Europska komisija

Take Control of Your VIRTUAL IDENTITY

#GDPR

june 2019.

Some companies make money by collecting and sharing your personal data with others.
This includes:

- Social networks
- Email providers
- Search engines
- Software solutions

They may collect more data than you voluntarily share. They track:

- Your email and calendar
- Your searches and locations
- Your messages and groups you belong to
- Pages and content you are interested in

This data helps them create your virtual profile, which is used for targeted advertising and profit.

As of May 2018, new data protection rules apply (General Data Protection Regulation – GDPR). If a company collects your data based on your consent, that consent must be:

✓ Voluntary
✓ Based on informed decision
✓ Given through a clear confirmation

In May 2018, many companies asked you to accept new terms and adjust your privacy settings. We recommend:

✅ Carefully reading the terms of use
✅ Adjusting your privacy settings
✅ Limiting the sharing of data you don't want to disclose

Some companies ask for additional consent to process data not necessary for their service.
This consent must not be a condition for providing the service.

YOU CAN WITHDRAW YOUR CONSENT AT ANY TIME.

Pravosuđe i zaštita potrošača

MOST EUROPEANS EXERCISE THEIR RIGHT TO CHANGE PRIVACY SETTINGS

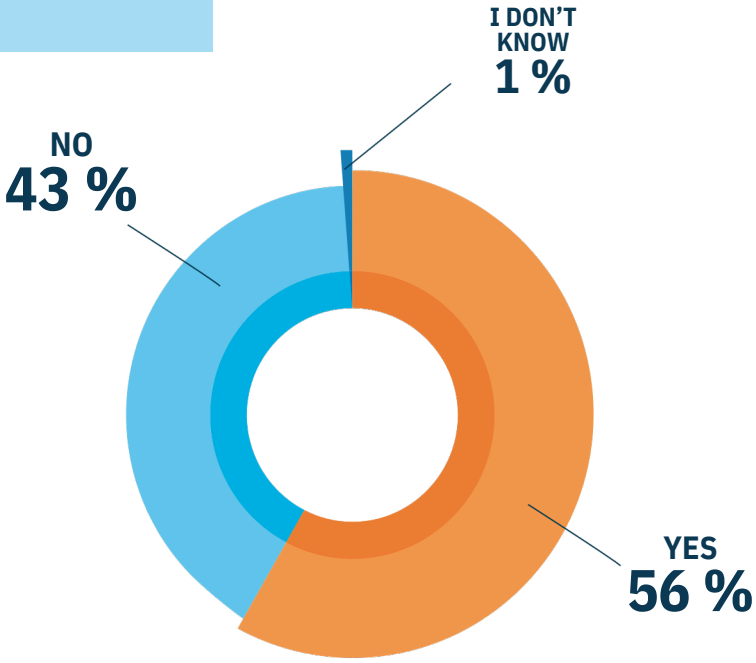
Have you ever tried to change privacy settings on social media?

A survey of 27,000 Europeans showed that most users tried to adjust their privacy settings. However, a large number of respondents never did.

Why don't some users change their privacy settings?

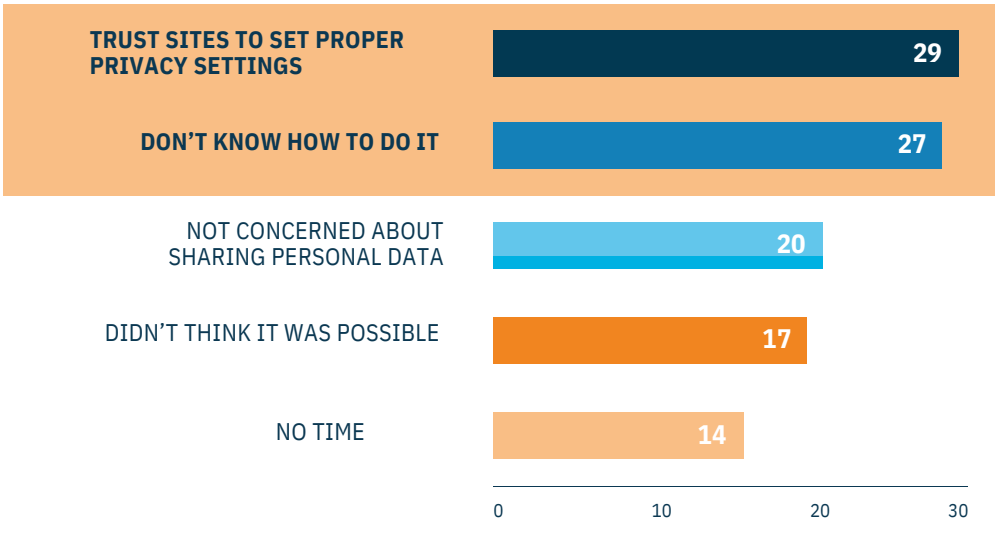
Main reasons:

- They believe the platform already ensures adequate privacy protection
- They don't know how or find it confusing to change settings



Source: Posebni Eurobarometar 487b QB11, 2019.

Have you adjusted your privacy settings? If not, what is stopping you?



Source: Posebni Eurobarometar 487b QB12b, 2019.

YOUR RIGHTS UNDER THE GENERAL DATA PROTECTION REGULATION

What does this mean in practice?

Data Protection by Design

- Platforms may collect and store only data necessary for use, and only for a limited time.
- Only authorized personnel may access this data.
- Users decide whether their data is publicly available.
- Companies must ensure a high level of data protection and consider potential risks.

✓ **Consent must be clearly visible.**
Giving and denying consent must be equal options. Consent must not be pre-selected.

Information about data processing

- You have the right to know what data is collected and how it's used.

✓ **Right to access data.**
You can request a document with the data a company has about you and check if you agree with it.

Right to object

- You can oppose the processing of your data for targeted advertising.

✓ **Data protection rules must be clear.**
You should understand what data is collected, for what purpose, and with whom it is shared.

Access to all stored data about you

- You have the right to request and receive a free copy of all personal data a company holds about you.

✓ **Data protection rules must be clear.**
You should understand what data is collected, for what purpose, and with whom it is shared.

Right to be informed in case of data breach

- If a data breach occurs, the company must notify the data protection authority.
- If the breach poses a high risk (e.g. credit card data exposure), the company must also inform you directly.

✓ **Right to data erasure.**
In certain situations, you can request permanent deletion of your profile and all collected data.

Right to be forgotten

- You can request the deletion of your personal data.
- Exception: Data of public interest (e.g. politicians, executives).

✓ **Right to object to marketing ads.**
Rejecting ads should not limit your platform access. If there's a "take it or leave it" policy, it may violate GDPR.

Optimize your privacy settings

Be sure you're the one controlling the data you share on online platforms!

Notice a data protection violation?

📢 File a complaint!

✅ You can contact your national data protection authority.

✅ Data protection authorities can:

- Impose sanctions on companies and platforms
- Order temporary suspension or termination of data processing
- Impose fines up to €20 million or 4% of a company's annual turnover

🔗 More information: **europa.eu/dataprotection**