



FACTSHEET #4

DATA PRIVACY

WHY DO YOU NEED TO KNOW ABOUT DATA PRIVACY?

As the world shifts online, our **personal data is increasingly requested** - by websites, companies, researchers, even your local club or society. And often, we give it. But is our data always kept private? Not everyone understands the issues around data privacy in our technology-led world, while a lot of people tend to ignore this issue, or see it as something that doesn't affect them. But **data privacy affects all of us**. This factsheet explains why it is important - and how you can keep your data secure.

KEY MESSAGES

- Data privacy relates to how our **personal data is collected, used and transferred**, and the measures in place to protect it.
- In the EU, laws and regulations - especially the GDPR - mean your **personal data should be treated as private** by everyone who collects it (e.g. companies, authorities).
- In most cases, you have the right to set out your **privacy preferences** when sharing data: who can use it and how it can be used, among others.
- There are several steps that you can take to **increase the privacy** of your personal data.

VULNERABLE PEOPLE AND DATA PRIVACY

Vulnerable people may be more at risk of their data privacy preferences not being respected. For example, refugees or migrants to a country may not be fluent in the national language and therefore cannot read, or do not fully understand, privacy policies. This puts them at risk of **having their data shared in ways they do not want**. Anyone requesting their personal data should consider the specific needs of these and other vulnerable groups - and do everything they can to ensure these people understand, and agree with, how their data will be used.

THE NEED FOR DATA PRIVACY

The mass collection and analysis of personal data means that governments and companies now **know more about us than ever before**. For example, many people voluntarily share their private information on social networks such as Facebook. But this gives huge power to anyone who can access this information. It gives



governments the ability to anticipate protests, for example. And tech companies can use it to anticipate our every move, which in turn gives them opportunities to influence our behaviour - and sell that influence to others. This text is adapted from an article by Carissa Véliz, which you can read here (in English): bit.ly/3qh30Kc

WHAT YOU CAN DO

- Read privacy policies before agreeing to them!
- Only share the information and data you want to - not everything that is being asked for.
- If you're not 100% sure about the person or company asking for your data, don't share it.
- Lots of websites provide advice on how to keep your online data private, such as Digital Guardian: bit.ly/3j5XsAM
- Remember, not all data is online - these recommendations also apply to your offline data.

FIND OUT MORE

READ: We recommend the EU's advice on data protection and online privacy: bit.ly/3vUnwBs. To understand the pitfalls better, the Cambridge Analytica case is a well-known example of what can happen when personal data isn't treated as private. You can read about this on *The Guardian*: bit.ly/3zQqpX9

WATCH: The PANELFIT monthly chat on 'Privacy, cybersecurity and society' explores how companies are accountable when using people's data (bit.ly/2UuUfQV) and in this interview, Carissa Véliz discusses the issues that can arise from sharing personal data: bit.ly/35KBnzB