

LEARNING NUGGET DIGITAL SOVEREIGNTY 4 OCTOBER 2026

# Who holds the key to your mailbox?

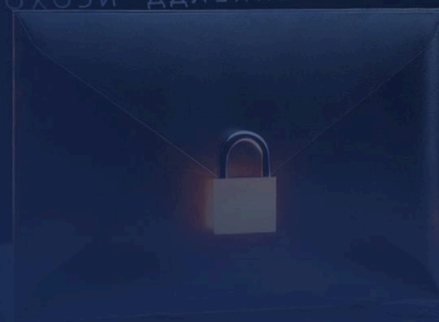
What an encrypted mailbox like Proton does differently from a regular one, what stays visible anyway, and what Swiss law, the 2021 case and the planned revision of the Swiss surveillance ordinance mean for it.

By Rico Eberle, e-learning expert for continuing education and municipal councillor in Dübendorf

RICO EBERLE · DIGITAL SOVEREIGNTY

## Who can read your emails?

**Often: the provider itself.**



### Video for this post

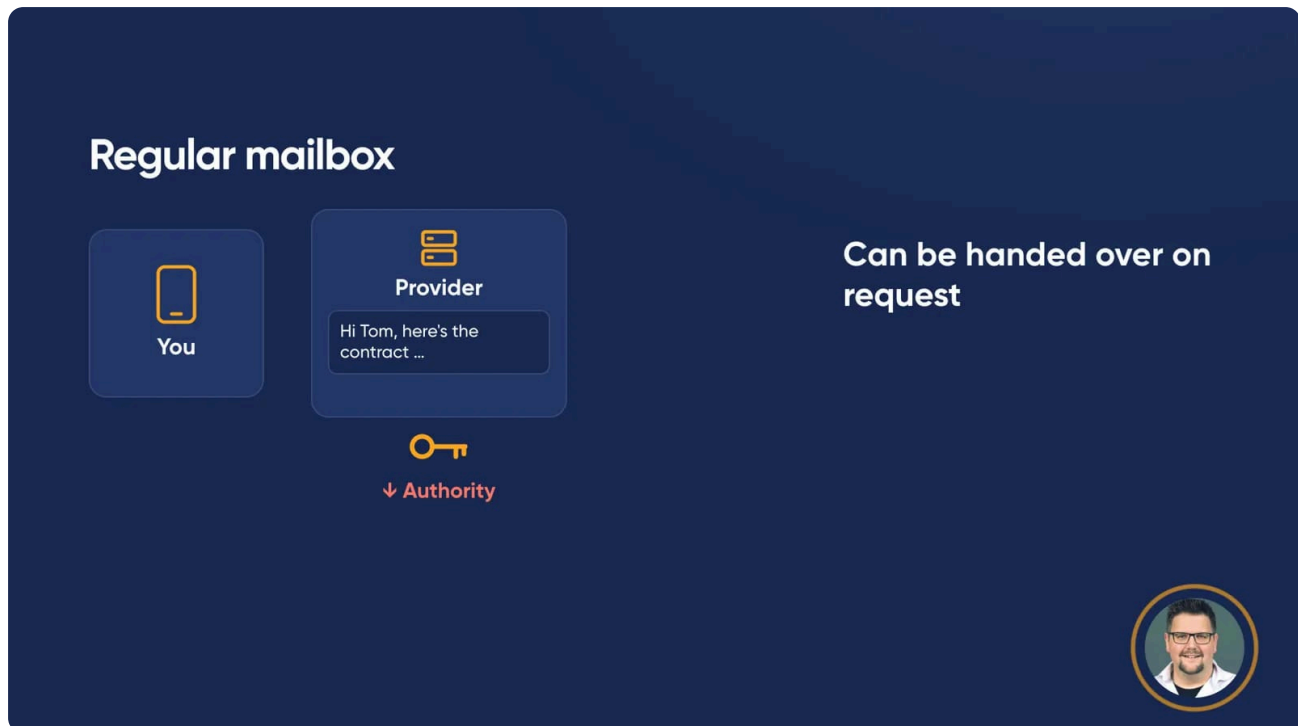
This learning nugget is also available as a video with transcript (1:37 min). Scan the QR code or open the link:

[ricoeberle.ch/en/blog/encrypted-email/](https://ricoeberle.ch/en/blog/encrypted-email/)

Who can read your emails? With most providers, the honest answer is: the provider itself. Encrypted mailboxes promise something different. Here is what they deliver and where the limits are, using Proton as an example.

## Regular mailbox: the provider holds the key

Even with a regular mailbox, emails are usually stored encrypted on the server. But the provider manages the key. It can technically read and search your emails, for search, spam filters or extra features. And when an authority arrives with a valid order, it can hand them over.



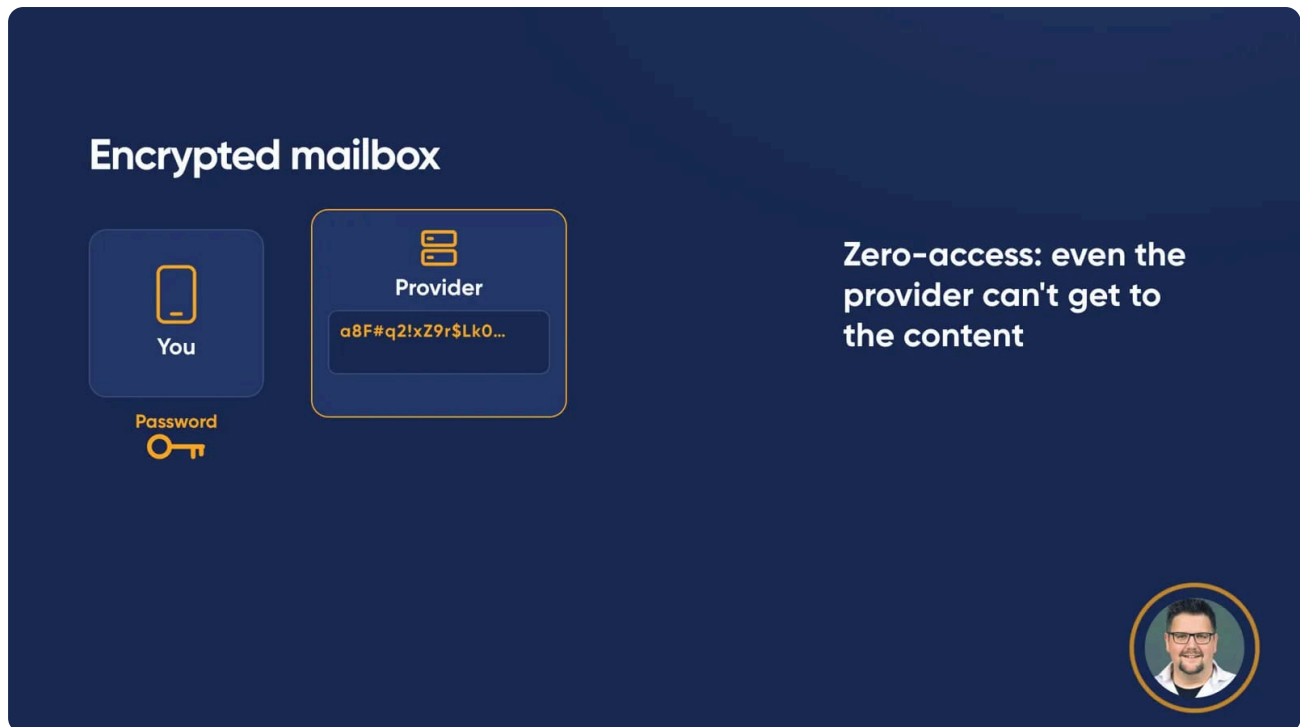
With a regular mailbox, the provider holds the key. It can read the emails and hand them over when ordered.

## Encrypted mailbox: the key stays with you

Encrypted mailboxes turn this around. The key is protected by your password, and only you know the password. The server only holds scrambled data. Proton calls this **zero-access encryption**: even the provider can't get to the content.

When two Proton users write to each other, it goes one step further. The email is then **end-to-end encrypted**, from the sender's device to the recipient's device. Nobody can read it in transit or on the server.

Simplified: behind the "key", Proton uses a private key based on the OpenPGP standard and the password that protects it.



Same diagram, roles reversed: the key is protected by your password, and the server only sees encrypted data.

## What stays visible anyway

Not everything is protected. According to Proton, **subject lines, sender and recipient addresses** are encrypted, but not end-to-end encrypted. Who writes to whom, when and about what is therefore not protected to the same degree as the content.

Emails to regular addresses, such as Gmail or Outlook, are not end-to-end encrypted either. The exception: you protect the email with a password that the recipient receives through another channel.

## What stays visible

|                                                                                                                                       |          |         |
|---------------------------------------------------------------------------------------------------------------------------------------|----------|---------|
| From                                                                                                                                  | Lea      | visible |
| To                                                                                                                                    | Tom      | visible |
| Subject                                                                                                                               | Contract | visible |
|  <b>Content encrypted</b><br>a8F#q2!xZ9r\$Lk0 Wm3... |          |         |

**To regular addresses: not  
end-to-end, unless  
password-protected**



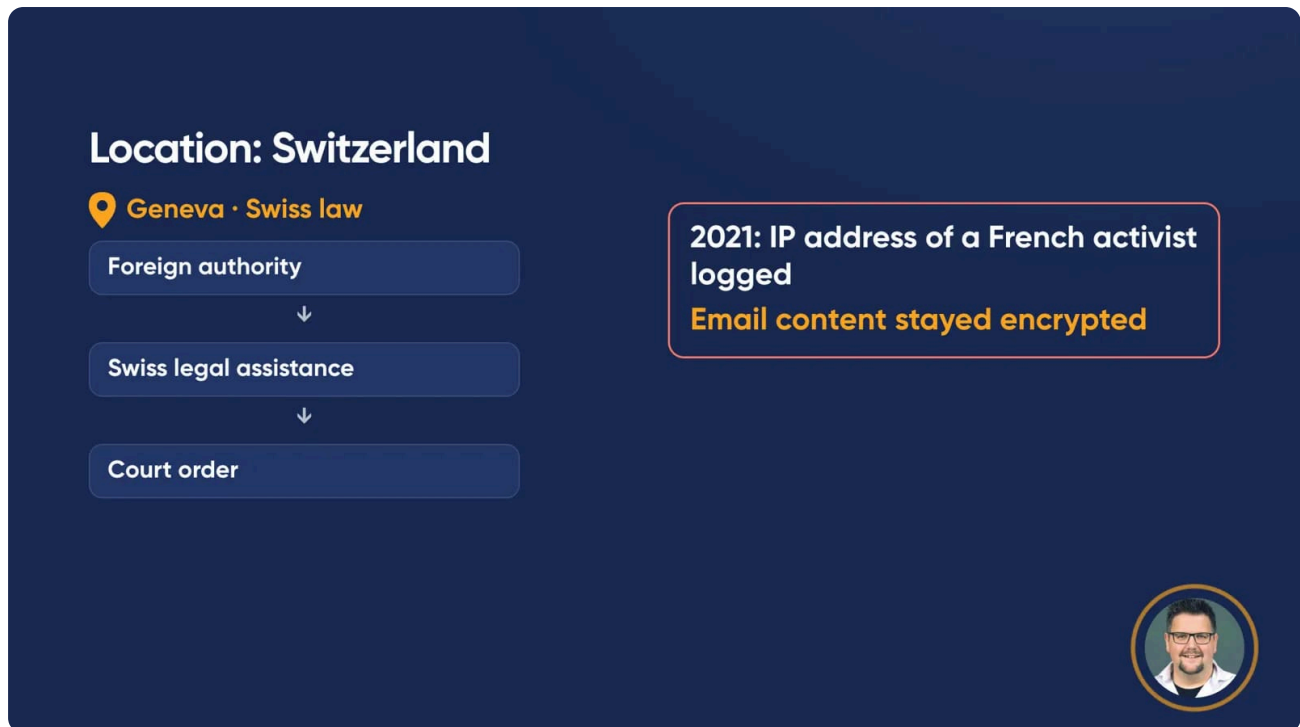
The content is protected; sender, recipient and subject are not end-to-end encrypted.

## Based in Switzerland: protection, not a free pass

Proton is based in Geneva and subject to Swiss law. Foreign authorities cannot force Proton to hand over data directly; Article 271 of the Swiss Criminal Code prohibits passing data directly to foreign authorities. They have to go through Swiss mutual legal assistance.

When a binding order under Swiss law arrives, Proton still has to provide data. The 2021 case shows this: French police sent their request via Europol to the Swiss authorities, who then required Proton to log the IP address of a French activist. Proton had to comply. The content of the emails stayed encrypted.

How often this happens is in Proton's transparency report: in 2025, there were 9,301 orders for Proton Mail, of which 8,313 were complied with and 988 contested. Proton can hand over things like account details and activity logs, but no encrypted content.



Foreign authorities have to go through Swiss mutual legal assistance. Proton then has to hand over metadata such as an IP address, but no encrypted content.

## Switzerland is changing too: the VÜPF revision

The Swiss ordinance on the surveillance of postal and telecommunications traffic (VÜPF) defines which providers have to assist with surveillance and how. The federal government wanted to tighten it. The draft failed in the 2025 consultation: the Greens, SP, GLP, FDP and SVP rejected it, as did industry associations and providers such as Threema and Proton.

Proton has already responded by moving parts of its infrastructure abroad. First, in 2025, its AI assistant Lumo moved to servers in Germany; further locations are being set up in Norway.

**As of 2 October 2026:** the revision is not in force. On 11 February 2026, the Federal Council took note of the consultation results, commissioned a regulatory impact assessment and announced a second consultation once the revised version is ready.

## Surveillance ordinance (VÜPF)

Tightening planned, not in force as of October 2026

Proton moves parts of its infrastructure

Switzerland



Germany · Norway



The revision is not yet in force. Proton has already responded anyway.

## Three questions for your mailbox

1. **Who holds the key?** You or the provider?
2. **What is end-to-end encrypted?** Only the content, or also subject and recipients? And does it apply to emails sent outside the service?
3. **Which law is the provider subject to?** And how does it handle orders, is there a transparency report?

## My view

This is my personal assessment, not a recommendation for every case.

I've been using Proton for years, mainly for email, plus other services from the bundle. Not because it's perfect: metadata stays visible, and Switzerland can change its rules too. But because the provider can't read my content. For me, that is digital sovereignty in everyday life: not complete independence, but deciding consciously who holds the key.

## And you?

Who holds the key to your mailbox?

## Frequently asked questions

### Can Proton read my emails?

Not the content. Proton stores emails with zero-access encryption: the key is protected by your password, and the server only holds encrypted data. Subject lines, sender and recipient addresses are encrypted, but not end-to-end encrypted.

### Is an email from Proton to a Gmail address end-to-end encrypted?

No. Emails between two Proton accounts are end-to-end encrypted. Emails to regular addresses are only end-to-end encrypted if you protect them with a password that the recipient receives through another channel.

### Does Proton have to hand data over to authorities?

Yes, when it receives a binding order under Swiss law, but not the content of encrypted emails, because Proton cannot decrypt it. It can hand over things like account details and activity logs. Foreign authorities have to go through Swiss mutual legal assistance. In 2021, such an order required Proton to log the IP address of a French activist.

## Sources

1. Proton: Proton Mail encryption explained (support)  
<https://proton.me/support/proton-mail-encryption-explained>
2. Proton: Transparency Report (updated 6 January 2026)  
<https://proton.me/legal/transparency>
3. TechCrunch: ProtonMail logged IP address of French activist after order by Swiss authorities (6 September 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 September 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. Swiss Federal Council: telecommunications surveillance, results of the consultation (11 February 2026, German)  
<https://www.admin.ch/de/newnsb/EXv-JkPBaZuL>
7. inside-it: VÜPF revision fails completely in consultation (7 May 2025, German)  
<https://www.inside-it.ch/vupf-revision-faellt-in-der-vernehmlassung-komplett-durch-20250507>



## ABOUT THE AUTHOR

### Rico Eberle

Rico Eberle is an e-learning expert, business economist (FH) and municipal councillor in Dübendorf, Switzerland. He chairs the foundation board of WBK Dübendorf, a continuing education foundation. In the learning nuggets he explains research on learning, AI and digital sovereignty, briefly and with sources.

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

## LICENCE

Text, transcript and video by Rico Eberle are licensed under CC BY 4.0 (music and sound effects in the video excluded). You may share and adapt the content, including for teaching, as long as you credit the source. [creativecommons.org/licenses/by/4.0/](https://creativecommons.org/licenses/by/4.0/)

## SUGGESTED CITATION

"Who holds the key to your mailbox?", Rico Eberle, [ricoeberle.ch](https://ricoeberle.ch), 2026, <https://ricoeberle.ch/en/blog/encrypted-email/>, CC BY 4.0