A one-page guide to the General Data Protection Regulation (GDPR).

I've heard about this "GDPR", but what is it?

Formally, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data wand on the free movement of such data, and repealing Directive 95/64/EC (General Data Protection Regulation), but most often shorted to "the GDPR"

It was adopted in 2016 and came into effect in May 2018.

You can find a full copy of the legislation in all EU official languages at <http://data.europa.eu/eli/reg/2016/679/oj>

The GDPR applies to data controllers established in the EU, and to personal data of people in the EU, even if processed by a controller not established in the EU. It does not apply to household or purely personal use of personal data.

The purpose of the GDPR is to update and modernise laws that **protect the personal information of individuals**, and to provide an equal level of protection across the EU.

**Personal data** is any information relating to an identified or identifiable natural person. This is a wide and inclusive definition. There are also some categories of *sensitive* personal data (such as racial or ethnic origin, political or religious beliefs, health data) that get extra protection because abuse of personal data in these categories is likely to lead to harmful consequences. Processing of personal data is any activity performed on personal data (such as collecting, storing or organising it).

The GDPR is based around **principles of lawfulness, fairness and transparency; purpose limitation; data minimisation, accuracy; storage limitation; integrity and confidentiality, and accountability**. To process personal data, an organisation (a "data controller") must have clear purposes and a legitimate ground for doing so. The data must be kept for no longer than necessary, must be accurate and up to date. The controller must also take measure to ensure the data is processed properly and securely. The principle of accountability means that organisations processing personal data are responsible for demonstrating that they are doing so in lawful, fair and transparent.

The GDPR grants people many **rights**. When their data is processed, they must be provided with contact details for the data controller, information on the purposes of processing, how long the data will be stored, if they are obliged to provide data, sources of data, if the data will be transferred to third parties, information about any automated decision making and information about their other data protection rights. These include rights to request access to, correction or erasure of personal data, restriction of processing, to object to processing and to receive their data in a portable form. They also have the right to lodge a complaint about data processing with a supervisory body.

If you have any further questions, or think you need further training on the GDPR, then please contact our Data Protection Officer:

Name: [user to complete]

Email: name@organisation.com

Phone: [user to complete]

This guide was produced by the STAR project(*Support Training Activities on the data protection Reform*; 2017-2019), which is co-funded by the European Union under the Rights, Equality and Citizenship Programme 2014-2020 (REC-RDAT-TRAI-AG-2016) under Grant Agreement No. 769138.

More information, and other GDPR training resources can be found at: **www.project-star.eu**



To protect those rights, the GDPR empowers independent supervisory bodies (sometimes also called **Data Protection Authorities** or Information Commissioners) to oversee compliance with the GDPRand to promote awareness of GDPR obligations and rights. These bodies work together as the European Data Protection Board.

The GDPR also introduces significant **penalties** for non-compliance. Supervisory bodies can carry out investigations, issue warnings and reprimands to controllers, and impose fines up to €20 million or 4% of worldwide turnover for serious infringements of the GDPR.