04-12-2025

Dear Mr. Federal Councilor Jans,

We, the undersigned human and digital rights organisations, would like to share our serious concerns regarding to the extension of general and indiscriminate retention of telecommunications and internet traffic data as part of the revision of the Swiss Ordinance on the Surveillance of Post and Telecommunications Traffic (VÜPF).

We urge you to amend the proposed Ordinance substantially for the following reasons:

1. Violation of the fundamental rights to privacy and data protection

As the Swiss Federal Supreme Court has rules, the case law of the Court of Justice of the European Union (CJEU) on privacy and data protection is relevant to Switzerland.[1] In declaring the EU Data Retention Directive (Directive 2006/24/EC) invalid in 2014, the CJEU holds that the general and indiscriminate retention of communications data by electronic communications service providers constitutes a disproportionate interference with the rights to data protection and privacy, guaranteed in Articles 7 and 8 of the Charter of Fundamental Rights.[2] The reason mass data retention is incompatible with European legal principles is that it targets the entire population, without differentiation or concrete suspicion of criminality. Furthermore it severely undermines the principle of confidentiality of communications, which is especially important in today's context of very widespread use of electronic communication means and their critical importance in people's everyday lives.

The proposed Ordinance, which significantly extends the obligation of metadata retention for large communications service providers[3] and imposes user identification requirements on virtually all service providers[4], would dramatically increase the amount of personal data retained and thus, further intensify the (already serious) interference with the right to privacy and data protection. Such level of surveillance is unacceptable in a democratic society.

---

[1] in BGer 1C_598/2016, E. 8.2.2.
[2] Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Luxembourg, 8 April 2014.
[3] Over-the-top service providers classified in the highest tier (1 million users or annual turnover above 100 million CHF)
[4] Service providers with more than 5,000 users

2. Chilling effect on the exercise of other rights and freedoms

The CJEU has rightly described general and indiscriminate data retention as being likely to generate in the minds of the population the feeling of being under constant surveillance. This creates a climate of self-censorship. In addition to the expanded data retention regime, the draft Ordinance also imposes an obligation on most service providers in scope to "identify" their users "by appropriate means".

The lack of a forum to enjoy secure, private and anonymous communications free from government scrutiny chills people's exercise of freedom of speech, freedom of thought, and freedom of assembly and association. These fundamental rights are essential foundations of a pluralist, democratic society and vitally important for journalists, lawyers, human rights defenders and activists. The chilling effect generated by mass data retention and mandatory identification erodes democratic discourse and civic participation, in a time where they are direly needed.

3. Incompatibility with the European Convention on Human Rights (ECHR)

Switzerland, a party to the European Convention on Human Rights, is also bound by the jurisprudence of the European Court of Human Rights (ECtHR), which has consistently ruled that surveillance regimes constitute an interference in the right to privacy, and so must be comply with the principles of necessity and proportionality to be compatible with the Convention. They must include adequate protection against arbitrariness such as substantive and procedural safeguards, including substantive and procedural rules governing access to data and independent oversight mechanisms. .

The draft Ordinance would substantially weaken the legal protections against arbitrary or abusive law enforcement access to personal data: it allows access to subscriber information and IP addresses without prior authorisation by a court and mandates the automatic execution of law enforcement access requests, i.e. data disclosure without the intervention of service providers. This would be contrary to the ECtHR case-law (see *Benedik v Slovenia*[5]) which requires that national legislation offers sufficient safeguards against arbitrary interference with the rights guaranteed by Article 8 of the European Convention on Human Rights (ECHR).

4. Risk posed to Switzerland's adequacy status with the EU

Switzerland's current legislation, mandating the general and indiscriminate retention of all traffic and location data, already appears incompatible with EU privacy and data protection law, as per the CJEU's settled case-law (notably *Digital Rights Ireland*[6], *Tele2 Sverige*[7], *La Quadrature du Net*[8] and subsequent cases).

The increased level of surveillance proposed by the draft Ordinance would further weaken the level of adequate protection and increase the gap with EU standards. As per Article 3a (3) and (4) of

---

[5] https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-182455%22]}
[6] https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2255180
[7] https://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d573c52441e12b44d0a94dfc5b5bdfc5ce.e34KaxiLc3qMb40Rch0SaxyKbN90?text=&docid=186492&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=165644
[8] https://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2421304

Commission Implementing Decision 2016/2295[9], "*if interferences by Swiss public authorities responsible for national security, law enforcement or other public interests with the right of individuals to the protection of their personal data go beyond what is strictly necessary, or that there is no effective legal protection against such interferences*", Switzerland's adequacy status could be called into question.

5. **Cybersecurity risks**

An obligation put on almost all internet service providers to retain sensitive data of all their users creates huge security risks. Cyberattacks targeting the tele- and electronic communications sector are on the rise and impact the online safety and privacy of millions of people across the world, but also business and public administrations.[10] The draft Ordinance would increase the amount of data subject to such data breaches.

6. **Existence of less intrusive alternative measures**

Any interference or limitation on the exercise of the rights and freedoms created by data retention requirements must be deemed necessary, meaning that if other less intrusive measures exist and can reasonably achieve the same objectives, the measure at stake cannot be considered necessary and therefore lawful. Yet, independent studies have consistently failed to establish that indiscriminate data retention contributes in a meaningful way to crime prevention and prosecution compared to targeted retention.

Preservation orders ("quick-freeze"), issued under judicial control, can provide law enforcement with access to necessary information for a specific investigation without subjecting the entire population to mass surveillance.

In light of the above, we urge you to abandon any proposals for wide-ranging, blanket data retention obligations, privacy-effacing identification obligations, weakening of crucial legal safeguards and automatic data disclosures in the revision of the VÜPF Ordinance. **We recommend instead to align the Swiss legislation with the highest standards of protection set by both the Court of Justice of the European Union and the European Court of Human Rights.**

We remain available to answer any question you may have and trust that together, we can find rights-respecting solutions to legitimate public interest objectives.

Sincerely,

Digitalcourage (Germany)
Digitale Gesellschaft (Germany)
Digitale Gesellschaft (Switzerland)
Electronic Frontier Norway (Norway)
epicenter.works – for digital rights (Austria)
European Digital Rights (EDRi) (International)
Homo Digitalis (Greece)

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016D2295
[10] https://therecord.media/eight-telcos-breached-salt-typhoon-nsc
https://www.computing.co.uk/news/2025/security/salt-typhoon-caught-hacking-a-european-telco-says-darktrace
https://wisdiam.com/publications/recent-cyber-attacks-telcos/

Human Rights Watch (International)
Initiative für Netzfreiheit (Austria)
ISOC Switzerland Chapter
IT-Pol (Denmark)
Liga voor Mensenrechten (Flemish Human Rights League) (Belgium)
Privacy International (International)
Statewatch (international)
Taler Operations AG (Switzerland)