DIGITALE GESELLSCHAFT

Digitale Gesellschaft, CH-4000 Basel

Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundeshaus West
CH-3003 Bern

Per E-Mail an: ptss-aemterkonsultationen@isc-ejpd.admin.ch

Basel, 2. Mai 2025

Stellungnahme zu den Änderungen der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) und Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF)

Sehr geehrter Herr Bundesrat Beat Jans
Sehr geehrte Empfänger:innen

Am 29. Januar 2025 eröffnete der Bundesrat die Vernehmlassung zur Teilrevision zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF).
Die Digitale Gesellschaft ist eine gemeinnützige Organisation, die sich für Grund- und Menschenrechte, eine offene Wissenskultur, weitreichende Transparenz sowie Beteiligungsmöglichkeiten an gesellschaftlichen Entscheidungsprozessen einsetzt. Die Tätigkeit orientiert sich an den Bedürfnissen der Bürgerinnen und Konsumenten in der Schweiz und international. Das Ziel ist die Erhaltung und die Förderung einer freien, offenen und nachhaltigen Gesellschaft vor dem Hintergrund der Persönlichkeits- und Menschenrechte.

Gerne nehmen wir zum Vorentwurf wie folgt Stellung:

Vorbemerkung

Die geplante Revision der VÜPF ist ein Frontalangriff auf unsere Grundrechte, die Rechtsstaatlichkeit sowie den IT- und Innovationsstandort Schweiz.

Mit ihrer Umsetzung würde geltendes Recht in einem Ausmass verletzt, das alarmieren muss: Die Revision ist in vielerlei Hinsicht unvereinbar mit dem Bundesgesetz betreffend die Überwachung des

Post- und Fernmeldeverkehrs (BÜPF), verstösst gegen das Datenschutzgesetz (DSG), steht in klarem Widerspruch zu den verfassungsmässigen Grundrechten und verstösst gegen Völkerrecht.
Die vorgesehenen Änderungen führen zu einer massiv ausgeweiteten Überwachung – ganz grundsätzlich und flächendeckend. Dies ist mit der Ausrichtung des BÜPF, das eine fein austarierte Interessenabwägung zwischen Freiheit und Privatsphäre einerseits und Sicherheit durch Überwachungsmassnahmen andererseits verfolgt, absolut nicht vereinbar.

Die Auswirkungen auf den Wirtschafts- und Innovationsstandort Schweiz wären verheerend: Die Ausweitung der Überwachung und die damit verbundenen, übermässigen Mitwirkungspflichten machen die Schweiz für IT-Anbieter äusserst unattraktiv. Renommierte Unternehmen wie Proton oder Threema, deren Geschäftsmodelle durch die Vorlage direkt ins Visier geraten, würden in ihrer Existenz bedroht. Die ersten Konsequenzen sind bereits sichtbar: Proton hat angekündigt, die Schweiz im Falle eines Inkrafttretens verlassen zu müssen (siehe Tages-Anzeiger vom 1. April 2025). Der Chef des Unternehmens erklärte in einem Interview: «Diese Entscheidung ist wirtschaftlicher Selbstmord für die Schweiz» (watson.ch vom 9. April 2025). Ähnlich äussert sich Threema-Chef Robin Simon: «Der Wirtschaftsstandort würde durch die Revision geschwächt und für Tech-Start-ups unattraktiv.» Aktuell lasse sich Threema alle Optionen offen (Tages-Anzeiger vom 8. April 2025). Diese Warnzeichen sind ernst zu nehmen und zeigen das verheerende Ausmass der geplanten Revision.

Neben den verheerenden wirtschaftlichen Auswirkungen wird gleichzeitig der grundrechtlich garantierte Anspruch auf sichere und vertrauliche Kommunikation ausgehöhlt. Wenn Anbieterinnen abwandern, bleibt jedoch – als wäre dies nicht genug – nicht nur privaten Nutzer:innen der Zugang zu geschützten Kommunikationsmitteln verwehrt.

Ebenso betroffen sind auch Personen, die einem Berufsgeheimnis unterstehen, wie Journalistinnen oder Anwälte. Die Änderungen treffen zudem schutzbedürftige Personengruppen besonders hart: Whistleblower:innen, Menschen mit ungeklärtem Aufenthaltsstatus oder ohne Papiere aber auch Aktivist:innen verlieren ebenso den Zugang zu vertraulichen Kommunikationsmitteln. Die Revision ignoriert diese Schutzbedürfnisse und erweitert stattdessen die Eingriffsbefugnisse des Staates in einer Weise, die hochgefährlich ist.

Besonders widersprüchlich erscheint das Vorgehen des Bundes angesichts der Tatsache, dass ausgerechnet der Bundesrat selbst Threema als Messenger nutzt – ein Dienst, den er nun faktisch aus dem Markt drängt. Damit sägt die Regierung ausgerechnet an jenem Ast, auf dem sie in Sachen sicherer Kommunikation bislang selbst sitzt.

Hinzu kommt: Die geplanten Regelungen sind technisch unausgereift, unnötig komplex und in Teilen schlicht nicht umsetzbar. Vielmehr wird ein kaum noch durchschaubares Normengeflecht geschaffen, das weder den Mitwirkungspflichtigen noch den Betroffenen ein Mindestmass an Rechtsklarheit bietet. Die Revision wird ausserdem präsentiert, als handle es sich dabei um Änderungen zur besseren Überblickbarkeit der Rechtslage und zur Schaffung von mehr Rechtssicherheit - tatsächlich aber wird der persönliche Anwendungsbereich der Mitwirkungspflichtigen enorm erweitert und eine Vielzahl neuer Anbieterinnen in den Kreis der Mitwirkungspflichtigen einbezogen. Von Transparenz kann nicht die Rede sein.

Es ist im Übrigen nicht haltbar, dass eine dermassen breit angelegte Ausweitung von Pflichten auf Verordnungsstufe angelegt wird. Solch einschneidende Veränderungen mit weitreichenden Konsequenzen sind in Gesetzesform zu erlassen. Der Bundesrat überschreitet seine Kompetenzen hier um ein Weites.

Diese Vorlage schwächt nicht nur den Innovations- und Wirtschaftsstandort Schweiz – sie untergräbt gleichzeitig im grossen Stil verfassungsmässig geschützte Rechte. Aus grundrechtlicher, datenschutzrechtlicher und gesellschaftspolitischer Sicht ist sie schlicht inakzeptabel. Die geplanten Änderungen stehen dem erklärten Ziel von mehr Freundlichkeit sowie allgemeinen rechtsstaatlichen Grundsätzen sowie Schutzbedürfnissen Einzelner diametral entgegen.

Deshalb lehnen wir die Revision vollumfänglich und in aller Deutlichkeit ab.

Bemerkungen zu einzelnen Artikeln der *VÜPF*

Alle Artikel

Um den Anforderungen des Datenschutzgrundsatzes der Datenminimierung (Art. 6 Abs. 3 DSG) gerecht zu werden, sollte generell bei allen Auskunftstypen die Datenherausgabe zwar im Rahmen einer überwachungsrechtlichen Anfrage erreicht werden können. Jedoch darf es nicht das Ziel sein, Unternehmen zu zwingen, mehr Daten über ihre Kund:innen auf Vorrat zu sammeln, als dies für deren Geschäftstätigkeit notwendig ist.

Aus diesem Grund soll allen relevanten Artikeln die Kondition «sofern verfügbar» o.ä. hinzugefügt werden, damit durch die Revision nicht unangemessene und teure Aufbewahrungspflichten geschaffen werden.

Antrag: Auskünfte bei allen relevanten Artikeln auf die tatsächlich vorhandenen Daten beschränken.

Art. 16b Abs. 1

Durch die neue Formulierung werden die Kriterien für FDA mit reduzierten Pflichten verschärft. Durch das Abstellen der Kriterien auf den Umsatz der gesamten Unternehmung anstelle nur der relevanten Teile (Art. 16b Abs. 1 lit. b Ziff. 2 VE-VÜPF) wird die Innovation bestehender Unternehmen, welche die Schwellenwerte bereits überschreiten, aktiv behindert, da sie keine neuen Dienstleistungen und Features auf den Markt bringen können, ohne hierfür gleich die vollen Pflichten als FDA zu erfüllen. Bestehende Unternehmen müssen so entweder komplett auf Neuerungen verzichten oder unverhältnismässige Mitwirkungspflichten in Kauf nehmen.

Dazu kommt, dass das Kriterium bezüglich der Überwachungsaufträge nicht vom BÜPF gestützt wird, denn: Die Anzahl von Überwachungsaufträgen ist von der wirtschaftlichen Bedeutung einer FDA völlig losgelöst. Die wirtschaftliche Bedeutung ist aber gemäss Art. 26 Abs. 6 BÜPF ausschlaggebend dafür, ob eine FDA von den vollen Pflichten (teilweise) befreit werden kann. Im Umkehrschluss ist die wirtschaftliche Bedeutsamkeit somit Erfordernis für die Auferlegung von vollen Pflichten. Wenn eine FDA nun aber rein aufgrund einer bestimmten Anzahl von Überwachungsaufträgen nach Art. 16b Abs. 1 lit. b Ziff. 1 VE-VÜPF als vollpflichtige FDA qualifiziert wird, steht dies im Widerspruch zum BÜPF und entbehrt damit einer Rechtsgrundlage.

Dieses bereits in der aktuellen Version der VÜPF vorhandene Problem sollte im Zuge einer Revision nicht bestehen bleiben, sondern muss behoben werden.

Antrag: Aufhebung der Formulierung von lit. b Ziff. 1 und 2: «Überwachungsaufträge zu 10 verschiedenen Überwachungszielen in den letzten 12 Monaten (Stichtag: 30. Juni) unter

Berücksichtigung aller von dieser Anbieterin angebotenen Fernmeldedienste und abgeleiteten Kommunikationsdienste;» und «Jahresumsatz in der Schweiz des gesamten Unternehmens von 100 Millionen Franken in den beiden vorhergehenden Geschäftsjahren.» Es ist auf die Regelung in Art. 26 Abs. 6 BÜPF abzustellen und eine Einzelfallbetrachtung zur Einstufung vorzunehmen.

Art. 16c Abs. 3

Die durch die neue Verordnung einmal mehr deutlich ausgeweitete automatische Abfrage von Auskünften entzieht den FDA die Möglichkeit, sich gegen falsche oder unberechtigte Anfragen zu wehren. Erstens wird die menschliche Kontrolle ausgeschaltet, zweitens werden bestehende Hürden für solche Auskünfte gesenkt. Doch gerade Kosten und Aufwand dienen als «natürliche» Schutzmechanismen gegen eine übermässige oder missbräuchliche Nutzung solcher Massnahmen durch die Untersuchungsbehörden. Die automatisierte Erteilung von Auskünften ist unverhältnismässig und widerspricht dem Prinzip der Datenminimierung. Die pauschale und undifferenzierte Regel beeinträchtigt zwangsläufig den Grundrechtsschutz.

Der vorgesehene Umsetzungszeitraum von 12 Monaten zur Umsetzung eines dermassen komplexen Systems ist ausserdem völlig unzureichend. Eine übereilte Umsetzung erhöht das Risiko schwerwiegender technischer und rechtlicher Mängel und ist inakzeptabel.

Antrag: Streichung von lit. a «automatisierte Erteilung der Auskünfte» (ebenso in Art. 18 Abs. 2).

Art. 16d

Gemäss erläuterndem Bericht stellen Kommunikationsdienste, die nicht zu den in Art. 16a Abs. 1 aufgezählten Fernmeldediensten gehören und auf die die Ausnahmen nach Art. 16a Abs. 2 nicht zutreffen, abgeleitete Kommunikationsdienste dar. Diese klarere Definition des Begriffs AAKD ist begrüssenswert, doch ist die Konkretisierung der abgeleiteten Kommunikationsdienste im erläuternden Bericht einerseits rechtsstaatlich problematisch und andererseits geht die neue Auslegung nach den Ausführungen im erläuterndem Bericht weit über den gesetzlichen Zweck hinaus. Besonders problematisch ist die generelle Nennung von Onlinespeicherdiensten wie iCloud, OneDrive, Google Drive, Proton Drive oder Tresorit (der Schweizer Post), die oft exklusiv zur privaten Speicherung (Fotos, Passwörter etc.) genutzt werden.

Art. 2 lit. c BÜPF definiert AAKD ausdrücklich als Dienste, die «Einweg- oder Mehrwegkommunikation ermöglichen». Dies trifft jedoch auf persönliche Cloud-Speicher nicht zu, womit deren Einbezug in die Auslegung unrechtmässig ist – auch hier setzt sich die Revision inakzeptabel über die gesetzlichen Vorgaben des BÜPF hinweg. Onlinespeicherdienste sind deshalb aus Art. 16d zu streichen.

Zudem anerkennt der erläuternde Bericht zwar, dass VPNs zur Anonymisierung der Nutzer:innen dienen (S. 19), doch die Kombination mit der Revision von Art. 50a nimmt ihnen diese Funktion faktisch, weil angebrachte Verschlüsselungen zu entfernen sind. Dies würde VPN-Diensten die Erbringung ihrer Kerndienstleistung, einer möglichst anonymen Nutzung des Internet, verunmöglichen. Das Bedürfnis, auch künftig VPN-Dienste in Anspruch nehmen zu können, ist zu schützen und darf nicht vereitelt werden. Anbieter von VPNs sind daher ebenfalls aus Art. 16d auszunehmen.

Es ist irritierend, dass die bewusst separat ausgestalteten Kategorien AAKD und FDA einander zunehmend angeglichen werden, und zwar zuungunsten der AAKD, die als Kategorie mit grundsätzlich weniger weitreichenden Pflichten als die FDA konzipiert wurde. Dies missachtet den Willen des Gesetzgebers, den es zu wahren gilt.

Antrag: Streichung von Onlinespeicherdiensten und VPN-Anbieterinnen aus der Aufzählung der möglichen abgeleiteten Kommunikationsdienste in den Ausführungen zu Art. 16d im erläuternden Bericht und in der Auslegung.

Art. 16e, Art. 16f und Art. 16g

Die geplante Revision der VÜPF soll laut Erläuterungsbericht die KMU-Freundlichkeit verbessern und willkürliche Hochstufungen von AAKD abmildern. Tatsächlich steht der vorgelegte Entwurf diesem erklärten Ziel jedoch komplett entgegen. Statt Verhältnismässigkeit zu schaffen, unterwirft die Revision neu die grosse Mehrheit der KMU, die abgeleitete Kommunikationsdienste betreiben, einer überaus strengen Regelung mit deutlich erweiterten Pflichten. Entscheidend ist, dass neuerdings das Kriterium von 5'000 Nutzer:innen allein zum Auferlegen massiver Überwachungspflichten ausreicht: Erreicht eine AAKD diese Grösse, fällt sie neu in die Kategorie der AAKD mit reduzierten Pflichten und untersteht somit bereits sehr weitgehenden Mitwirkungspflichten, insbesondere der Identifikationspflicht.

Die Einführung von 5'000 Nutzer:innen als gesondert zu beurteilende Untergrenze verletzt Art. 27 Abs. 3 BÜPF, denn 5'000 Personen sind keinesfalls eine «grosse Nutzerzahl», bei der die neuen, deutlich strengeren Überwachungsmassnahmen, gerechtfertigt wären. 5'000 Nutzer:innen werden in der digitalen Welt vielmehr sehr rasch erreicht – die Revision verkennt technische Realitäten.

Zusätzlich führt das Einführen eines Konzerntatbestandes in Art. 16f Abs. 3 zu massiven Problemen: Produkte und Dienste müssen nicht mehr für sich allein bestimmte Schwellenwerte erreichen – es genügt, wenn das Mutterunternehmen oder verbundene Gesellschaften diese überschreiten. Insbesondere bei Unternehmen mit Beteiligungsstrukturen führt dies dazu, dass sämtliche Angebote pauschal der höchsten Überwachungsstufe unterstellt werden – unabhängig davon, ob sich einzelne Dienste noch im frühen Entwicklungsstadium befinden oder faktisch kaum genutzt werden. Somit müsste jedes neue Projekt von Beginn an mit vollumfänglichen Überwachungspflichten geplant und eingeführt werden, was Innovation behindert. Zudem missachtet der Konzerntatbestand das Verhältnismässigkeitsgebot: Unterschiedliche organisatorische Einheiten mit eigenständigen Angeboten werden unrechtmässig zusammengefasst, obwohl sie individuell zu prüfen wären. Die Anwendung starrer Schwellen auf ganze Konzerne statt auf einzelne Dienste umgeht eine notwendige Einzelfallprüfung.

Eine solche Regelung stünde sodann *im klaren Widerspruch zu Postulat 19.4031 von Albert Vitali*, das die zu seltene Anwendung von Downgrades kritisierte:

«Schlimmer noch ist die Situation bei den Anbieterinnen abgeleiteter Kommunikationsdienste [AAKD]. Sie werden über die Verordnungspraxis als Normadressaten des BÜPF genommen, obschon das so im Gesetz nicht steht. Das heisst, praktisch jede Firma, die Online-Dienste anbietet, fällt unter das BÜPF.»

Statt KMU zu entlasten, führt die Revision neu zu einem *«automatischen» Upgrade per Verordnung ohne Verfügung* (Erläuternder Bericht, S. 23). Dieser Ansatz ist offensichtlich unverhältnismässig und verschärft nicht nur die Anforderungen, sondern zwingt bereits kleine AAKD zu aktiver Mitwirkung mit hohen Kosten.

Eine Analyse der offiziellen VÜPF-Statistik unterstreicht diese offensichtliche Unverhältnismässigkeit. Im Jahr 2023 betrafen 98,97% der total 9'430 Überwachungen allein Swisscom, Salt, Sunrise, Lycamobile und Postdienstanbieter – übrig bleiben nur 1,03% für den gesamten Restmarkt. Bei den Auskünften zeigt sich ein ähnliches Muster, wobei 92,74% wieder allein auf Swisscom, Salt, Sunrise und Lycamobile entfallen. Durch die Revision nun nahezu 100% des Marktes inklusive der KMU und Wiederverkäufer unter dieses Gesetz zu zwingen, das faktisch nur fünf Giganten – darunter zwei milliardenschwere Staatsbetriebe – betrifft, ist offensichtlich weder verhältnismässig noch KMU-freundlich.

Die neue Vorlage schliesst nun ebenfalls sowohl die Registrierung via normaler E-Mail als auch die komplett anonyme Registrierung (z. B. Signal oder Telegram) aus, da AAKD bereits mit reduzierten Pflichten neu automatisch zwingend die Endnutzer:innen identifizieren müssen. Hiervon betroffen sind nicht nur alle AAKD mit reduzierten Pflichten, sondern auch all deren Wiederverkäufer. Faktisch resultiert das Gesetz somit darin, dass man sich bei keinem Dienst mehr anmelden können soll, ohne den Pass, Führerschein oder die ID entweder direkt oder indirekt zu hinterlegen. Dass Nutzer:innen künftig hierzu gezwungen wären, stellt einen massiven Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 13 BV) dar und ist unzumutbar.

Ein weiteres Kernproblem, das die automatische Hochstufung mit sich bringt, ist die Rechtsunsicherheit. Die Vorlage will mit klarer definierten Kategorien und Pflichten ein übersichtlichere Situation schaffen, verfehlt dieses Ziel jedoch gänzlich. Bislang fand die Hochstufung per Verfügung statt, wodurch es für die Mitwirkungspflichtigen klar erkennbar war, wann sie unter welche Pflichten fallen. Ausserdem bewirkt diese Praxis eine sinnvolle Einzelfallbetrachtung anstelle pauschaler und unzweckmässiger automatischer Hochstufungen. Unter dem revidierten System entfällt dieser Schritt, und eine AAKD wird automatisch hochgestuft, sobald sie den massgebenden Schwellenwert erreicht. Genau diese Frage nach dem Erreichen des Schwellenwertes kann aber im Zweifelsfall nur schwer zu beantworten sein. Gerade deshalb besteht ein schutzwürdiges Interesse der Anbieter an Klarheit über ihre Pflichten, da sie fortan eventuell die umfangreichen und kostspieligen mit der Hochstufung verbundenen zusätzlichen Massnahmen treffen müssen. Die AAKD müssten sich diesbezüglich jedoch aktiv mittels Feststellungsverfügung erkundigen. Diese Umstrukturierung lässt ich nicht mit der Funktionsweise von Verwaltungsverfahren vereinbaren. Die Pflicht zur Abklärung, wann eine Hochstufung vorliegt und was diese für das Unternehmen bedeutet, darf nicht in die Verantwortung der Unternehmen fallen. Der Staat zieht sich hier aus der Verantwortung und schiebt diese den Unternehmen zu, wodurch diesen zwangsläufig zeitlicher und finanzieller Mehraufwand entsteht. Von einer automatischen Hochstufung von AAKD ist daher abzusehen.

Verschärfend wirkt sich hier die kaum verständlichen Sprache des Verordnungsentwurfs aus, welche es Laien und kostensensitiven KMUs (ohne eigene Rechtsabteilung) verunmöglicht, einen Überblick über ihre neuen Pflichten zu erlangen.

Gegenüber der geltenden VÜPF *erweitert die Revision die Pflichten zur Automatisierung noch einmal deutlich auf neu alle AAKD mit vollen Pflichten, und sie schafft mehrere neue problematische Abfragetypen wie z. B. "IR_59" und "IR_60", welche ebenfalls automatisiert und ohne manuelle Intervention abgefragt werden können sollen*. Durch die Automatisierung steigt das Risiko eines Missbrauchs der Überwachungsinstrumente erheblich, und damit auch das Risiko für die Grundrechte der betroffenen Personen. Die Ausweitung der automatisierten Auskünfte muss daher ersatzlos gestrichen werden.

Ebenfalls problematisch ist die Streichung des Kriteriums des «grossen Teils der Geschäftstätigkeit» in Art. 16g Abs. 1 (im Vergleich zu Art. 22 Abs. 1 lit. b der geltenden VÜPF), die dazu führt, dass eine Unternehmung nicht mehr abgeleitete Kommunikationsdienste als einen «grosse[n] Teil ihrer

Geschäftstätigkeit» anbieten muss, um als AAKD zu gelten. *Damit fallen auch Unternehmen, die nur experimentell oder in kleinem Rahmen, ja aus rein gemeinnützigen Motiven, ein Online-Tool bereitstellen, von Anfang an voll unter das Gesetz*.

Die Folgen sind gravierend, denn schon ein öffentliches Pilotprojekt löst umfangreiche Verpflichtungen aus, etwa Pikettdienste (Art. 16g Abs. 3 lit. a Ziff. 1) oder automatisierte Auskunftserteilungen (Art. 16g Abs. 3 lit. b Ziff. 1). Auch hiermit werden neue Hürden für Innovation geschaffen. Die Regelung ist unverhältnismässig und nicht sachdienlich.

Auch Non-Profit-Organisationen geraten unter die verschärften Vorgaben. Unter den neuen Kriterien wird aber allein auf die Anzahl der Nutzer:innen abgestellt für die Einstufung als AAKD. Dieses Kriterium greift jedoch zu kurz: Es berücksichtigt insbesondere nicht die wirtschaftliche Tragfähigkeit der Anbieter:innen. Gerade bei Open-Source- und Non-Profit-Lösungen mit grosser Reichweite, aber geringem Budget, führt dies zu einer verheerenden finanziellen Belastung: Anbieter:innen mit solchen Projekten würden gezwungen, umfangreiche Überwachungsmassnahmen einzuführen. Solche Anbieter:innen würden gezielt aus dem Schweizer Markt gedrängt, während gleichzeitig bestehende Monopole wie WhatsApp (96% Marktanteil in der Schweiz) gestärkt würden.

Es muss ausserdem klar festgehalten werden, dass sich das BÜPF und die VÜPF nur auf Anbieter:innen beziehen können, die in der Schweiz tatsächlich tätig sind. Die Erlasse dürfen nicht so ausgelegt werden, dass sie eine extraterritoriale Wirkung entfalten und internationale Dienste wie Signal, WhatsApp oder Microsoft Teams erfasst sind.

Das Kriterium der reinen Nutzer:innenzahl ist ungeeignet und muss gestrichen werden.
Die Regelung schwächt auch die nationale Sicherheit: Gerade in Zeiten zunehmender Cyberangriffe und abnehmender Zuverlässigkeit gerade us-amerikanischer Anbieter (angesichts der aktuellen Regierungsführung ist keinesfalls sichergestellt, dass deren Daten weiterhin geschützt bleiben) ist dies sicherheitspolitisch kontraproduktiv. Die neue VÜPF will den Bürger:innen der Schweiz den Zugang zu bewährten sicheren Messengern faktisch verwehren, dabei wäre das Gegenteil angebracht: Die Nutzung sicherer, End-zu-End-verschlüsselter Kommunikation ist heute wichtiger denn je und fällt in den Bereich grundrechtlich geschützter Ansprüche, die es zu wahren gilt. Diese Ansprüche dürfen nicht aufs Spiel gesetzt werden, um ein knallhartes Überwachungsregime der Kommunikation in der Schweiz durchzusetzen – die Prioritäten werden höchst fragwürdig gesetzt.

Die durch die neue Verordnung ausgeweitete Vorratsdatenspeicherung – ein Konzept, das in der EU seit bald einer Dekade illegal ist (C-203/15 und C-698/15, Tele2 Sverige and Watson and Others) – wächst das Risiko für die Sicherheit und die Privatsphäre der Nutzer:innen dramatisch. So werden durch die Vorlage nicht nur mehr Daten mit schwächeren Schutzmassnahmen gesammelt, diese zu erhebenden Datenmengen sind von enormem Ausmass und bergen folglich massive Risiken für Hackerangriffe.

Des Weiteren ist nicht belegt, dass die Speicherung der betreffenden Daten zu spürbar mehr erfolgreichen Ermittlungen führt. So kam auch der Bericht des Bundesrates zu «Massnahmen zur Bekämpfung von sexueller Gewalt an Kindern im Internet und Kindsmissbrauch via Live-Streaming» zum Schluss, dass die Polizei möglicherweise «nicht über ausreichende personelle Ressourcen» verfüge, um Verbrechen im Netz effektiv zu bekämpfen. Ebenfalls wurden weitere Massnahmen wie die «Ausbildung der Strafverfolgungsbehörden» als zentral eingestuft und auch die «nationale Koordination zwischen Kantons- und Stadtpolizeien» hervorgehoben. Das Gebot der Verhältnismässigkeit verlangt, dass zuerst diese einfachen und nicht-invasiven Methoden mit direktem Gegenwert ausgeschöpft werden müssen, bevor kritische Massnahmen mit grossem Risiko für die Gesamtbevölkerung implementiert werden.

Die Massnahmen wären zudem angesichts ihrer schweren Eingriffswirkung in die Grundrechtssphäre in jedem Fall auf Ebene des Gesetzes, und nicht durch eine reine Verordnung zu implementieren. Diese Handhabe bedeutet einen Verstoss gegen das Legalitätsprinzip und untergräbt legislative Kompetenzen. Ausserdem verfügt die Schweiz bereits über reichlich Mittel zur Aufklärung und Verfolgung von Straftaten, die Behörden können bereits heute auf sicherheitsrelevante Daten zurückgreifen. Unternehmen wie Proton (s. «Positionspapier zur Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)» von Proton) kooperieren seit Jahren mit den Schweizer Strafverfolgungsbehörden und dem Nachrichtendienst des Bundes (NDB). Wenn nun solche Unternehmen aus bereits genannten Gründen zur Abwanderung gezwungen werden, bewirkt die Revision auch hier das genaue Gegenteil ihrer erklärten Ziele: Anstatt der Schaffung besserer Möglichkeiten zur Strafverfolgung würden die Schweizer Behörden wie etwa Fedpol den Zugriff auf wichtige Partner bei der Beschaffung sicherheitsrelevanter Daten verlieren.

Erst kürzlich wurde in Kantonen wie Genf oder Neuenburg die digitale Integrität in die Kantonsverfassungen aufgenommen, weswegen die Romandie als «weltweite Pionierin eines neuen digitalen Grundrechts» (NZZ) betitelt wurde. In weiteren Kantonen wie Basel-Stadt, Jura, Waadt, Zug und Zürich sind ähnliche Bestrebungen im Gange. Der vorliegende Entwurf stellt auch diese Regelungen bewusst in Frage.

Gesamthaft gesehen fehlt der vorgeschlagenen Einführung einer neuen Stufe von Überwachungspflichtigen somit nicht nur eine ausreichende Rechtsgrundlage im BÜPF, sondern sie untergräbt auch die Bundesverfassung, mehrere Kantonsverfassungen sowie das DSG. Der Entwurf bringt nicht, wie der Begleitbericht den Leser:innen weismachen will, eine Entlastung der KMU, geschweige denn eine Entspannung der Hochstufungsproblematik, sondern er verengt den Markt, fördert bestehende Monopole von US-Unternehmen, behindert Innovation in der Schweiz, schwächt die innere Sicherheit, steht in direktem Gegensatz zum besagten Postulat 19.4031 und bedeutet massive Eingriffe in grundrechtlich geschützte Sphären, sowohl von Unternehmen als auch von Nutzer:innen.

Die vorgeschlagene Dreistufenregelung ist deshalb strikt abzulehnen und das bestehende System muss beibehalten werden.

Antrag: Streichung der Artikel und Beibehaltung der bestehenden Kriterien und der zwei Kategorien von AAKD. + Ausnahmen für Pilotprojekte (auch von grossen Firmen) und Non-Profits per se. Streichung der Automatisierten Auskünfte (Art. 16g Abs. 3 lit. b Ziff. 1).

Art. 16h

Art. 16h konkretisiert die Kategorie der «Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen» aus Art. 2 lit. e BÜPF. Die Vorschrift verfehlt ihr Ziel – anstatt Unsicherheiten darüber zu beheben, wer unter diese Kategorie fällt, schafft sie weitere Unklarheiten. Der schwammig formulierte Verordnungstext könnte dem Wortlaut nach auch Technologien wie TOR oder I2P erfassen. Diese werden von Journalist:innen, Whistleblower:innen und Personen in autoritären Staaten zum Schutz ihrer Privatsphäre genutzt. Betreiber:innen solcher Nodes können technisch nicht feststellen, welche Person den Datenverkehr erzeugt. Eine Identifikationspflicht wäre somit nicht nur technisch unmöglich, sondern würde auch die Sicherheit dieser Nutzer:innen gefährden und diese unschätzbar wichtigen Systeme grundsätzlich infrage stellen.

Es ist daher zumindest klarzustellen, dass der Betrieb solcher Komplett- oder Teilsysteme wie Bridge-, Entry-, Middle- und Exit-Nodes nicht unter das revidierte VÜPF fällt. Die Unklarheit bezüglich der Einordnung von TOR-Servern wirft weitere Fragen auf, denn wenn TOR nicht als PZD zu qualifizieren

ist, müsste TOR – gleich wie die VPNs – der Kategorie der AAKD zugeordnet werden. Somit stünden Betreiber:innen von TOR-Servern – wie etwa die Digitale Gesellschaft – unter der Identifikationspflicht. Diese ist jedoch, wie dargelegt, nicht umsetzbar.

Es braucht somit entweder die Zusicherung, dass Betreiberinnen von TOR-Nodes nicht dem BÜPF und der VÜPF unterstellt sind oder aber Kategorien von Mitwirkungspflichten, die so gestaltet sind, dass ein:e Betreiber:in eines TOR-Nodes nicht einer Identifikationspflicht unterstellt wird – z. B. indem die Schwelle für das Auferlegen der Identifikationspflicht auf 1 Mio. Nutzer:innen angehoben wird.
Wären Betreiber:innen von TOR-Nodes von der Identifikationspflicht erfasst, würde dies fundamentale Grundrechte wie das Recht auf Privatsphäre und die informationelle Selbstbestimmung (Art. 13 BV, Art. 8 EMRK), die Meinungs- und Informationsfreiheit (Art. 16 BV, Art. 10 EMRK) gefährden. Ebenso würde das datenschutzrechtliche Prinzip der Datensicherheit (Art. 8 DSG) komplett unterlaufen. Diese Eingriffe in national und international geschützte Rechtsansprüche sind nicht hinzunehmen.
Dieser potentielle Angriff auf die genannten Grundrechte ist hochproblematisch und setzt ein politisches Statement: Die Schweiz bewegt sich weg von Grundrechtsschutz hin zum hochgerüsteten Überwachungsstaat.

Antrag: Es muss sichergestellt werden, dass Technologien wie TOR oder I2P nicht vom Anwendungsbereich der VÜPF erfasst sind.

Art. 16h Abs. 2

Art. 16h Abs. 2 des Entwurfs definiert einen öffentlichen WLAN-Zugang als professionell, wenn mehr als 1'000 Endbenutzer:innen den Zugang nutzen können. Der erläuternde Bericht führt dazu aus, dass «nicht die tatsächliche Anzahl, die gerade die jeweiligen WLAN-Zugänge benutzt» entscheidend ist, sondern «die praktisch mögliche Maximalanzahl (Kapazität).» Diese Auslegung ist viel zu breit und schafft untragbare Risiken für die FDA in Kombination mit Art. 19 Abs. 2 VE-VÜPF: Gemäss diesem Artikel trägt die das WLAN erschliessenden FDA die Verantwortung zur Identifikation der Nutzer:innen. Die Regelung führt also dazu, dass FDA, die einen Vertrag haben mit «Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen» (PZD), sehr schnell für die Identifikation der Endnutzer:innen ihrer Vertragspartner zuständig sind. Diese Regelung ist unsinnig und schlicht nicht umsetzbar.

Technisch gesehen ist es trivial, ein Netzwerk so zu konfigurieren, dass es potenziell 1'000 gleichzeitige Nutzer:innen zulassen kann, etwa durch die Nutzung mehrerer Subnetze (z.B. 192.168.0.0/24 bis 192.168.3.0/24), die Aggregation von IP-Adressbereichen (z.B. 192.168.0.0/22) oder der Verwendung von IPv6. Bereits mit handelsüblichen Routern für den Privatkundenmarkt könnte somit nahezu jeder Internetanschluss in der Schweiz unter diese Regelung fallen. Damit würden FDA unverhältnismässige Pflichten auferlegt, da die Unterscheidung nicht mehr anhand der Funktion des Netzwerks erfolgt. Ein privates offenes WLAN, das gemäss bisherigem Merkblatt nicht unter diese Regelung fällt, könnte nun als professionelles Netz klassifiziert werden.

Art. 16h Abs. 2 ist daher ersatzlos zu streichen, und die bestehende Regelung ist beizubehalten: FDA resp. Anbieterinnen von öffentlichen WLAN-Zugängen dürfen nur unter einer Identifikationspflicht stehen, wenn die PZD, die den Zugang der FDA nutzt, «professionell betrieben» ist – und zwar nach der aktuellen Auslegungsform (s. Erläuternder Bericht zur (letzten)Totalrevision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs):

«Mit «professionell betrieben» ist gemeint, dass eine FDA oder eine auf öffentliche WLAN-Zugangspunkte spezialisierte IT-Dienstleisterin den technischen Betrieb des öffentlichen WLAN-

Zugangspunktes durchführt, die dies auch noch für andere öffentliche WLAN-Zugangspunkte an anderen Standorten macht. Wenn eine natürliche oder juristische Person an ihrem Internetzugang selbst einen öffentlichen WLAN-Zugangspunkt technisch betreibt und diesen Zugang Dritten zur Verfügung stellt, muss die FDA, die den Internetzugang anbietet, keine Identifikation der Endbenutzenden sicherstellen.»

So wird sichergestellt, dass FDA nicht unmöglich umzusetzenden Pflichten unterstellt werden.

Antrag: Streichung der Ausführung im erläuternden Bericht. Das Kriterium «professionell betrieben» ist nach der bislang geltenden Regelung zu verstehen. Art. 16h Abs. 2 ist ersatzlos zu streichen und im Zusammenhang mit Art. 19 Abs. 2 ist auf die aktuelle Definition von «professionell betrieben» abzustellen.

Art. 16b Abs. 2, Art. 16f Abs. 3, Art. 16g Abs. 2

Bei Konzernen knüpft die VE-VÜPF nicht mehr an die Umsatz- und Nutzer:innenzahlen des betroffenen Unternehmens an, neu sind die Zahlen des Konzerns ausschlaggebend für eine Hoch- oder Herunterstufung. Die Begründung, dies diene der Vereinfachung, ist unlogisch und irreführend: Unternehmen müssen ihre Zahlen ohnehin produktbezogen ausweisen, die nötigen Daten liegen also längst vor. Das Argument, die Zusammenfassung der Zahlen führe zu einer Vereinfachung, ist falsch.

Antrag: Streichung des «Konzerntatbestand» und Beibehaltung der bestehenden Regelung.

Art. 19 Abs. 1

Die Einführung einer Pflicht zur Identifikation von Teilnehmenden für neu die grosse Mehrheit der AAKD – erfasst sind die AAKD mit reduzierten und mit vollen Pflichten – widerspricht direkt der Regelung des BÜPF, welche eine solche Pflicht nur für sehr wenige AAKD vorsieht. Durch die neuen Schwellenwerte zur Einstufung findet eine beachtliche Ausweitung der Identifikationspflicht statt.

Die Einführung einer Pflicht zur Identifikation widerspricht zudem den Grundsätzen des DSG, insbesondere jenem der Datensparsamkeit, indem es Unternehmen zwingt, mehr Daten zu erheben als für ihre Geschäftstätigkeit nötig, wodurch insbesondere der Grundrechtsschutz von Nutzer:innen in der Schweiz massiv beeinträchtigt wird. Die Identifikationspflicht greift immens in das Recht auf informationelle Selbstbestimmung ein und hält einer Grundrechtsprüfung nach Art. 36 BV schon allein aufgrund ihrer Unverhältnismässigkeit nicht stand.

Bezüglich einschneidender Pflichten, die potentiell schwere Grundrechtseingriffe bedeuten – wie es bei Identifikationspflichten zweifellos der Fall ist – muss Rechtsetzung in jedem Fall mit äusserster Sorgfalt und unter strenger Beachtung des Verhältnismässigketisgebots erfolgen. Ausserdem darf sich eine solche Pflicht nicht über gesetzliche Vorgaben, wie in diesem Fall vom BÜPF vorgegeben, hinwegsetzen.

Durch die breite Auferlegung einer solchen Pflicht werden datenschutzfreundliche Unternehmen bestraft, da ihr Geschäftsmodell untergraben und ihr jeweiliger Unique Selling Point (USP), der oftmals just in der Datensparsamkeit und einem hervorragenden Datenschutz liegt, zerstört wird.
Statt der neuen Identifikationspflicht muss weiterhin die Übergabe der bereits vorhandenen Daten genügen. Nur so können datenschutzrechtliche Vorgaben und die Rechte Betroffener gewahrt werden.

Antrag: Streichung «AAKD mit reduzierten Pflichten» oder Änderung zur Pflicht zur Übergabe aller erhobenen Informationen, aber OHNE Einführung einer Pflicht zur Identifikation von Teilnehmenden.

Art. 18

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinaus geht, untragbar für KMU. Art. 18 Abs. 3 ist zu streichen.

Antrag: Streichung Teil «Anbieter mit reduzierten Pflichten»

Art. 19 Abs. 2

Das Kriterium «professionell betrieben» ist nach der bestehenden Regelung auszulegen (s. vorstehen). Es sei ausserdem darauf hingewiesen, dass sich aus dieser Regelung eine vertragsrechtliche Problematik zwischen den FDA und den PZD ergeben würde, die nicht tragbar ist.

Antrag: Auslegung des Kriteriums «professionell betrieben» nach der bestehenden Regelung und nicht i. S. v. Art. 16h Abs. 2.

Art. 21 Abs. 1 lit. a

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher aus Art. 21 Abs. 1 lit. a zu streichen.

Antrag: Streichung

Art. 22

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 22 ist daher beizubehalten.

Antrag: beibehalten

Art. 11 Abs. 4

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. AAKD mit reduzierten Pflichten sind daher von den Pflichten nach Art. 11 zu befreien und Art. 11 Abs. 4 ist zu streichen.

Antrag: Streichung

Art. 16b

Wie bereits zu Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 16b (AAKD mit reduzierten Pflichten) ist ersatzlos zu streichen.

Antrag: Streichung

Art. 31 Abs. 1

Wie bereits bei Art. 16e bis 16f dargelegt ist, ist alles, was über eine Duldungspflicht hinausgeht, untragbar für KMU. AAKD mit reduzierten Pflichten sind daher von allen Pflichten nach Art. 31 zu befreien.

Antrag: Streichung Teil «Anbieter mit reduzierten Pflichten»

Art. 51 und 52

Wie bereits bei Art. 16e bis 16f dargelegt, soll die bestehende zweistufige Aufteilung beibehalten werden. Art. 51 und 52 sind daher beizubehalten.

Antrag: beibehalten

Art. 60a

Rückwirkende Massnahmen sind aus verfassungsrechtlicher Sicht mit grosser Skepsis zu beurteilen. Durch die neue Massnahme aus Art. 60a kann eine anordnende Behörde laut den Erläuterungen bewusst auch falsch-positive Ergebnisse herausverlangen. Dies birgt das Risiko der Vorveruteilung objektiv unschuldiger Personen und verstösst somit gegen die Unschuldsvermutung und gegen den datenschutzrechtlichen Grundsatz der Richtigkeit von Daten. Art. 60a ist zu streichen.

Antrag: Streichung des Artikels

Art. 42a und 43a

Die Art. 42a und 43a führen neu die Abfragetypen «IR_59» und «IR_60» ein, über die sensible Daten automatisiert abgefragt werden können. Sie verlangen von Anbietern, dass sie jederzeit Auskunft geben können bezüglich des letzten vergangenen Zugriffs auf einen Dienst, inklusive eindeutigem Dienstidentifikator, Datum, Uhrzeit und IP-Adresse. Auch für das Auferlegen diese Pflicht gilt die fragliche Schwelle von 5'000 Nutzer:innen. Erfasst ist somit nahezu die gesamte AAKD-Landschaft der Schweiz.

Das Problem liegt darin, dass die «IR_»-Abfragen zu Informationen nach Art. 42a und 43a neu automatisiert abgerufen werden können – im Gegensatz zu den «HD_»- (historische Daten) und «RT-» (Echtzeitüberwachung) Abfragen, die strengeren Regeln und einer juristischen Kontrolle unterliegen.

Bei den «IR_59»- und «IR_60»-Abfragen handelt es sich allerdings um sensible Informationen wie etwa das Abrufen einer IP-Adresse. Solche Informationen mussten bislang zurecht über strengere Abfragetypen eingeholt werden. Es ist nicht nachvollziehbar, warum Abfragen nach IR_59 und IR_60 weniger strengen Regeln unterworfen werden sollen als die für die ursprünglichen Zugriffe selber. Hinzu kommt, dass sich aus dem Verordnungstext keine Limite für die Frequenz der Stellung dieser automatisierten Auskünfte ergibt. Unternehmen sind daher nur unzulänglich geschützt vor missbräuchlichen Anfragen und vor Kosten, die ihnen durch die Pflicht, diese Auskünfte automatisch weiterzugeben, entstehen wird.

Künftig könnten so umfangreiche Informationen über die neuen Abfragetypen beschafft werden, die bislang zurecht den strengeren Regeln der rechtlich sichereren Informations-/Überwachungstypen «HD_» und «RT_» unterworfen waren. «IR_59» und «IR_60» ermöglichen damit nahezu eine Echtzeitüberwachung des Systems, ohne den erforderlichen Kontrollen dieser invasiven Überwachungstypen unterworfen zu sein.

Die Entwicklung, dass mittels «IR_»-Abfragen neu auch personenbezogene sensible Nutzungsdaten eingeholt werden können, widerspricht der Logik der unterschiedlichen Abfragetypen und öffnet Tür und Tor für missbräuchliche Abfragen und eine Echtzeitüberwachung von Millionen von Nutzer:innen. Auch hier stehen grundrechtlich geschützte Ansprüche auf dem Spiel, die mit einer solchen Regelung auf nicht nachvollziehbare Weise untergraben und missachtet werden.

Ebenfalls scheint der Wortlaut darauf abzuzielen, dass AAKD die vorgeschriebenen Informationen liefern müssen, und nicht mehr nur jene Daten, die bei ihr ohnehin vorhanden sind. Die AAKD müssten künftig gewisse Datenkategorien systematisch erheben, um dieser Pflicht nachzukommen.
Art. 27 Abs. 2 BÜPF erklärt allerdings, dass AAKD «auf Verlangen die *ihnen zur Verfügung stehenden* Randdaten des Fernmeldeverkehrs der überwachten Person liefern» müssen. Bei einer dahingehenden Auslegung des Bestimmungen bedeutete dies einen weiteren Verstoss gegen das BÜPF.

Unter rechtsstaatlichen Gesichtspunkten gilt es ausserdem die geplante Schwächung der Institution des Zwangsmassnahmengerichts auf das Schärfste zu kritisieren. Mit der Schaffung der zwei neuen Auskunftstypen, die mittels einfacher Auskunftsanfrage automatisch abgerufen werden können, werden rechtliche Kontrollmechanismen wie das Zwangsmassnahmengericht umgangen und der Einflussbereich der Staatsanwaltschaft noch weiter ausgebaut. Art. 42a und 43a sind daher vollumfänglich zu streichen.

Antrag: Streichung der Artikel

Art. 50a

Art. 50a sieht vor, dass Anbieter:innen verpflichtet werden, die von ihnen selbst eingerichtete Verschlüsselung jederzeit wieder aufzuheben. Auch diese Pflicht soll eine Vielzahl neuer Unternehmen erfassen: Betroffen sind nicht mehr nur FDA (Art. 26 BÜPF) und ausnahmsweise AAKD (Art. 27 BÜPF), sondern sämtliche Anbieter:innen mit mehr als 5'000 Nutzer:innen. Im Ergebnis wäre fast die gesamte Schweizer AAKD-Branche betroffen (kaum ein Produkt ist lebensfähig mit weniger als 5'000 Teilnehmer:innen).

Die Ausdehnung dieser Pflicht auf AAKD stellt eine erhebliche und vom Gesetz nicht gedeckte Ausweitung der bisherigen Verpflichtungen dar: Es findet keine Einzelfallprüfung statt und die AAKD werden dieser Pflicht unterworfen, auch wenn sie keineswegs «Dienstleistungen von grosser

wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten», was jedoch gesetzliche Vorgabe ist (Art. 27 Abs. 3 BÜPF).

Problematisch ist zudem, dass aufgrund dieser Vorgabe Anbieter:innen ihrer Verschlüsselungen so konfigurieren müssen, dass sie von ihnen aufgehoben werden können – eine durch Anbieter:innen aufhebbare Verschlüsselung reduziert die Wirksamkeit der Verschlüsselung allerdings in jedem Fall. Dies führt zu schwächeren Verschlüsselungen und der Abnahme der Sicherheit von Kommunikationsdiensten.

Daraus ergibt sich eine Grundrechtsproblematik von erheblicher Tragweite: Das Verhältnismässigkeitsgebot aus Art. 36 BV kann nicht eingehalten werden, weil das Resultat – die Schwächung der Verschlüsselung des beinahe gesamten Schweizer Online-Ökosystems – in keiner Weise in einem angemessenen Verhältnis zur beabsichtigten Vereinfachung der Behördenarbeit steht. Die Interessenabwägung darf hier nicht zuungunsten der Grundrechtsträger:innen erfolgen, da es sich bei deren Interessen um solche von fundamentalem Gewicht – dem Zugang zu sicherer Kommunikation und damit direkt verbunden dem Recht auf freie Meinungsäusserung – handelt.

Wichtig ist, dass Verschlüsselungen, die auf dem Endgerät der Nutzer:innen erfolgen – also End-zu-End-Verschlüsselungen – nicht unter die Pflicht zur Aufhebung gemäss Art. 50a VE-VÜPF fallen dürfen. Diese Form der Verschlüsselung liegt ausschliesslich in der Sphäre der Nutzer:innen und es wäre untragbar, die Pflicht zur Aufhebung von Verschlüsselungen in dieser Sphäre zu verlangen. Die Anbieter:innen dürfen daher nicht dazu verpflichtet werden, diese Inhalte zu entschlüsseln und zugänglich zu machen. Im Gegensatz dazu betrifft die Transportverschlüsselung «lediglich» die Verbindung zwischen Client und Server und kann von Anbieter:innen kontrolliert werden. Es ist wichtig, dass diese technischen Unterscheidungen und unterschiedlichen Schutzwirkungen und -richtungen bei rechtlichen Umsetzungen beachtet werden. Wir begrüssen die Klarstellung im erläuternden Bericht, dass die End-zu-End-Verschlüsselung vom Anwendungsbereich ausgenommen ist. Es muss jedoch ebenso klar sein, dass das ganze Endgerät von Nutzer:innen aus dem Anwendungsbereich von Art. 50a VE-VÜPF ausgenommen ist.

Es braucht im Übrigen auch eine Klarstellung darüber, dass eine rückwirkende Möglichkeit zur Aufhebung klar ausgeschlossen ist. Eine solche würde de facto eine Vorratsdatenspeicherung verschlüsselter Inhalte und Keys darstellen, die mit dem Prinzip der Datenminimierung (Art. 6 Abs. 3 DSG) und dem Schutz der Privatsphäre (Art. 13 BV) unvereinbar ist.

Antrag: Streichung der «Anbieterin mit reduzierten Pflichten» aus dem Anwendungsbereich sowie eine Klarstellung darüber, dass die Aufhebung von Verschlüsselungen auf dem Endgerät der Nutzer:innen sowie eine rückwirkende Verpflichtung zur Aufhebung ausgeschlossen sind.

Bemerkungen zu einzelnen Artikeln der *VD-ÜPF*

Art. 14 Abs. 3 VD-ÜPF

Wie bereits bei Art. 16e bis 16f VE-VÜPF angesprochen ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer:innen) unverhältnismässig und wirtschaftlich nicht tragbar, was das Einführen von Fristen obsolet werden lässt. Der Absatz ist daher ersatzlos zu streichen.

Antrag: Streichung

Art. 14 Abs. 4 VD-ÜPF

Die neue Formulierung erweitert den Anwendungsbereich und erhöht die Anzahl der Unterworfenen AAKD – da auch AAKD mit reduzierten Pflichten erfasst sind – massiv. Dies ist wie bereits ausgeführt weder durch das BÜPF gedeckt noch mit dem Zweck der Revision, KMU zu schonen, in Übereinstimmung zu bringen.

Antrag: Änderung des Begriffs «AAKD mit minimalen Pflichten» zu «AAKD ohne vollwertige Pflichten»

Art. 20 Abs. 1 VD-ÜPF

Wie bereits bei Art. 16e bis 16f VE-VÜPF angesprochen, ist ein aktives Tätigwerden für alle AAKDs (auch für solche mit mehr als 5'000 Nutzer:innen) unverhältnismässig und nicht wirtschaftlich tragbar. Der Teilsatz ist zu streichen.

Antrag: Streichung des Teilsatzes «und die Anbieterinnen mit reduzierten Pflichten»

Schlussbemerkung

Trotz des Umfangs dieser Stellungnahme gilt: Das Ausbleiben einer expliziten Bemerkung zu einzelnen Bestimmungen bedeutet keine Zustimmung der Digitalen Gesellschaft. Die Ablehnung der Revision bleibt vollumfänglich bestehen.

Freundliche Grüsse

Erik Schönenberger
Geschäftsleiter