

# TOP 10 things you need to know about the #GDPR



- ONE** The GDPR is an EU Regulation which means that it will have **direct effect** throughout the EU in on **25 May 2018**. The UK will still be in the EU at that time and UK Government has stated that the GDPR will take effect in the UK.
- TWO** **Data Processors** will also have obligations under the GDPR to look after personal data. Data Processors will also be subject to enforcement action, including fines and compensation if they do not comply with the GDPR.
- THREE** Certain organisations (public bodies, organisations whose core business is processing personal data on a large scale and organisations processing data about crime on a large scale) must have a **Data Protection Officer**.
- FOUR** You will require to carry out a **Data Privacy Impact Assessment** when processing personal data is likely to involve a high risk to the rights and freedoms of the individuals. Data protection will be **By Design**.
- FIVE** There will be an obligation to **report personal data breaches** to the ICO within 72 hours of them occurring where the breach is likely to involve significant risks to data subjects' rights and freedoms.
- SIX** In the event of a personal data breach **data subjects must be notified** without delay if the breach is likely to result in a high risk to the rights and freedoms of the individuals.
- SEVEN** The **maximum fine** that can be imposed for breaches is €20,000,000 or 4% global turnover whichever is higher. This is a significant increase from the current maximum in the UK of £500,000.
- EIGHT** **Privacy Policies** will have to be in clear language without endless small print and the provision of **explicit consent** will have to be through an affirmative act ruling out in law the use of pre-ticked boxes.
- NINE** Even if your organisation is **not based in the EU**, and when the UK leaves, if you are processing the personal data of EU citizens and residents you will have to comply with the GDPR.
- TEN** You will **no longer need to notify the ICO** that you are processing personal data.