Umsetzung und der Reaktion der Unternehmen werden die Quantifizierungen bewusst als Bandbreiten präsentiert.

4.3.1 Annahmen

Beibehaltung des Status quo

Im Status quo wird davon ausgegangen, dass die Schweizer Wirtschaft und der Digital Trust-Sektor weitgehend im Einklang mit bestehenden Projektionen wachsen. Die Schweiz würde ihre etablierte Position als vertrauenswürdige Rechtsordnung für datenintensive und sicherheitskritische digitale Dienste beibehalten und die «Swiss Trust Premium» würde intakt bleiben. Unternehmen könnten weiterhin innerhalb der Schweiz skalieren und neue Marktteilnehmerinnen würden den hiesigen Standort weiterhin als attraktive Option betrachten. Zudem würden Netzwerkeffekte innerhalb des «Digital Trust Valley» das Wachstum unterstützen. In diesem Szenario betrifft die Unsicherheit hauptsächlich das Wachstumstempo – und nicht seine Richtung –, weshalb eine relativ breite, aber strikt positive Bandbreite von Schätzungen resultiert.

Das Szenario des Status quo geht von regulatorischer Klarheit aus. Es wird angenommen, dass alle Akteure eine Revision der VÜPF-Mitwirkungspflichten für AAKD als politisch vom Tisch betrachten und in absehbarer Zukunft keine erneuten Gesetzgebungsversuche zur Einführung vergleichbarer Bestimmungen erwarten. Es geht somit nicht einfach nur um die Fortführung des aktuellen Regimes, sondern um das Ausbleiben erneuter regulatorischer Unsicherheit, die andernfalls Investitionen, Skalierungsentscheidungen oder den Markteintritt verzögern könnte.

Hinsichtlich des künftigen Wachstums bestehen dabei zwei Unsicherheiten: Erstens ist die Entwicklung des Schweizer Digital Trust-Sektors eng mit der globalen Dynamik verknüpft. Sie wird somit stark davon abhängen, wie sich die internationale Nachfrage nach den entsprechenden Diensten entwickelt. Zweitens besteht auch im Status quo eine gewisse Unsicherheit hinsichtlich der Entwicklung des relativen Marktanteils des Digital Trust-Sektors in der Schweiz. Die vorliegenden Erkenntnisse deuten jedoch grundsätzlich darauf hin, dass die Schweiz angesichts der steigenden Nachfrage nach Datensouveränität und

vertrauenswürdigen Rechtsräumen gut positioniert ist, um ihren Anteil am wachsenden globalen Markt auszubauen.[68]

Vollständige Umsetzung der VÜPF-Revision

Die zweite Option geht von einer vollständigen Umsetzung der revidierten VÜPF aus. Es wird angenommen, dass die Schweizer Wirtschaft im Einklang mit bestehenden Projektionen wächst und weiterhin ein Digital Trust-Sektor in der Schweiz existiert. Im Gegensatz zum Szenario Status quo wird jedoch davon ausgegangen, dass seine aggregierte Grösse über einen Fünf- bzw. Zehnjahreszeitraum weitgehend unverändert bleibt, was einem Nettowachstum von null entspricht.

Diese Annahmen sind aus nachfolgenden Gründen konservativ:

- Erstens wären AAKD unmittelbar und unverhältnismässig stark von der VÜPF-Revision betroffen. Höhere Compliance-Kosten, operative Einschränkungen und Rechtsunsicherheit würden viele bestehende Anbieterinnen zwingen, ihre Geschäftsmodelle grundlegend anzupassen oder Aktivitäten ins Ausland zu verlagern.
- Zweitens – und entscheidend – wären die Auswirkungen kaum auf AAKD beschränkt. Aufgrund der starken Integration der Digital Trust-Branche und des kollektiven Rufs der Schweiz als verlässlicher Rechtsraum würde eine als vertrauensmindernd wahrgenommene Regulierung sich auch auf nicht betroffene Unternehmen auswirken. Die «Swiss Trust Premium» würde erodieren, was die internationale Wettbewerbsposition schwächt und Verlagerungen oder Marktaustritte begünstigen könnte. Zudem könnten, wie in Abschnitt 4.2 diskutiert, auch andere vertrauensbasierte Sektoren und die Gesamtwirtschaft betroffen sein, was das Wachstum dämpfen dürfte.

Insgesamt dürften diese Effekte das Schweizer Wirtschaftswachstum bremsen und den Digital Trust-Sektor zumindest teilweise wegbrechen lassen. Insbesondere ginge aber seine Rolle als Wachstumstreiber verloren: Selbst wenn die Branche fortbesteht, dürfte ihre derzeitige Expansions- und Clustering-Dynamik weitgehend entfallen. Vor diesem Hintergrund ist die Annahme einer unveränderten Gesamtgrösse des digitalen Sektors als konservativ zu werten.

[68] Würde regulatorische Klarheit überdies mit strukturell verbesserten und innovationsfördernden Rahmenbedingungen einhergehen, könnte das Wachstum die Obergrenze des Szenarios Status quo sogar überschreiten. Dieser optimistische Fall wird vorliegenden nicht weiter berücksichtigt.

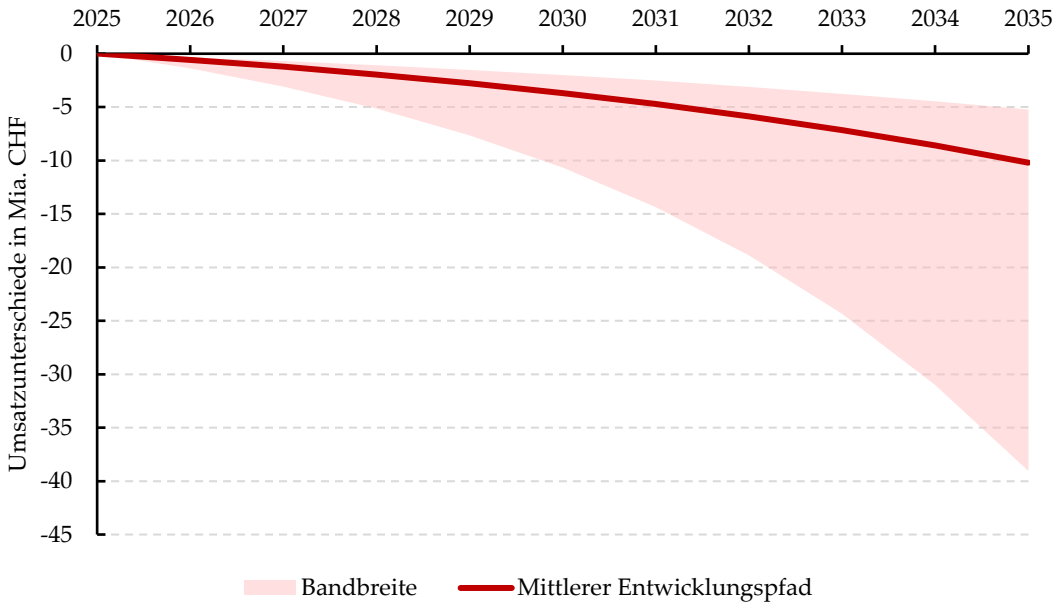
4.3.2 Quantifizierung der wirtschaftlichen Auswirkungen

Nachfolgend werden die wirtschaftlichen Auswirkungen auf Umsätze, Wohlfahrt, Beschäftigung und Steuerauswirkungen quantifiziert. Dabei wird die Differenz zwischen dem Entwicklungspfad im Status quo und dem Szenario einer vollständigen Umsetzung der VÜPF-Revision dargestellt.[69]

Auswirkungen auf die Umsätze der Digital Trust-Branche

Derzeit wird das Marktvolumen der Digital Trust-Branche in der Schweiz auf CHF 3.2 bis 6.4 Mrd. geschätzt. Das projizierte Wachstum unterscheidet sich jedoch erheblich je nach Entwicklungspfad. Unter dem Status quo wird erwartet, dass der Sektor im nächsten Jahrzehnt mit einer durchschnittlichen jährlichen Wachstumsrate von 12 Prozent wächst (mit einer Bandbreite von 10.1 bis 21.6 Prozent). Bei Umsetzung der VÜPF-Revision wird hingegen annahmegemäss davon ausgegangen, dass der Sektor über denselben Zeitraum ein Nullwachstum verzeichnet. Die Auswirkungen der geplanten VÜPF-Revision auf die Digital Trust-Branche lassen sich als Differenz zwischen diesen zwei Entwicklungspfaden über die nächsten zehn Jahre darstellen (vgl. Abbildung 4).

Abbildung 4: Geschätzter Umsatzverlust bis 2035



Quelle: Eigene Darstellung

Abbildung 4 illustriert die exponentiell zunehmenden negativen Auswirkungen anhaltender Wachstumsunterschiede im Zeitverlauf. Die sich ausweitende Bandbreite ist dabei auf den klassischen «Zinseszinseffekt» zurückführen, verdeutlicht aber gleichzeitig die mit dem Projektionshorizont zunehmende Prognoseunsicherheit. Bis 2030 belaufen sich die

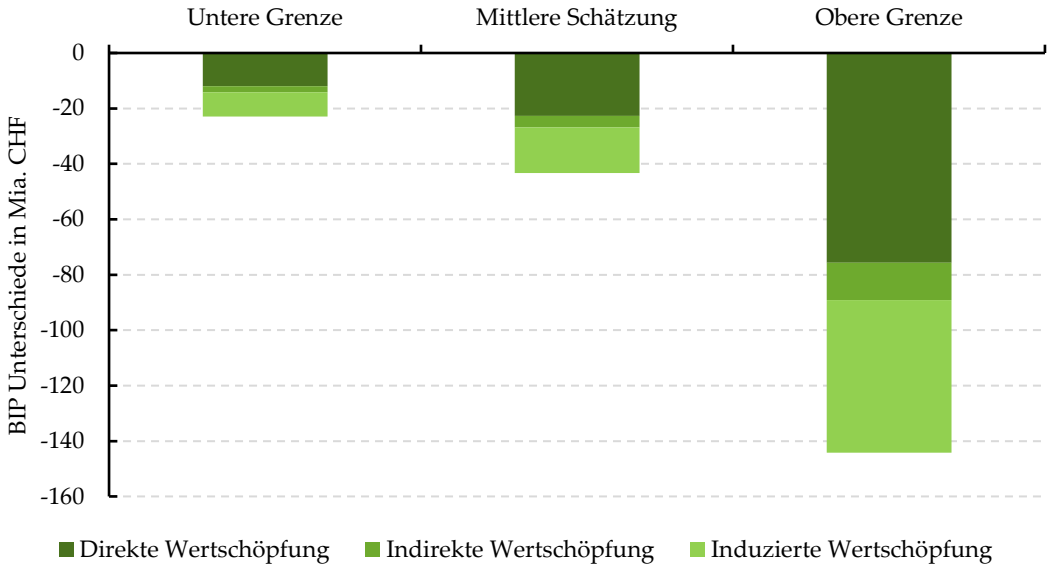
[69] Für das methodische Vorgehen, die zugrundliegenden Annahmen, detaillierten Berechnungen und Datenquellen vgl. Anhang B.

potenziellen jährlichen Umsatzverluste auf CHF 2 bis 10.7 Mrd. und steigen bis 2035 auf CHF 5.2 bis 39.1 Mrd. Obschon die kurzfristigen Auswirkungen moderat erscheinen, zeigt der Entwicklungspfad, dass die kumulativen, langfristigen Konsequenzen erheblich sein können. Es ist ferner zu beachten, dass die negativen Effekte über die Zeit bei höherem prognostiziertem Sektorwachstum überproportional höher ausfallen. Unsere mittlere Schätzung legt kumulierte Verluste von rund CHF 46.8 Mrd. bis 2035 nahe.

Auswirkungen auf die Wohlfahrt

Die Wohlfahrtsanalyse konzentriert sich auf die Schätzung der Grössenordnung der kumulierten Wohlfahrtsverluste über den Zeitraum 2025 bis 2035. Die entsprechenden Auswirkungen werden mithilfe von Input-Output-Tabellen abgeleitet, die eine Zerlegung der Effekte in direkte, indirekte und induzierte Komponenten ermöglichen. Direkte Wohlfahrtsverluste spiegeln dabei die entgangene Wertschöpfung innerhalb des Digital Trust-Sektors selbst wider. Indirekte Effekte erfassen hingegen Wertschöpfungsverluste entlang vorgelagerter Lieferketten, während induzierte Effekte aus rückläufigem Haushaltseinkommen und -konsum entstehen. Die Schätzungen werden über den Projektionshorizont aggregiert, um eine Gesamtbeurteilung der Wohlfahrtsimplikationen zu erlauben. Abbildung 5 stellt die Ergebnisse für die Untergrenze, die mittlere Schätzung und die Obergrenze der Entwicklung dar.

Abbildung 5: Kumulierte Wohlfahrtsunterschiede (2025-2035)



Quelle: Eigene Darstellung

Für den Fall, dass nur direkte und indirekte Effekte berücksichtigt werden, zeigen die Ergebnisse einen kumulierten Wohlfahrtsverlust von rund CHF 14 Mrd. als Untergrenze. Je nach Annahmen über das Sektorwachstum kann die Obergrenze dieser direkten und indirekten Wohlfahrtsverluste jedoch bis zu CHF 89 Mrd. betragen. Werden auch induzierte Effekte einbezogen, könnte der kumulierte Effekt im Extremfall auf bis zu CHF 144 Mrd. ansteigen. Da induzierte Effekte jedoch stark von den getroffenen Annahmen abhängen,

sollten diese Zahlen nicht als präzise Punktschätzungen interpretiert werden. Wiederum deutet die grosse Differenz zwischen Unter- und Obergrenze auf erhebliche Unsicherheit der Folgen einer möglichen Revision der VÜPF hin.

Box 5: Quantifizierung sektorübergreifender Spillover

Neben den direkten Auswirkungen im Digital Trust-Sektor, ist nicht auszuschliessen, dass die geplante VÜPF-Revision, wie in Abschnitt 4.2 diskutiert, mit negativen Spillover auf die breitere Schweizer Wirtschaft einhergeht. Obschon diese Effekte potenziell erheblich sind, lassen sie sich naturgemäss nur schwer quantifizieren. Eine Möglichkeit, das potenzielle Gewicht solcher Spillover zu veranschaulichen, bietet jedoch der «CEBR Trust Index»:[70] Die Schweiz erzielt derzeit 73 Indexpunkte, was einem hohen Mass an Vertrauen in digitale Dienste, Governance und Datenschutz entspricht. Ein Vertrauensrückgang würde diesen Wert voraussichtlich senken.

Würden die Vertrauenswerte der Schweiz auf das Niveau von Ländern wie Deutschland oder den USA fallen (rund 20 Indexpunkte tiefer), könnte das BIP pro Kopf über die Zeit um rund USD 12'000 sinken – etwa 10 Prozent seines aktuellen Niveaus.[71] Obschon diese Schätzung mit Vorsicht zu interpretieren ist, zeigt sie, dass eine solche Entwicklung einen erheblichen Wohlfahrtsverlust für die Schweizer Bevölkerung implizieren könnte.

Die meisten Interviewpartner waren nicht in der Lage, die negativen Auswirkungen auf die Schweizer Wirtschaft konkret zu quantifizieren. Sie hoben jedoch eine wichtige Asymmetrie hervor: Die direkten wirtschaftlichen Auswirkungen sind für Unternehmen der Digital Trust-Branche am ausgeprägtesten – mit Wohlfahrtsverlusten einschliesslich induzierter Effekte von bis zu CHF 36 Mrd. oder 3 bis 4 Prozent des BIP im Jahr 2035.[72] Die grössten Kosten dürften jedoch aus sektorübergreifenden Spillover und gesamtwirtschaftlichen Vertrauensverlusten resultieren.

Auswirkungen auf die Beschäftigung in der Digital Trust-Branche

Die Beschäftigung in der Digital Trust-Branche wurde 2025 auf 13'800 bis 36'200 Stellen geschätzt. Wie in Anhang B beschrieben, wird die Beschäftigungsentwicklung unter Verwendung derselben Wachstumsbandbreite projiziert, die auch für die Umsätze angewendet wird. Dies gewährleistet Konsistenz über die Wirtschaftsindikatoren hinweg. Die erwarteten Auswirkungen des VÜPF-Revisionsvorschlags werden dabei wiederum als

[70] The digital trust index [20.01.2026]. Wir haben die Zahl für die Schweiz auf Anfrage von CEBR erhalten.

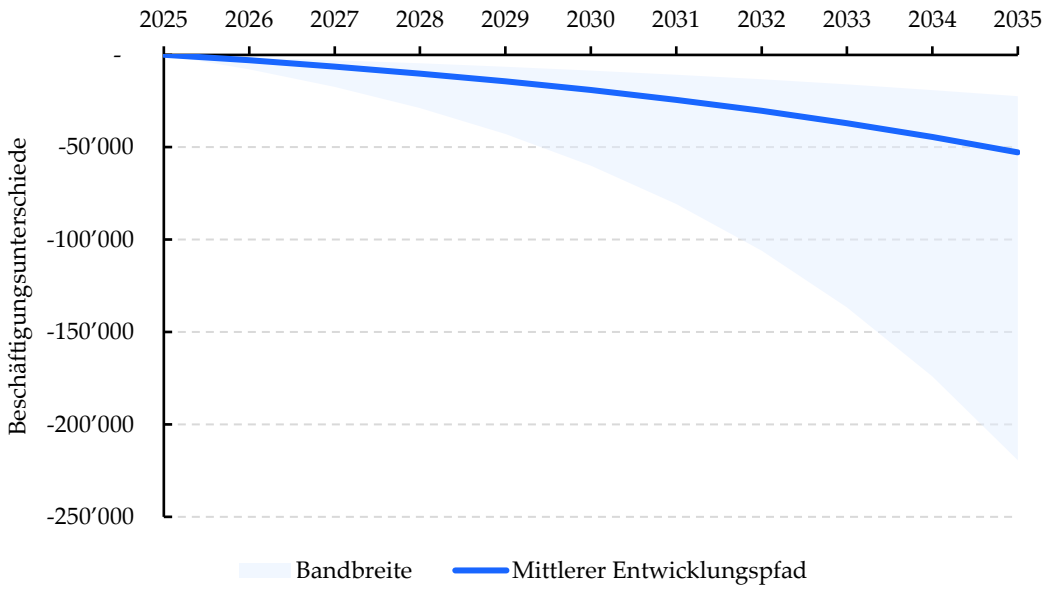
[71] Die CEBR -Analyse kommt zum Ergebnis, dass ein Anstieg des digitalen Vertrauens um einen Indexpunkt mit einem durchschnittlichen Anstieg des BIP pro Kopf um USD 596 verbunden ist (The digital trust index [20.01.2026]). Entsprechend ist ein Rückgang um 20 Indexpunkte mit einem durchschnittlichen Rückgang des BIP pro Kopf von rund USD 12'000 verbunden. Der IWF schätzt das BIP pro Kopf in der Schweiz für das Jahr 2025 dabei auf USD 111'050 (IMF Switzerland Country Data [06.03.2026]). Der Rückgang von rund USD 12'000 entspricht damit etwa 10 Prozent des aktuellen Niveaus des BIP pro Kopf.

[72] CHF 36 Mrd. entsprechen im Jahr 2035 rund 3 bis 4 Prozent des Schweizer BIP, sofern das nominale BIP-Wachstum im Durchschnitt zwischen 0.75 und 3.25 Prozent liegt. Es ist davon auszugehen, dass die tatsächliche Wachstumsrate innerhalb dieser Bandbreite liegen wird (vgl. z.B. Energieperspektiven 2050+ Volkswirtschafltiche Auswirkungen [06.03.2026] veröffentlicht vom Bundesrat).

Abweichung zwischen dem Status quo und einer vollständigen Umsetzung der VÜPF-Revision quantifiziert. Abbildung 6 veranschaulicht die resultierenden Beschäftigungsentwicklungen über die nächsten zehn Jahre.

Wie schon bei den Umsatzprojektionen zeigt sich ein rasch zunehmender negativer Effekt, mit einer sich im Zeitverlauf ausweitenden Bandbreite der Ergebnisse. Bis 2030 werden die Beschäftigungsverluste im Digital Trust-Sektor auf 8'500 bis 60'000 Stellen geschätzt; bis 2035 dürften sie auf 22'400 bis 219'300 Stellen ansteigen. Auch bei der Beschäftigung zeigt sich somit, dass die kurzfristigen Auswirkungen eher moderat sind, die Effekte über die Zeit jedoch zunehmend an Gewicht gewinnen. Auch im mittleren Entwicklungsszenario werden die Beschäftigungsverluste bis 2035 noch immer auf rund 53'000 Stellen geschätzt. Insgesamt kann aus diesen Zahlen geschlossen werden, dass ein erhebliches Risiko eines signifikanten Verlusts an hochqualifizierten Arbeitsstellen in der Schweizer Digital Trust-Industrie besteht. Die geplante VÜPF-Revision könnte mit anderen Worten einen massiven «Brain Drain» auslösen.

Abbildung 6: Beschäftigungsunterschiede bis 2025



Quelle: Eigene Darstellung

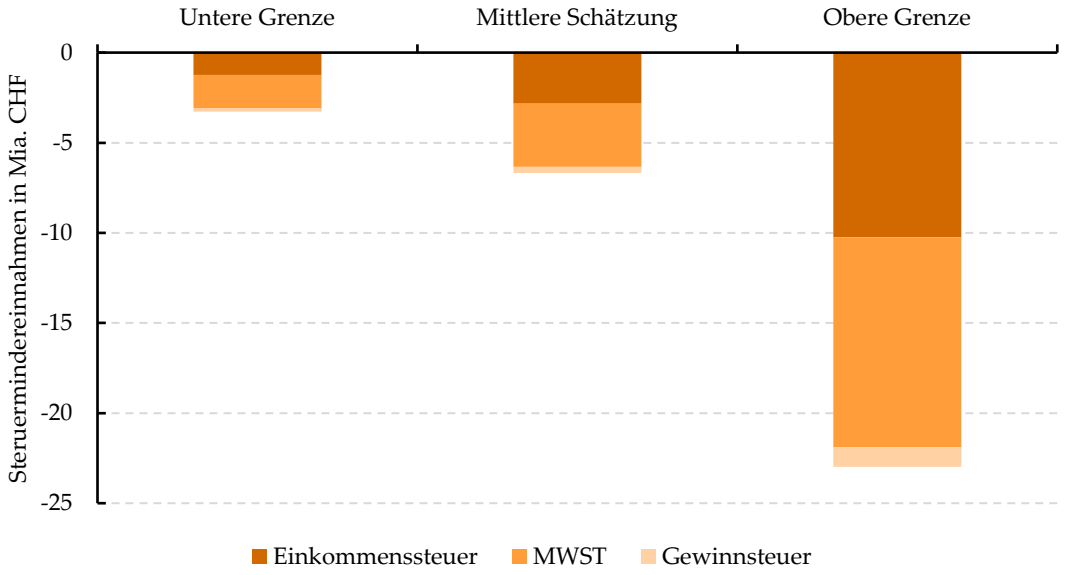
Auswirkungen auf die Steuereinnahmen

Auch die Schätzung der potenziell entgangenen Steuereinnahmen ist mit Unsicherheit konfrontiert und weist dementsprechend eine erhebliche Bandbreite auf. Vor diesem Hintergrund sind die Ergebnisse wiederum als indikative Werte zu interpretieren. Die Schätzung der Steuereffekte bezieht sich auf den Zeitraum 2025 bis 2035, wobei wir uns auf

Steuereinnahmen aus Mehrwertsteuer (MWST), Gewinnsteuern sowie Einkommenssteuern (einschliesslich Gemeinde-, Kantons- und direkter Bundessteuern) konzentrierten.[73]

Die Ergebnisse sind in Abbildung 7 dargestellt. Insgesamt belaufen sich die geschätzten kumulierten Steuerausfälle über den Projektionshorizont auf rund CHF 3 bis 22 Mrd. Im mittleren Szenario erreichen die prognostizierten kumulierten Steuermindereinnahmen einen Wert von knapp CHF 7 Mrd. Anteilsmässig sind dabei jeweils die Mindereinnahmen aus der Mehrwertsteuer, gefolgt von den Einkommenssteuern, am bedeutendsten.

Abbildung 7: Kumulierte Steuermindereinnahmen (2025–2035)



Quelle: Eigene Darstellung

4.4 Zusammenfassung

Dieses Kapitel bewertet die makroökonomischen Auswirkungen einer vollständigen Umsetzung der revidierten VÜPF im Vergleich zur Beibehaltung des Status quo. Da AAKD und FDA in ein breites Spektrum wirtschaftlicher Aktivitäten eingebettet sind, ist davon auszugehen, dass die Auswirkungen der Revision sektorübergreifend heterogen ausfallen. Die grössten Auswirkungen werden jedoch klar in der Digital Trust-Branche erwartet, wo die Geschäftsmodelle auf Glaubwürdigkeit, Vertraulichkeit und sicheren Datenumgang beruhen.

Die Analyse zeigt, dass aufgrund der VÜPF-Revision die Wachstumsaussichten der Digital Trust-Industrie in der Schweiz erheblich geschwächt würden. Obschon nur ein Teil der Unternehmen direkt betroffen wäre, besteht die reale Gefahr, dass eine Erosion der Vertrauenswürdigkeit der Schweiz eintreten würde, die das gesamte Ökosystem

[73] Anhang B.4 enthält eine detaillierte Beschreibung der zugrundliegenden Annahmen und methodischen Entscheidungen, die für jede Steuerkategorie bei der Berechnung getroffen wurden.

beeinträchtigt. Interviewergebnisse und das beobachtete Unternehmensverhalten deuten dann auch auf ein hohes Risiko stockender Investitionen, Verlagerung von Aktivitäten ins Ausland und einer Dämpfung von Cluster-Dynamiken hin. Der Sektor würde mittel- bis langfristig bestenfalls stagnieren.

Quantitativ fällt die Divergenz zwischen den zwei Regulierungsoptionen erheblich aus. Gegenüber dem Status quo wird der jährliche Umsatzverlust im Digital Trust-Sektor bis 2035 auf CHF 5 bis 39 Mrd. geschätzt. Die kumulierten Umsatzverluste belaufen sich in der mittleren Schätzung im betrachteten Zeitraum auf rund CHF 47 Mrd. und spiegeln Zinseszinseffekte entgangenen Wachstums wider. Die Wohlfahrtsverluste, gemessen mittels einer Input-Output-Analyse, werden für direkte und indirekte Effekte über den Zeitraum 2025 bis 2035 auf CHF 14 bis 89 Mrd. geschätzt.

Die gleiche Dynamik findet sich auch bei der Beschäftigung: Bis 2035 werden die Beschäftigungsverluste gegenüber dem Status quo auf 22'400 bis 219'300 Stellen geschätzt, mit einer mittleren Schätzung von rund 47'200 entgangener Stellen. Die entgangenen Steuereinnahmen über denselben Zeitraum belaufen sich – einschliesslich MWST, Gewinnsteuern und Einkommenssteuern – gemäss unseren Schätzungen kumuliert auf CHF 3 bis 22 Mrd.

Über diese quantifizierbaren Effekte hinaus birgt die VÜPF-Revision das Risiko weitergehender makroökonomischer Auswirkungen, die durch Reputationsfaktoren getrieben werden. Eine Schwächung der internationalen Stellung der Schweiz als vertrauenswürdige Rechtsordnung würde voraussichtlich auch andere vertrauensbasierte Sektoren beeinträchtigen und den Ausgangsschock verstärken. Obschon diese Effekte schwer zu quantifizieren sind, könnten sie letztlich die grössten wirtschaftlichen Kosten darstellen. Zusammenfassend lässt sich somit festhalten, dass dem VÜPF-Revisionsvorschlag ein erhebliches strukturelles Risiko für negative Auswirkungen auf Wachstum, Beschäftigung, Wohlfahrt und öffentliche Finanzen innewohnt.

A Kategorien und Pflichten von FDA und AAKD

A.1 Referenzszenario (Status quo)

Tabelle 3 fasst die Kategorien und Pflichten der FDA zusammen, Tabelle 4 gibt denselben Überblick für AAKD. Beide Zusammenfassungen basieren auf der aktuellen Fassung der VÜPF. Die detaillierten Pflichten sind in der VÜPF vom 26. März 2024 festgelegt.

Tabelle 3: FDA-Unterkategorien und ihre jeweiligen Pflichten

Kategorie	Einstufungskriterien	Pflichten
FDA mit reduzierten Pflichten (Art. 51)	Herabstufung auf Antrag an den Dienst ÜPF, sofern die gesetzlichen Voraussetzungen erfüllt sind. Hauptkriterien: (a) die Anbieterin bietet Fernmeldedienste **ausschliesslich im Bereich Bildung und Forschung** an, *oder* (b) sie hat in den **letzten 12 Monaten höchstens 10 Überwachungsanordnungen** betreffend **10 verschiedene Überwachungsziele** erhalten, *und* (c) der gesamte inländische Umsatz aus Fernmelde- und abgeleiteten Kommunikationsdiensten beträgt in jedem der letzten zwei Geschäftsjahre **weniger als CHF 100 Mio**. Die Beurteilung basiert auf dem **Umsatz aus Fernmelde- und abgeleiteten Kommunikationsdiensten**, nicht auf dem gesamten Unternehmensumsatz.	Grundlegende Pflichten umfassen: ▪ Nutzer mit geeigneten Mitteln identifizieren;[74] ▪ für Auskunftsersuchen erforderliche Bestandesdaten aufbewahren; ▪ standardisierte und besondere Auskünfte erteilen; ▪ Auskunftsbereitschaft nachweisen; ▪ Überwachungsmassnahmen zulassen, Systemzugang gewähren, wo erforderlich, und durch die Anbieterin angebrachte Verschlüsselung entfernen; ▪ auf Anfrage verfügbare Randdaten übermitteln, ohne Speicherungspflicht.
FDA mit vollen pflichten	Standardkategorie: Jede FDA gilt zunächst als FDA mit vollen Pflichten. Eine Herabstufung wird erst wirksam, wenn der Dienst ÜPF sie formell genehmigt. Werden die Kriterien von Art. 51 nicht mehr erfüllt, muss die FDA den Dienst ÜPF benachrichtigen, der daraufhin die Heraufstufung in die Kategorie mit vollen Pflichten erklärt.	Alle Pflichten der reduzierten Kategorie zuzüglich: ▪ 24/7-Bereitschaftsdienst; ▪ Speicherung der für bestimmte Auskunftsersuchen und rückwirkende Überwachung erforderlichen Verkehrsmetadaten; ▪ Auskunftserteilung über die automatisierte Auskunftsschnittstelle des Dienstes ÜPF und Nachweis der Bereitschaft zu deren Nutzung; ▪ automatisierte Auskunftserteilung und obligatorische Nutzung der Auskunftsschnittstelle; ▪ technische Fähigkeit zur Lieferung von Inhalts- und Randdaten für die Echtzeitüberwachung und rückwirkende Überwachung. Neu heraufgestufte FDA profitieren je nach Komplexität der Pflichten von Übergangsfristen von 2 oder 12 Monaten.

[74] Im erläuternden Bericht werden einige Beispiele genannt, die als geeignete Mittel im Sinne von Art. 19 gelten könnten. Dazu gehören beispielsweise die Identifizierung mittels Kreditkarte und die Speicherung der Autorisierungsdaten oder die Identifizierung mittels SIM-Karte und die Speicherung der International Mobile Subscriber Identity (IMSI).

Tabelle 4: AAKD-Unterkategorien und ihre jeweiligen Pflichten

Kategorie	Einstufungskriterien	Pflichten
AAKD ohne weitergehende Pflichten	**Standardkategorie,** anwendbar, solange weder die Kriterien für weitergehende Auskunftspflichten (Art. 22) noch für weitergehende Überwachungspflichten (Art. 52) erfüllt sind.	Nur grundlegende Mitwirkungspflichten: ▪ formlose Auskünfte erteilen; ▪ Überwachungsmassnahmen zulassen und Systemzugang gewähren, wo erforderlich; ▪ alle für die Überwachung erforderlichen Auskünfte erteilen; auf Anfrage verfügbare Verkehrsmetadaten übermitteln, ohne Speicherungspflicht.
AAKD mit weitergehenden Auskunftspflichten (Art. 22)	Der Dienst ÜPF erklärt eine AAKD zur Anbieterin mit weitergehenden Pflichten, wenn per Stichtag 30. Juni gilt: **mehr als 100 Auskunftsersuchen** (12-Monats-Durchschnitt über alle abgeleiteten Kommunikationsdienste) *oder* ein inländischer Umsatz von **mehr als CHF 100 Mio.** in den letzten zwei Geschäftsjahren, sofern ein grosser Teil der Geschäftstätigkeit abgeleitete Kommunikationsdienste erbringt *und* **mehr als 5'000 Teilnehmende** vorhanden sind.	Ähnliche Pflichten wie FDA mit vollständigen Pflichten bezüglich Auskunftspflichten. Es gelten jedoch einige Ausnahmen und Herabstufungen: ▪ Anstelle eines 24/7-Pikettdienstes sind Kontaktangaben eines internen Pikettdienstes (sofern vorhanden) für besonders dringende Fälle bereitzustellen; ▪ Auskunftserteilung gemäss Art. 48a–48c nicht erforderlich. Übergangsfristen: 2 Monate für einfachere Pflichten, 12 Monate für technisch komplexe.
AAKD mit weitergehenden Überwachungspflichten (Art. 52)	**Der Dienst ÜPF erklärt** eine AAKD zur Anbieterin mit weitergehenden Pflichten, wenn per Stichtag 30. Juni gilt: **10 oder mehr verschiedene Überwachungsziele** (12-Monats-Durchschnitt über alle abgeleiteten Kommunikationsdienste) *oder* ein inländischer Umsatz von **mehr als CHF 100 Mio.** in den letzten zwei Geschäftsjahren, sofern ein grosser Teil der Geschäftstätigkeit abgeleitete Kommunikationsdienste erbringt *und* **mehr als 5'000 Teilnehmende** vorhanden sind.	Ähnliche Pflichten wie FDA mit vollständigen Pflichten bezüglich **Überwachungspflichten**. Es gelten jedoch einige Ausnahmen und Herabstufungen: ▪ Überwachung gemäss Art. 56a, 56b, 67 Buchstaben b und c sowie 68 Absatz 1 Buchstaben b und c nicht erforderlich; ▪ Auskunftserteilung gemäss Art. 48a–48c nicht erforderlich. Übergangsfristen: 2 bis 12 Monate je nach Pflicht.

A.2 Vollständige Umsetzung der VÜPF-Revision

Definition und Pflichten von FDA

Eine Fernmeldedienstanbieterin (FDA) ist eine Anbieterin, die für die technische Übertragung von Informationen verantwortlich ist. Anders als Dienstanbieterinnen, die auf einem fremden Netz aufbauen, bieten FDA Netzzugangs- oder Transportdienste direkt für Dritte an und tragen die vertragliche Verantwortung für die Zustellung von Kommunikationen. Dazu gehören Anbieterinnen, die ein öffentliches Fernmeldenetz betreiben, direkten Zugang zu einem solchen Netz anbieten (z.B. Internetzugang), öffentliche Mobilkommunikationsdienste erbringen oder öffentliche Telefondienste zusammen mit Netzzugang anbieten.

Die Verordnung sieht abgestufte Verpflichtungen für FDA vor. Diese gliedern sich in zwei Unterkategorien: FDA mit reduzierten Pflichten und FDA mit vollen Pflichten. Letztere bildet den Standardfall unter der revidierten Verordnung. Tabelle 5 fasst die zwei Kategorien und ihre jeweiligen Pflichten zusammen.

Tabelle 5: FDA-Unterkategorien und ihre jeweiligen Pflichten

Kategorie	Einstufungskriterien	Pflichten
FDA mit reduzierten Pflichten (Art. 16b)	Herabstufung auf Antrag an den Dienst ÜPF, sofern die gesetzlichen Voraussetzungen erfüllt sind. Hauptkriterien: (a) die Anbieterin bietet Fernmeldedienste **ausschliesslich im Bereich Bildung und Forschung** an, *oder* (b) sie hat in **den letzten 12 Monaten höchstens 10 Überwachungsanordnungen betreffend 10 verschiedene Überwachungsziele** erhalten, *und* (c) der gesamte inländische Unternehmensumsatz beträgt in jedem der letzten zwei Geschäftsjahre **weniger als CHF 100 Mio.** Die Beurteilung basiert auf dem **gesamten Unternehmensumsatz**, d.h. nicht nur auf dem fernmeldebezogenen Umsatz.	Grundlegende Pflichten umfassen: ▪ Personen mit geeigneten Mitteln identifizieren; ▪ für Auskunftsersuche erforderliche Bestandesdaten aufbewahren; ▪ standardisierte und besondere Auskünfte erteilen; ▪ Auskunftsbereitschaft nachweisen; ▪ Überwachungsmassnahmen zulassen, Systemzugang gewähren, wo erforderlich, und durch die Anbieterin angebrachte Verschlüsselung entfernen; ▪ auf Anfrage verfügbare Randdaten übermitteln, ohne Speicherungspflicht.
FDA mit vollen Pflichten (Art. 16c)	Standardkategorie: Jede FDA gilt zunächst als FDA mit vollständigen Pflichten. Eine Herabstufung wird erst wirksam, wenn der Dienst ÜPF sie formell genehmigt. Werden die Kriterien von Art. 16b nicht mehr erfüllt, muss die FDA den Dienst ÜPF benachrichtigen, der daraufhin die Heraufstufung in die Kategorie mit vollständigen Pflichten erklärt.	Alle Pflichten der reduzierten Kategorie zuzüglich: ▪ 24/7-Pikettdienst; ▪ Speicherung der für bestimmte Auskunftsersuchen und rückwirkende Überwachung erforderlichen Randdaten; ▪ Auskunftserteilung über die automatisierte Auskunftsschnittstelle des Dienstes ÜPF und Nachweis der Bereitschaft zu deren Nutzung; ▪ automatisierte Auskunftserteilung und obligatorische Nutzung der Auskunftsschnittstelle; ▪ technische Fähigkeit zur Lieferung von Bestandes- und Inhaltdaten für die Echtzeitüberwachung und rückwirkende Überwachung. Neu heraufgestufte FDA profitieren je nach Komplexität der Pflichten von Übergangsfristen von 6 oder 12 Monaten.

Definition und Pflichten von AAKD

Eine AAKD ist eine Anbieterin, die zwischenmenschliche Kommunikation zwischen Nutzern ermöglicht, dies jedoch auf Basis der Kommunikationsinfrastruktur eines anderen Fernmeldedienstes tut. AAKD betreiben ihre Kommunikationsdienste unabhängig vom Netzzugang; stattdessen bieten sie Kommunikationsfunktionalitäten «Over The Top (OTT)» eines primären Fernmeldedienstes an. Dazu gehören beispielsweise Messaging-, Anruf- oder andere zwischenmenschliche Kommunikationsfunktionen, die in Online-Plattformen, Apps oder digitale Dienste integriert sind. AAKD können eigenständige Anbieterinnen sein oder Kommunikationsfunktionen als Teil eines umfassenderen digitalen Ökosystems anbieten.

Was AAKD rechtlich kennzeichnet, ist nicht das Geschäftsmodell, sondern die technische Tatsache, dass sie auf der zugrundliegenden Kommunikationsinfrastruktur einer anderen Anbieterin aufbauen und dabei dennoch direkte zwischenmenschliche Kommunikation ermöglichen. Da sie als Intermediär im Kommunikationsprozess agieren und überwachungsrelevante nutzer- oder nachrichtenbezogene Informationen vorhalten können, unterwirft die Verordnung sie je nach Grösse abgestuften Pflichten. Ein wichtiges Ergebnis des Vernehmlassungsverfahrens ist, dass die Definition der AAKD selbst für Fachleute nicht vollständig klar ist und daher erhebliche Rechtsunsicherheit darüber besteht, welche Unternehmen – über die genannten Beispiele hinaus (vgl. Abschnitt 3.2.1) – ebenfalls als AAKD qualifizieren könnten.

Die Pflichten der AAKD werden in drei Unterkategorien unterteilt: AAKD mit minimalen Pflichten, AAKD mit reduzierten Pflichten und AAKD mit vollständigen Pflichten. Tabelle 6 fasst die drei Kategorien und ihre jeweiligen Pflichten zusammen.

Tabelle 6: AAKD-Kategorien und ihre jeweiligen Pflichten

Kategorie	Einstufungskriterien	Pflichten
AAKD mit minimalen Pflichten (Art. 16e)	**Standardkategorie,** anwendbar, solange weder die Kriterien für reduzierte Pflichten noch für vollständige Pflichten erfüllt sind. Konkret: **weniger als 5'000 Teilnehmende** (12-Monats-Durchschnitt) *und* **weniger als CHF 100 Mio.** inländischer Umsatz in jedem der letzten zwei Geschäftsjahre.	Nur grundlegende Mitwirkungspflichten: ▪ formlose Auskünfte erteilen; ▪ Überwachungsmassnahmen dulden und Systemzugang gewähren, wo erforderlich; ▪ alle für die Überwachung erforderlichen Auskünfte erteilen; ▪ auf Anfrage verfügbare Randdaten übermitteln, ohne Speicherungspflicht.
AAKD mit reduzierten Pflichten (Art. 16f)	**Automatische Heraufstufung,** wenn per Stichtag 30. Juni gilt**: mehr als 5'000, aber weniger als 1 Mio. Teilnehmende** (12-Monats-Durchschnitt über alle abgeleiteten Kommunikationsdienste) *und* ein inländischer Umsatz von **weniger als CHF 100 Mio.** in den letzten zwei Geschäftsjahren.	Pflichten in Anlehnung an FDA mit reduzierten Pflichten: ▪ Personen mit geeigneten Mitteln identifizieren; ▪ Aufbewahrung der für die Auskunftserteilung erforderlichen Daten; ▪ standardisierte und besondere Auskünfte erteilen; ▪ Auskunftsbereitschaft nachweisen; ▪ durch die Anbieterin angebrachte Verschlüsselung entfernen. Zusätzliche Pflichten sind innerhalb von 6 Monaten nach dem 30. Juni umzusetzen.
AAKD mit vollständigen Pflichten (Art. 16g)	**Zweite Heraufstufung** für Anbieterinnen mit erheblicher wirtschaftlicher oder nutzerbezogener Relevanz. Kriterien: (a) **mindestens 1 Mio.** Teilnehmende (12-Monats-Durchschnitt, Stichtag 30. Juni) oder (b) ein inländischer Umsatz von **mehr als CHF 100 Mio.** in den letzten zwei Geschäftsjahren.	Pflichten in Anlehnung an FDA mit vollständigen Pflichten. Alle Pflichten der reduzierten Kategorie zuzüglich: ▪ 24/7-Pikettdienst; ▪ Speicherung der für bestimmte Auskunftserteilung und rückwirkende Überwachung erforderlichen Randdaten (Speicherung während 6 Monaten); ▪ automatisierte Auskunftserteilung und obligatorische Nutzung der Auskunftsschnittstelle; ▪ technische Fähigkeit zur Lieferung von Inhalts- und Randdaten für die Echtzeitüberwachung und rückwirkende Überwachung. Übergangsfristen: 6 Monate für einfachere Pflichten, 12 Monate für technisch komplexe.

B Quantifizierung des Schweizer Digital Trust-Markts

Dieser Anhang erläutert die Quantifizierung der in dieser Studie berücksichtigten wirtschaftlichen Auswirkungen. Anhang B.1 beschreibt die zur Schätzung der Umsätze verwendete Methodik, Anhang B.2 behandelt die Beurteilung der Wohlfahrtseffekte, Anhang B.3 skizziert den Ansatz zur Quantifizierung der Beschäftigung, und Anhang B.4 stellt die Schätzung der Steuereffekte dar. Alle Datenquellen und wesentlichen Referenzen, die diesen Quantifizierungen zugrunde liegen, sind in Anhang B.5 zusammengefasst.

B.1 Umsatz

Zur Schätzung der Grösse des Schweizer Digital Trust-Markts (DTM) im Jahr 2025 werden zwei komplementäre Ansätze verwendet:

- **Top-down-Allokation des globalen DTM auf die Schweiz,** basierend auf dem Anteil der Schweiz am globalen BIP sowie an den globalen Märkten für Informations- und Kommunikationstechnologie (IKT) und Cybersicherheit.
- **Extrapolation ausgehend von Frankreich,** unter Verwendung veröffentlichter Umsatzdaten für den französischen DTM und Hochrechnung auf die Schweiz basierend auf der relativen Marktgrösse.

Beide Ansätze werden zunächst detailliert beschrieben, bevor die daraus resultierenden Schätzungen für den Schweizer DTM präsentiert werden.

Aufschlüsselung des globalen DTM 2025

Der Schweizer Anteil am globalen DTM wird anhand der folgenden Formel berechnet:

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

wobei DTM_{Global} den geschätzten globalen DTM bezeichnet, $Anteil_{CH/Global}$ den Anteil der Schweiz an der globalen Wirtschaft oder an relevanten Märkten repräsentiert und $FX_{USD/CHF}$ den USD/CHF-Wechselkurs darstellt.

Schätzungen des globalen DTM aus sechs Marktstudien reichen von USD 110 bis 482 Mrd. Der Schweizer Anteil wird anhand des Anteils der Schweiz am globalen BIP sowie an den globalen IKT- und Cybersicherheitsmärkten approximiert. Über fünf verschiedene Indikatoren hinweg liegen die resultierenden Anteile zwischen 0.4 und 2.5 Prozent.[75] Der Wechselkurs basiert auf dem von der Eidgenössischen Steuerverwaltung (ESTV) veröffentlichten Jahresdurchschnittskurs USD/CHF für 2025 von 0.83.

[75] BIP Anteil von IMF, IKT Anteil von Mordor Intelligence und Cybersicherheit Anteil von Mordor Intelligence, Data Bridge Market Research und Ken Research.

Extrapolation des französischen DTM 2025

Als zweiter Ansatz wird ein von der französischen Allianz für Digital Trust (*Alliance pour la Confiance Numérique*, ACN) veröffentlichtes Marktobservatorium verwendet. In ihrem Observatorium 2025 weist die ACN für den französischen Digital Trust-Sektor Umsätze von EUR 21.3 Mrd. im Jahr 2024 aus, gegenüber einem gesamten globalen Umsatz französischer Unternehmen von EUR 33.5 Mrd.

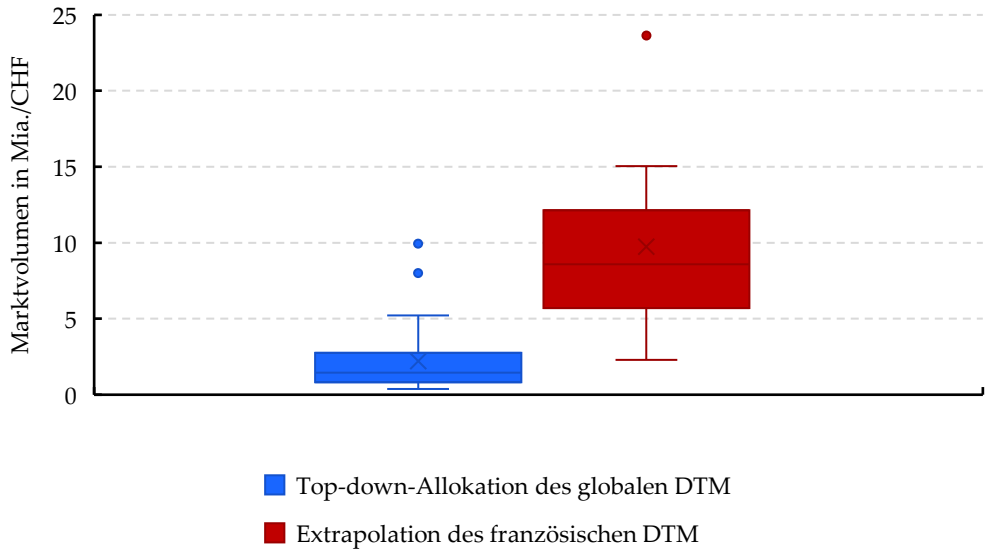
Um Zahlen für 2025 zu erhalten, werden die Umsätze unter Annahme einer konstanten jährlichen Wachstumsrate von 7.6 Prozent extrapoliert, was der zwischen 2018 und 2024 in Frankreich beobachteten durchschnittlichen jährlichen Wachstumsrate entspricht. Dies ergibt französische DMT-Umsätze von EUR 22.9 bis 36.0 Mrd. für das Jahr 2025.

Der Schweizer DTM wird dann durch Anpassung von Gleichung (1) an die französischen Umsatzzahlen und Skalierung gemäss dem Anteil der Schweiz relativ zu Frankreich abgeleitet. Fünf alternative Schätzungen dieses Anteils werden berücksichtigt, die zwischen 11 und 70 Prozent liegen.[76] Der EUR/CHF-Wechselkurs wird auf 0.94 festgesetzt.

Schweizer DTM im Jahr 2025

Angesichts der breiten Streuung der Eingangsparameter ist die geschätzte Grösse des Schweizer DTM mit erheblicher Unsicherheit behaftet (vgl. Abbildung 8).

Abbildung 8: Marktvolumen des Schweizer DTM im Jahr 2025



Quelle: Eigene Darstellung

Die Schätzungen legen nahe, dass der Schweizer DTM im Jahr 2025 zwischen CHF 0.4 und 23.6 Mrd. liegt. Diese grosse Bandbreite wird von drei Hauptfaktoren getrieben: Erstens unterscheiden sich die Projektionen des globalen DTM erheblich je nach Quelle, wobei

[76] BIP Anteil von IMF, IKT Anteil von Mordor Intelligence und Cybersicherheit Anteil von Mordor Intelligence, Data Bridge Market Research und Ken Research.

Schätzungen von Precedence Research mehr als viermal kleiner sind als jene von Mordor Intelligence. Zweitens liefert die Top-down-Aufschlüsselung des globalen Markts generell tiefere Schätzungen als die Extrapolation basierend auf französischen Daten. Drittens variieren die angenommenen Schweizer Marktanteile erheblich je nach Indikator: Cybersicherheitszahlen von Ken Research implizieren einen Schweizer DTM, der mehr als sechsmal grösser ist als Schätzungen auf Basis von Cybersicherheitsdaten von Mordor Intelligence.

Um einen plausibleren zentralen Korridor abzuleiten, wird den auf Frankreich basierenden Schätzungen ein höheres Gewicht beigemessen, da diese auf beobachteten, sektorspezifischen Umsätzen eines klar definierten inländischen DTM beruhen und nicht auf groben globalen Marktschätzungen. Die Analyse konzentriert sich daher auf die inländischen französischen Umsätze unter Ausschluss der internationalen Umsätze, um die Möglichkeit eines klaren Aufwärtsausreissers auszuschliessen. Auf dieser Grundlage werden sowohl die niedrigsten globalen Schätzungen als auch die oberen Ergebnisse, die sich aus der Extrapolation der internationalen französischen Umsätze ergeben, ausgeschlossen. Zudem erscheinen die von Mordor Intelligence und Ken Research implizierten Schweizer Marktanteile inkonsistent mit dem BIP- und IKT-Anteil der Schweiz, der hingegen in den von Data Bridge Market Research ausgewiesenen Schätzungen gut abgebildet ist. Aus diesen Überlegungen werden ein Schweizer Anteil von 1 Prozent am globalen DTM und 30 Prozent am französischen Inlandsmarkt als plausibelste Werte angenommen. Auf dieser Basis wird der Schweizer DTM im Jahr 2025 auf eine Bandbreite von rund CHF 3.2 bis 6.4 Mrd. geschätzt.

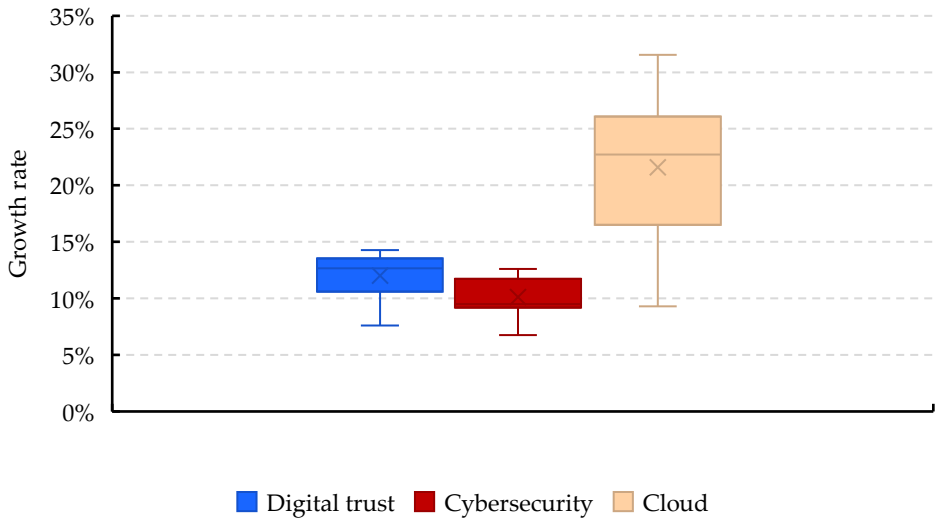
Indirekte Umsatzverluste in Bezug auf vorgelagerte Aktivitäten werden von der quantitativen Analyse ausgeschlossen. Eine übergeordnete Einschätzung auf Basis von Input-Output-Tabellen zeigt jedoch, dass die Berücksichtigung dieser indirekten Effekte zusätzliche Umsatzverluste in der Grössenordnung von 60 Prozent implizieren würde.

Marktwachstum

Es wurden mehrere Wachstumsraten identifiziert, die eine plausible Bandbreite für die Entwicklung des Schweizer DTM über die nächsten 5 bis 10 Jahre liefern.

- **Digital Trust:** Diese Kategorie umfasst verfügbare Wachstumsschätzungen für den globalen und den französischen DTM. Dedizierte Projektionen für den Schweizer DTM wurden nicht identifiziert, was die Unsicherheit bezüglich seiner Entwicklung unterstreicht.
- **Cybersicherheit:** Diese Kategorie umfasst Wachstumsschätzungen für die globalen, französischen und Schweizer Cybersicherheitsmärkte. Da Cybersicherheit ein Kernsegment des DTM darstellt, liefern diese Zahlen einen relevanten Anhaltspunkt für die erwarteten Marktdynamiken.
- **Cloud:** Diese Kategorie enthält Schätzungen für globale und Schweizer Cloud-Märkte (z.B. Cloud-Speicher, Public Cloud). Cloud ist Teil der digitalen Sicherheit und stellt damit einen relevanten Bereich des DTM dar.

Abbildung 9: Geschätzte Wachstumsraten



Anmerkung: Obschon gewisse Quellen darauf hindeuten, dass der Schweizer Cloud-Markt das globale Wachstum in jüngster Zeit übertroffen hat, werden globale Richtwerte ohne Aufwärtsanpassung beibehalten, um einen konservativen Beurteilungsrahmen zu gewährleisten.[77]

Quelle: Eigene Darstellung

Die Abbildung zeigt, dass die geschätzten Wachstumsraten aller Bereiche erheblich variieren. Im Durchschnitt wächst Cybersicherheit mit 10.13 Prozent am geringsten und Cloud mit 21.59 Prozent am stärksten. Diese Divergenz ist konsistent mit den Branchenlebenszyklen: Während Cybersicherheit einen reiferen, etablierten Markt darstellt, befindet sich der Cloud-Sektor noch in einer frühen Expansionsphase, die durch dynamisches Wachstum gekennzeichnet ist. Die eruierte Bandbreite bietet einen strukturierten Korridor für die Szenariokalibrierung. Cybersicherheit repräsentiert das reifste Kernsegment des DTM und bildet daher die Untergrenze. Cloud-Märkte erfassen demgegenüber die dynamischsten und innovationsgetriebenen Komponenten des Digital Trust-Ökosystems und definieren damit eine wirtschaftlich plausible Obergrenze. Die DTM-Durchschnittsschätzung dient als zentraler Richtwert. Die Verwendung dieser drei sektoralen Durchschnittswerte gewährleistet Konsistenz, vermeidet die selektive Auswahl einzelner Ausreisser und verankert die Schweizer DTM-Projektion in den Marktdynamiken eng verwandter Segmente. Entsprechend werden 10.13 Prozent als konservative Untergrenze, 21.59 Prozent als Obergrenze (die hohe Wachstumsdynamiken widerspiegelt) und 12.01 Prozent als plausible zentrale Wachstumsrate für den Schweizer DTM über die nächsten 5 bis 10 Jahre angewendet.

B.2 Wohlfahrt

Die BIP-Auswirkung wird mithilfe von Input-Output-Tabellen für NOGA-Klassen 62 und 63 (IT- und Informationsdienstleistungen) geschätzt, die als Proxy für die Digital Trust-Industrie dienen. Dieser Rahmen erlaubt die Ableitung von direkten, indirekten und

[77] Cloud Computing 2022 [17.02.2026].

induzierten Wertschöpfungseffekten basierend auf den oben dargestellten Umsatzschätzungen. Die direkte Wertschöpfung spiegelt den innerhalb der Digital Trust-Branche selbst generierten Beitrag wider. Die resultierende Schätzung für die Schweiz, basierend auf NOGA 62 und 63, ist weitgehend konsistent mit den entsprechenden ACN-Schätzungen für den französischen Digital Trust-Sektor. Die indirekte Wertschöpfung erfasst vorgelagerte Spillover-Effekte entlang der Lieferkette und wird unter Verwendung etablierter sektoraler Inputkoeffizienten aus dem Input-Output-Rahmen abgeleitet.

Während die Schätzung der direkten und indirekten Effekte relativ robust und in den Ausgangsdaten gut verankert ist, unterliegt die induzierte Wertschöpfung – die primär durch zusätzlichen Konsum, der durch höhere Haushaltseinkommen finanziert wird, getrieben wird – erheblich grösserer Unsicherheit. Da sie von Verhaltensannahmen und Multiplikatoreffekten abhängt, sollte die induzierte Komponente daher eher als Obergrenze der Wohlfahrtseffekte und nicht als zentrale Schätzung interpretiert werden.

B.3 Beschäftigung

Die Beschäftigung im Schweizer DTM im Jahr 2025 wird anhand von zwei Ansätzen geschätzt.

- **Extrapolation ausgehend von Frankreich:** Dieser Ansatz stützt sich auf veröffentlichte Beschäftigungszahlen für den französischen Digital Trust-Sektor und rechnet diese basierend auf relativen Marktgrössen auf die Schweiz hoch.
- **Umsatz-pro-Mitarbeitenden-Verhältnis:** Diese Methode stützt sich auf das veröffentlichte Umsatz-pro-Vollzeitäquivalent-Verhältnis (VZÄ)[78] in den Input-Output-Tabellen für die NOGA-Codes 62 und 63 in der Schweiz und skaliert es mit der durchschnittlichen Beschäftigungsquote. Dieses Verhältnis wird dann auf die geschätzten mittleren Umsätze angewendet.

Eine Top-down-Allokation ausgehend vom globalen DTM ist aufgrund fehlender zuverlässiger Daten zur globalen Beschäftigung nicht möglich. Die Extrapolation folgt daher derselben Methodik wie in Anhang B.1 dargelegt; indirekte Beschäftigungsverluste in Bezug auf vorgelagerte Aktivitäten werden ebenfalls von der quantitativen Analyse ausgeschlossen.

Der französische Digital Trust-Sektor beschäftigt gemäss ACN im Jahr 2024 rund 107’000 Personen. Die Anwendung des Skalierungsansatzes (vgl. Anhang B.1) ergibt eine Bandbreite von 12’900 bis 84’400 Beschäftigten für die Schweizer Digital Trust-Branche im Jahr 2025. Die Verwendung des zuvor identifizierten plausiblen Marktanteils von 30 Prozent ergibt eine Punktschätzung von rund 36’200 Beschäftigten.

[78] Intuitiv beschreibt diese Kennzahl, wie viel Umsatz ein Unternehmen in diesem Sektor im Durchschnitt pro VZÄ erwirtschaftet. Wenn die Umsatzkennzahl pro VZÄ dann mit der durchschnittlichen Beschäftigungsquote multipliziert wird, gibt sie an, wie viel Umsatz im Durchschnitt pro Mitarbeiter erwirtschaftet wird.

Wird sodann das Umsatz-pro-Mitarbeitenden-Verhältnis von CHF 352'000 pro Mitarbeitenden[79] auf die mittleren Umsätze im Schweizer DTM im Jahr 2025 angewendet, um die Beschäftigung im Schweizer DTM zu berechnen, ergibt sich eine Schätzung von 13'800 Beschäftigten. Die Auftraggeberin schätzt die aktuelle Beschäftigung auf rund 25'000 Personen. Entsprechend wird die Schätzung der Auftraggeberin als mittlere Schätzung verwendet, das Umsatz-pro-Mitarbeitenden-Verhältnis als Untergrenze und die extrapolierte Zahl als Obergrenze für die Beschäftigungsprojektionen.

Beschäftigungswachstum

Das Beschäftigungswachstum wird anhand historischer Daten für den französischen DTM kalibriert. Gemäss ACN stieg die Beschäftigung von 52'300 Mitarbeitenden im Jahr 2018 auf 107'000 im Jahr 2024, was einer durchschnittlichen jährlichen Wachstumsrate von 12.67 Prozent über den Zeitraum 2018 bis 2024 entspricht. Das Wachstum war besonders stark zwischen 2023 und 2024, als die Beschäftigung von 89'000 auf 107'000 stieg (eine Zunahme von 20 Prozent).

Diese jüngste Wachstumsrate übersteigt die für den Gesamtmarkt in Frankreich ausgewiesenen Wachstumsraten erheblich und wird daher als Ausreisser behandelt und von der Basisanalyse ausgeschlossen. Um konservativ zu bleiben, wird auf die Beschäftigung dieselbe Bandbreite von Wachstumsraten wie auf die Umsätze angewendet, obschon historische Belege für Frankreich darauf hindeuten, dass das Beschäftigungswachstum das Umsatzwachstum durchschnittlich um rund fünf Prozentpunkte übertroffen hat.

B.4 Steuern

Die Schätzung entgangener Steuereinnahmen unterliegt Unsicherheit, insbesondere über längere Zeithorizonte. Im Einklang mit den methodischen Leitlinien[80] werden dennoch die Grössenordnungen eingeschätzt, da die Präsentation einer plausiblen Bandbreite von Ergebnissen einen grösseren analytischen Mehrwert bietet als der Verzicht auf eine Quantifizierung. Die Schätzung umfasst Auswirkungen auf Einnahmen aus Mehrwertsteuern (MWST), Einkommens- und Gewinnsteuern.

MWST

Die MWST-Auswirkung wird aus den geschätzten Umsatzverlusten abgeleitet und wendet einen konstanten MWST-Satz von 8.1 Prozent an.[81] Um konservativ zu bleiben, wird die

[79] Berechnet als CHF 420'000 pro VZÄ multipliziert mit der Beschäftigungsquote von 83.5 Prozent. Der Einfachheit halber wird davon ausgegangen, dass die sich daraus ergebende Quote in den nächsten zehn Jahren konstant bleibt.

[80] Leitfaden zur Schätzung der Regulierungskosten [20.01.2026]. Die Leitlinie basiert auf dem *Unternehmensentlastungsgesetz*.

[81] Vermutlich eine konservative Annahme, da die Mehrwertsteuer in den letzten Jahrzehnten schrittweise angehoben wurde und derzeit zwei Gesetzesvorlagen im Parlament diskutiert werden, die zu weiteren Erhöhungen führen könnten.

MWST von den ausgewiesenen Umsatzzahlen abgezogen und nicht zusätzlich dazu hinzugerechnet, um eine Überschätzung zu vermeiden.

Einkommenssteuern

Die Einkommenssteuerschätzung geht von einem jährlichen Bruttoeinkommen von CHF 108'000 aus, entsprechend dem niedrigsten Medianeinkommen, das im Jahr 2024 über die relevanten Sektoren hinweg beobachtet wurde, d.h. Telekommunikation (NOGA 61), IT-Dienstleistungen (NOGA 62) und Informationsdienstleistungen (NOGA 63). Die Verwendung des Medians statt des Durchschnitts und die Annahme eines konstanten Einkommensniveaus über die Zeit entspricht wiederum einem konservativen Ansatz. Der durchschnittliche effektive Steuersatz wird auf 13 Prozent festgesetzt, basierend auf dem Schweizer Steuerrechner[82] und entsprechen einer 35-jährigen, ledigen Person mit Wohnsitz in Zürich im Jahr 2025. Es ist anzumerken, dass die Digital Trust-Industrie derzeit in den Kantonen Genf und Waadt konzentriert ist, wo der effektive Steuersatz für dasselbe Einkommensniveau zwischen 15 und 18 Prozent läge. Die gewählte Annahme unterschätzt daher die potenziellen Einkommensteuerausfälle, anstatt sie zu überschätzen.

Gewinnsteuern

Die geschätzte Auswirkung auf die Gewinnsteuern wird aus den kumulierten Umsätzen über den Zeitraum 2025 bis 2035 abgeleitet. Da der Digital Trust-Sektor noch in einer starken Wachstumsphase ist und durch einen hohen Anteil an Startups gekennzeichnet ist, wird eine konservative Gewinnmarge von 5 Prozent angenommen. Diese Annahme liegt deutlich unter der in der Schweizer Software-Industrie-Erhebung 2023 dokumentierten durchschnittlichen Gewinnmarge der Softwarebranche von 8.8 Prozent im Jahr 2022. Für die Besteuerung wird der geltende effektive Gewinnsteuersatz von 14 Prozent für Gewinne bis CHF 10 Mio. des Kantons Waadt angewendet.

[82] Tax calculator [28.01.2026].

B.5 Datenquellen

Wert	Bedeutung	Quelle	Link
EUR 21.3 Mrd.	Umsatz in FR von französischen Digital Trust-Firmen 2024	ACN	https://www.confiance-numerique.fr/wp-content/uploads/2025/06/acn-observatory-of-digital trust-2025.pdf
EUR 33.5 Mrd.	Weltweite Umsätze von franz. Digital Trust-Firmen 2024	ACN	https://www.confiance-numerique.fr/wp-content/uploads/2025/06/acn-observatory-of-digital trust-2025.pdf
7.6 %	⌀ Wachstumsrate des franz. Digital Trust-Sektors 2016-24	ACN	https://www.confiance-numerique.fr/wp-content/uploads/2025/06/acn-observatory-of-digital trust-2025.pdf
107'000	Beschäftigte im franz. Digital Trust-Sektor 2024	ACN	https://www.decision.eu/wp-content/uploads/2024/06/Observatory-of-digital trust-sector-2024.pdf
89'000	Beschäftigte im franz. Digital Trust-Sektor 2023	ACN	https://www.confiance-numerique.fr/wp-content/uploads/2025/06/acn-observatory-of-digital trust-2025.pdf
52'300	Beschäftigte im franz. Digital Trust-Sektor 2018	ACN	https://www.confiance-numerique.fr/wp-content/uploads/2023/11/Observatoire-ACN-de-la-Confiance-numerique-2019.pdf
USD 3'360 Mrd. USD 1'000 Mrd. USD 117'170 Mrd.	BIP FR BIP CH BIP Welt	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 Mrd. 14.28 %	Globaler DTM 2025 CAGR	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/digital trust-market
USD 135 Mrd. 13.3 %	Globaler DTM 2025 CAGR	FMI	https://www.futuremarketinsights.com/reports/digital trust-market
USD 133 Mrd. 13.3 %	Globaler DTM 2025 CAGR	GVR	https://www.grandviewresearch.com/industry-analysis/digital trust-market-report
USD 110.47 Mrd. 11.6 %	Globaler DTM 2025 CAGR	Presedence research	https://www.precedenceresearch.com/digital trust-market
USD 388.54 Mrd. 12 %	Global DTM 2025 CAGR	Market Research Future	https://www.marketresearchfuture.com/reports/digital trust-market-21989
USD 118 Mrd.	Global DTM 2024	Ken Research	https://www.kenresearch.com/global-digital trust-market

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

CHF pro Monat 9’380 9’874 9’014	Med. Einkommen 2024 Telekommunikation IT Dienstleistungen Informationsdienste	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	Direkte Wertschöpfung Indirekte Wertschöpfung Induzierte Wertschöpfung Umsatz pro VZÄ	FSA	https://www.bfs.admin.ch/bfs/de/home/statistiken/volkswirtschaft/input-output.html
5.362 Mio. 4.480 Mio.	Beschäftigte VZÄ	FSA	https://www.bfs.admin.ch/bfs/de/home/statistiken/arbeit-erwerb/erwerbstaetigkeit-arbeitszeit/erwerbsbevoelkerung/arbeitsmarktstatus.html
14 %	Gewinnsteuern Waadt	KPMG	https://kpmg.com/ch/de/medien/medienmitteilungen/2025/05/clarity-swiss-taxes.html
8.8 %	EBIT Software Industrie 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 Markt global CAGR	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/cloud-storage-market
24.41 %	Cloud Storage Markt global CAGR	DBMR	https://www.databridgemarketresearch.com/reports/global-cloud-storage-market
31.1 %	Cloud AI Markt global CAGR	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/cloud-ai-market
31.53 %	Cloud AI Markt global CAGR	DBMR	https://www.databridgemarketresearch.com/reports/global-cloud-ai-market
9.31 %	Cloud Managed Services Markt global CAGR	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/cloud-managed-services-market
17.69 %	Public Cloud Markt global CAGR	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/public-cloud-market
22.95 %	Public Cloud Migration Markt global CAGR	DBMR	https://www.databridgemarketresearch.com/reports/global-public-cloud-migration-market
22.5 %	Public Cloud Markt 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 Markt CH CAGR	DBMR	https://www.databridgemarketresearch.com/nucleus/switzerland-cloud-service-market
20 %	IaaS & SaaS CH Wachstumsrate	Kellerhals Carrard	https://kellerhals-carrard.ch/download/204/2022_cloud_computing_switzerland.pdf