GDPR (General Data Protection Regulation) is for the European Union (EU)

It is your data - take control within the EU. One set of rules for the whole of the EU.

THE RIGHT TO KNOW WHO IS PROCESSING WHAT, AND WHY.

You have the right to request access to the personal data an organization has about you, free of charge, and obtain a copy in an accessible format.

If an organization is processing your personal data you may have the right to object.

You also have the right to object at any time to receiving direct marketing.

If you believe that personal data held by an organization might be incorrect, incomplete or inaccurate you can ask for it to be corrected. This must be done without undue delay.

You have the right to have data deleted and to be forgotten.

You have the right to have a say when decisions are automated.

You have the right to move your data (data portability).

Data lost or stolen? The rules make sure you are protected.

Opt out of tracking:

A lot of websites, including Facebook and Google, store and sell your personal data. It is how they make money, and it is what we have sacrificed for a more connected world.

This is how to protect your privacy; opt out of tracking:

1. Facebook:

Login to Facebook:

> Go to Home page > Click on ˅ > Click on Settings > Click on Ads

2. Google:

Login to Google:

> Click on My Account > Personal Info & Privacy > Ads Settings
> Manage ad settings > Ad personalization (toggle off)

Now you can click on Ad settings and see what happens.

3. Amazon:

Login to Amazon:

> Click on Bulls eye > Account > App preferences > Advertising preferences > Change to "Do Not".

4. NAI (National Advertising Initiative):

Input this on address line: optout.networkadvertising.org

Click on "Manage My Browser's Opt Outs"

A "User's Current IBA Status" will be generated.

Then you can opt out of certain web sites.

Also:

1. Turn off browser cookies if you can.

2. You can use a browser plug-in to limit data tracking.

3. Go incognito or InPrivate browsing. Major browsers, such as Chrome, Firefox, Edge and Safari, have a private browsing setting. Using this feature means your browser will ignore cookies, including ad-tracking cookies and will not record your history.

4. A lot of websites, including Facebook and Google, store and sell your personal data. It is how they make money, and it is what we have sacrificed for a more connected world.

5. Limit website linking. Avoid using the “login with Facebook or Google” feature on websites you visit.

Protect your privacy by these tricks:

1. See Who Has Shared Your Private Data:

   Here is a neat trick for ferreting out which companies are sharing your data with email lists.

   If you have a Gmail account:

   Type “+” before the “@” symbol and add the website’s name. Email addressed to YourName+Websitename@gmail.com will go to the regular inbox for YourName@gmail.com. But now it will carry an extra crumb of data, and if you get spam from a company you have never heard of, you will know who to blame.

2. Check Your Data Breach Status:

Wondering whether your personal data is for sale on the web? Type on the address line: haveibeenpwned.com and then at the website that comes up type in your email address and press Enter. You will see the results. You can check your email address and usernames against lists from 120 known breaches of companies including Adobe, LinkedIn, and Snapchat. (You will need to register to check the full database) If your name pops up, change the password for the compromised account and any other site where you were using the same password.

3. Use long passwords or unique passwords and use a password manager.

4. Shut Off the Flow of Credit Card Offers:

These unsolicited mailings can be taken and filled out by identity thieves who have credit cards sent to their own addresses, with your information and then start piling up debt in your good name. You can put a stop to most of these offers by going to optoutprescreen.com or calling 888-567-8688. The service, run by the Consumer Credit Reporting Industry, will turn off the spigot permanently or for five years. You can always opt back in.