European Commission

Take control of your VIRTUAL IDENTITY

#GDPR

June 2019

For some companies, a large component of their business model is to collect your personal data and share it with third parties. These are typically social media platforms, email providers, search engines and software providers. The data they collect may go beyond what you actively share with them on your public profile. They might also track your emails, calendar, searches, locations, messages, pages you are interested in, and groups you take part in. With this data, they map your virtual identity based on your interests and your preferences. They then monetise your virtual identity for targeted advertising.

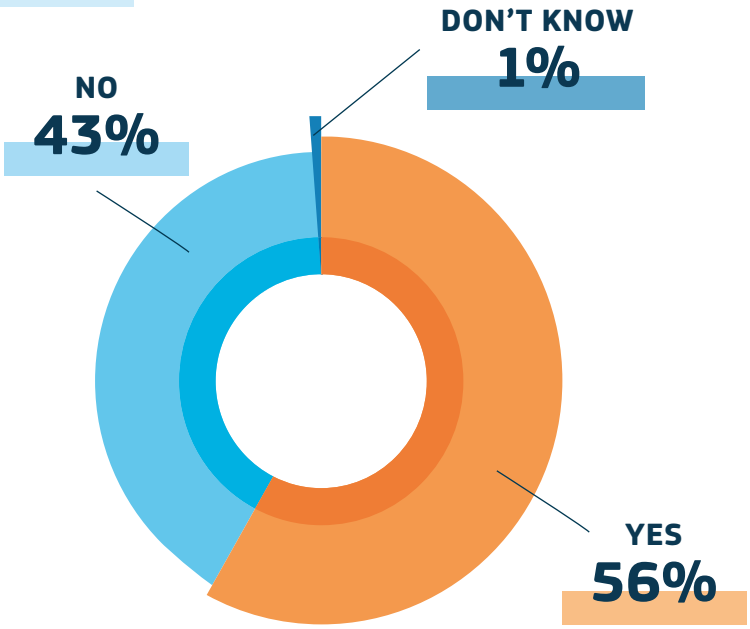
According to the new rules on data protection that have to be applied since May 2018 (General Data Protection Regulation), when the processing of your personal data is based on your consent, this **consent** needs to be based on an **informed decision** and expressed through an **affirmative action** from your side. You may have experienced many companies directly contacting you to accept their new terms and conditions and review your privacy settings in May 2018. We strongly encourage you to carefully read the terms and conditions, and optimise your privacy settings so that the platforms do not process and disclose to third parties, data you are not willing to share. The platforms might also have asked for your consent for processing of additional personal data that are not necessary for the provision of the service. This consent should be freely given, i.e. not made conditional on the provision of the service. In any case you can withdraw your consent at any time.

Justice and Consumers

THE MAJORITY OF EUROPEANS DOES MAKE USE OF THEIR RIGHT TO CHANGE PRIVACY SETTINGS

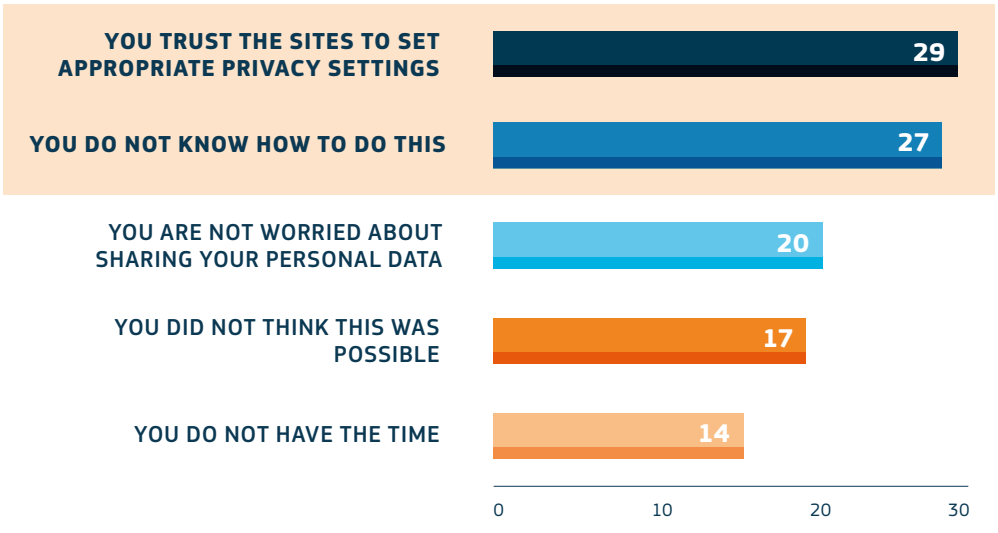
Have you ever tried to change the privacy settings of your personal profile from the default settings on an online social network?

We asked 27,000 Europeans about their social media habits. While a majority did try to change their privacy settings, there is still a large share that did not. The main reasons for not doing so is people either trust the social media platform to provide appropriate privacy settings, or they do not know how to change the settings themselves.



Source: Special Eurobarometer 487b QB11, 2019

Why have you not tried to change the privacy settings of your personal profile(s)?



Source: Special Eurobarometer 487b QB12b, 2019

YOUR RIGHTS UNDER THE GENERAL DATA PROTECTION REGULATION

What does this mean in practice?

Data Protection by default

By default, the only data that should be processed and stored for a limited time, is the data which is necessary in order to use the platform. Data should only be accessible by a limited number of authorised persons. It should be up to the user to decide to make their data publicly accessible. Companies are obliged to assure a high standard of security around their users' personal data and must take into account the risks associated with the data they hold.

When asked for consent the opt-in or opt-out choice should be given equal prominence and the opt-in should not be ticked by default.

Information about the processing of your data

You have the right to receive clear information about the processing of your personal data. Companies must tell you what data they are processing and for what purposes they are processing it.

The company's data protection rules should be presented to you in clear and plain language. It should be easy to understand which data is being processed, for which purpose and with whom the data is being shared.

The right to object

You always have the right to object if an organisation is processing your personal data with the purpose of sending tailored advertisements to you.

If you do not want to receive direct marketing advertising, you can always object. This should not mean that you no longer have access to the online platform's services as such. If you are faced with a 'take-it-or-leave-it' option, chances are that this is a breach of data protection rules.

Access all the data kept about you

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

You can ask any company to send you a copy of all the data they have ever collected about you. By going through this document, you can see if you are comfortable with the company collecting this data about you.

The right to be informed if your data has leaked

The company holding your data is required to inform the national Data Protection Authority (DPA) if there is a data breach. If the breach poses a high risk to you, for example, if your credit card details were exposed by a breach and those data were not encrypted, then you should be personally informed.

If the data breach constitutes a high risk, the company must inform you and the national DPA without undue delay.

The right to be forgotten

With the right to be forgotten you can ask a company to delete your personal data. This is with the exception of circumstances where there is a legitimate reason for the data to be kept, such as it is in the public interest to know information about the actions of a public figure, such as a political figure or a Chief Executive Officer.

Under certain circumstances you can ask the company to delete all the data they keep about you and to permanently delete your profile.

Optimise your privacy settings.

Make sure you control the data you share on online platforms.

DOES REALITY NOT CORRESPOND TO THE RULES ON DATA PROTECTION? LODGE A COMPLAINT!

You can lodge a complaint with your **national Data Protection Authority**. The Data Protection Authorities can impose a range of sanctions on companies, platforms and organisations, including suspending or stopping data processing and imposing a fine of up to €20 million or 4 % of the business annual global turnover.

europa.eu/dataprotection