Regain some privacy online

How can you regain ownership about your data and behavior online? Here is how I did it.

- Browser
- Email
- Password Manager
- Cloud
- Calendar/Contacts
- Instant Messenger
- Google Privacy Settings

Browser

My recommendation: Firefox

Install the following extensions:

- Privacy Badger - Automatically block invisible trackers
- HTTPS Everywhere - Always use HTTPS as default
- uBlock Origin - Ad blocker, removes advertisements
- (Bitwarden - Password manager)

Set duckduckgo as your default search engine (How To)

Email

Use a **secure** and **privacy focused** email provider (list of suggested providers).

My recommendation:

protonmail-logo.png

Steps to change your email provider (to protonmail)

1. Register a new account.

> Think about registering two accounts. One to use for personal and official affairs and one for spam (e.g. registering an account on an untrusted site).

2. Forward all incoming emails from your old email address/es to your new email address. (e.g. How to forward in Gmail)

3. Delete all emails saved in your old email account/s. If you want to keep emails, you can either copy/send them manually to your new email address or use the protonmail Import-Export app.

> To use the protonmail Import-Export app you need a premium account. The cheapest way is to just upgrade your account to Pro for one month, which will cost you 5€ one time.

4. Change all your existing online accounts, newsletter subscriptions and etc. to you use your new email address/es.

> I recommend to connect this step with the updating and upgrading of your passwords.

5. Delete your old email account/s.

> Wait a few weeks/month before doing this. Maybe you forgot to change your email address somewhere important and still need the address active.

Password Manager

Always use unique, long and difficult to guess passwords for each account you own. To make your life easier handling all these passwords: Use a password manager!

My recommendation: Bitwarden

Cloud

My recommendation: Nextcloud

Calendar/Contacts

My recommendation: Nextcloud

Instant Messenger

My recommendation: Signal

Download: Google Play Store | Apple Store | Desktop

Why should you use Signal?

- **Privacy of your data.** Signal does not sell, rent or monetize your personal data or content in any way. Furthermore, it does not store any of your data, which is not necessarily needed for the messenger to work (or may be legally required of course). (source)
- **Default end-to-end encryption.** Every message and every call transmitted via Signal is automatically encrypted and secure from being read or altered by a third party. (source)
- **Open Source.** Everyone can audit and contribute to Signals code base, which guarantees that the company behind Signal can not lie about how secure their messenger is and how your personal data is being handled or maybe misused and mistreated
- **Founded by the non profit Signal Foundation.** The company behind Signal does not see you as their product, they don't have to earn money with you and your data. The Signals Foundation aim is "to develop open source privacy technology that protects free expression and enables secure global communication" (source).

Why not WhatsApp?

- **WhatsApp is owned by Facebook.** Do I have to say more? The Cambridge Analytica scandal alone should have been enough, to show that Facebook can not be trusted with any personal data.
- **Closed source.** Only Facebook knows how WhatsApp works. However, they use the open source end-to-end encryption solution Signal provides and enable it by default, so the usage of WhatsApp is at least relatively secure. Just not private.

Why not Telegram?

- **No default end-to-end encryption.** This is a no-go. Everyone could possibly be reading your messages.
- **No end-to-end encryption for group chats at all.** What???? That's even worse.
- **Closed source.** Yes, they provide a public API, but their server side code is completely closed.

Disclaimer: By trying to keep this page short and simple, I have simplified technical descriptions and/or made pretty generalized statements. Please keep this in mind.

Google Privacy Settings

Share as less data as possible with google. Here are my recommendations for how to configure your google settings.

1. Go to your Google Dashboard

2. Change the following services:

- Calendar (export and delete all existing calendars) [only on switch to other calendar service]
- Contacts (export and delete all existing contacts) [only on switch to other contact service]
- Photos (export and delete all photos) [if you want cloud backup of your photos, use something like nextcloud]
- Drive (export and delete all data) [use something like nextcloud]

3. Change your activity data

- Search Activity: off (delete existing data) [don't forget to change your search engine to duckduckgo]
- Location History: off (delete existing data)
- Device Information: off (delete existing data)
- Voice & Audio Activity: off (delete existing data)

4. Turn Ad personalisation off