

Eidgenössisches Justiz- und  
Polizeidepartement EJPD  
Bundeshaus West  
3003 Bern

Ausschliesslich per E-Mail an:  
[ptss-aemterkonsultationen@isc-ejpd.admin.ch](mailto:ptss-aemterkonsultationen@isc-ejpd.admin.ch)

6. Mai 2025

**Teilrevisionen zweier Ausführungserlasse zur Überwachung des Post- und Fernmeldeverkehrs (VÜPF, VD-ÜPF): Stellungnahme economisesuisse**

Sehr geehrte Damen und Herren

Mit Schreiben vom 29. Januar haben Sie uns eingeladen, zu den im Betreff genannten Vorlagen Stellung zu nehmen. Wir danken Ihnen für diese Möglichkeit. Als Dachverband der Wirtschaft bündelt economisesuisse die Interessen von rund 100 Branchenverbänden, 20 Handelskammern und insgesamt etwa 100'000 Schweizer Unternehmen.

**economisesuisse lehnt die vorgeschlagenen Anpassungen an VÜPF und VD-ÜPF mit Nachdruck ab.** Die Vorlage lässt jegliche Verhältnismässigkeit vermissen und es ist im hohen Masse fragwürdig, ob die gesetzlichen Grundlagen für die vorgeschlagenen Anpassungen auf Verordnungsstufe überhaupt gegeben sind. Im Spannungsfeld zwischen Persönlichkeitsschutz, Wirtschaftsfreiheit und Sicherheit muss Fernmeldeüberwachung auf einer klaren gesetzlichen Grundlage basieren, die den Willen des Gesetzgebers und die Auslegung der Gerichte klar widerspiegelt. Solche Überwachungsmassnahmen müssen unterschiedliche Interessen abwägen und dabei Rücksicht auf die wirtschaftliche Machbarkeit, die Wettbewerbsfähigkeit, den Datenschutz und die Cybersicherheit nehmen. All diese Aspekte sind in den vorliegenden Ausführungserlassen zu Gunsten eines sehr weitgehenden Überwachungsanspruchs des Staates zurückgedrängt. Dies war aus unserer Sicht nicht die Absicht des Gesetzgebers. Wir fordern deshalb die Rückweisung und umfassende Überarbeitung der Vorlagen. Sie sind grundlegend neu zu gestalten, mit Rücksicht auf die Grundrechte und den internationalen Kontext, einem gesetzeskonformen Kategorisierungsmodell und ohne massive Mehrbelastung der Unternehmen. Diese grundlegende Korrektur ist zwingend notwendig, um eine zweckdienliche Fernmeldeüberwachung ohne massiven Kollateralschaden zu schaffen.

Weitere Ausführungen zu unserer Position finden sie nachfolgend.

**1 Grundsatzkritik:**

**Auch bei der Sicherheit im digitalen Raum muss Verhältnismässigkeit der Massstab staatlicher Eingriffe sein.** Sicherheitspolitisch motivierte Eingriffe in Grundrechte müssen verhältnismässig sein. Das bedeutet: Sie dürfen nur erfolgen, wenn sie einem legitimen öffentlichen Interesse dienen,

geeignet und erforderlich sind und die Interessenabwägung zugunsten des öffentlichen Wohls ausfällt. Gerade in sicherheitsrelevanten Bereichen ist Zurückhaltung geboten – Eingriffe dürfen nicht über das hinausgehen, was zum Schutz der Gesellschaft zwingend nötig ist. Eine freiheitlich-demokratische Ordnung lebt davon, dass der Staat auch unter Druck rechtsstaatlich handelt.

Der Staat trägt Verantwortung für die Sicherheit seiner Bevölkerung – auch im digitalen Raum. Er muss dazu in der Lage sein, schwere Straftaten im Internet wirksam zu verfolgen. Doch es gilt auch hier: Sicherheitsmassnahmen dürfen die Freiheitsrechte nicht unverhältnismässig einschränken. Die digitale Strafverfolgung muss rechtsstaatlich eingebettet und zielgerichtet sein, nicht pauschal oder flächendeckend, wie dies in den Vernehmlassungsvorlagen leider der Fall ist. Nur so lässt sich ein verantwortungsvoller Ausgleich zwischen Freiheit und Sicherheit wahren – auch in einer zunehmend vernetzten Gesellschaft. Dies ist mit der vorliegenden Vorlage nicht gewährleistet. Letztlich fehlt auch ein Nachweis, dass die aktuellen Mittel und Kompetenzen der Strafuntersuchungsbehörden nicht mehr ausreichen, um eine effiziente Aufgabenerfüllung zu ermöglichen.

## **2 Standortvorteile nicht unnötig gefährden**

Nebst diesen grundlegenden Kritikpunkten ist aus Sicht der Wirtschaft vor allem darauf hinzuweisen, dass die weitgehenden Forderungen der Vorlagen einen erheblichen Standortnachteil für unser Land zur Folge hätten. Die Schweiz ist ein hochkompetitiver Technologiestandort, der sich gerade auch im Startup-Bereich als Biotop der «Privacy Champions» international behauptet. Diese Dienste legen besonderen Wert auf Datensicherheit und besetzen damit ein wachstumsträchtiges Marktsegment. Auch etablierte Firmen finden hierzulande bisher günstige Rahmenbedingungen vor. International tätige Dienstleister versorgen nicht nur die Schweizer Firmen und Bevölkerung mit kostengünstigen, modernen und sicheren OTT-Diensten, sie stellen hierzulande auch mehrere Tausend Arbeitsplätze bereit, bilden Fachkräfte aus und liefern Steuersubstrat ab. Mit einer Ausweitung der fernmelderechtlichen Überwachungspflichten, wie sie die Vernehmlassungsvorlagen beinhalten, wären die günstigen Rahmenbedingungen für solche Dienstleister in der Schweiz akut gefährdet. Der technische, administrative und infrastrukturelle Mehraufwand wäre besonders für KMU enorm und liesse sich kaum mit entsprechenden Vorteilen für den Strafvollzug und die Sicherheit der Bevölkerung rechtfertigen. Wir sind dezidiert der Ansicht, dass eine schlankere Regulierung mit weniger erfassten Unternehmen und risikobasierten Pflichten mindestens vergleichbaren Nutzen für die Strafvollzugsbehörden bringt, wie die breite Vorratsdatenspeicherung, allerdings ohne, dass ein massiver wirtschaftlicher Kollateralschaden entsteht.

## **3 Geltungsbereich FDA und AAKD: Es braucht endlich gesetzeskonforme Ausführungsbestimmungen**

Knackpunkt der Vorlagen sind vor allem die neu definierten Kategorien und Mitwirkungspflichten in der VÜPF. Dabei halten wir die umfassende Regulierung von AAKD für besonders problematisch. Sie ist einerseits so nicht vom Gesetzgeber vorgesehen, resp. sprengt den Rahmen der gesetzlichen Verweisungsnorm im BÜPF. Dieser Auffassung sind bekanntlich auch das Bundesgericht und das Bundesverwaltungsgericht, die sich in den letzten Jahren mehrfach mit der Thematik befasst haben<sup>1</sup>. Andererseits folgen die Definitionen nicht den einschlägigen internationalen Standards<sup>2</sup>, bspw. indem die Ausführungsbestimmungen auf Mehrwegkommunikation über die interpersonelle Kommunikation hinaus ausgeweitet werden.

Darüber hinaus wirken die Abgrenzungen und Schwellenwerte der Kategorien nach Umsatz und Anzahl Kunden beliebig gewählt, auch wenn dies bereits im geltenden Recht so geregelt ist. Der

<sup>1</sup> Siehe bspw. Bundesgerichtsurteil 2C\_544/2020 und Urteil [A-5373/2020](#) des Bundesverwaltungsgerichts.

<sup>2</sup> Siehe bspw.

räumliche Geltungsbereich bleibt derweil unklar, also die Betroffenheit von Diensteanbietern ausserhalb der Schweiz und der Datenzugriff der Behörden, insb. wenn es sich um weitere Daten als «nur» Randdaten handelt. Insgesamt braucht es aus unserer Sicht ein pragmatischeres Konzept, das mit etablierten Standards und technischen Richtlinien im Einklang steht.

#### **4        Datenschutz und Cybersicherheit nicht aufs Spiel setzen**

Neben der Breite ist auch die Tiefe der angedachten Regulierung problematisch. Die rückwirkenden, pauschalen Überwachungspflichten, die auch vielen OTT-Anbietern auferlegt würden, hätten für die betroffenen Firmen empfindliche Kostenfolgen. In diesem Zusammenhang ist vor allem die Pflicht einer rund um die Uhr besetzten Pikett-Stelle zu nennen oder die generell notwendige, aufwändige Hardware-Infrastruktur. Besonders einschneidend wären jedoch die Folgen für die Bevölkerung, die man mit der vorgeschlagenen Stossrichtung faktisch einer Massenüberwachung mit Vorratsdatenspeicherung aussetzen würde, bspw. durch weitreichende Aufbewahrungs- und Identifikationspflichten. Dies ist mit dem politischen Willen, einen angemessenen und funktionalen Datenschutz in der Schweiz zu schaffen (bspw. Grundsatz der Datenminimierung im DSG), der gerade in der Privatwirtschaft mit erheblichem Aufwand umgesetzt wird, dies nicht zu vereinbaren. Hinzu kommt, dass eine umfassende Vorratsdatenspeicherung auf europäischer Ebene schon mehrfach durch die Gerichte als unverhältnismässig und damit unzulässig eingestuft wurde. Zu guter Letzt muss davon ausgegangen werden, dass die technische Umsetzung der Überwachung und Vorratsdatenspeicherung auch zu einer Schwächung der Cybersicherheit der Unternehmen führt. «Hintertüren» und andere Vorkehrungen wie Entschlüsselungspflichten, welche den Zugriff der Behörden gewährleisten sollen, stellen nämlich auch Angriffsvektoren für Dritte dar, seien sie kriminell, nachrichtendienstlich oder gar kriegerrisch motiviert.

Insgesamt braucht es folglich auch hier klar mehr Augenmass. Die Bedürfnisse der Justizvollzugsbehörden müssen zwingend mit den Interessen der Unternehmen und der breiten Bevölkerung abgewogen werden.

Wir fordern damit eine grundlegende Überarbeitung der Vorlage unter Berücksichtigung unserer diversen und grundlegenden Kritikpunkte.

Bei Rückfragen stehen wir jederzeit gerne zur Verfügung.

Freundliche Grüsse

economiesuisse

Erich Herzog  
Mitglied der Geschäftsleitung,  
Bereichsleiter Wettbewerb & Regulatorisches

Lukas Federer  
Stv. Bereichsleiter Energie,  
Infrastruktur & Umwelt