

Eidgenössisches Departement für Umwelt,
Verkehr, Energie und Kommunikation (UVEK)
Bundesamt für Kommunikation (BAKOM)
Zukunftstrasse 44
Postfach 256
2501 Biel

Ausschliesslich per E-Mail an:
rtvg@bakom.admin.ch

Zürich, 16.02.2026

Neues Bundesgesetz über Kommunikationsplattformen und Suchmaschinen (KomPG)

Sehr geehrter Herr Bundesrat Rösti
Sehr geehrte Damen und Herren

Gerne nehmen wir die Möglichkeit wahr, innerhalb der festgesetzten Frist Stellung zu nehmen zum Entwurf des «Neuen Bundesgesetzes über Kommunikationsplattformen und Suchmaschinen (KomPG)».

Swico ist der Wirtschaftsverband der Digitalindustrie und vertritt die Interessen etablierter Unternehmen sowie Start-ups in Politik, Wirtschaft und Gesellschaft und betreibt das nationale Rücknahmesystem «Swico-Recycling» für Elektro- und Elektronikgeräte. Swico zählt über 750 Mitglieder aus der ICT- und Internetbranche. Diese Unternehmen beschäftigen rund 60'000 Mitarbeitende und erwirtschaften jährlich einen Umsatz von über 40 Milliarden Franken.

Zusammenfassung:

Swico lehnt den Vorentwurf für ein «Neues Bundesgesetz über Kommunikationsplattformen und Suchmaschinen» (VE-KomPG) in der vorliegenden Form ab.

Die Schweiz verfügt über einen stabilen, technologieneutralen Rechtsrahmen. Zudem greifen etablierte Sorgfaltspflichten, wie der **Swico Code of Conduct Hosting**. Des Weiteren bekennen sich sehr grosse Suchmaschinen und Kommunikationsplattformen bereits heute zu internationalen Standards in Bezug auf die Rechte von Nutzerinnen und Nutzern und Transparenz, wovon die Schweiz profitiert.

Unbestritten ist, dass die Rechte und Standards für Nutzende, gerade im grenzüberschreitenden Kontext, durchzusetzen sind. Von grosser Bedeutung sind überdies die Anforderungen an die Transparenz.

Gleichzeitig stellen wir fest, dass mit der Vorlage ein neues Spezialgesetz geschaffen würde, das mit zusätzlichen Anforderungen – insbesondere auch nationalen Spezifika («**Swiss Finish**») – unverhältnismässige Compliance-Kosten, eine Fragmentierung des digitalen Raums und falsche Anreize erzeugt. Das ist nachteilig hinsichtlich Innovation und Wirtschaftlichkeit einerseits, sowie Informations- und Meinungsfreiheit andererseits.

Schliesslich verweisen wir auf die internationalen Entwicklungen im Bereich der Regulierung des digitalen Raums. So unterzieht die Europäische Union (EU) ihre Regulierung einer kritischen Überprüfung, vor allem hinsichtlich der Bürokratie, der Verhältnismässigkeit sowie der Innovationsfreundlichkeit (u.a. «Digital Omnibus» und kommende «Digital-Services-Act-Evaluation»). Aus Sicht der Digitalwirtschaft müssen diese internationalen Entwicklungen berücksichtigt werden. Es muss verhindert werden, dass die Schweiz hier potenziell einen gegenteiligen Weg einschlägt. **Darum fordern wir, dass die Erfahrungen der EU in diesem Bereich Eingang finden in die Schweizer Regulierung.**

Mit Bezug auf den vorliegenden Entwurf fordern wir, dass sich die Vorlage darauf konzentriert, die Schutzziele zu erreichen. Hierzu gehören namentlich die (grenzüberschreitenden) Rechte von Nutzerinnen und Nutzern in Bezug auf Rechtsdurchsetzung und Transparenz.

Es sind ausschliesslich die für den Kommunikations- und Informationsraum relevanten Dienste zu erfassen. Eine Ausweitung der Regelungs-Adressaten und des -Bereichs lehnen wir ausdrücklich ab. Zudem fordern wir zwingende Verbesserungen der Vorlage. Dies mit dem Ziel, den Entwurf effizient, möglichst praktikabel, verhältnismässig und für alle beteiligten unbürokratisch zu gestalten.

Swico fordert insbesondere Verbesserungen in folgenden Bereichen:

- **Richtigstellung der Rolle von Kommunikationsplattformen:** Der Hauptzweck von Kommunikationsplattformen besteht darin, Nutzenden zu ermöglichen, Inhalte zu speichern und zugänglich zu machen. Die Publikation von Inhalten ist dagegen nicht der Hauptzweck der Plattformen.
- **Kein Swiss Finish:** Anforderungen, die – ohne die Schutzziele zu stärken – von internationalen Standards abweichen, beispielsweise hinsichtlich Transparenzberichte und Risikobewertungen, schaffen unnötige Bürokratie. Darauf ist konsequent zu verzichten. Wir fordern stattdessen eine gezielte Harmonisierung.
- **Verzicht auf ein ineffizientes Streitbeilegungsverfahren:** Aufgrund der Erfahrungen in der EU zweifeln wir am Mehrwert des vorgeschlagenen aussergerichtlichen Streitbeilegungsverfahrens. Sollte ein solches geschaffen werden, so muss dieses effizient ausgestaltet sein. Potenzieller Missbrauch ist zu verhindern und eine klare Kaskade, vom internen Meldeverfahren über die aussergerichtliche Streitbeilegung bis hin zu gerichtlichen Verfahren, ist sicherzustellen.
- **Die Informations- und Meinungsfreiheit ist zu schützen:** Die Informations- und Meinungsfreiheit ist in einer Demokratie ein hohes Gut, das es zu schützen gilt. Von Fehlanreizen mit Blick auf drohendes «Overblocking» ist entschieden abzugehen. Das betrifft zum Beispiel die Transparenzberichte und Risikobewertungen, die Notwendigkeit, dass Empfehlungen aufgrund von Audits unverbindlichen Charakter haben müssen, sowie das Sanktionsregime. Sollte eine Ausweitung der vom Meldesystem erfassten Tatbestände stattfinden, fordern wir zudem ein Haftungsprivileg, um dem drohenden «Overblocking» und der Asymmetrie von Rechten und Pflichten aus Sicht der Anbieter entgegenzuwirken.
- **Aufsichts- und Sanktionsregime ist unverhältnismässig und inakzeptabel:** Die für das Bundesamt für Kommunikation (BAKOM) vorgesehenen Kompetenzen gehen weit über das Verhältnismässige hinaus. Gerade die Bussenkompetenz und der entsprechende, masslose und extraterritoriale Ansatz (z.B. bis zu 6% des weltweiten Jahresumsatzes) sind zu korrigieren. Auch lehnen wir die vorgeschlagenen Netzsperrungen als unverhältnismässiger Eingriff in die Grundrechte ab.
- **Keine nationalen Leerläufe:** Wir erachten es als richtig, dass die Schweiz den «Digital Services Act» (DSA) nicht übernimmt. Dieser gilt aber für Plattformen, die in der EU tätig sind. Deshalb ist eine Fragmentierung der Regulierung im Digitalen Raum unbedingt zu

verhindern. Vor diesem Hintergrund lehnt Swico unnötige (nationale) Doppelspurigkeiten entschieden ab. Konkret ist für Anbieter, die bereits internationalen Standards nachkommen (z.B. DSA), ein alternativer Erfüllungsweg anzubieten. Wo sie nachweisen können, dass sie die Wirkungsziele aufgrund mindestens gleichwertiger Massnahmen bereits erfüllen, ist dies durch das BAKOM als Aufsichtsbehörde anzuerkennen. Internationale Anbieter sollen sich insbesondere auf bereits etablierte Compliance-Prozesse verlassen können, soweit diese dem Schutzziel nach identisch sind. So werden die Schutzziele erreicht ohne unnötige Bürokratie zu schaffen.

1 Allgemeine Würdigung

Die technologischen Entwicklungen haben verbunden mit angepasstem menschlichem (Nut-zenden-) Verhalten die öffentliche Kommunikation und die Informationsbeschaffung grundlegend verändert. Kommunikationsplattformen und Suchmaschinen sind fester Bestandteil unseres gesellschaftlichen und wirtschaftlichen Alltages. Dabei leisten sie einen wertvollen Beitrag: Entsprechende Dienste haben nachhaltig den Informationszugang erleichtert und demokratisiert indem sie den effizienten Zugang zu vielfältigen Quellen und Fakten ermöglichen. Mit ihren Angeboten ermöglichen sie weltweit Milliarden von Menschen miteinander in Kontakt zu treten bzw. zu bleiben sowie den jeweiligen Austausch von Informationen und Meinungen über Grenzen hinweg. Sie dienen auch als wichtige Werbeplattformen für alle Wirtschaftszweige. Zusätzlich unterstützen sie – unter Einhaltung von klaren Bestimmungen, beispielsweise hinsichtlich des Datenschutzes – mit ihren Zugängen und Daten die Forschung. Bei all dem wirken Kommunikationsplattformen und Suchmaschinen als Innovationstreiber mit massgeblichen positiven – direkten und indirekten – Effekten für den Wohlstand in der Schweiz.

Mit dem beschriebenen technologischen Wandel und verändertem Verhalten der Nutzerinnen und Nutzer stellen sich rechtliche Fragen. Konkret will der Bundesrat mit dem vorliegenden VE-KompG insbesondere Fragen der Durchsetzung des geltenden Rechts adressieren. Das impliziert, und hier stimmen wir mit dem Bundesrat überein, dass sich der digitale Raum in der Schweiz klar nicht in einem rechtlichen Vakuum bewegt. Im Gegenteil: Die Schweiz verfügt über einen stabilen technologieutralen Rechtsrahmen, der auch im Internet zur Anwendung kommt und dem (sehr grosse) Suchmaschinen und Kommunikationsplattformen unterliegen.

Hinsichtlich der Frage der Rechtsdurchsetzung bietet die Digitalindustrie über die bestehenden gesetzlichen Bestimmungen hinaus klare Standards und Prozesse, die sich als massgeblicher Sorgfaltsmassstab etabliert haben und anerkannt sind. Konkret regelt beispielsweise der [Swico Code of Conduct Hosting](#) (CCH) bereits heute den Umgangs mit (potenziell) illegalen Inhalten, was Anbietern und Nutzenden zugutekommt. Damit deckt er bereits das Anliegen betreffend des Melde- und Abhilfeverfahrens ab (siehe Erläuternder Bericht, S. 16).

Swico, als herausgebende Branchenorganisation, passt den CCH laufend den technologischen und rechtlichen Entwicklungen an. So wird Swico in einer geplanten Revision auch die Instrumente der Branche im Kampf gegen pädokriminelle Inhalte freiwillig ausbauen und stärken. Über diesen Branchenstandard hinaus setzen Plattformen und Suchmaschinen bereits heute freiwillig umfassende Massnahmen bezüglich der Rechte von Nutzerinnen und Nutzern, Jugendschutz sowie Sicherheit und Transparenz um, die mit hohen globalen Standards abgestimmt sind (beispielsweise «Community Standards» oder Aufsichts-Gremien).

Die Wichtigkeit der Durchsetzung beispielsweise der oben genannten Rechte und Standards für Nutzende und hinsichtlich Transparenz, gerade im grenzüberschreitenden Kontext, anerkennen wir.

Vor dem Hintergrund der Überprüfung der Digitalregulierung in der EU («Digital Omnibus», «Digital Fitness Check» sowie «Digital-Services-Act-Evaluation») stehen wir der Einführung einer «lex specialis» im Sinne des VE-KomPG kritisch gegenüber. Wir begrüßen, dass der Bundesrat einen Regulierungsvorschlag präsentiert, der deutlich weniger weit reicht als der DSA.

Eine per-se-Übernahme des europäischen DSA wäre nicht angebracht und Swico würde eine solche Übernahme entschieden ablehnen. Die Kritikpunkte an dieser Regulierung sind vielfältig: Konflikte mit der DSGVO (Datenschutz-Grundverordnung) und Datenschutz (z.B. bei Datenaustausch mit Forschern), übermässige Einmischung in die Inhaltsmoderation mit entsprechenden Risiken für Meinungsbildung und Pluralismus, sowie übermässiger administrativer Aufwand verbunden mit hohen Compliance-Kosten mit negativen Folgen für Innovation und Wirtschaftsleistung.

Mit Blick auf den VE-KomPG selbst gibt es berechtigte Bedenken: Mit einzigartigen Abweichungen von internationalen Standards (z.B. im Bereich der Transparenzberichte und Risikobewertung) würde die Schweiz einen «Swiss Finish» schaffen. Dieser fragmentiert den digitalen Raum und bringt doppelte Compliance-Kosten für globale Anbieter für einen – in globalen Dimensionen gesprochen – vergleichsweise kleinen Markt. Dies wirkt als Barriere für Innovation und isoliert die Schweizer (Digital-) Wirtschaft, ohne massgebliche Vorteile für Nutzende zu schaffen.

Sollte der Bundesrat am Regulierungsvorhaben festhalten, so ist einerseits zwingend der enge Regulierungsgegenstand und Adressatenkreis beizubehalten. Andererseits sind notwendige Verbesserungen umzusetzen, so dass das Kern-Wirkungsziel, Rechtsdurchsetzung für Nutzende und Transparenz, erreicht wird, ohne unnötige Bürokratie zu kreieren und ein gefährliches «Overblocking» zu verhindern, um das Grundrecht der Meinungs- und Informationsfreiheit nicht zu untergraben. Bestehende Compliance-Prozesse, welche die Ziele und Mindeststandards des VE-KomPG zuverlässig abdecken, sind als gleichwertig erfüllt anzuerkennen. Wir fordern, dass auf einen «Swiss Finish» verzichtet wird. Dafür sind gezielt Pflichten zu verschlanken und, wo sinnvoll, international abzustimmen. Auf die Schaffung ineffizienter aussergerichtlicher Strukturen und Prozesse mit Parallelität oder Schweiz-spezifischen Anforderungen, beispielsweise im Bereich Transparenz oder Risikobewertung, ist zu verzichten. Zwingend ist auch, dass das vorgeschlagene Sanktionsregime der Schweizer Rechtstradition und Marktdimension angepasst wird. Dies, ebenfalls aufgrund der Gefahr falscher Anreize hin zu «Overblocking», aber auch aus einer Standort- und handelspolitischen Perspektive.

2 Regulierungsbereich und -Ansatz

Hinsichtlich des vorgeschlagenen Regulierungsansatzes, bzw. der Adressaten der Regulierung und des Regulierungsbereichs, geben wir Nachfolgendes zu bedenken und stellen konkrete Forderungen.

2.1 Keine Ausweitung des Regelungsbereichs

Mit dem VE-KomPG greift der Bundesrat, wie in Kapitel 1 dargelegt, das Anliegen nach Rechtsdurchsetzung im digitalen Raum vor allem aus einer Nutzenden-Perspektive auf. Dafür setzt er bewusst auf einen fokussierten Regelungsbereich: Im Zentrum der Vorlage steht der

Umgang mit mutmasslich strafbaren Inhalten rund um öffentlich verbreitete Hassrede – also ein präzise umrissener Teilbereich plattformspezifischer Herausforderungen. Dieser Fokus ist sachgerecht. Die Herausforderungen von (Suchmaschinen und) Plattformen unterscheiden sich je nach Diensttyp stark; Geschäftsmodelle, technische Abläufe, Schutzbedürfnisse etc. Daher ist es wichtig und richtig, bei den angewendeten (regulatorischen) Instrumenten zu differenzieren. Ein gezielter Ansatz erlaubt es, verfahrensbezogene Mindeststandards schutzguts- und risikogerecht zu kalibrieren, statt sehr unterschiedliche Plattformkonstellationen und Schutzgüter einem Einheitsregime zu unterstellen. Gerade im grundrechtssensiblen Kommunikationsbereich ist Zurückhaltung zwingend angezeigt: Instrumente, die in anderen Plattformbereichen (z.B. E-Commerce) denkbar und wirksam sein könnten, würden im Kontext der Meinungs- und Informationsfreiheit unverhältnismässige Nebenwirkungen entfalten. Eine Ausweitung des Regelungsbereichs auf andere Dienste bzw. Plattfortmtypen lehnen wir deshalb ab.

2.2 Jugendschutz und Medienkompetenz

Für Swico ist das Anliegen eines wirksamen Schutzes von Minderjährigen im digitalen Raum unbestritten. Auch stellt sich die ICT-Branche klar gegen den Missbrauch ihrer Dienste zum Nachteil oder Schaden von Kindern und Jugendlichen. Bereits heute treffen Anbieter von digitalen Diensten weitgehende Massnahmen zum entsprechenden Schutz. Auch hat die Branche bereits freiwillig in Aussicht gestellt, ihren anerkannten [Swico Code of Conduct Hosting](#) um Bestimmungen zur weiteren Stärkung dieses Schutzes zu erweitern.

Somit ist für uns klar, dass wir uns nicht gegen «geeignete und verhältnismässige Massnahmen» (siehe offizielles [Begleitschreiben](#)) zum Schutz von Minderjährigen im digitalen Raum aussprechen. Die Begriffe «geeignet», im Sinne von wirksam, und «verhältnismässig» sind entscheidend und betonen, dass allfällige regulatorische Massnahmen einer sehr bewussten und sorgfältigen Abwägung bedürfen. Wir verweisen in diesem Zusammenhang auf erste Erfahrungen aus den ergriffenen Social-Media-Verboten, beispielsweise in Australien, welche in ihrer Absolutheit und Konsequenz Kindern und Jugendlichen massgebliche Nachteile verschaffen und in ihre Grundrechte eingreifen (Meinungs- und Informationsfreiheit). Auch weisen wir darauf hin, dass wichtige Dienste bereits heute ein Mindestalter zur Nutzung vorsehen und dies in ihren Bestimmungen auch so festhalten. In diesem Zusammenhang geben wir zu bedenken, dass vermeintlich «einfache» Lösungen, wie Alterskontrollen, auch mit relevanten Risiken einhergehen. So können sie zu Überidentifikation führen und den Datenschutz unterminieren, wie dies namhafte zivilgesellschaftliche sowie Kinder- und Jugendschutzorganisationen in Deutschland selbst festhalten (siehe [Grundsatzpapier](#)). Das ist auch mit ein Grund, dass nach jahrelangen, aktiven Bestrebungen vieler Akteure derzeit noch keine allgemein anerkannte Lösung zur akkuraten und datensparsamen Bestimmung des Alters von Nutzenden gegeben ist und beispielsweise auch im DSA auf entsprechende Pflichten verzichtet wurde.

Wichtig ist, dass in der Schweiz eine fundierte und ausgewogene Diskussion über das Thema stattfindet und keine regulatorischen «Reflexe» und «Schnellschüsse» unternommen werden, die zu unverhältnismässigen und unpraktikablen Eingriffen und einem regulatorischen Flickenteppich führen können. Zumal es einerseits darum geht, erste Erfahrungen beispielsweise aus der Umsetzung des Jugendschutzes im Bereich Film und Gaming zu erzielen (beispielsweise im Bereich der Altersverifikation bei Abrufdiensten). Andererseits sind auch die Erkenntnisse des Bundesrats zu laufenden Analysen zu berücksichtigen. So ist er bereits mit der Erstellung eines Berichts in Erfüllung der Postulate Vara und Graf ([24.4480](#) und [24.4592](#))

beauftragt, der die Risiken und mögliche Schutz-Massnahmen im Zusammenhang mit Kommunikationsplattformen für Kinder und Jugendliche darlegen soll. Hierzu geben wir, wie auch der Bundesrat, klar zu bedenken, dass Sensibilisierung, Aufklärung und Begleitung von Kindern- und Jugendlichen im digitalen Raum ebenso wichtige Massnahmen sind (siehe Antwort des Bundesrats in Erfüllung der Frage Farinelli ([24.7527](#))).

Weiter zweifeln wir daran, dass das mögliche KomPG der systematisch richtige Ort für Kinder- und Jugendschutzregelungen ist. Die entsprechenden Ziele lassen sich nicht sinnvoll in ein Gesetz integrieren, das konzeptionell auf verfahrensbezogene Mindeststandards im öffentlichen Kommunikationsraum zugeschnitten ist. Der Kern des KomPG liegt darin, geltendes Recht im digitalen Diskurs über rechtsstaatlich abgesicherte Verfahren (noch) durchsetzbarer zu machen (Melde- und Beschwerdewege, Begründungspflichten, Transparenz, Nachvollziehbarkeit), ohne inhaltliche Steuerung oder risikomindernde Eingriffspflichten vorzugeben. Gerade dieser verfahrensorientierte Zuschnitt ist im grundrechtssensiblen Kommunikationsbereich eine Leitplanke: Wo staatlich oder faktisch «wirksame» Risikominderung eingefordert wird, steigt der Druck, Grenzfälle vorsorglich zu entfernen oder Reichweiten zu drosseln. Das erhöht das Risiko von «Overblocking» und beeinträchtigt die Meinungs- und Informationsfreiheit. Eine Integration von Jugendschutz würde den Zuschnitt der Vorlage systematisch verschieben und – politisch wie dogmatisch – den Ruf nach materiellen Pflichten auslösen, die im Kommunikationskontext besonders heikel sind.

Folglich fordern wir, dass das Thema «Kinder- und Jugendschutz» im digitalen Raum aktiv zu behandeln ist. Allerdings hat dies im Rahmen eines breiten und gleichzeitig fundierten Dialogs auf Basis eines ordentlichen Verfahrens zu geschehen und nicht aufgrund eines «Fragekatalogs» als Teil einer möglichen spezialgesetzlichen Regulierung von sehr grossen Kommunikationsplattformen und Suchmaschinen.

2.3 Künstliche Intelligenz

Im Rahmen eines möglichen, künftigen KomPG sollte Künstliche Intelligenz (KI) nicht voreilig erfasst und mitreguliert werden. Der VE-KomPG richtet sich gezielt auf sehr grosse Kommunikationsplattformen und Suchmaschinen aus; (generative) KI-Systeme lassen sich hingegen funktional und regulatorisch anders abgrenzen. Eine Integration über Pflichten für Suchmaschinen würde den deutlichen Dienstbezug des Gesetzes verwischen und zu Abgrenzungs- sowie Vollzugsherausforderungen führen, ohne nachvollziehbaren Mehrwert für die beabsichtigte Wirkung der Vorlage zu bieten.

Diese Abgrenzung ist insofern vorzunehmen, als dass KI bereits Teil eines eigenständigen, abgestimmten Regulierungsprozesses ist. Der Bundesrat hat am 12. Februar 2025 den Grundsatzentscheid zur Ratifikation der KI-Konvention des Europarats getroffen. Dazu hat sich Swico bereits separat geäussert und eine Umsetzung mit Augenmass gefordert (siehe [Medienmitteilung](#)). Das EJPD ist aktuell mit der Erarbeitung einer entsprechenden Vernehmlassungsvorlage bis Ende 2026 beauftragt. Regelungen zu KI im KomPG würden diese Bemühungen vorwegnehmen und das Risiko von Überschneidungen unnötig erhöhen. Angesichts dessen ist es sachlich angemessen, KI-Fragen dem zuständigen Verfahren zu überlassen und das KomPG auf seinen eigentlichen Regelungsgegenstand zu beschränken.

2.4 Fokus auf Qualität und Mindeststandards – keine aktiven Eingriffe mit Gefahr zum «Overblocking»

Der Vorentwurf ist im Ausgangspunkt zurecht verfahrensorientiert. Es ist sachgerecht, dass der VE-KomPG – anders als der DSA – keine eigenständige Pflicht zur Risikominderung vorsieht. Die Risikobewertung nach Art. 20 VE-KomPG dient als Transparenzinstrument: Sie soll systemische Risiken sichtbar machen und eine informierte Aufsicht ermöglichen, ohne den Anbietern operativ vorzuschreiben, welche Eingriffe zur Risikoreduktion zu ergreifen sind. Diese Zurückhaltung ist im Kommunikationsbereich zentral, weil materielle Interventionspflichten typischerweise den Druck erhöhen, Grenzfälle vorsorglich zu entfernen, und damit «Overblocking»-Risiken verstärken.

Diese Linie wird jedoch dort verwischt, wo der Vorentwurf über die unabhängige Evaluation und ihre Folgemechanik faktisch in eine Ergebnissteuerung kippen kann. Die jährliche Evaluation erstreckt sich auf die Einhaltung sämtlicher Pflichten des 2. Kapitels des VE-KomPG und erfasst damit auch die Risikobewertung. Werden Mängel festgestellt, sieht der Entwurf operative Empfehlungen und eine Nachbesserungslogik vor, die durch Berichts- und Begründungspflichten gegenüber dem BAKOM flankiert wird; hinzu kommt eine Sanktionsdrohung bei Verstössen gegen die Evaluations- und Folgeberichtspflichten. In der Praxis entsteht dadurch ein erheblicher Handlungsdruck, der über die Sicherstellung verlässlicher Verfahren hinausgeht. Die Grenze zwischen der Prüfung der Verfahrensqualität einerseits und einer faktischen Erwartung materieller Eingriffe andererseits wird unscharf, obwohl der Entwurf gerade keine Risikominderungspflicht vorsehen will. Daher ist jede faktische Bindungswirkung, sei es durch Berichtspflichten, Begründungszwang bei Abweichung oder Sanktionsdrohungen, abzulehnen.

Vor diesem Hintergrund fordern wir, dass die Evaluation nach Art. 24 und 25 VE-KomPG (siehe auch Kapitel 3.17) strikt auf die Einhaltung der gesetzlichen Mindeststandards bzw. die Qualität der Verfahren zu begrenzen ist. Zu prüfen sind insbesondere Vollständigkeit, Nachvollziehbarkeit und Methodik der Risikobewertung sowie die Funktionsfähigkeit der vorgesehenen Melde-, Beschwerde- und Transparenzprozesse. Empfehlungen der Evaluationsstelle müssen als unverbindlich ausgestaltet werden; Sanktionen sind auf klare formale Pflichtverletzungen zu beschränken, namentlich auf das Unterlassen von Evaluationen oder Berichten beziehungsweise auf fehlende Mitwirkung. Eine Sanktionierung oder faktische Steuerung materieller Moderations- oder Risikominderungsmassnahmen ist dem verfahrensorientierten Ansatz fremd und erhöht das Risiko von «Overblocking» unnötig.

2.5 Kein «Swiss Finish» aufgrund doppelspuriger Strukturen und Prozesse

Wir begrüssen, dass mit dem VE-KomPG keine per-se-Übernahme des DSA stattfinden soll und sich die vorgeschlagenen Pflichten grundsätzlich dennoch an internationalen Standards orientieren. Trotzdem kreiert der VE-KomPG unnötige «Swiss Finishes», von denen entschieden abzusehen ist.

Mit seinen detaillierten Umsetzungsvorgaben pro Wirkungsziel bzw. Pflicht gerade für international agierende, sehr grosse Suchmaschinen und Kommunikationsplattformen – die aktuell und in absehbarer Zukunft auch die einzigen Adressaten des Gesetzes sind – schafft der VE-KomPG Doppelspurigkeit in den Compliance-Prozessen. Dies, ohne die eigentlichen Wirkungs- bzw. Schutzziele besser zu erreichen, dafür aber zusätzlichen Aufwand, nicht nur für die Anbieter, sondern auch das BAKOM als zuständige Behörde, zu schaffen. Das zeigt sich

beispielsweise besonders deutlich bei den Anforderungen betreffend Transparenzberichten und Risikobewertungen (siehe Kapitel 3.13 und 3.14).

2.6 Vollzugstauglichkeit und Gleichwertigkeitsprinzip sicherstellen

Der VE-KomPG verfolgt im Kern vor allem auch die Absicht, die Rechte von Nutzerinnen und Nutzern bzw. deren Durchsetzung weiter zu stärken und zusätzlich allfällige systemische Risiken bei sehr grossen Kommunikationsplattformen und Suchmaschinen adressierbar zu machen. Unter unserem Vorbehalt der Notwendigkeit des gesetzlichen Eingriffs (siehe Kapitel 1), erachten wir den schlanken, verfahrensorientierten Ansatz mit Transparenz-, Melde- und Evaluationsinstrumenten als richtig.

Für die Wirksamkeit der Vorlage ist jedoch entscheidend, dass der Vollzug praxistauglich bleibt und auf Wirkung statt Formalismus ausgerichtet wird. Das Gesetz sollte deshalb Ziele und Mindeststandards definieren und bewusst offenlassen, wie Anbieter diese organisatorisch umsetzen – solange die gesetzlich verlangte Schutzwirkung zuverlässig erreicht wird. Der Vorentwurf bildet dieses Äquivalenzprinzip bislang nicht ab. Notwendig sind Bestimmungen, die klarstellen, dass die Implementierung analoger internationaler Standards zumindest als alternativer Weg akzeptiert und zur Erfüllung der hiesigen gesetzlichen Mindestziele angerechnet wird. Ohne eine solche Anerkennung drohen nationale Parallelprozesse mit separaten Abläufen und Nachweisen; dies erhöht Komplexität und Kosten, ohne dass daraus ein zusätzlicher Schutzgewinn folgt.

2.7 Konkrete Umsetzung: Ko-Regulierung und «Gleichwertigkeit» als notwendiger Ansatz

Der Vorentwurf legt die Pflichten und deren Erfüllung entlang nationaler Prozesse fest. Was fehlt, ist ein zusätzlicher, ausdrücklich geregelter Erfüllungsweg, der es Anbietern ermöglicht, bereits bestehende, funktionierende Mechanismen als gleichwertig anerkennen zu lassen, wenn sie die im möglichen, künftigen KomPG definierten Ziele und Mindeststandards zuverlässig erreichen. Ohne eine solche Regelung droht in der Praxis, dass international etablierte Compliance-Strukturen trotz gleicher Schutzwirkung nicht anerkannt werden und faktisch zusätzliche, unnötige nationale Parallelprozesse aufgebaut werden müssen.

Swico fordert deshalb ausdrücklich, dass das Gesetz neben der direkten Erfüllung einen zweiten Erfüllungsweg vorsieht: Anbieter sollen gegenüber dem BAKOM eine verbindliche Erklärung abgeben können, wonach sie für den Schweizer Anwendungsbereich bereits implementierte Standards und Prozesse anwenden (insbesondere DSA-basierte Melde-, Beschwerde-, Transparenz- und Evaluationsmechanismen). Das BAKOM prüft, ob diese Verfahren die gesetzlichen Ziele und Mindeststandards gleichwertig erfüllen. Wird die Gleichwertigkeit bejaht, gelten die Pflichten als erfüllt, ohne dass zusätzliche nationale Parallelprozesse aufgebaut werden müssen.

Der zusätzliche Erfüllungsweg ist ein zentraler Baustein für einen praxistauglichen Vollzug: Er reduziert Doppelspurigkeiten, schafft Rechtssicherheit und richtet die Umsetzung auf die Einhaltung der materiellen Anforderungen aus, statt auf formale Prozessidentität. Dieser Erfüllungsweg ist umso mehr angezeigt, als dass damit – aus Sicht der Nutzerinnen und Nutzer – keinerlei Einschränkungen der Rechtspositionen einhergeht.

2.8 Möglichkeit der Standardisierung für die Gleichwertigkeitsprüfung schaffen

Damit die Gleichwertigkeitsanerkennung handhabbar bleibt, soll eine mögliche, künftige Gesetzesgrundlage (KomPG) die Option eines Branchen-Gefässes vorsehen (z.B. Ko-Regulierungsorganisation oder anerkannter Branchenstandard). Dieses Regelwerk kann die gesetzlichen Ziele und Mindeststandards konkretisieren und einheitliche Kriterien und Nachweise für die Gleichwertigkeitsprüfung definieren (z.B. akzeptierte Berichtsformate, Qualitätsanforderungen, Vorgaben zur Evaluation und Nachführung). Das würde die Aufsicht weiter entlasten, ohne die Schutzziele zu tangieren.

Das BAKOM behält dabei die Aufsicht: Anerkennung des Branchenstandards oder Prüfung einer individuellen Erklärung samt Gleichwertigkeitsfeststellung; Eingriffe bei unzureichender Wirksamkeit (Auflagen, Nachbesserung, Widerruf). Für die Zumutbarkeit ist zentral, dass der Geltungsbereich eng bleibt (überschaubare Zahl sehr grosser Dienste), was die Standardisierung die Prüf- und Nachweisanforderungen konsistent und effizient macht.

3 Zu den einzelnen Bestimmungen

Sollte der Gesetzgeber, unter Anerkennung der Durchsetzung der Rechte von Nutzerinnen und Nutzern und entsprechender Standards sowie hinsichtlich Transparenz, trotz vorgehend geäusselter Kritik am Regulierungsvorhaben festhalten, so sind zwingend Verbesserungen vorzunehmen – insbesondere unter Berücksichtigung der vorangehend, dargelegten Forderungen zum Regulierungsbereich und -Ansatz (Kapitel 2).

3.1 Zweck und Geltungsbereich (Art. 1 und 2)

Der VE-KomPG adressiert einen engen Regelungsbereich und beschränkt sich auf den Kommunikations- und Suchbereich. Diese Eingrenzung ist mit Blick auf den Regulierungszweck (Art. 1) sachgerecht und sollte unbedingt beibehalten werden. Herausforderungen in anderen Plattformkontexten beruhen auf anderen Funktionslogiken und Schutzgütern; sie erfordern andere Instrumente. Deren Einbindung in den VE-KomPG wäre der falsche Ansatz.

Hinsichtlich des Geltungsbereichs (Art. 2 Lit. a Ziff. 1) stellen wir fest, dass der Hauptzweck von Kommunikationsplattformen falsch erfasst ist. Ihr Hauptzweck besteht darin, dass Sie, eben als Plattformen, den Nutzenden ermöglichen, Inhalte zugänglich zu machen und Inhalte als Plattform nicht selbst «publizieren». Da eine solche Formulierung zu falschen rechtlichen Schlüssen führt, fordern wir eine zwingende Anpassung der entsprechenden Bestimmung. Bei der entsprechenden Einschränkung (siehe oben) ist zudem festzuhalten, dass geringfügige und untergeordnete Hilfsfunktionen mit «Kommunikationscharakter» nicht erfasst werden (beispielsweise digitale Karten-Dienste mit Kommentarfunktion). Wir empfehlen, zwecks zusätzlicher Stärkung der Rechtssicherheit, sich bei der konkreten Formulierung möglichst an internationale Standards zu halten.

Art. 2 Lit. a Ziff. 1: *«deren Hauptzweck darin besteht, eine elektronische Plattform zur Verfügung zu stellen, um Nutzerinnen und Nutzern zu ermöglichen, verschiedene Formen von Kommunikationsinhalten zu speichern und öffentlich zugänglich zu machen, sofern diese Tätigkeit nicht eine geringfügige oder rein untergeordnete Funktion eines anderen Dienstes oder eine geringfügige Funktion des Hauptdienstes darstellt. Dabei bestimmt der Anbieter der elektronischen Plattform die Organisation der nutzergenerierten Inhalte, ohne jedoch eine redaktionelle Verantwortung für diese Inhalte zu tragen.»*

Die vorgeschlagene «Grössenschwelle» (Art. 2 Bst. a Ziff. 2) erachten wir dahingehend als sachgerecht, als das Nutzende eine geringere Zahl an Alternativen mit gleichem Funktionsumfang und Wirkung zur Verfügung steht und entsprechende Angebote mit Blick auf die demokratische Debatte eine grössere Bedeutung einnehmen. Eine Ausweitung bzw. Herabsetzung der Grössenschwelle erachten wir – gerade mit Blick auf die vorgeschlagenen, sehr umfassenden Pflichten – als unverhältnismässig. Einerseits aufgrund des damit verbundenen Umsetzungsaufwands für die Anbieter selbst. Gerade für Start-Ups und Scale-Ups bzw. KMU wäre solch ein bürokratische Last kaum zu tragen und würde ein massgebliches Innovationshindernis darstellen. Andererseits aber auch mit Blick auf den potenziellen Eingriff in die Meinungsäusserungs- und Informationsfreiheit sowie die öffentliche Debatte. Das heisst, dass Dienste mit wenig oder ohne Bezug zum öffentlichen Diskurs nicht zu erfassen sind. Wo Kommunikationsfunktionen in erster Linie einem anderen Zweck dienen (z.B. interne Arbeits- oder Ausbildungsumgebungen), besteht regelmässig weder dieselbe Reichweite noch derselbe grundrechtliche Kontext. Eine klarere Abgrenzung reduziert Fehladressierungen und Vollzugsaufwand, ohne Schutzwirkung im Kernbereich einzubüssen.

3.2 Meldeverfahren (Art. 4)

Melde- und Abhilfeverfahren sind bereits heute Standard bei sehr grossen Suchmaschinen und Kommunikationsplattformen. Diese erlauben es Nutzenden Inhalte unter verschiedenen Kategorien (Hassrede, Belästigung usw.) zu melden. Mit dem [Swico Code of Conduct Hosting \(CCH\)](#) kennt die Digitalwirtschaft bereits klare Prozesse, die den entsprechenden Sorgfaltsmassstab bei illegalen Inhalten definieren. Die Kodifizierung in starres Gesetzesrecht (Art. 4) verfestigt ohne Not einen klaren und gleichzeitig dynamisch weiterentwickelbaren Standard. Sollte der Gesetzgeber auf das Vorhaben bestehen, so ist an der Begrenzung der in Art. 4 Abs. 1 aufgeführten Straftaten festzuhalten. Ein breiterer Anwendungsbereich ist weder zweckmässig noch verhältnismässig. Erstens würde eine Ausweitung über den DSA hinausgehen. Anbieter würden gezwungen, komplexes Schweizer Strafrecht auszulegen – eine Aufgabe, die zur Judikative gehört, nicht zu privaten Unternehmen. Zweitens würde eine mögliche Ausweitung der Tatbestände die Gefahr des ungewünschten und grundrechtskritischen «Overblockings» weiter erhöhen.

Sollte der Gesetzgeber gar eine Ausweitung der unter Art. 4 Abs. 1 gefassten Tatbestände vornehmen, fordern wir für die Regulierungsadressaten ein entsprechendes Haftungsprivileg. Dieses schafft für betroffene Anbieter die notwendige Rechtssicherheit, sofern sie ihren Pflichten nachkommen. Die Einführung eines solchen konditionalen Haftbefreiungstatbestands ist angemessen und sachgerecht. Erstens, weil mit dem VE-KomPG die bestehenden Rechte von Nutzerinnen und Nutzern eine Verrechtlichung erfahren, was neue, umfassende gesetzliche Pflichten für die Anbieter schafft. Dabei orientiert sich der VE-KomPG am DSA – letzterer kennt bereits ein entsprechendes Haftungsprivileg. Hier nachzuziehen, erscheint vernünftig und fair. Gerade auch mit Blick auf das massive Aufsichts- und Sanktionsregime (siehe Kapitel 3.24 und 3.25). Eine entsprechende Regelung wäre zudem auch im Sinne der Nutzenden sowie dem öffentlichen Interesse. Dies, weil damit der grundrechtskritische Anreiz zum «Overblocking» mitigiert wird.

Die Anforderungen in Art. 4 Abs. 2 (URL, Begründung, Kontaktinformation) erachten wir als grundsätzlich praktikabel. Allerdings muss die Anforderung, eine «Begründung» anzugeben, nicht dahingehend ausgelegt werden, dass Nutzende eine Gerichtsentscheidung vorbringen müssen, noch sollten die Plattformen zu längeren Korrespondenzen gezwungen werden.

Wir fordern, dass im Sinne eines effizienten und effektiven Meldeverfahrens, qualitative Anforderungen an die Nutzenden-Meldungen gestellt werden: Nutzende sollten zumindest die Rechtsvorschrift nennen müssen, deren Verstoss sie sehen bzw. vermuten. So wird die Effizienz des Verfahrens erhöht und dessen Grundlage bildet ein konkreter Rechtsanspruch und nicht eine subjektive Behauptung von möglicher Rechtswidrigkeit. Dass Nutzende ihrerseits dieser Verantwortung nachkommen müssen, erscheint uns schlüssig, und verhindert, dass Nutzende willkürlich Inhalte ohne rechtliche Grundlage melden.

3.3 Bearbeitung der Meldungen und Mitteilungspflicht gegenüber meldenden Nutzerinnen oder Nutzern (Art. 5)

Der Begriff «zeitnah» in Art. 5 Abs. 1 bietet angemessene Flexibilität, um der unterschiedlichen Komplexität von Berichten Rechnung zu tragen. Wir unterstützen diesen Ansatz, der mit vergleichbaren Rahmenregelungen übereinstimmt und es ermöglicht, ausreichend Zeit für eine gründliche Bewertung jedes jeweils anders gelagerten Falls zu haben. Dies kommt schliesslich der Qualität bei der Bearbeitung von Meldungen zugute.

3.4 Mitteilungspflicht gegenüber Nutzenden, die von einschränkenden Massnahmen betroffen sind (Art. 6)

Art. 6 schreibt die Benachrichtigung von Nutzenden vor, wenn Inhalte eingeschränkt werden. Transparenz ist zwar wichtig, aber Ausnahmen müssen robust und der Benachrichtigungsmechanismus praktikabel sein. So reichen die vorgesehenen Ausnahmen der Mitteilungspflicht nicht aus, wenn Kontaktdaten unbekannt sind (Art. 6 Abs. 3). Wir fordern, dass Ausnahmen auch explizit dann vorgesehen sind, falls Nutzende falsche Daten angegeben haben oder eine Benachrichtigung eine laufende Ermittlung oder Sicherheitsoperation gefährden würde (z. B. Benachrichtigung eines Spam-Bot-Betreibers).

Zur Benachrichtigungsmethode regen wir an, dass klargestellt wird, dass eine Benachrichtigung über die internen Kommunikationskanäle der Plattform (z.B. Support-Postfach, In-App-Mitteilungen) ausreicht, um die entsprechende Verpflichtung zu erfüllen. Die Anforderung, Benachrichtigungen an externe E-Mail-Adressen zu versenden, ist einerseits operativ belastend und andererseits weniger zuverlässig, da diverse Dienste ohne Angabe einer E-Mail-Adresse verwendet werden können und selbst in Fällen, in welchen entsprechende Daten vorhanden sind, können diese veraltet oder nicht korrekt sein. Diese Konkretisierung ist somit im Interesse von Anbietern und Nutzenden.

3.5 Internes Beschwerdeverfahren (Art. 7)

Die 6-Monats-Frist zur Einreichung einer Beschwerde entspricht den Bestimmungen des DSA. Dass die gleichen Anforderungen gewählt werden, erscheint sachgerecht. Allerdings muss die Anforderung in Art. 7 Abs. 4, dass die Beschwerden nicht «ausschliesslich durch automatisierte Mittel» bearbeitet werden und unter Aufsicht «qualifizierten Personal» erfolgen, so ausgelegt werden, dass Skalierbarkeit explizit ermöglicht wird. Andernfalls lehnen wir solch eine Bestimmung ab. Denn, eine Anforderung der menschlichen Überprüfung für jede – möglicherweise Spam-Mail – ist operativ schlicht unmöglich und unverhältnismässig. Die menschliche Überprüfung sollte auf die sensibelsten und schwierigsten Bereiche beschränkt bleiben. Dies, zumal moderne KI-Systeme – einschliesslich fortgeschrittener Large Language Models (LLM) – in vielen Bereichen schnellere und konsistentere Ergebnisse als manuelle Prozesse bieten.

3.6 Aussergerichtliche Streitbeilegung (Art. 8 – 12)

Wie bereits in Kapitel 2.5 dargelegt, stehen wir dem vorgeschlagenen (aussergerichtlichen) Streitbeilegungsverfahren aus vielerlei Gründen kritisch gegenüber und lehnen dieses in der vorliegenden, ineffizienten Form ab.

Die Notwendigkeit einer Einrichtung eines Mechanismus zur aussergerichtlichen Streitbeilegung stellen wir in Frage. Denn, die Erfahrung mit vergleichbaren «Out-of-Court Dispute Settlement-Organen» (ODS-Organen) unter dem DSA haben massgebliche praktische Probleme aufgedeckt: Mögliche Konflikte zwischen Datenschutz und Informationsaustausch mit einem ODS-Organ (insbesondere wenn diese den Abschluss von Datenschutzvereinbarungen verweigern), Behandlung von Fällen, die nicht mehr eine aktive Streitbeilegung darstellen (beispielsweise durch Löschung eines Inhalts durch Nutzende selbst), inkonsistente Gebührenstrukturen oder in Teilen auch betreffend der Sachverständigkeit von ODS-Organen. Zudem schafft der ODS-Mechanismus erhebliche Kosten und administrativen Aufwand, obwohl bereits interne Verfahren wie auch der gerichtliche Weg zur Verfügung stehen. Sollte der Gesetzgeber an einer aussergerichtlichen Streitbeilegung festhalten, so sind zwingend Verbesserungen vorzusehen.

Wir anerkennen zwar, dass es gerade mit Blick auf eine mögliche gerichtliche Vorgehensweise verankerte (Prozess-) Fristen gibt, die einzuhalten sind. Dennoch stellen wir klar: Die Gleichzeitigkeit der drei Verfahrenswege – internes Beschwerdeverfahren, aussergerichtliche Streitbeilegung und Gerichtsverfahren – ist intransparent, bürokratisch und schlicht ineffizient. Sie schafft vor allem Unsicherheiten und mögliche Doppelspurigkeiten. Die Formulierung «jederzeit» in Art. 8 Abs. 1 untergräbt zudem die Fähigkeit der Anbieter, ihre (möglichen) eigenen Fehler zu korrigieren, und überschwemmt ODS-Organen mit verfrühten Fällen. Deshalb fordern wir, dass eine klar definierte Kaskade, die einen transparenten und effizienten Mechanismus ermöglicht, vorgesehen wird. Nutzende sollen zuerst das interne Beschwerdeverfahren ausschöpfen, bevor sie eine aussergerichtliche Streitbeilegung in Anspruch nehmen können. Erst in einem Folgeschritt sollte die gerichtliche Streitschlichtung in Anspruch genommen werden können.

Ausserdem ist der «aussergerichtliche Mechanismus» nicht mit unnötigen Verfahren zu belasten. Das heisst, dass es gezielte und verhältnismässige Einschränkungen zum Zugang eines Verfahrens geben sollte (Art. 8): Nutzende sollten keine Streitigkeiten über Inhalte einleiten können, die nicht mehr aufgrund von Datenspeicherrichtlinien oder längst abgelaufener Entscheidungen vorhanden sind. ODS-Organen sollten sich nicht mit Streitigkeiten befassen, die sich auf rückgängig gemachte Content-Moderation-Entscheidungen, von Nutzern gelöschte Inhalte oder anderweitig inaktive Streitigkeiten beziehen. Solche Fälle stellen keine echten Streitigkeiten dar, die einer Lösung bedürfen.

Betreffend des aussergerichtlichen Verfahrens ist zwingend daran festzuhalten, dass das Streitbeilegungsorgan keine verbindliche Streitbeilegung verhängen kann (Art. 9 Abs. 2).

Die «Kosten-Regelung» in Art. 10 erscheint grundsätzlich sachgerecht. Wir weisen hinsichtlich einer möglichen Umsetzung bzw. Konkretisierung auf Verordnungsstufe darauf hin, dass die Kostenverteilung effektive Schutzvorrichtungen beinhalten muss: eine niedrigere Schwelle zur Kostenverlagerung auf missbräuchliche Antragsteller, eine faire und klare Gebührenverteilung verbunden mit einer transparenten und nachvollziehbaren Kostenstruktur sowie strikte Grenzen für den Umfang der ODS-Überprüfung. So werden auch Fehlanreize verhindert und der Mechanismus nicht unnötig be- bzw. überlastet.

3.7 Allgemeine Geschäftsbedingungen bzw. Transparenzverpflichtungen (Art. 13)

Die Transparenzanforderungen in Art. 13 sind unseres Erachtens mit bestehenden internationalen Standards und der aktuellen Praxis von Anbietern abgestimmt. Plattformen veröffentlichen bereits heute Nutzungsbedingungen in mehreren Sprachen und bieten zugängliche Informationen über ihre Richtlinien an.

Dennoch: Wir geben klar zu bedenken, dass eine nationale Fragmentierung der Anforderungen an allgemeine Geschäftsbedingungen unbedingt zu vermeiden ist. Auch sollte den Anbietern die notwendige Flexibilität im Umgang mit Verstössen – im Rahmen des VE-KomPG zur Diskussion stehenden Pflichten – eingeräumt werden.

Die Anforderung, Nutzer über «wesentliche Änderungen» von Nutzungsbedingungen zu benachrichtigen (Art. 13 Abs. 4), bedarf einer Klarstellung: Der Benachrichtigungsmechanismus sollte verhältnismässig sein – er sollte nicht zu eindringlichen Push-Benachrichtigungen für routinemässige Richtlinienaktualisierungen führen. Plattformen müssen Flexibilität bei der Art behalten, wie sie Änderungen an Nutzende kommunizieren, vorausgesetzt, die Information ist leicht zugänglich.

3.8 Sorgfaltspflichten (Art. 14)

Wir geben zu bedenken, dass sich Anbieter bereits heute den in Art. 14 Abs. 1 deklarierten Grundsätzen verpflichten, wie diese Swico in seinem [Verhaltenskodex](#) als auch dem [Code of Conduct Hosting](#) bereits als Sorgfaltsmassstab definiert. Die weiteren Anforderungen (Art. 14 Abs. 2 und 3) erachten wir als grundsätzlich schlüssig. Wir geben jedoch zu bedenken, dass Suchmaschinen nicht unter die Sorgfaltspflichten gemäss Art. 14 fallen sollten, zumal sie zu recht den Pflichten gemäss den Abschnitten 1 und 3 des VE-KomPG nicht unterstehen. Es gilt diesen Normenwiderspruch aufzulösen.

3.9 Werbung (Art. 15)

Dass Werbung gekennzeichnet werden soll, ist aus Sicht Swico nachvollziehbar. Die Art und Weise, wie Werbung gekennzeichnet wird, ist den Anbieter offen zu lassen, denn so ist die laufende Weiterentwicklung nach international anerkannten Best Practices laufend möglich. Sollte der Gesetzgeber dennoch genauer spezifizieren, fordern wir (insbes. betreffend Art. 15 Abs. 2), dass der Schutz von Geschäftsgeheimnissen und des geistigen Eigentums zwingend gewahrt bleibt und im konkreten Abwägungsfall letztere entsprechend berücksichtigt werden. Deshalb ist explizit festzuhalten, dass Transparenzverpflichtungen nicht die Offenlegung beispielsweise von Quellcodes oder sensiblen Geschäftsdaten erfordern. Dies insbesondere auch, um Systeme vor Manipulationen zu schützen.

3.10 Werbearchiv (Art. 16)

Das Anliegen des Führens eines Werbearchivs können wir grundsätzlich nachvollziehen und verweisen darauf, dass sehr grosse Suchmaschinen und Plattformen bereits entsprechende globale «Ad Libraries» unterhalten. Hinsichtlich der konkreten Anforderungen gemäss Art. 16 VE-KomPG stellen wir fest, dass diese grundsätzlich mit den Anforderungen des DSA übereinstimmen. Allerdings – und mit Blick auf die Kernabsicht eines Werbearchivs – erscheint die Eingrenzung des Zugangs auf die Aufsichtsbehörde und Forschende angemessen.

Betreffend den (noch zu konkretisierenden) Bestimmungen (siehe Art. 16 Abs. 5) ist auf einen «Swiss Finish» zu verzichten.

3.11 Kommerzielle Inhalte von Nutzenden (Art. 17)

Übereinstimmend mit den Anforderungen der verhältnismässigen Transparenz in Sachen «Werbung» (siehe Kapitel 3.9), sind für uns die Anforderungen hinsichtlich kommerzieller Inhalte von Nutzenden gemäss Art. 17 nachvollziehbar. Dies, zumal Anbieter bereits heute Funktionalitäten zur Verfügung stellen, die es Nutzenden bzw. «Influencern» ermöglichen, kommerzielle Inhalte zu deklarieren. Diese existierenden Funktionalitäten sind auch für die Schweiz entsprechend anzuerkennen.

3.12 Empfehlungssysteme (Art. 18)

Hinsichtlich der vorgeschlagenen Anforderungen an Empfehlungssysteme (Art. 18) betonen wir, dass Anbieter ihren Nutzenden bereits heute Möglichkeiten zur Verfügung stellen, um Ihre Inhaltspräferenzen anzupassen. Die Abstimmung dieser Anforderungen mit dem DSA zwecks Verhinderung eines unnötigen «Swiss Finish» erscheint sachgerecht. Mit Blick auf Art. 27 DSA heisst dies auch, dass Suchmaschinen von den Bestimmungen gemäss Art. 18 VEG-KomPG nicht zu erfassen sind.

Insbesondere hinsichtlich Art. 18 Abs. 1 Lit. b und Art. 18 Abs. 2 geben wir zu bedenken, dass beispielsweise eine chronologische Darstellung von Inhalten – oft als vermeintlich «neutrale» Alternative vorgeschlagen – keineswegs neutral ist. Sie privilegiert «Vielveröffentlicher», erzeugt Druck zu ständigem Engagement und verhindert, dass relevante Inhalte, die zu einem ungünstigen Zeitpunkt veröffentlicht wurden, die Nutzenden erreichen. Eine chronologische Darstellung wäre zudem anfällig für Manipulation durch koordinierte Massenveröffentlichungen.

3.13 Transparenzpflicht (Art. 19)

Mit Blick auf die Regulierungsadressaten (sehr grosse Suchmaschinen und Kommunikationsplattformen), die den Tatsachen entsprechend vorwiegend auch in andere Jurisdiktionen mit wesentlich grösseren Märkten, wie beispielsweise der EU, tätig sind, erschliesst sich uns der Mehrwert von gesonderten Anforderungen an die Transparenzpflichten nicht. So führt die Segregation von Daten, spezifisch für die Schweiz, zu statistisch unbedeutenden Ergebnissen und erfordert gleichzeitig massive «Engineering-Ressourcen» mit entsprechenden doppelten Compliance-Prozessen. Dies, zumal beispielsweise die systemischen «Themen» bzw. allfällige Risiken nicht bloss einen Schweiz-Bezug aufweisen. Zwar könnten die vorgeschlagenen Anforderungen für mögliche, künftige sehr grosse Suchmaschinen oder Kommunikationsplattformen mit (reinem) Schweiz-Bezug eine Option sein. Die Fragmentierung und die unnötige Bürokratie für grenzüberschreitende Anbieter lassen sich damit aber nicht rechtfertigen – auf ein «Swiss Finish» ist zu verzichten.

Dieser Logik folgend, sollten neben den Anforderungen an Inhalt und Form auch Berichtszeiträume und Einreichungsfristen dem in der EU geltenden System entsprechen. Dies erlaubt nicht nur eine effiziente Ausarbeitung, sondern stellt sicher, dass entsprechende Zusammenhänge zwischen übereinstimmenden Zeiträumen erkannt werden können.

Um diesen Unzulänglichkeiten am effizientesten zu begegnen, ohne das Schutzinteresse zu tangieren, fordern, wie bereits in Kapitel 2.7 dargelegt, mit Nachdruck die Schaffung eines alternativen Erfüllungswegs: Anbieter sollen gegenüber dem BAKOM eine verbindliche Erklärung abgeben können, wonach sie für den Schweizer Anwendungsbereich bereits implementierte Standards und Prozesse anwenden (beispielsweise betreffend Transparenzpflichten).

Das BAKOM prüft, ob diese Verfahren die gesetzlichen Ziele und Mindeststandards gleichwertig erfüllen. Wird die Gleichwertigkeit bejaht, gelten die Pflichten als erfüllt, ohne dass zusätzliche nationale Parallelprozesse aufgebaut werden müssen.

3.14 Risikobewertung (Art. 20)

Art. 20 verlangt eine jährliche Bewertung systemischer Risiken in der Schweiz. Hierzu geben wir zu bedenken, dass systemische Risiken (z.B. Desinformation oder illegale Inhalte) sich kaum auf die Schweiz beschränken; es handelt sich klar um grenzüberschreitende Themen. Gerade deshalb sehen wir keinen Mehrwert einer Schweiz-spezifischen Risikobewertung mit Blick auf die damit zu schaffende Bürokratie – analog den Transparenzpflichten (siehe Art. 19 bzw. Kapitel 3.13). Einen entsprechenden «Swiss Finish» lehnen wir ab. Wir wiederholen hier unsere Forderung nach der Schaffung eines alternativen Erfüllungswegs (siehe Kapitel 2.7).

3.15 Anlaufstelle (Art. 21 und 22)

Wir anerkennen das Bedürfnis einer angemessenen Kommunikationsmöglichkeit mit Anbietern von sehr grossen Suchmaschinen und Kommunikationsplattformen. Gleichzeitig verweisen wir – insbesondere betreffend Art. 21 – auf bereits bestehende Kommunikationskanäle der entsprechenden Anbieter, die grundsätzlich jurisdiktionsübergreifend effektiv funktionieren. Anstelle neuer Kontaktstellen sollten die bestehenden Kanäle effizient genutzt werden, die auch Nutzenden in der Schweiz zur Verfügung stehen. Sollte der Gesetzgeber auf dezidierte Anlaufstellen beharren, so sollen diese mit der Rechtsvertretung (siehe 3.16) kongruent sein können.

Vorbehaltlich unserer obenstehenden Bedenken fordern wir betreffend der «Kommunikation» (Art. 22) Folgendes: Das «Verbot von ausschliesslich automatisierten Antworten» (Art. 22 Abs. 2) muss gerade für sehr grosse Suchmaschinen und Kommunikationsplattformen realistisch und praktikabel ausgelegt werden. Automatisierte Systeme – einschliesslich fortgeschrittener KIs und LLMs – sind für effiziente Triage und Bearbeitung routinemässiger Anfragen zentral. Ein Blick auf die bestehenden Transparenzberichte sehr grosser Kommunikationsplattformen und Suchmaschinen zeigt die grosse Menge an Inhalten, die entsprechende Dienste gemäss ihrer Community-Richtlinien wie auch lokaler Gesetze moderieren. Maschinenbasierte Bearbeitung erlaubt einerseits eine schnelle, skalierbare Bearbeitung von möglichen Verstössen und verhindert andererseits, dass sich menschliche Moderationen eindeutige Verstösse mit potenziell verstörenden Inhalten ansehen müssen. Die menschliche Überprüfung sollte in den empfindlichsten und schwierigsten Bereichen stattfinden, wo automatisierte Systeme weniger genau sind oder die Beurteilung menschliches Urteilsvermögen effektiv erfordert ist. Die Verpflichtung, menschliche Beteiligung in jeder Interaktion zu fordern, ist unverhältnismässig, nicht operativ realisierbar und auch nicht erforderlich, um die Schutzziele zu erreichen. Zudem ist der Begriff «benutzerfreundlich» in Art. 22 Abs. 3 zu streichen, denn er ist im Kern «bedeutungslos» und riskiert gar zu einer Grundlage für willkürliche Durchsetzung zu werden. Der genannte Begriff gibt keine echte Orientierung.

3.16 Rechtsvertretung (Art. 23)

Wir weisen darauf hin, dass die vom Regelungsbereich adressierten Akteure bereits etablierte Kanäle – auch für die juristischen Kommunikation – bieten. Gleichzeitig können wir das Bedürfnis nach einer offiziellen Rechtsvertretung in der Schweiz nachvollziehen mit dem Hinweis,

dass dies für die vom Regelungsbereich adressierten Unternehmen mit nennenswertem Aufwand verbunden ist.

3.17 Unabhängige Evaluation sowie Evaluations- und Massnahmenbericht (Art. 24 und 25)

Art. 24 verlangt einen jährlichen unabhängigen Audit, dessen Spezifika bzw. Anforderungen in Art. 25 vorgesehen sind. Dass Audits stattfinden, ist nachvollziehbar. Aber, auch hier weisen wir mit Nachdruck darauf hin, dass wiederum unnötige Doppelspurigkeit geschaffen werden. Wir fordern deshalb, dass im Sinne des notwendigen alternativen Erfüllungswegs (Kapitel 2.7) erfolgte Audits unter dem DSA auch in der Schweiz anerkannt werden. Das entlastet wirksam die Anbieter, ohne die Schutzziele zu tangieren. Im Falle einer Gleichwertigkeit bestehender Audits (gemäss Kapitel 2.6) sollte eine separate, Schweiz-spezifische Bewertung komplett entfallen – analog den Transparenzpflichten (siehe Kapitel 3.13).

Gleichzeitig verweisen wir auf unsere Ausführungen betreffend der unerwünschten Ergebnissteuerung (Kapitel 2.4). Die vorgeschlagenen Audits sind strikt auf die Einhaltung der gesetzlichen Mindeststandards und die Qualität der Verfahren zu begrenzen. Empfehlungen der Evaluationsstelle müssen als «unverbindlich» ausgestaltet sein.

3.18 Datenzugang für Forschungsorgane und zivilgesellschaftliche Organisationen (Art. 26)

Wie bereits in der allgemeinen Würdigung (Kapitel 1) dargelegt, leisten sehr grossen Suchmaschinen und Kommunikationsplattformen bereits heute einen wertvollen Beitrag zu Forschung und Innovation, bspw. in dem sie Zugänge für Forschende anbieten.

Wir halten fest und fordern zugleich, dass die Anforderungen für Forschungszugang bzw. Datenzugang und die Sicherheit im Umgang mit entsprechenden Daten angemessen hoch sein müssen. Konkret fordern wir grundsätzlich die Einschränkung des Zugangs auf Forschungsinstitutionen verbunden mit dem Schutz vor dem Missbrauch von Daten und der Verletzung von Geschäftsgeheimnissen. Dies, um letztere zu schützen und gleichzeitig die Integrität der Wissenschaft zu erhalten. Dabei spielen wir insbesondere auch darauf an, dass die Studienziele und angewendeten Methoden der Antragsstellenden angemessen geprüft werden müssen (gemäss Art. 26 Abs. 1 Lit. a). Die Verfolgung von Partikularinteressen aufgrund der Agenda einer jeweiligen Organisation darf nicht Forschungsmotivation sein. Dies ist bei der Beurteilung von Anträgen gemäss Art. 26 Abs. 2 bzw. für eine Bewilligung nach Art. 26 Abs. 3 zu berücksichtigen. Hinsichtlich des konkreten Zugangs zu Datenplattformen für die Forschung (Art. 26 Abs. 4 und 5) fordern wir mit Nachdruck, keine Schweiz-spezifischen Anforderungen zu schaffen. Einerseits wäre ein «Schweizer Datenportal» technisch unverhältnismässig aufwendig und würde andererseits die Schweizer Forschung isolieren. Stattdessen ist auf bestehende, bewährte und international kompatible Zugangs-Plattformen und -Schnittstellen abzustellen.

3.19 Aufsicht (Art. 27)

Dass die Aufsicht beim Bundesamt für Kommunikation (BAKOM) angesiedelt werden soll, erscheint uns insbesondere hinsichtlich der Sach-Kompetenz bzw. dem -Verständnis nachvollziehbar. Betreffend die Ausführungsbestimmungen zur Aufsicht und «notwendigen Verfügungen» bringen wir jedoch klare Vorbehalte an. Die vorgesehenen Einschränkungen des Zugangs zu Diensten (siehe Kapitel 3.24) sowie die Verwaltungssanktionen (siehe Kapitel 3.25) erachten wir als insgesamt unverhältnismässig. Dies auch deshalb, weil das BAKOM als Organ

der Verwaltung – und damit Teil der Exekutive – solche, (zu) drastische Sanktionen verhängen könnte.

3.20 Auskunftspflicht (Art. 28)

Hinsichtlich der vorgesehenen, umfangreichen Informationsrechte des BAKOM fordern wir, dass diese dort Begrenzung erfahren, wo Verhältnismässigkeit oder der Schutz von Geschäftsgeheimnissen oder der Privatsphäre verletzt werden können. Insbesondere muss der Schutz explizit auch sicherheitsrelevante Informationen erfassen – etwa Details zur Funktionsweise von Spam-Filtern, Betrugserkennungssystemen oder anderen Sicherheitsmechanismen. Eine Offenlegung solcher Informationen würde böswilligen Akteuren ermöglichen, diese Systeme zu umgehen. Zudem darf das BAKOM nicht zum Lagerort sensibler Nutzendendaten werden.

3.21 Beaufsichtigte Unternehmen (Art. 29)

Der vorgeschlagene Mechanismus zur Bestimmung und Verpflichtung der beaufsichtigten Unternehmen gemäss Art. 27 erscheint schlüssig. Für Swico ist hierbei entscheidend, dass die Befugnisse zur Bestimmung von Unternehmen auf transparenten, objektiven Metriken und nicht auf administrativem Ermessen basieren.

3.22 Gebühren (Art. 30)

Hinsichtlich der Gebühren fordern wir eine Präzisierung, sodass in Art. 30 klar festgehalten wird, dass die Gebühren nach dem Prinzip der Kostendeckung erhoben werden.

Art. 30 Abs. 2: «Der Bundesrat legt die Höhe der Gebühren unter Berücksichtigung des Verwaltungsaufwands *kostendeckend* fest.»

3.23 Aufsichtsabgabe (Art. 31)

Der vorgesehenen Aufsichtsabgabe, insbesondere aber deren vorgeschlagenen Ausgestaltung, stehen wir äusserst kritisch gegenüber. Zwar erscheinen die Parameter gemäss Art. 31 Abs 2 grundsätzlich transparent und nachvollziehbar. Allerdings schafft die globale Orientierung gemäss Art. 31 Abs. 3 («die Höhe der Abgabe darf 0,05 Prozent des weltweiten Gewinns der Anbieterin [...] nicht übersteigen»), gerade auch mit Blick auf den vergleichsweise kleinen Schweizer Markt, einen absolut unverhältnismässigen, extraterritorialen Ansatz. Die so definierte Aufsichtsabgabe kann denn auch als eine «Digital-Steuer» interpretiert werden, was den Äusserungen des Bundesrats im Kontext der laufenden Handelsgespräche mit den USA widerspricht. Wir verweisen dazu auch auf unsere standort- und handelspolitische Einordnung in Kapitel 4. Auch erachten wir den vorgeschlagenen Ansatz als nicht kohärent mit der Schweizer Aufsichts- und Rechtstradition. Deshalb weisen wir den vorgeschlagenen Ansatz entschieden zurück.

3.24 Verwaltungsmassnahmen und Verfahren bei Einschränkung des Zugangs zum Dienst (Art. 32 und 33)

Der Vorentwurf sieht enorm weitgehende bzw. zu weitgehende Instrumente zur Aufsicht und Durchsetzung vor. Konkret soll das BAKOM Fernmeldedienstanbieter anweisen können, den Zugang zu einem Dienst einzuschränken, wenn vorgelagerte Massnahmen unwirksam sind oder bereits Grund zur Annahme besteht, dass sie unwirksam sind (Art. 32 Abs. 2). Das dafür vorgeschlagene Verfahren mildert die Eingriffsintensität nur sehr begrenzt: Betroffene, sehr grosse Suchmaschinen und Kommunikationsplattformen werden vorgängig angehört und

erhalten eine 30-Tage-Frist zur Stellungnahme und zum Nachweis der Behebung; wird dieser Nachweis nicht erbracht, kann die Sperre für höchstens 30 Tage angeordnet und bei Fortdauer oder Wiederholung erneuert werden; aufgehoben wird sie erst nach Behebung.

Zum einen treffen solche Massnahmen entsprechende Dienste stark – es geht um einen massiven Eingriff in die Wirtschaftsfreiheit. Die Verhältnismässigkeit dieser Massnahme mit Blick auf Art. 36 BV sehen wir nicht gegeben. Andererseits sind entsprechende Dienste, wie der Bundesrat mit dem VE-KomPG selbst begründet, von Bedeutung für den allgemeinen Informationszugang und die Kommunikation. Das heisst, dass solch eine Zugangsbeschränkung nicht nur die betroffenen Anbieter, sondern zwangsläufig auch Dritte, die diese Kanäle rechtmässig nutzen, enorm einschränkt. Damit wirkt die Massnahme im Ergebnis «bloss» wie ein überdimensioniertes Druckmittel: Sie unterbindet nicht gezielt eine konkrete Pflichtverletzung, sondern kappt den Zugang zu einem gesamten Kommunikationsraum – und belastet damit auch jene Nutzung, deren Schutz und geordnete Ausübung das Gesetz im Kern adressieren will.

Hinzu kommt, dass sich Netzsperrern je nach Technik auch umgehen lassen. In der Praxis wird damit die Schutz- und Durchsetzungswirkung relativiert, während die Kosten und Fehlblockierungsrisiken bei den Fernmeldedienstanbieterinnen anfallen (eine Entschädigung ist nicht vorgesehen) und Kollateralschäden («Overblocking» rechtmässiger Angebote) systemisch angelegt werden.

Wir fordern deshalb ausdrücklich, dass von Netzsperrern abgesehen wird. Ein so massiver Eingriff in die Grundrechte aller Beteiligten bzw. die notwendige Abwägung darf nicht im Rahmen einer behördlichen Vollzugsmassnahme vorgenommen werden. Dies auch, weil die im Vorentwurf vorgesehene Karenzfrist und der nachgelagerte Rechtsschutz nicht genügen sind. Eine Sperre entfaltet ihre Wirkung bereits, bevor ein Gericht die Verhältnismässigkeit vollumfänglich prüfen kann.

3.25 Verwaltungssanktionen (Art. 34)

Die Vorlage will insbesondere die Rechtsdurchsetzung gegenüber sehr grossen Anbietern, die international tätig sind, stärken. Dabei orientiert sich der VE-KomPG, vor allem auch bei den Verwaltungssanktionen, klar erkennbar am DSA. Der DSA und auch der VE-KomPG sehen für sehr grosse Anbieter Bussen von bis zu 6 % des weltweiten Jahresumsatzes vor. Dieser Ansatz ist aus vielerlei Gründen hochproblematisch und klar abzulehnen.

Erstens schafft der vorgesehene, drakonische Bussenrahmen eine Anreizstruktur, die dem Regulierungsziel zuwiderläuft: Ein Vollzug, der mit existenzrelevanten Sanktionen operiert, begünstigt defensives Risikomanagement – im Zweifel wird entfernt oder gesperrt, auch wenn Inhalte rechtmässig sind. Auch hier wird wieder das Risiko des «Overblocking» erhöht, mit negativen Auswirkungen auf die freie Meinungsäusserung. Erste empirische Hinweise legen nahe, dass diese Gefahr real ist: In einer Auswertung des [«Future of Free Speech»-Projekts](#) lag der Anteil rechtlich zulässiger Inhalte unter gelöschten Kommentaren je nach Land und Plattform in einzelnen Auswertungen zwischen rund 88 % und nahe 100 %. Auch die DSA-Streitbeilegung deutet auf eine erhebliche Fehlerquote hin: Das [«Appeals Centre Europe»](#) berichtet, es habe in 77 % von 1'565 entschiedenen Fällen (Januar bis August 2025) die ursprünglichen Plattformentscheide aufgehoben, typischerweise verbunden mit der Wiederherstellung von Inhalten oder Accounts. Diese hohe Quote deutet darauf hin, dass unter dem Druck drohender Sanktionen systematisch zu viele Inhalte entfernt werden könnten. Konkreter: Die

Zahlen verdeutlichen, dass ein sanktionsgetriebenes Vollzugsdesign die Tendenz verstärkt, «Entfernung statt Genauigkeit» zu belohnen.

Zweitens ist zu beachten, dass ein zunehmend restriktives Regulierungsumfeld in der EU Anbieter dazu veranlasst hat, politische Werbung ganz einzustellen. Aus Sicht der Anbieter sind solche «Risk-Off»-Entscheidungen verständlich, wenn Rechts- und Sanktionsrisiken (zu) hoch und (zu) schwer abschätzbar sind. Für eine direkte Demokratie wie die Schweiz wäre ein derartiger Effekt jedoch besonders bedenklich: Politische Kommunikation – einschliesslich digitaler Kanäle – gehört zum demokratischen Prozess und darf nicht verdrängt werden.

Drittens ist die Gefahr des «Overblockings» und «Risk-Offs» umso grösser, als dass der vorgeschlagene Ansatz (6% des weltweiten Umsatzes) für den vergleichsweise geringen Schweizer Markt noch unverhältnismässiger ist.

Viertens ist festzuhalten, dass umsatzabhängige Unternehmensbussen, gerade in dieser Größenordnung, und mit einem extraterritorialen Ansatz (die Sanktionen beziehen sich auf den weltweiten Umsatz) nicht an die etablierte schweizerische Sanktionspraxis anschliessen. In vergleichbaren Regulierungsfeldern bewegen sich Bussen typischerweise im fünf- bis sechsstelligen Bereich (z.B. DSG bis 250'000 CHF; FINIG bis 500'000 CHF; MWSTG bis 100'000 CHF). Zwar gibt es Ausnahmen, namentlich im Kartellrecht. Gerade dort zeigt sich aber auch, dass sich umsatzabhängige Sanktion an dem in der Schweiz erzielten Umsatz orientieren – nicht am weltweiten Umsatz (Art. 49a KG). Die im VE-KomPG vorgesehene Bezugsgrösse verschärft die Sanktionswirkung zusätzlich und verstärkt die beschriebenen Fehlanreize.

Fünftens ist eine vergleichbare Bussgeldhöhe im Verhältnis zum weltweiten Umsatz auf EU-Ebene bereits enorm; für ein Markt von der Grösse der Schweiz ist der vorgeschlagene Ansatz gänzlich unnachvollziehbar. Er könnte im schlimmsten Fall dazu führen, dass zukünftige Plattformen oder Suchmaschinen, die eine willkommene Ergänzung zum digitalen Ökosystem darstellen, davor zurückschrecken, ihre Dienste in der Schweiz anzubieten.

Sechstens kann der gewählte, extraterritoriale Ansatz (siehe oben) sich auch in anderen, für die Schweiz relevanten Dossiers, beispielsweise in der Handelspolitik, negativ auswirken (siehe Kapitel 4).

Aus den genannten Gründen fordern wir ausdrücklich, dass der Bussenrahmen deutlich tiefer und verhältnismässiger ausgestaltet wird. Das beinhaltet auch den Verzicht auf einen extraterritorialen Ansatz bzw. die Orientierung beispielsweise am weltweiten Umsatz eines Dienstes. Zudem ist in der Systematik sicherzustellen, dass Sanktionen primär an klar definierten, formalen Pflichtverletzungen anknüpfen und nicht – direkt oder indirekt – die inhaltliche Moderationspraxis als Ergebnis steuern.

Zudem fordern wir mit Blick auf Art. 34 Abs. 3, dass jegliche persönliche Haftung aus dem Gesetz zu streichen ist. Einzelne Mitarbeiter zur Verantwortung zu ziehen ist unverhältnismässig und setzt aus Standortsicht die falschen Signale.

3.26 Vollzug (Art. 36 bis 39)

Bei der Erarbeitung der Ausführungsbestimmungen (im Sinne von Art. 36) sind die Digitalindustrie und insbesondere die betroffenen Anbieter aktiv einzubeziehen, um eine wirksame und gleichzeitig unbürokratische, praktikable Lösung – ohne Fragmentierungen und «Swiss Finishes» – zu erzielen.

Vor diesem Hintergrund bzw. dieser Forderungen erscheint es uns zielführend, dass das BAKOM die Öffentlichkeit über seine Tätigkeit und Verfügungen informiert, sofern «keine Berufs-, Geschäfts- oder Fabrikationsgeheimnisse [preisgegeben werden]» (Art. 37 Abs. 3). Wir regen hierzu die Präzisierung an, dass dieser Schutz explizit auch sicherheitsrelevante Informationen erfasst, wie beispielsweise zu Spam-Filter-Funktionieren oder die Nutzenden-Privatsphäre, um zu verhindern, dass Sicherheitssysteme rückwärts «rekonstruiert» werden. Diese Präzisierung ist in unseren Augen im Sinne des Regulators, der Öffentlichkeit, der Nutzenden als auch den Anbietern.

Daraus folgt aus Sicht von Swico auch, dass die Bearbeitung von Daten juristischer Personen und Personendaten durch das BAKOM klar den Bestimmungen des Datenschutzes unterliegt und darüber hinaus das BAKOM nicht zum Lagerort sensibler Daten werden darf.

3.27 Evaluation (Art.40)

Eine Überprüfung der Vorlage hinsichtlich Zweckmässigkeit und Wirksamkeit, gemäss Art. 40 Abs. 1, ist notwendig. Dies vor allem auch im Hinblick auf technologische und (internationale) regulatorische Entwicklungen. Den vorgesehenen «Zwischenbericht» begrüssen wir (Art. 40 Abs. 2).

4 Standort- und handelspolitische Einordnung

Die Schweiz hat sich traditionell als innovationsfreundlicher Standort positioniert, der mit pragmatischer, verhältnismässiger und «smarter» Regulierung Investitionen und Know-How – namentlich auch von internationalen Technologieunternehmen – anzieht. Dieser Positionierung ist unbedingt Sorge zu tragen. Dies, zumal einerseits drohende Überregulierungen und Bürokratie die Attraktivität des Innovationsstandorts schwächen. Andererseits scheint in der EU das Verständnis um die negativen Konsequenzen unverhältnismässiger Regulierungen – insbesondere auch Digitalbereich – zu verfangen. So sind die Entwicklungen hinsichtlich einer möglichen Deregulierung in der EU, beispielsweise aufgrund des «Digital Omnibus» und dem «Digital Fitness Check» sowie der absehbaren «DSA-Evaluation», zwingend zu berücksichtigen. Wir verweisen hierzu beispielsweise auf die Interpellation Michel ([25.4621](#)) «Der «Digital Omnibus» der EU entlastet die Wirtschaft. Was macht die Schweiz?» sowie die Motion Cottier ([25.4715](#)) «Cybersicherheit stärken, Bürokratie abbauen. Harmonisierung der Meldewege für die digitale Schweiz».

Daran, sowie an unsere eingangs angebrachte Kritik am Regulierungsvorhaben selbst (siehe Kapitel 1) angeknüpft, weisen wir mit Blick auf die offizielle [Regulierungsfolgenabschätzung](#) (S.49) ausdrücklich darauf hin, dass die vorgeschlagene Regulierung zusätzliche Kosten für betroffene Unternehmen mit sich bringt und eine gewisse Markteintrittshürde für kleine, schnell wachsende Online-Plattformen mit wenig Personal und niedrigem Werbeertrag darstellt. Dies insbesondere dann, wenn sie schnell die Regulierungsschwelle überschreiten. Dies ist ein realistisches Szenario in diesem dynamischen, von der Technologie getriebenen Markt – auch für mögliche künftige Schweizer Suchmaschinen und Kommunikationsplattformen, die in den Regelungsbereich eines künftigen KomPG fallen könnten. Dieser Aspekt ist aus einer standortpolitischen Perspektive aktiv mitzuberücksichtigen, auch wenn aktuell vor allem 5 – 15 Unternehmen, meist mit US-amerikanischem Sitz, betroffen sind.

Weiter ist gerade auch die beschriebene internationale Dimension zu berücksichtigen, wenn es um eine mögliche Umsetzung des vorgeschlagenen Regulierungsvorhabens geht. Internationale Erfahrungen zeigen, dass die US-Regierung Regulierungsregime, die primär oder faktisch grosse US-Technologieunternehmen betreffen als potenzielle Handelshemmnisse interpretiert und politisch thematisiert. Es geht dabei insbesondere um Regelungen, die potenziell marktabstottend, als einseitige Belastung ausländischer Anbieter und / oder als extraterritorial wirksam verstanden werden. Letzteres bezieht sich insbesondere auch auf das unverhältnismässige Sanktionsregime des VE-KomPG (siehe Kapitel 3.25). Für den hiesigen innovativen Digitalstandort wie auch die Wirtschaft insgesamt ist die Berücksichtigung der handelspolitischen Dimension zentral.

Wir bedanken uns für die Berücksichtigung unserer Anliegen und stehen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse
Swico



Dr. Jon Fanzun
CEO



Simon Ruesch
Head Legal und Public Affairs
Mitglied der Geschäftsleitung