



EN

How will the data protection reform affect social networks?

Right to be forgotten: An Austrian law student requested all the information that a social networking site kept about him on his profile. The social network sent him 1,224 pages of information. This included photos, messages and postings on his page dating back several years, some of which he thought he had deleted. He realised that the site was collecting much more information about him than he thought and that information he had deleted – and for which the networking site had no need – was still being stored.

What are the problems with social networking?

Social networks provide a useful tool for staying in touch with friends, family and colleagues, but they also present a risk that your personal information, photos and comments might be viewed more widely than you realise. In some cases, this can have financial, reputational and psychological consequences. **A large majority of Europeans (71%)** think that the disclosure of personal data is an **increasing part of modern life**. At the same time, more than six out of ten users say that they do not trust landline or mobile phone companies and internet service providers (62%) or online businesses (63%). They feel they do not have complete control of their data.

What are the changes about?

The new rules strengthen the **right to be forgotten** so that if you no longer want your personal data to be processed, and there is no legitimate reason for an organisation to keep it, it must be removed from their system. Data controllers must prove that they need to keep the data rather than you having to prove that collecting your data is not necessary. Providers must take account of the principle of **'data protection by default'**, which means that the default settings should be those that provide the most privacy. Companies will be obliged to **inform you** as clearly, understandably and transparently as possible about how your personal data will be used, so that you are in the best position to decide what data you share. This information may be provided in combination with easy to understand standardised icons.

Attitudes towards data protection

- **71%** of Europeans see disclosing personal information as an **increasing part of modern life**.
- The most important reason for disclosure is to make a payment online (46%), or to have a purchase delivered (44%) and to access a service (36%).
- A majority of people are uncomfortable about Internet companies using their personal information to tailor advertisements
- Only one fifth of respondents say they are always informed about the conditions of data collection and its potential uses when they are asked to provide personal information online.
- Just over four in ten of those who use online social networks have not tried to change their privacy settings.
- Out of those who have not changed their privacy settings, about a quarter have not done so because they trust sites to set the appropriate settings.

Special Eurobarometer 431 - Data protection, June 2015

The reform of data protection will make it easier for you to access your data and give you a right to data portability, which means it will be **easier to transfer personal data** from one service provider to another. It will also make sure that when users give their consent for companies to use their personal data, that agreement is given **by means of a clear affirmative action** and with their full awareness. This will give users control over their data, and help foster **trust** in the online environment.

Why is this good for the digital economy?

A high level of data protection is essential to foster **people's trust in online services** and in the digital economy in general. Privacy concerns are among the top reasons for people not buying goods and services online. With the technology sector directly contributing to 20% of overall productivity growth in Europe and 40% of overall investment aimed at the sector, individual trust in online services is vital for **stimulating economic growth in the EU**.

With the increasing **globalisation of data flows**, and the growth of cloud computing, there is a risk of people losing control of their online data. The new rules will put people in **control of their personal data**, and will foster trust both in **social media and in online shopping and communication in general**.

What will be the key changes?

- Strengthening the **'right to be forgotten'** to help people better manage data protection risks online. When individuals no longer want their data to be processed and there are no legitimate grounds for retaining it, the data will be deleted. The rules are about empowering people, not about erasing past events, re-writing history or restricting the freedom of the press.
- Guarantee **easy access to your own data**.
- Establishing a right for individuals **to freely transfer personal data** from one service provider to another (data portability).
- Ensuring that **consent must be given by a statement or by a clear affirmative action** when this is used as a legal basis for processing;
- Increasing the responsibility and accountability of those processing data by introducing **data protection officers for companies** whose core activities involve the processing of personal data in large scale and the principles of **'data protection by default'** and **'data protection by design'** to ensure that goods and services integrate, from the conception stage, appropriate data protection settings and safeguards.