FACTSHEET #2
THE GENERAL DATA PROTECTION REGULATION / GDPR

WHY DO YOU NEED TO KNOW ABOUT THE GDPR?

The GDPR regulates how European citizens' personal data is processed. It sets out the laws through which your **personal data is protected and kept private**. The GDPR is a long, complex document, with 99 separate articles, and it can seem daunting to anyone not familiar with data or privacy laws - and many citizens don't know where to start. However, the GDPR is important: it gives you **better control over how your personal data is used**. This factsheet provides an introduction to the GDPR and explains what it does - and what it doesn't do.

KEY MESSAGES

- The GDPR puts p**ower in the hands of citizens** - to control how their data is used and who can use it.
- It is one of the **strongest regulations about data protection and privacy** in the world.
- If you are an EU citizen, all organisations and companies must **follow these rules when handling your data** - even if they are outside of the EU.
- It is **the responsibility** of organisations and companies to make sure they comply with the GDPR; you do not need to tell them to do so when using your personal data.

VULNERABLE PEOPLE AND THE GDPR

The GDPR does not have a specific section dedicated to the protection of vulnerable people's data. Nor does it define who counts as a 'vulnerable data subject', although it does reference the special care that should be taken with children. However, this does not mean that the GDPR does not protect vulnerable people. It covers all EU citizens - including those who are, for any reason, vulnerable. A PANELFIT talk looks at this subject in more detail: https://bit.ly/3zKZpZj

THE SEVEN PRINCIPLES OF THE GDPR

The GDPR outlines seven principles that data controllers (i.e. those who use your data) must comply with.

1. The processing of personal data must be **lawful, fair and transparent.**
2. **Purpose limitation** means data controllers can only use your data for the purposes they specified when asking for it.
3. They should only collect and process data they really need (**data minimisation**).
4. Data controllers must ensure the **accuracy** of personal data they collect.
5. Data controllers can only keep data that personally identifies you for as long as needed (**storage limitation**).
6. Data processing must be done in a way that ensures **security, integrity and confidentiality**.
7. The data controller must be able to demonstrate compliance with these principles (**accountability**).

You can read more here: https://bit.ly/3xLpvtm

WHAT YOU CAN DO

- The GDPR.EU website contains a lot of useful information; we suggest you start with the 'Key Issues' page (https://bit.ly/2SqFrCg) or the 'Overview' (https://bit.ly/3qiefBY).
- Perform a personal data 'health check'; this blog post provides tips on how to do this (in English): https://bit.ly/3d26hr9

FIND OUT MORE

READ: Chapter 2 of the PANELFIT Guidelines (Part 1) provides an in-depth look at the GDPR: www.panelfit.eu/
This journal article provides an in-depth look at this complex issue: https://bit.ly/3zRL4dy
This link explains who data 'controllers' and 'processors' are: https://bit.ly/3xHEGDK