Partei für Rationale Politik, Allgemeine
Menschenrechte und Teilhabe
Vorstand
Stefan Thöni
Parkstrasse 7
6312 Steinhausen
stefan.thoeni@parat.swiss
parat.swiss

Stefan Thöni, Parkstrasse 7, 6312 Steinhausen

Eidg. Departement für Umwelt, Verkehr,
Energie und Kommunikation UVEK
Bundeshaus Nord
CH-3003 Bern

3. August 2025

Vernehmlassung zur Revision der Postverordnung

Sehr geehrte Damen und Herren

Wir bedanken uns für die Gelegenheit, unsere Vernehmlassungsantwort zur Revision der Postverordnung einreichen zu dürfen.

Formelles

Wir protestieren gegen die Anforderung an Vernehmlassungsantworten, ein Word-Dokument mitzuliefern. Dies ist für uns unmöglich, da wir weder Word noch eine kompatible Software, sondern LaTeX verwenden, um unsere Dokumente abzufassen. Zudem ist das Word-Format ein proprietäres Format und kein offener Standard.

Im Sinne der Barrierefreiheit liefern wir Ihnen eine HTML-Datei, welche Sie mit dem Browser öffnen können, bitten aber darum zukünftig von den Teilnehmer*innen der Vernehmlassung anstelle einer Word-Datei eine maschinenlesbare oder einfach zu kopierende Datei oder aber ein offenes, standardisiertes Format wie HTML, Textile oder Markdown zu anzufordern.

Zustellung der Briefpost

Wir sind der Meinung, dass die Zustellung von Briefen weiterhin im aktuellen geografischen und zeitlichen Umfang erfolgen muss, solange das Zivilrecht bei vielen wichtigen

Schreiben wie Kündigungen, Erklärungen, Mahnungen und gesetzlich vorgeschriebener Information auf den Zeitpunkt des Zugangs abstellt.

Es kann nicht sein, dass der Sender solcher zivilrechtlich fristwahrenden oder fristauslösenden Briefen zukünftig nicht mehr davon ausgehen kann, diese alle Adressaten zur rechten Zeit erreichen. Aus diesen Gründen lehnen wir die Änderungen in Art. 31 Abs. 1 sowie Art. 31a Abs. 3 und Art. 32 Abs. 1 ab, solange das Zivilrecht weiter auf den Zugang von Sendungen abstellt.

Elektronisches Zustellsystem

Ende-zu-Ende-Verschlüsselung

Aktuell werden fast täglich sensible Daten von den IT-Systemen von Unternehmen und Behörden jeder Grösse durch Angreifer gestohlen. Es besteht kein Anlass zur Annahme, dass die Post selbst bei höchsten Anstrengungen hiervon verschont bleiben könnte. Im Gegenteil wäre ein elektronisches Zustellsystem, auf welchem auch nur vorübergehend auf Inhalten von Postsendungen zugegriffen werden könnte, ein besonders verlockendes Ziel für kriminelle und staatliche Angreifer und zudem ein für die Bevölkerung und Wirtschaft der Schweiz inakzeptables Klumpenrisiko.

Aus diesem Grund muss für elektronische Zustellsystem zwingend die Ende-Zu-Ende-Verschlüsselung vorgeschrieben werden. Die Empfänger*in muss zu diesem Zweck einen öffentlichen Schlüssel beglaubigen lassen und bei der Post hinterlegen. Dazu sollte ein ähnliches Verfahren zur Anwendung kommen wie zur Erstellung der E-ID. Die Sender*in kann diesen Schlüssel abrufen, seine Authentizität prüfen und den Inhalt der elektronischen Sendung damit Verschlüsseln. Nur so ist sichergestellt, dass kein Angreifer auf bei der Post lagernde Inhalte zugreifen kann.

Dabei sollte festgeschrieben werden, dass die Ende-zu-Ende-Verschlüsselung nach einem offenen Standard erfolgen muss und nicht etwa durch eine proprietäre App der Post.

Automatisierter Abruf

Im Gegensatz zum hybriden System ist für das elektronische Zustellsystem nicht festgelegt, dass Sender*innen und Empfänger*innen diskriminierungsfrei und automatisiert mit ihren Fachanwendungen auf das elektronische Zustellsystem zugreifen können (Art. 35g e contrario). Dies sollte korrigiert werden.

Insbesondere sollte auch festgelegt werden, dass der nicht diskriminierende Zugang auch automatisiert erfolgen können muss, also keine Authentifizierungsverfahren gemäss Art. 35e Abs. 5 zum vorausgesetzt werden dürfen, die einen manuellen Schritt eines Menschen erfordern.

Zudem sollte vorgeschrieben werden, dass für den nicht diskriminierenden Zugang für Sender*innen und Empfänger*innen keine über das Versandentgelt hinausgehenden Kosten erhoben werden dürfen, die technische Dokumentation frei Verfügbar sein muss und das Anlegen und Freischalten eines entsprechenden Accounts auch für Einzelpersonen und kleine Vereine problemlos möglich sein muss.

Hybrides Zustellsystem

Da sich das hybride Zustellsystem nicht implementieren lässt ohne das die Inhalte von Briefen bei der Post zumindest vorübergehend im Klartext vorliegen und somit von kriminellen und staatlichen Angreifern gestohlen werden können, sollte auf dieses System gänzlich verzichtet werden.

Falls doch am hybriden Zustellsystem festgehalten wird, sollte zumindest festgeschrieben werden, dass es für besonders schützenswerte Daten im Sinne der Datenschutzgesetzgebung nicht verwendet werden darf.

Zudem sollten Empfänger*innen im Sinne der Selbstverantwortung und selbstbestimmten Kontrolle ihrer Personendaten die Möglichkeit haben, das hybride Zustellsystem nur für bestimmte Sender*innen freizugeben (Whitelisting) oder bestimmte Sender*innen, gerade auch Behörden, blockieren zu können (Blacklisting).

Haftung für Verletzungen des Postgeheimnisses

Die Verordnung sollte für Schäden aus der Verletzung des Postgeheimnisses, d.h. für den unerlaubten Zugriff auf Inhalten Postsendungen im elektronischen und hybriden Zustellsystem, sei es durch Insider*innen oder externe Angreifer*innen eine Haftung der Post vorsehen. Das Verschulden der Post für den unerlaubten Zugriff sollte gesetzlich unwiderlegbar fingiert werden, da aus dem Fakt des verbotenen Zugriffs bereits folgt, dass die Sicherheitsmassnahmen der Post ungenügend waren. Zudem sollte ein gesetzliche fingiertes Minimum des Schadens aus dem unerlaubten Zugriff auf Sendungsinhalten von 100 Franken pro Sendung festgeschrieben werden.

Freundliche Grüsse

Stefan Thöni