Sessionsempfehlungen Wintersession 2025

#	Titel	Behandelnder Rat	Position
24.4596	Mo. Gössi. Besserer Schutz des geistigen Eigentums vor KI-Missbrauch	Ständerat	Annahme der angepassten Motion. Zentral ist in der Umsetzung eine Opt-Out Lösung, die den Wissenschafts- und Wirtschaftsstandort der Schweiz nicht benachteiligt und schädigt.
25.3011	Mo. SiK-N. Die Rolle von Hosting- und Cloudanbietern bei der Bewältigung von Cyberbedrohungen stärken	Ständerat	Ablehnung der Motion. Swico unterstützt die Minderheit (Umformulierung der Motion in einen Prüfauftrag).
24.4020	Mo. Bulliard. Das Hosting von Kinderpornografie in der Schweiz nicht hinnehmen	Ständerat	Ablehnung der Motion. Allfällige Umsetzung im Strafgesetzbuch (StGB) verbunden mit möglicher Strafbefreiung und zwingender Berücksichtigung der etablierten Selbstregulierung.
25.4273	Mo. Gapany. Überwachung des Post- und Fernmeldeverkehrs. Erhalt der Wettbewerbsfähigkeit unserer Wirtschaft, Schaffung von Arbeitsplätzen und Wahrung der Grundrechte	Ständerat	Annahme der Motion.
25.3191	Mo. Salzmann. Ausreichende Mittel für die zivile Cybersicherheit.	Nationalrat	Annahme der Motion.
25.3259	Mo. Michel. Mehr Beteiligung, bessere Digitalisierung	Nationalrat	Annahme der Motion.
25.4402	Mo. KVF-N Digitalisierung der Führerausweise	Nationalrat	Annahme der Motion.
23.086	BRG. Investitionsprüfgesetz	In beiden Räten	Grundsätzlich Rückkehr zum bundesrätlichen Entwurf bzw. Orientierung an den Beschlüssen des Ständerats, wo diese nicht bereits mit denen des Bundesrats übereinstimmen.
23.039	BRG. Bundesgesetz über das nationale System zur Abfrage von Adressen natürlicher Personen (Adressdienstgesetz, ADG)	In beiden Räten	Zustimmung zum Gesetzesentwurf, Annahme der Anträge der SPK-S.

Geschäfte im Ständerat

24.4596 Mo. Gössi. Besserer Schutz des geistigen Eigentums vor KI-Missbrauch

Darum geht es:
In der Absicht die Urheberrechte im Kontext von KI zu schützen, **hätte die Motion in ihrem ursprünglichen Wortlaut eine Schweizer Insellösung geschaffen mit einem «Opt-In»-Ansatz und der Entfernung von Schrankenbestimmungen im Urheberrecht im Kontext von KI-Training.** Damit würde die KI-Forschung, -Entwicklung und -Kommerzialisierung, namentlich das Trainieren von grossen, auch eigenständigen KI-Sprachmodellen in der Schweiz, praktisch verunmöglicht. Auch wären Schweizer Daten in relevanten KI-Sprachmodellen nicht mehr angemessen vertreten. Dies hätte **negative Konsequenzen für alle Anwendungsbereiche von KI** (Mobilität, Gesundheit, Medien etc.) **und bedroht massgebliche Wertschöpfungsgewinne und damit wichtige Arbeitsplätze in der Schweiz.**

Wir begrüssen deshalb, hat zuletzt der Nationalrat eine Anpassung des Motionstextes mit 121 Stimmen beschlossen. Er ist damit seiner vorberatenden Kommission gefolgt. Der Nationalrat hat erkannt, dass es eine schädliche Regulierung von KI im Urheberrecht unbedingt zu verhindern gilt und insbesondere auch die Interessen der Digitalwirtschaft zu berücksichtigen sind. Diesem Ansatz hat sich schliesslich auch der Bundesrat angeschlossen. **66 Volksvertreter brachten mit ihrer Ablehnung zudem zurecht zum Ausdruck, dass bei der Regulierung von KI keine voreiligen Schlüsse zu ziehen sind, da wir uns bereits heute in einem stabilen Rechtsrahmen bewegen**. In der Folge hat sich die Kommission für Wissenschaft, Bildung und Kultur des Ständerats (WBK-S) nochmals mit dem Vorstoss auseinandergesetzt. Sie empfiehlt ihrem Rat die Motion mit angepasstem Text zur Annahme.

Argumente:
Für Swico steht ausser Frage, dass das Urheberrecht auch im KI-Zeitalter gilt und das geistige Eigentum zu schützen ist. Wir anerkennen die Absicht der Motion, diese Rechte zu schützen. Dies darf aber nicht zulasten des Forschungs-, Innovations- und Wirtschaftsstandorts Schweiz gehen. Genau dies wäre jedoch mit der Annahme der Motion im ursprünglichen Wortlaut der Fall gewesen.

Gerne verweisen wir hierzu auf das **Positionspapier «KI & Urheberrecht» von Swico** und fassen hinsichtlich der vorliegenden Motion nachfolgend zusammen.

KI hat das Potenzial unser Wirtschaftswachstum wesentlich zu stärken und damit Arbeitsplätze zu sichern und neue zu schaffen, wie Swico auch in einem kürzlich erschienen Gastkommentar darlegte. Aktuelle Studien gehen von einem Wachstumspotenzial von 3.6% bis 11% des BIP aus.[1] **Es ist gilt, das enorme Potenzial**

[1] pwc, economiesuisse & Swico, «Die Schweiz als KI-Vorreiterin: Wirtschaftliches Potential und neue Wege zur Regulierung» abgerufen am 07.08.2025 von https://www.swico.ch/de/news/detail/die-schweiz-als-ki-vorreiterin-wirtschaftliches-potenzial-und-neue-wege-zur-regulierung; bzw. Implement Consulting, «Das wirtschaftliche Potenzial von generativer KI in der Schweiz»,

von KI – gerade in den aktuell herausfordernden Zeiten – nicht zu gefährden – im Gegenteil: Die Chancen von KI sind aktiv zu nutzen und die Schweiz soll sich weiter als globaler KI-Hub etablieren.

Wir halten auch fest, dass kein unmittelbarer gesetzgeberischer Handlungsbedarf besteht. Dies, zumal das Urheberrechts technologieneutral ist und für Rechteinhaber bereits griffige Instrumente zur Verfügung stehen: Einerseits Bezahlschranken, wobei deren Umgehung als eine Straftat gewertet würde (Art. 143bis StGB). Andererseits sogenannte «Metatags» oder «Robots.txt» für den etablierten «Opt-Out-Mechanismus». Deren Vorteil: Sie zielen auf ganz bestimmte Crawler ab, sodass sichergestellt ist, dass beispielsweise Daten nicht für das Training der KI-Anwendung X verwendet, aber weiterhin in den Resultaten einer Suchmaschine Y angezeigt werden.

Gleichzeitig anerkennen wir den von der WBK-N erarbeiteten und vom Nationalrat bestätigten modifizierten Motionstext als einen «gutschweizerischen» Kompromiss. Dieser will dem ausgleichenden Charakter des schweizerischen Urheberrechts Rechnung tragen und die Thematik «Urheberrecht und KI» umfassend angehen. Sollte der Ständerat zum Schluss kommen, dass gesetzgeberischer Handlungsbedarf besteht, empfehlen wir die Mo. Gössi mit modifiziertem Text als Kompromiss anzunehmen.

Wir weisen in diesem Zusammenhang zusätzlich auf die Botschaft zur Änderung des Urheberrechts («Leistungsschutzrecht für Medienunternehmen», LSR) hin. Swico lehnt dieses, wie im «Positionspapier zum Leistungsschutzrecht für Medienunternehmen» dargelegt, klar ab. Mit dem LSR schlägt der Bundesrat eine Regulierung vor, die unnötig und von der Realität völlig überholt worden ist. Das mit der Vorlage verfolgte Ziel, die Medienvielfalt zu schützen, lässt sich nach unserer Ansicht nicht mit der finanziellen Belastung einzelner Marktteilnehmer erreichen. Wir begrüssen es deshalb, hat die Kommission für Verkehr und Fernmeldewesen des Nationalrates (KVF-N) die Branche angehört und ist zum Schluss gekommen, die Botschaft an den Bundesrat zurückzuweisen. **Dass die Kommission die Anliegen des LSR in die Motion Gössi integrieren möchte, sehen wir kritisch.**

Position:

Annahme der abgeänderten Motion. Zentral ist in der Umsetzung eine Opt-Out Lösung, die den Wissenschafts- und Wirtschaftsstandort der Schweiz nicht benachteiligt und schädigt.

---

abgerufen am 07.08.2025 von https://implementconsultinggroup.com/article/the-economic-opportunity-of-generative-ai-in-switzerland

25.3011 Mo. SiK-N. Die Rolle von Hosting- und Cloudanbietern bei der Bewältigung von Cyberbedrohungen stärken

Darum geht es:
Mit der Motion soll der Bundesrat beauftragt werden, gesetzliche Grundlagen auszuarbeiten, welche Hosting- und Cloudanbieter bei der Bewältigung von Cyberbedrohungen «die nötigen» Rechte und Pflichten erteilen, um den Missbrauch der von ihnen angebotenen Infrastrukturen und Dienste für Cyberangriffe zu bekämpfen. Der Nationalrat hat die Motion angenommen. Die Sicherheitspolitische Kommission des Ständerats (SiK-S) beantragt ihrem Rat mit 7 zu 4 Stimmen bei 1 Enthaltung, der Motion zuzustimmen. Eine Minderheit möchte zuerst eine Analyse, die aufzeigt, ob und wo Handlungsbedarf auf Gesetzesebene besteht. Im Vorfeld hat die Kommission Vertreter aus der Branche angehört. Einig ist sich die Kommission, dass die Regulierung nicht im Fernmeldegesetz, sondern im Informationssicherheitsgesetz erfolgen soll.

Argumente:
Die SiK-S hat die Branche und ihre Anliegen angehört, was wir sehr begrüssen.
Cybersicherheit ist ein gemeinsames Anliegen von Staat und Privatwirtschaft. Swico ist der Ansicht, dass die aktuelle Regulierung und private Massnahmen (namentlich der Swico Code of Conduct) funktionieren. Aus Sicht der Branche sind Zielsetzung und Anliegen der Motion unklar. Sie bringt nicht mehr Cybersicherheit, sondern mehr Bürokratie. Es drohen überdies Rechtsunsicherheit und Umsetzungsprobleme. Swico empfiehlt deshalb, die Minderheit der Kommission zu unterstützen und zuerst den gesetzgeberischen Handlungsbedarf zu eruieren, bevor reguliert wird. Eine Umformulierung der Motion in einen Prüfauftrag ist deshalb der richtige Weg.
Sollte der Gesetzgeber Regulierungsbedarf sehen, dann ist das **Informationssicherheitsgesetz** der richtige Regulierungsort. Rechenzentren und Cloud-Dienste fallen bereits unter das Informationssicherheitsgesetz.

Unsere Argumente im Einzelnen:

1. **Bestehende Rechtsgrundlagen sind ausreichend:** Für Swico ist nicht nachvollziehbar, welche Rechtslücke mit dieser Motion geschlossen werden soll. Hosting- und Cloud-Anbieter verfügen über die notwendigen Rechte, Schutzmassnahmen ergreifen sie selbstständig und halten sich an verschiedene Rechtsvorschriften. Seitens Branche sind die Rechtsgrundlagen ausreichend. Zu prüfen wären allenfalls operative Klarheiten bei Zuständigkeiten und Meldewegen.
2. **Die Branche verfügt bereits über genügend Rechte/Pflichten:**
   a. Vertragsrecht (OR/AGB): Die missbräuchliche Nutzung durch Ihre Kunden regeln die Anbieter in ihren AGB. Die missbräuchliche Nutzung ist ausdrücklich untersagt. Die Anbieter sichern sich ab, dass sie mögliche Verstösse gegen diese Richtlinien untersuchen und allenfalls den Zugriff auf die entsprechenden Ressourcen unterbinden können.
   b. Informationssicherheitsgesetz (Pflicht zur Meldung von Cyberangriffen): Organisationen müssen dafür sorgen, dass dem BACS Cyberangriffe auf ihre Informatikmittel gemeldet werden. Dazu gehören gemäss Art. 74b Abs. 1 lit. t auch Anbieterinnen und Betreiberinnen von Cloudcomputing, Suchmaschinen, digitale Sicherheits- und Vertrauensregister sowie Rechenzentren, sofern sie einen Sitz in der Schweiz haben.

c. Datenschutzgesetz: Aus Datenschutzgründen dürfen Hosting- und Cloud-Anbieter nicht in die Kundensysteme Einsicht nehmen. Über ihre Infrastruktur und Systeme können Hosting- und Cloud-Anbieter jedoch Cyberangriffe erkennen und entsprechend reagieren (Art. 9 „Bearbeitung durch Auftragsbearbeitung“).
d. Bundesgesetz betreffend die Überwachung der Post- und Fernmeldeverkehr (BÜPF) und deren Ausführungsverordnung (VÜPF): Hosting- und Cloud-Anbieter verfügen über explizite Pflichten zur Zusammenarbeit mit den Behörden, etwa bei Auskunftsbegehren, Echtzeitüberwachung oder Sperrmassnahmen.

3. **Cybersicherheit ist im Eigeninteresse der privaten Anbieter:** Bei global erreichbaren IT-Infrastrukturen gibt es täglich automatisierte Angriffsversuche von mehreren zehntausend Scans und Exploit-Versuchen am Tag. Das ist für die ICT-Branche und spezifisch für Hosting- und Cloud-Anbieter nichts Neues. Diese Aktivitäten sind jedoch nicht spezifisch auf Schweizer Infrastrukturen ausgerichtet, sondern Teil eines globalen, automatisierten Bedrohungsumfelds. Professionelle Hosting- und Cloud-Anbieter setzen aus wirtschaftlichen Überlegungen alles daran, um einen Angriff zu verhindern, ihn schnellstmöglich zu beenden sowie seine Ausbreitung und weiteren Schaden zu verhindern.
4. **Wird die Infrastruktur des Anbieters oder des Kunden angegriffen, wehren Hosting- und Cloud-Anbieter Angriffe ab:** Hosting- und Cloud-Anbieter unternehmen alles, um die Verfügbarkeit ihrer Services und die Sicherheit ihrer Kunden zu gewährleisten. Das ist ihr Geschäftsmodell und ihr Versprechen an die Kunden. Hosting- und Cloud-Anbieter haben bereits heute agile Massnahmen getroffen, die bereits heute über Mindeststandards gehen.
5. **Der geforderte, regulatorische Eingriff ist sachfremd und schafft Rechtsunsicherheit:** Die Motion zieht falsche Analogien zwischen FDA sowie Hosting- und Cloud-Anbieter. FDA müssen die fernmeldetechnische Übertragung von Informationen sicherstellen. Sie unterliegen dabei der Transportpflicht, der Netzneutralität und dem Fernmeldegeheimnis. Demgegenüber sind Hosting- und Cloud-Anbieter privatrechtlich geregelt. Sie unterliegen weder der Netzneutralität noch der Transportpflicht. Die Motion würde faktisch dazu führen, dass der Datenschutz geschwächt und zentrale rechtsstaatliche Grundlagen (Fernmeldegeheimnis) in Frage gestellt würden, da die Hosting- und Cloud-Anbieter die Daten ihrer Kunden überwachen müssten. Diese Entwicklung ist dringend zu hinterfragen, ergreifen sie bereits heute erfolgreich Massnahmen und verfügen über die nötigen Rechte und Pflichten.

Position:

Ablehnung der Motion und Unterstützung der Kommissionsminderheit: Umformulierung der Motion in einen Prüfauftrag.

24.4020 Mo. Bulliard. Das Hosting von Kinderpornografie in der Schweiz nicht hinnehmen

Darum geht es:
Die Motion will den Bundesrat beauftragen, eine gesetzliche Grundlage zu schaffen, damit Hosting- und Cloud-Anbieter (CHA) in der Schweiz verpflichtet sind, ihre Kunden über Meldemöglichkeiten von Kinderpornografie zu informieren, sowie Meldungen von pädokriminellen Inhalten an die Strafverfolgungsbehörden weiterzureichen und diese Inhalte zu sperren. Diesen regulatorischen Eingriff begründet die Motionärin mit angeblichen Schwächen des Schweizer Abwehrdispositivs gegen kinderpornographische Inhalte.

Zuletzt hat die Kommission für Verkehr und Fernmeldewesen des Ständerats (KVF-S) den Vorstoss beraten. Wir begrüssen und schätzen es ausdrücklich, dass sie dabei die Branche angehört hat. Damit hat die Kommission die Möglichkeit geschaffen, das starke Engagement der Branche und das bestehende Dispositiv darzulegen, das anerkennt wird. Gleichzeitig hat die Kommission beschlossen an einem entsprechenden Regulierungsauftrag festzuhalten. Sie schlägt ihrem Rat einen angepassten Motionstext vor, der alle relevanten Intermediäre und technischen Dienstleister verpflichten will, Verdachtsfälle von kinderpornografischen Inhalten den Behörden zu melden. Die Motion geht nun in den Ständerat als Zweitrat.

Argumente:
Wir halten klar fest: Die ICT-Branche toleriert keinen Missbrauch ihrer Dienste für pädokriminelle Inhalte. Swico teilt das Anliegen der Motion, Kinder- und Jugendliche angemessen zu schützen. **Gleichzeitig stellen wir mit Blick auf das wirksame Dispositiv fest, dass der geforderte, regulatorische Eingriff nicht angezeigt ist.**

Zum einen bietet 197 Abs. 4 StGB eine griffige rechtliche Handhabe, die das Speichern und Verfügbarmachen von pädokriminellen Inhalten adressiert: *«Wer Gegenstände oder Vorführungen im Sinne von Absatz 1, die sexuelle Handlungen mit Tieren oder nicht tatsächliche sexuelle Handlungen mit Minderjährigen zum Inhalt haben, herstellt, einführt, lagert, in Verkehr bringt, anpreist, ausstellt, anbietet, zeigt, überlässt, zugänglich macht, erwirbt, sich über elektronische Mittel oder sonst wie beschafft oder besitzt, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.»* Alle relevanten Intermediäre und technische Dienstleister haben bereits heute – nebst ihrer ethischen Verpflichtung und aus Reputationsgründen -das ureigene Interesse, solche Inhalte nicht zu speichern oder verfügbar zu machen.

Zum anderen regelt der «Swico Code of Conduct Hosting» (CCH) das konkrete Melde- und Sperrverfahren bei illegalen Inhalten. Der CCH, der zuletzt im April 2025 unter Berücksichtigung des EU Digital Service Act (DSA) aktualisiert wurde, baut auf den obenstehenden strafrechtlichen Bestimmungen auf. **Das Kernanliegen der ursprünglichen Motion wird damit bereits erfüllt:**

1. **Information der Kunden:** Bereits heute sind Kunden über Meldemöglichkeiten vis-à-vis den Anbietern informiert, da das Melde- und Sperrverfahren vertraglich geregelt wird (Ziff. 7 CCH)

2. **Meldung an Anbieter:** «Bei Offizialdelikten [ist] keine besondere Betroffenheit des Melde-Absenders erforderlich». Kunden wie auch Dritte können, daher bei pädokriminellen Inhalten auf einfache Weise Meldung erstatten (Ziff. 3.4 CCH). Wichtig: Es steht ihnen jederzeit frei, den Behörden eine Meldung zu erstatten.
3. **Aktive Sperrung:** Auf Basis des CCH sehen die Anbieter in den Verträgen mit ihren Kunden die Möglichkeit vor, zweifelhalte Inhalte unmittelbar zu sperren. Insbesondere, wenn sich die Anbieter als Folge der Kenntnisnahme der Meldung selbst strafrechtlich verantwortlich oder zivilrechtlich haftbar machen würden, wie das gemäss Art. 197 Abs 4 StGB der Fall wäre (Ziff. 6.1 CCH).
4. **Meldung an Behörden:** Weiter können Anbieter bei «Straftatbeständen Meldung an das Bundesamt für Cybersicherheit BACS (BACS Report (admin.ch)) und / oder an die Strafverfolgungsbehörden erstatten» (Ziff. 6.4 CCH). Dies geschieht aus Eigeninteresse und mit Blick auf Art. 197 Abs 4 StGB.

Auch Plattform und Content-Sharing-Anbieter verfolgen einen «Null-Toleranz-Ansatz». Nutzende sind über Nutzungsbedingungen der jeweiligen Dienste informiert und können entsprechende Inhalte bspw. über «In-Produkt-Meldeoptionen» melden. Anbieter sperren bzw. löschen diese Inhalte (Art. 197 Abs. 4 StGB gilt auch hier) und nutzen die Möglichkeit, Meldung zu erstatten. Die Branche engagiert und bekennt sich zu entsprechenden Massnahmen, bspw. auch im Kontext der «WeProtect Global Alliance» und den entsprechenden «Voluntary Principles to Counter Online Child Sexual Exploitation»

Gerade auch wegen diesem, umfassenden Dispositiv ist die Schweiz klar kein Hotspot - weniger als 1% der gemeldeten, pädokriminellen Inhalte werden über die Schweiz verfügbar gemacht. Hauptstandorte befinden sich im Ausland. Die Motion verweist auf den unrühmlichen Rang der Schweiz im Internet Watch Foundation Report (IWF) für das Jahr 2023 (8%- Anteil). Gemäss IWF ist dieser Rang «lediglich» auf 2 URLs zurückzuführen, die in der Schweiz gehostet wurde. Dahinterstehen «1 bis 2 Bad Actors». **Es handelt sich beim Ranking 2023 klar um einen Ausreisser, wie die Datenreihe zeigt: 2021: 1%; 2022: 0%; 2024: 0%.**

Zudem stellt die Motion auch eine unzutreffende Analogie her zwischen Fernmeldedienstanbietern (FDA) und Anbietern anderer Dienste. FDA müssen die fernmeldetechnische Übertragung von Informationen sicherstellen. Sie unterliegen der Transportpflicht, der Netzneutralität und dem Fernmeldegeheimnis. Deshalb sind sie auf eine rechtliche Grundlage für Sperrungen im FMG (Art. 46a) angewiesen. Sie setzen Sperrverfügungen des FedPol um. CHA aber auch Kommunikations- sowie Content-Sharing-Plattformen sind privatrechtlich geregelt und unterliegen weder der Transportpflicht, Netzneutralität noch dem Fernmeldegeheimnis. **CHA wie auch Kommunikations- sowie Content-Sharing-Plattformen handeln erfolgreich aufgrund des oben erläuterten Dispositivs und benötigen keine (weiteren) gesetzlichen Grundlagen, um wirksam einzugreifen.**

Den geforderten, regulatorischen Eingriff erachten wir deshalb als nicht angezeigt, ungeeignet und unverhältnismässig:

1. **Der Eingriff ist nicht begründet.** Aus den verfügbaren Daten (IWF) wird klar, dass das Dispositiv in der Schweiz wirksam ist.

2. **Keine echte Effizienzsteigerung des Dispositivs**, denn die Forderungen adressieren nicht die Notwendigkeit, dass Kunden oder Dritte überhaupt Meldungen absetzen müssen, damit Massnahmen ergriffen werden können.
3. **Unverhältnismässig:** Eine Anzeigepflicht für entsprechende Dienstanbieter ist unverhältnismässig. Nicht einmal im «analogen Leben» bestehen Anzeigepflichten für Gruppen, die Schutzbedürftigen wesentlich näherstehen, bspw. Lehrerinnen und Lehrer. Das gilt aber auch für andere privatwirtschaftliche Organisationen im analogen und digitalen Raum.
4. **Eine Regelung im FMG wie auch in einer Spezialregulierung wäre sachfremd.** Es würden neue Rechtsunsicherheiten geschaffen.

Sollte der Gesetzgeber dennoch zum Schluss kommen, dass regulatorischer Handlungsbedarf besteht, so wäre nicht eine FMG- oder spezialgesetzliche Regelung, sondern eine Umsetzung von Meldepflichten im Strafgesetzbuch (StGB) zu verfolgen. Diese Pflichten dürfen sich klar «nur» auf sogenannte Zufallsfunde und Meldungen gegenüber den Anbietern beziehen. Damit verbunden wäre auch die Schaffung eines Strafbefreiungsgrunds zu prüfen, der bspw. die Speicherung von entsprechenden Inhalten nicht unter Strafe stellt, sofern diese den Behörden gemeldet werden. Damit könnte die Strafverfolgung gestärkt werden. **Zudem fordern wir, dass die etablierte Branchenregulierungen bei der allfälligen Umsetzung zu berücksichtigen.**

Position:
Ablehnung der Motion: Swico teilt das Kernanliegen der Motion. Den geforderten, regulatorischen Eingriff erachten wir jedoch als nicht angezeigt und unverhältnismässig. Eine Regelung im FMG oder eine Spezialregulierung wäre zudem sachfremd und würde neue Unsicherheiten schaffen. Sollte der Gesetzgeber regulatorisch aktiv werden, so wäre eine Umsetzung von Meldepflichten, die sich auf Meldungen gegenüber dem Anbieter und Zufallsfunde beziehen, im Strafgesetzbuch (StGB) – gegebenenfalls verbunden mit einem Haftungsprivileg – zu verfolgen. Etablierte Selbstregulierungen sind zu berücksichtigen.

25.4273 Mo. Gapany. Überwachung des Post- und Fernmeldeverkehrs. Erhalt der Wettbewerbsfähigkeit unserer Wirtschaft, Schaffung von Arbeitsplätzen und Wahrung der Grundrechte

Darum geht es:
Mit der Motion soll der Bundesrat damit beauftragt werden, den Entwurf zur Revision der beiden Ausführungsverordnungen zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), die vom 29. Januar bis zum 6. Mai 2025 in Vernehmlassung waren, grundlegend zu überarbeiten. Im Nationalrat ist eine gleichlautende Motion von Nationalrat Olivier Feller (25.4206) eingereicht worden. Der Bundesrat empfiehlt die Motion zur Annahme.

Argumente:

Hintergrund für die beiden Motionen ist die grosse Kritik, die im Rahmen des Vernehmlassungsverfahrens zu den beiden Ausführungserlassen zur Überwachung des Post- und Fernmeldeverkehr (VÜPF, VD-ÜPF) geäussert wurde. Auch Swico äusserte sich kritisch zur Vernehmlassungsvorlage (Stellungnahme). Swico lehnte die Teilrevision entschieden ab, weil sie in weiten Teilen unverhältnismässig und nicht gesetzeskonform ist. Der Entwurf stellt einen unverhältnismässigen Eingriff in die Freiheitsrechte dar, bringt sicherheitspolitisch keinen Mehrwert, schwächt den Wirtschafts- und Innovationsstandort und verursacht unnötige Mehrkosten und Bürokratie für die betroffenen Unternehmen.

Zusammengefasst haben wir die folgende zentralen Kritikpunkte an der Vernehmlassungsvorlage geäussert:

1. Die **erweiterte Betrachtung** auf Basis des Gesamtumsatzes eines Unternehmens sowie bei den Schwellenwerten bei den Anbietern abgeleiteter Kommunikationsdienste (AAKD) betreffend die Teilnehmer wird die Anzahl Unternehmen, welche einer reduzierten oder vollständigen Pflicht unterliegen, deutlich erhöhen. Diese Ausweitung betrachtet Swico als unverhältnismässig.
2. Faktisch werden die meisten AAKD (mit mehr als 5'000 Teilnehmenden) mit **signifikanten neuen Pflichten** belegt. Diese Praxisänderung bedarf einer Gesetzesänderung. Die Einführung entsprechender, neuer Pflichten auf dem Verordnungsweg verletzt Art. 164 der Bundesverfassung, wonach die wichtigen rechtssetzenden Bestimmungen auf Gesetzesstufe zu erlassen sind. Diese Pflichten-Erweiterung ist zudem inhaltlich in keiner Weise gerechtfertigt.
3. **AAKD sind grundsätzlich von aktiven Überwachungspflichten zu befreien.** Insbesondere die Pflicht zur Vorratsdatenspeicherung lehnen wir ab.
4. Bei der Kategorisierung der Mitwirkungspflichtigen ist unseres Erachtens vielmehr auf die **Bedeutung der einzelnen Dienste** abzustellen.
5. **Nur AAKD mit Diensten «von besonderer wirtschaftlicher Bedeutung» sind allenfalls zusätzliche Pflichten aufzuerlegen.** Die Beurteilung, ob diese Qualifikation erreicht ist, hat sich auf den jeweiligen Dienst zu beziehen und darf nicht abhängig sein von allfälligen weiteren Aktivitäten des Anbieters. Das Abstellen auf den (Konzern-)Umsatz eines Unternehmens widerspricht den Vorgaben des Bundesgesetzes über die Überwachung des Post- und Fernmeldeverkehrs (BUPF).
6. **Die zusätzlichen Pflichten wirken sich klar negativ auf den Innovations- und Wirtschaftsstandort Schweiz aus.** Dies zumal Technologieanbieter, die im Verordnungsentwurf formulierten, umfassenden Überwachungspflichten bei der Sitzwahl und den Investitionsentscheiden kritisch beurteilen. Die Schweiz gelangt im Vergleich zu anderen Standorten ins Hintertreffen.

Position:

Annahme der Motion. Eine grundlegende Überarbeitung der Verordnungen ist aus Sicht von Swico zwingend. Wir fordern die Rückweisung und eine umfassende, verhältnismässige und gesetzeskonforme Überarbeitung der beiden Vorlagen.

Geschäfte im Nationalrat

25.3191 Mo. Salzmann. Ausreichende Mittel für die zivile Cybersicherheit.

Darum geht es:
Die Motion will den Bundesrat beauftragen, für das Bundesamt für Cybersicherheit (BACS) im Jahr 2026 statt 16.3 Millionen CHF 26.3 Millionen CHF und für die Finanzplan-Folgejahre statt 16.4 Millionen 31.4 Millionen Franken im Voranschlag 2026 einzustellen. Das BACS soll mit den notwendigen Mitteln ausgestattet werden, um den zunehmenden Cyberbedrohungen zu begegnen und die neuen Aufgaben aus dem revidierten Informationssicherheitsgesetz bewältigen zu können. Motionär Salzmann fordert, dass die Mittel für das BACS innerhalb des IT-Budgets der Armee kompensiert wird. Im Nationalrat ist eine gleichlautende Motion (25.3227) von Nationalrat Gerhard Andrey hängig. Der Ständerat hat die Motion in der Sommersession entgegen der Empfehlung des Bundesrates angenommen.

Argumente:
Swico anerkennt die wichtige Rolle und Kernaufgabe des BACS bei der Bekämpfung von Cyberkriminalität. Die vergangenen Revisionen (neues Bundesamt und Revision des Informationssicherheitsgesetz) gingen auch mit einer Ausweitung des Aufgabenbereichs und der Kompetenzen einher. Für eine effiziente Cybersicherheit ist es unerlässlich, stehen dem Amt die notwendigen Mittel zur Abwicklung seiner gesetzlichen Aufgaben zur Verfügung.
Swico setzt sich für eine eng koordinierte Cybersicherheit zwischen Staat und Wirtschaft ein. Aufgrund der oben geschilderten Situation erachtet es Swico als gerechtfertigt, im Rahmen einer vollständigen, VBS-internen Kompensation das Budget für die Cybersicherheit der Schweiz zu erhöhen. Auch unter dem Blickwinkel der stetig steigenden Meldungen von Cybervorfällen erachten wir eine Budgeterhöhung als angezeigt.[2]

Bereits im Vorfeld haben wir zur Geltung gebracht, dass die zusätzlichen Mittel zur Erfüllung der bestehenden Aufgaben verwendet werden und nicht in regulatorische und politische Kompetenzausweitungen investiert werden. In diesem Zusammenhang weisen wir auf die Motion 24.3810 «Durchführung dringend notwendiger Cybersicherheitsprüfungen» hin, womit der Test-Umfang auf praktisch alle IT-Produkte ausgeweitet werden soll. Die Motion wurde an den Bundesrat überwiesen und es liegt nun an ihm, die nötigen gesetzlichen Vorgaben auszuarbeiten. In diesem Zusammenhang möchten wir nochmals darauf hinweisen, dass neue Test-Pflichten nur dort angezeigt sind, wo mit Tests auf wirtschaftliche Weise ein Mehrwert geschaffen werden kann. In diesem Zusammenhang sollen die Mittel für das BACS lediglich zur Erfüllung bestehender Kompetenzen eingesetzt werden. Sollten die erhöhten Mittel zukünftig für solche Tests eingesetzt werden, erachten wir die Budgeterhöhung als ungerechtfertigt.

Cybersicherheit hat für die ICT- und Internetbranche höchsten Stellenwert. Die Anbieter und Betreiber von digitalen Lösungen und Systemen, wie Geräten und Anwendungen, haben mit Blick auf ihre gesellschaftliche Verantwortung und ihren

[2] Alle 8,5 Minuten eine Meldung zu einem Cybervorfall. Abgerufen unter: news.admin.ch/de/nsb?id=103072

nachhaltigen wirtschaftlichen Erfolg (bspw. Reputation und drohende Konventionalstrafen) allergrösstes Interesse daran, sichere Produkte und Dienstleistungen anzubieten bzw. sichere Systeme zu betreiben. Sie kommen bereits heute zahlreichen Pflichten im Bereich der Informations- und Cybersecurity nach, bspw. im Rahmen des Datenschutzgesetzes (DSG), Fernmeldegesetzes (FMG), Informationssicherheitsgesetzes (ISG) sowie deren Ausführungsverordnungen, als auch im Bereich der öffentlichen Beschaffung (siehe z.B. die «Mustervertragsklausel der BKB betreffend Cyberangriffen» oder die «Standardbestimmungen Informationssicherheit für Beschaffungsverträge») oder im Rahmen des Produktehaftpflichtgesetzes (PrHG).

Zusammenfassend ist festzuhalten, dass die Schweiz eine genügend robuste Gesetzesgrundlagen für eine effiziente und starke Cybersicherheit hat. Die zusätzlichen Mittel sollen gezielt für die Erhöhung der systemischen Cybersicherheit verwendet werden und nicht zu neuen Regulierungen führen, welche Wirtschaftsakteure zusätzlich belasten ohne erkennbaren Mehrwert zu schaffen. Swico setzt sich für mehr Cybersicherheit ein, lehnt jedoch mehr Bürokratie vehement ab.

Position:
Annahme der Motion im Sinne der Stärkung der Cybersicherheit und der Forderung nach einer klaren strategischen Fokussierung der Mittel.

25.3259 Mo. Michel. Mehr Beteiligung, bessere Digitalisierung

Darum geht es:
Die Motion will den Bundesrat beauftragen, in Gesetzgebungs- und weiteren Projekten im digitalen Bereich, die sich dafür eignen, schnellstmöglich partizipative, transparente und über die verschiedenen involvierten Bundesämter koordinierte Prozesse zu etablieren. Ziel dieses Ansatzes des «Community Building» ist der verstärkte Einbezug des Wissens und der Ideen breiter interessierter Kreise aus Wissenschaft, Zivilgesellschaft und Wirtschaft. Damit soll der Dynamik in digital geprägten Dossiers, insbesondere im Bereich der KI, angemessen Rechnung getragen und die etablierten Prozesse im Sinne eines transparenten und offenen Ansatzes erweitert werden. Zu diesem Zweck soll der Bundesrat für die nötigen zeitlichen, finanziellen und personellen Ressourcen sorgen.

Der Ständerat hat die Motion in der Sommersession bereits angenommen und ist damit dem Antrag des Bundesrates gefolgt.

Argumente:
Swico befürwortet ein koordiniertes Vorgehen der Bundesverwaltung und den breiten Einbezug relevanter Akteure, insbesondere auch der Wirtschaft, bei Digitalisierungs-Themen. Wichtig ist, dass der entsprechende Ansatz vor allem bei Schlüsselprojekten im digitalen Bereich verfolgt wird, bei welchen insbesondere Vertrauen, Akzeptanz und Innovation einen hohen Stellenwert einnehmen. Als gelungene Beispiele

möchten wir den Partizipationsprozess zur e-ID und der Vertrauensinfrastruktur sowie die Plateforme Tripartite zu KI und das Swiss Internet Governance Forum, welches unter dem Patronat des Bundesamts für Kommunikation (BAKOM) steht, hervorheben. Bei der e-ID hat der Bund bspw. verschiedene Formate des Informationsaustausches und der Partizipation geschaffen. Bewusst wurde der Prozess offen gestaltet und Privatpersonen, Firmen, Vereine, Behörden und weitere Akteure eingebunden, um ihre Erfahrung einzubringen.

Position:
Annahme der Motion.

25.4402 Mo. KVF-N Digitalisierung der Führerausweise

Darum geht es:
Mit der Motion soll der Bundesrat beauftragt werden, die Gesetze so anzupassen, damit digitale Führer- und Fahrzeugausweise als gleichwertige elektronische Nachweise anerkannt werden und bei Kontrollen digital vorgewiesen werden können. Zudem soll die Pflicht zum Mitführen physischer Dokumente aufgehoben werden. Im Vordergrund der Gesetzesanpassungen stehen die folgenden Gesetze: Strassenverkehrsgesetz (SVG), Verordnung über die Zulassung von Personen und Fahrzeugen zum Strassenverkehr (VZV) sowie die Verkehrsregelnverordnung (VRV).

Argumente:
Swico befürwortet die Einführung eines digitalen Führerausweises. Der Bund hat bereits Erfahrungen mit dem elektronischen Lernfahrausweis gesammelt, der seit 2022 als Pilotprojekt zur E-ID geführt wird. Dieser wird seit Sommer 2025 in verschiedenen Kantonen ausgestellt. Auch der digitale Führerausweis befindet sich bereits in Entwicklung. Mit dem Ja zur e-ID am 28. September 2025 sollte der Einführung eines digitalen Fahrausweises nichts entgegenstehen. Ein entsprechend digitaler Führerausweis soll auf der e-ID Vertrauensinfrastruktur eingeführt werden. Die Anerkennung digitaler Führerscheine als gleichwertige Nachweise mit dem analogen Führerausweis erachten wir in der zunehmend digitalen Welt als kundenzentriertes Angebot.

Position:
Annahme der Motion.

In beiden Räten

23.086 BRG. Investitionsprüfgesetz

Darum geht es:
Das Parlament hat den Bundesrat mit der Annahme der Motion Rieder vom 26. Februar 2018 (18.3021 «Schutz der Schweizer Wirtschaft durch Investitionskontrollen») beauftragt, die gesetzlichen Grundlagen für eine Prüfung von ausländischen Direktinvestitionen zu schaffen. Der vorliegende Entwurf für ein Investitionsprüfgesetz (E-IPG) setzt diesen Auftrag um. Den Geltungsbereich dieses Entwurfs hat der Nationalrat in der Herbstsession 2024 massiv erweitert. Dabei ging er deutlich über den Entwurf des Bundesrats hinaus, welcher von Anfang an der Ansicht war, dass es keine Investitionsprüfung braucht. Der Ständerat hat in der vergangenen Session zwar am Regulierungsvorhaben festgehalten, möchte aber weniger weit gehen als zuletzt der Nationalrat. Letzterer behandelt die Vorlage in der Wintersession, wobei ihm seine vorberatende Kommission weitgehend ein Einschwenken auf die Beschlüsse des Ständerats empfiehlt.

Argumente:
Swico steht der Einführung einer Investitionsprüfung grundsätzlich kritisch gegenüber. Ein Investitionsprüfgesetz steht im klaren Widerspruch zur bewährten Schweizer Aussenwirtschaftspolitik. Der Wohlstand der Schweiz, selbst ein global betrachtet überschaubarer Markt, beruht auf offenen Märkten und internationaler Vernetzung. Da inländisches Kapital den Investitionsbedarf nicht zu decken vermag, sind ausländische Direktinvestitionen zentral – gerade in den aktuell volatilen Zeiten. Anstatt Unternehmen mit zusätzlichen Auflagen und Prüfverfahren zu konfrontieren, braucht es nun dringend wirksame Entlastungen. Denn, diese Bestimmungen schaffen Unsicherheiten für Investoren und zusätzliche Regulierungskosten für Bund und Unternehmen. Dies, obwohl die Schweiz bspw. im Vergleich zu ihren Nachbarländern, bereits restriktiv gegenüber ausländischen Direktinvestitionen agiert.[3]

Vor diesem Hintergrund empfehlen wir dem Nationalrat im Rahmen der laufenden Differenzbereinigung und sofern er am Vorhaben festhalten will, einen möglichst liberalen, unbürokratischen und praktikablen Ansatz zu verfolgen.

Position:
Grundsätzlich Rückkehr zum bundesrätlichen Entwurf bzw. Orientierung an den Beschlüssen des Ständerats, wo diese nicht bereits mit dem Bundesrat übereinstimmen.

---

[3] OECD, «FDI Regulatory Restrictiveness Index», abgerufen am 27.08.2025 von https://www.oecd.org/en/topics/sub-issues/sustainable-investment/fdi-regulatory-restrictiveness-index.html

23.039 BRG. Bundesgesetz über das nationale System zur Abfrage von Adressen natürlicher Personen (Adressdienstgesetz, ADG)

Darum geht es:
Der vorliegende Gesetzesentwurf schafft die Grundlagen für einen nationalen Adressdienst. Verwaltungsstellen in Bund, Kantonen und Gemeinden sollen zentral auf die Adressen der Bevölkerung zugreifen können und ein schweizweiter Datenabgleich ermöglicht werden.

Das zentrale Adressdienstgesetz könnte nach langen Diskussionen nun in der Wintersession abgeschlossen werden. Das Dossier gestaltete sich als harzig, lag dem Nationalrat in der Frühjahrssession 2025 noch ein Antrag seiner Staatspolitischen Kommission (SPK-N) auf Rückweisung vor. Der Nationalrat ist trotzdem auf die Vorlage eingetreten und hat die Rückweisung an den Bundesrat abgelehnt. Es liegen noch zwei Differenzen vor, die geklärt werden müssen. Die vorberatende Kommission des Ständerats beantragt ihrem Rat bei Art. 9 Abs. 1 ^{bis} an seiner Version festzuhalten. Entgegen dem Nationalrat soll das kantonale Recht bei der Datenübertragung keinen Vorrang haben. Zudem soll Art. 14 Abs. 2 Bst. b eine Gebührenbefreiung durch die Einwohnerdienste möglich sein, aber nicht für die Gemeinden und Kantone, die für die Führung der Einwohnerdienste zuständig sind.

Argumente:
Swico befürwortet, wie auch der Bundesrat und die Kantone, die Vorlage. Für die Verwaltungen bringt die Vorlage eine wesentliche administrative Entlastung und einfachere Prozesse. Dieser Effizienzgewinn kommt auch Privaten und Unternehmen zugute. Bezüglich der Umsetzung weisen wir darauf hin, dass die im Register enthaltenen Personendaten von hoher Sensibilität sein werden und daher ein attraktives Ziel für Cyberkriminelle darstellen. Damit unterstreichen wir die Notwendigkeit, dass die Schutzmassnahmen für diese Daten technisch und organisatorisch besonders rigoros gestaltet werden müssen.

Position:
Zustimmung zum Gesetzesentwurf gemäss SPK-S, Annahme der Anträge der SPK-S.