

LEARNING NUGGET DIGITALE SOUVERÄNITÄT 4. OKTOBER 2026

Wer hat den Schlüssel zu deinem Postfach?

Was ein verschlüsseltes Postfach wie Proton anders macht als ein normales, was trotzdem sichtbar bleibt und was Schweizer Recht, der Fall von 2021 und die geplante VÜPF-Revision dazu beitragen.

Von Rico Eberle, E-Learning-Experte für Weiterbildung und Gemeinderat in Dübendorf

RICO EBERLE · DIGITALE SOUVERÄNITÄT

Wer kann deine E-Mails lesen? Oft: der Anbieter selbst.



Video zum Beitrag

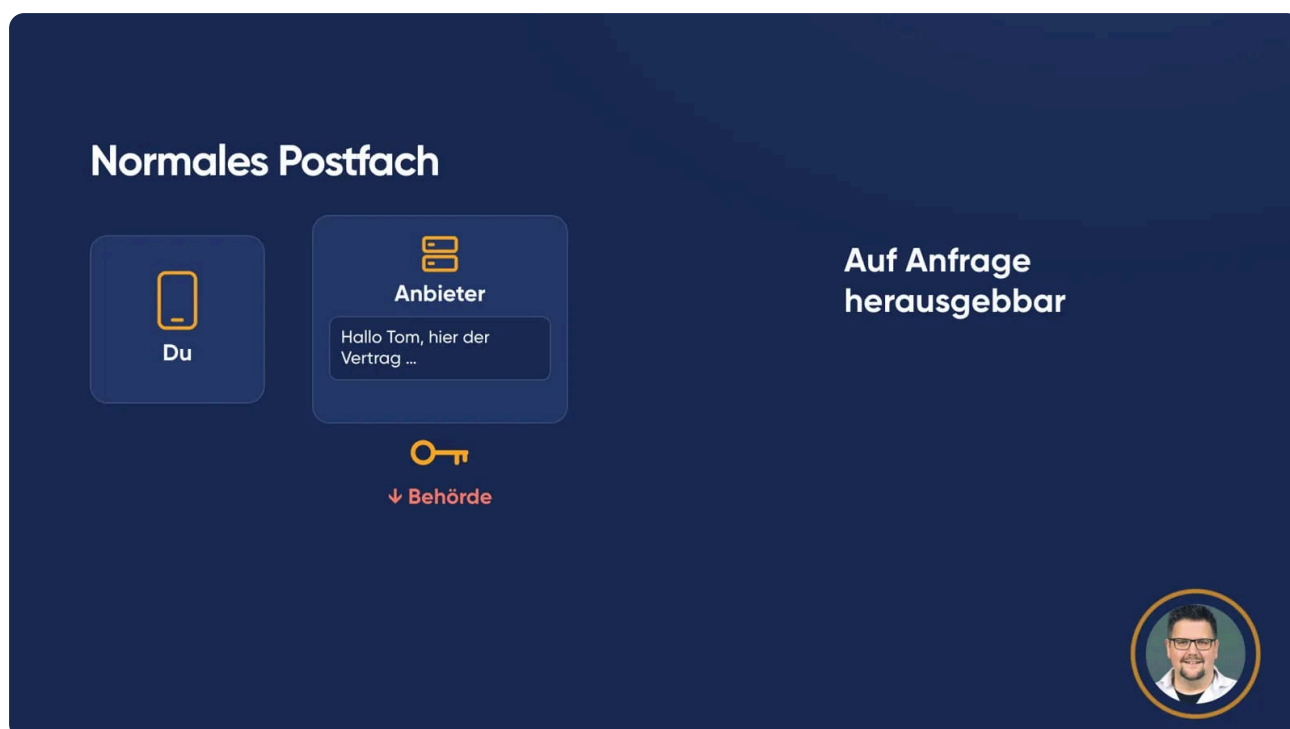
Dieses Learning Nugget gibt es als Video mit Transkript (1:41 Min.). QR-Code scannen oder Link öffnen:

ricoeberle.ch/blog/verschlusselfte-mail/

Wer kann deine E-Mails lesen? Bei den meisten Anbietern lautet die ehrliche Antwort: der Anbieter selbst. Verschlüsselte Postfächer versprechen etwas anderes. Was sie halten und wo die Grenzen liegen, zeige ich hier am Beispiel von Proton.

Normales Postfach: Der Anbieter hat den Schlüssel

Auch bei einem normalen Postfach liegen die Mails meist verschlüsselt auf dem Server. Den Schlüssel verwaltet aber der Anbieter. Er kann die Mails technisch lesen und durchsuchen, etwa für die Suche, für Spamfilter oder für Zusatzfunktionen. Und wenn eine Behörde mit einer gültigen Anordnung kommt, kann er sie herausgeben.



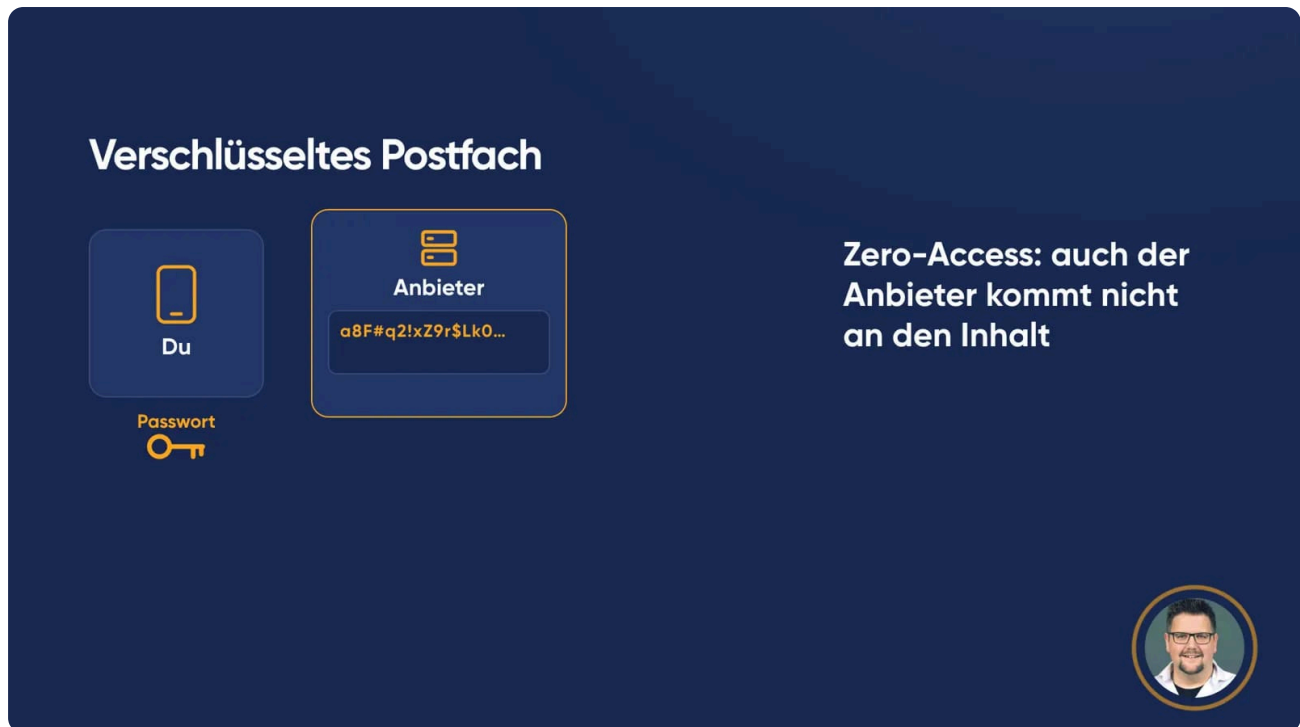
Beim normalen Postfach liegt der Schlüssel beim Anbieter. Er kann die Mails lesen und auf Anordnung herausgeben.

Verschlüsseltes Postfach: Der Schlüssel bleibt bei dir

Verschlüsselte Postfächer drehen das um. Der Schlüssel ist mit deinem Passwort geschützt, und das Passwort kennst nur du. Auf dem Server liegt nur Zeichensalat. Proton nennt das **Zero-Access-Verschlüsselung**: Selbst der Anbieter kommt nicht an den Inhalt.

Schreiben sich zwei Proton-Nutzer, geht es noch einen Schritt weiter. Dann ist die Mail **Ende-zu-Ende verschlüsselt**, also vom Gerät der Absenderin bis zum Gerät des Empfängers. Unterwegs und auf dem Server kann sie niemand lesen.

Vereinfacht: Hinter dem «Schlüssel» stecken bei Proton ein privater Schlüssel nach dem Open-PGP-Standard und das Passwort, das ihn schützt.



Gleiches Schema, umgekehrte Rollen: Der Schlüssel ist mit deinem Passwort geschützt, der Server sieht nur verschlüsselte Daten.

Was trotzdem sichtbar bleibt

Nicht alles ist geschützt. Laut Proton sind **Betreff, Absender und Empfänger** nicht Ende-zu-Ende verschlüsselt. Wer mit wem wann über welches Thema schreibt, ist also nicht im gleichen Mass geschützt wie der Inhalt.

Und Mails an normale Adressen, etwa an Gmail oder Outlook, sind ebenfalls nicht Ende-zu-Ende verschlüsselt. Ausnahme: Du schützt die Mail mit einem Passwort, das die Empfängerin auf einem anderen Weg erhält.

Was trotzdem sichtbar bleibt

Von	Lea	sichtbar
An	Tom	sichtbar
Betreff	Vertrag	sichtbar
 Inhalt verschlüsselt a8F#q2!xZ9r\$Lk0 Wm3...		

**An normale Adressen:
nicht Ende-zu-Ende,
ausser mit Passwort**



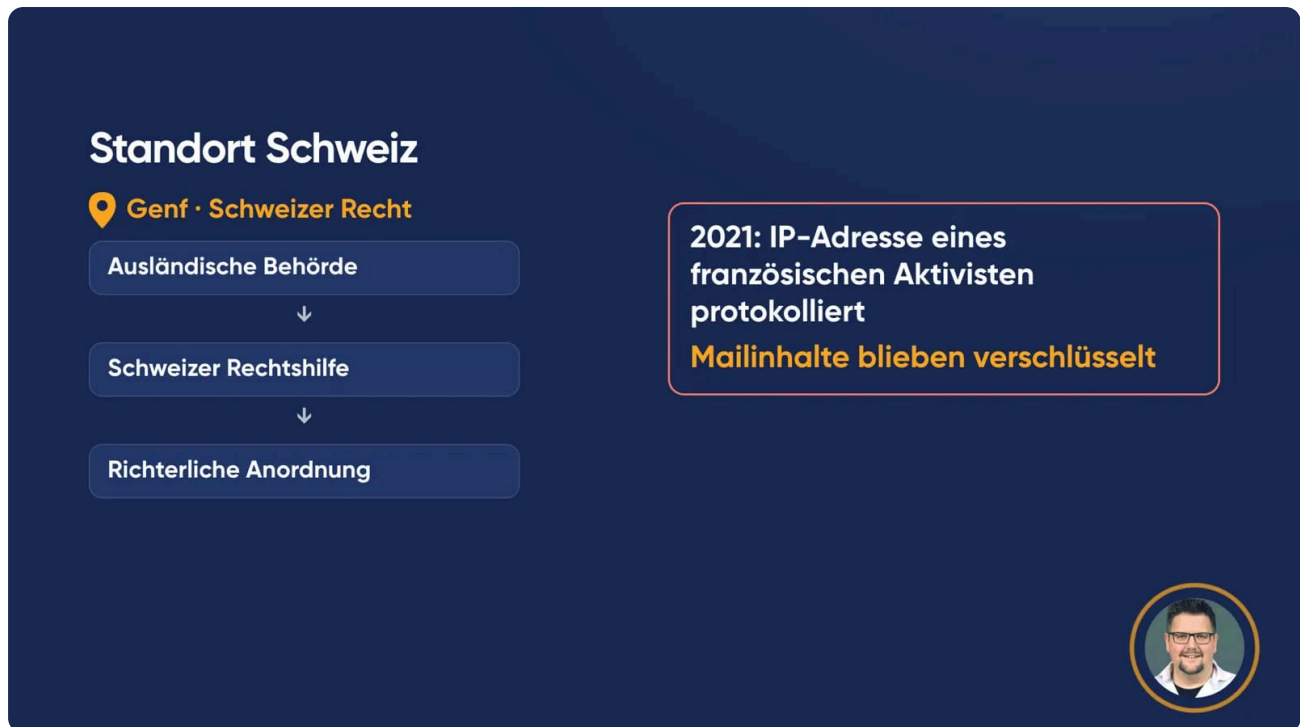
Der Inhalt ist geschützt, Absender, Empfänger und Betreff sind nicht Ende-zu-Ende verschlüsselt.

Standort Schweiz: Schutz, aber kein Freipass

Proton sitzt in Genf und untersteht Schweizer Recht. Ausländische Behörden können Proton nicht direkt zur Herausgabe zwingen; Art. 271 StGB verbietet die direkte Weitergabe an fremde Behörden. Sie müssen den Weg über die Schweizer Rechtshilfe gehen.

Auf eine verbindliche Anordnung nach Schweizer Recht muss Proton trotzdem Daten liefern. Das zeigt der Fall von 2021: Die französische Polizei schickte ihre Anfrage über Europol an die Schweizer Behörden. Diese verpflichteten Proton, die IP-Adresse eines französischen Aktivisten zu protokollieren. Proton musste das tun. Die Inhalte der Mails blieben verschlüsselt.

Wie oft das vorkommt, steht in Protons Transparenzbericht: 2025 waren es 9'301 Anordnungen für Proton Mail, davon 8'313 befolgt und 988 angefochten. Herausgeben kann Proton etwa Kontoangaben und Aktivitätsprotokolle, aber keine verschlüsselten Inhalte.



Ausländische Behörden müssen über die Schweizer Rechtshilfe gehen. Herausgeben muss Proton dann Metadaten wie eine IP-Adresse, keine verschlüsselten Inhalte.

Auch die Schweiz ändert sich: die VÜPF-Revision

Die Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) regelt, welche Anbieter wie bei der Überwachung mitwirken müssen. Der Bund wollte sie verschärfen. Der Entwurf fiel 2025 in der Vernehmlassung durch: Grüne, SP, GLP, FDP und SVP lehnten ihn ab, dazu Branchenverbände und Anbieter wie Threema und Proton.

Proton hat darauf bereits reagiert und Teile seiner Infrastruktur ins Ausland verlegt. Als Erstes kam 2025 der KI-Assistent Lumo auf Server in Deutschland, weitere Standorte entstehen in Norwegen.

Stand 2. Oktober 2026: Die Revision ist nicht in Kraft. Der Bundesrat hat am 11. Februar 2026 das Ergebnis der Vernehmlassung zur Kenntnis genommen, eine Regulierungsfolgenabschätzung in Auftrag gegeben und eine zweite Vernehmlassung angekündigt, sobald die überarbeitete Fassung vorliegt.

Überwachungsverordnung (VÜPF)

Verschärfung geplant, Stand Oktober 2026 nicht in Kraft

Proton verlegt Teile der Infrastruktur

Schweiz



Deutschland · Norwegen



Die Revision ist noch nicht in Kraft. Proton hat trotzdem schon reagiert.

Drei Fragen an dein Postfach

- 1. Wer hält den Schlüssel?** Du oder der Anbieter?
- 2. Was ist Ende-zu-Ende verschlüsselt?** Nur der Inhalt, oder auch Betreff und Empfänger? Und gilt das auch für Mails nach aussen?
- 3. Welchem Recht untersteht der Anbieter?** Und wie geht er mit Anordnungen um, steht das in einem Transparenzbericht?

Meine Sicht

Das ist meine persönliche Einschätzung, keine Empfehlung für jeden Fall.

Ich nutze Proton seit Jahren, vor allem für Mail, daneben auch weitere Dienste aus dem Paket. Nicht, weil es perfekt ist: Metadaten bleiben sichtbar, und auch die Schweiz kann ihre Regeln ändern. Sondern weil der Anbieter meine Inhalte nicht lesen kann. Das ist für mich digitale Souveränität im Alltag: nicht vollständige Unabhängigkeit, sondern bewusst entscheiden, wer den Schlüssel hat.

Und bei dir?

Wer hat den Schlüssel zu deinem Postfach?

Häufige Fragen

Kann Proton meine E-Mails lesen?

Nicht den Inhalt. Proton speichert Mails mit Zero-Access-Verschlüsselung: Der Schlüssel ist mit deinem Passwort geschützt, auf dem Server liegen nur verschlüsselte Daten. Betreff, Absender und Empfänger sind aber nicht Ende-zu-Ende verschlüsselt.

Ist eine Mail von Proton an eine Gmail-Adresse Ende-zu-Ende verschlüsselt?

Nein. Ende-zu-Ende verschlüsselt sind Mails zwischen zwei Proton-Konten. Mails an normale Adressen sind es nur, wenn du sie mit einem Passwort schützt, das die Empfängerin auf einem anderen Weg erhält.

Muss Proton Daten an Behörden herausgeben?

Auf eine verbindliche Anordnung nach Schweizer Recht ja, aber keine Inhalte verschlüsselter Mails, weil Proton sie nicht entschlüsseln kann. Herausgeben kann Proton etwa Kontoangaben und Aktivitätsprotokolle. Ausländische Behörden müssen über die Schweizer Rechtshilfe gehen. 2021 musste Proton auf eine solche Anordnung die IP-Adresse eines französischen Aktivisten protokollieren.

Quellen

1. Proton: Proton Mail encryption explained (Support)
<https://proton.me/support/proton-mail-encryption-explained>
2. Proton: Transparency Report (aktualisiert 6.1.2026)
<https://proton.me/legal/transparency>
3. TechCrunch: ProtonMail logged IP address of French activist after order by Swiss authorities (6.9.2021)
<https://techcrunch.com/2021/09/06/protonmail-logged-ip-address-of-french-activist-after-order-by-swiss-authorities>
4. WeLiveSecurity: ProtonMail forced to log user's IP address (7.9.2021)
<https://www.welivesecurity.com/2021/09/07/protonmail-log-users-ip-address/>
5. heise: Proton relocates parts of its infrastructure from Switzerland (2025)
<https://www.heise.de/en/news/Surveillance-Proton-relocates-parts-of-its-infrastructure-from-Switzerland-10538664.html>
6. Bundesrat: Fernmeldeüberwachung, Ergebnis der Vernehmlassung zur Kenntnis genommen (11.2.2026)
<https://www.admin.ch/de/newnsb/EXv-JkPBAZuL>
7. inside-it: VÜPF-Revision fällt in der Vernehmlassung komplett durch (7.5.2025)
<https://www.inside-it.ch/vupf-revision-faellt-in-der-vernehmlassung-komplett-durch-20250507>



ÜBER DEN AUTOR

Rico Eberle

Rico Eberle ist E-Learning-Experte, Betriebsökonom FH und Gemeinderat in Dübendorf. Er präsidiert den Stiftungsrat der Stiftung Weiterbildungskurse Dübendorf (WBK). In den Learning Nuggets erklärt er Forschung zu Lernen, KI und digitaler Souveränität kurz und mit Quellen.

Kontakt: ricoeberle.ch · LinkedIn: [linkedin.com/in/rico-eberle](https://www.linkedin.com/in/rico-eberle)

LIZENZ

Text, Transkript und Video von Rico Eberle stehen unter der Lizenz CC BY 4.0 (ausgenommen Musik und Soundeffekte des Videos). Du darfst die Inhalte teilen und bearbeiten, auch im Unterricht, wenn du die Quelle nennst.
creativecommons.org/licenses/by/4.0/deed.de

ZITIERVORSCHLAG

«Wer hat den Schlüssel zu deinem Postfach?», Rico Eberle, ricoeberle.ch, 2026,
<https://ricoeberle.ch/blog/verschlueselte-mail/>, CC BY 4.0