This leaflet explains how the GPR regulations affect your organisation and the steps you need to take.

Data protection has changed

Are you ready?

smartimpact
Intelligent solutions

What is GDPR?

The General Data Protection Regulation (**GDPR**) is a new EU-wide regulation which came into force on 25th May 2018. It superseded the UK's Data Protection Act 1998 (DPA). If you are required to comply with the DPA then you will be required to comply with GDPR.

Britain's exit from the EU will NOT affect the enforcement of this regulation. And, if you operate in the EU, it applies to you even if you are not based in the EU.

What are the key changes?

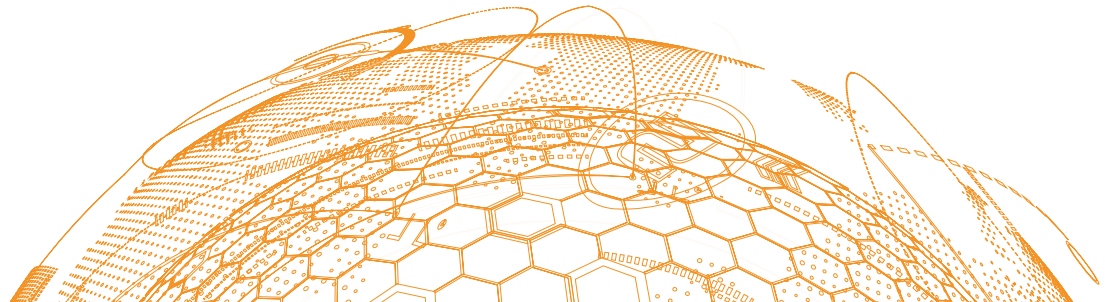
GDPR aims to put control of personal data back in the hands of the customer. It also focuses on bringing an international consistency to data protection rules.

⚠ It affects data 'controllers' and 'processors'

Previously, under the DPA, processors had fewer obligations. Not any more. If you have anything to do with customer data you need to adhere to data regulations.

⚠ Online identifiers like IP addresses and cookies are now included

If you use Google Analytics or any other website tracking tools this change affects you. You will need to consider how you gather and manage this data.



⚠ You need to prove you are 'lawfully processing' contact data

There are three ways in which you can do this:

- Consent from the 'data subject' (the individual) - this will be the most common method BUT it is not the only one
- For the necessary performance of a contract/service
- It is in the data controller's legitimate interest - this is a delicate method as you must balance the individual's needs with the business's needs. Beware - this sounds like the easy option but the Information Commissioner's Office (ICO) will be watching organisations claiming this method carefully

You may use different lawful processing methods for different types of data, that's fine. But, remember, consent is required for each type of data collected - this is known as 'granular consent'.

⚠ Recording of consent

If choosing the consent method, you must record the fact that consent has been given, preferably in your CRM system. You will need to record who consented & how, when consent was given and what the consent policy was at the time.

⚠ Privacy by design

In order to ensure you can effectively do what's required, such as recording consent, the regulation suggests you follow a 'privacy by design' attitude. Work with your various data management providers (email marketing platforms, CRM systems etc.) to ensure that your contact data is suitably protected.

⚠ Data protection officer

If you are a public authority, or carry out large scale monitoring of individuals or carry out large scale processing of data, you will need to appoint a Data Protection Officer.

⚠ Data impact assessments

If you process sensitive data - e.g. race, ethnicity, political opinions, biometric/genetic, religious beliefs, trade union membership, physical/mental health, sexual life, criminal offences - or if you are deploying a new technology, you will need to conduct a Data Impact Assessment.

⚠ A person's rights are increased

Under GDPR, people's rights are increased. They have more rights to access their own data; the right to be forgotten by your organisation; and they now have the right to object to being profiled (generally done for automated marketing purposes). They also have the right to move their data to another organisation and you have to provide it in an easy to use format.

⚠ Data breaches

You must now have a process in place to detect, report and investigate data breaches. You must also now report data breaches to the ICO within 72 hours.

What do you need to do?

☑ Conduct an audit

Understand where you stand currently when comparing your current data practices against new GDPR requirements. Create a plan of what needs addressing.

☑ Review all internal policies

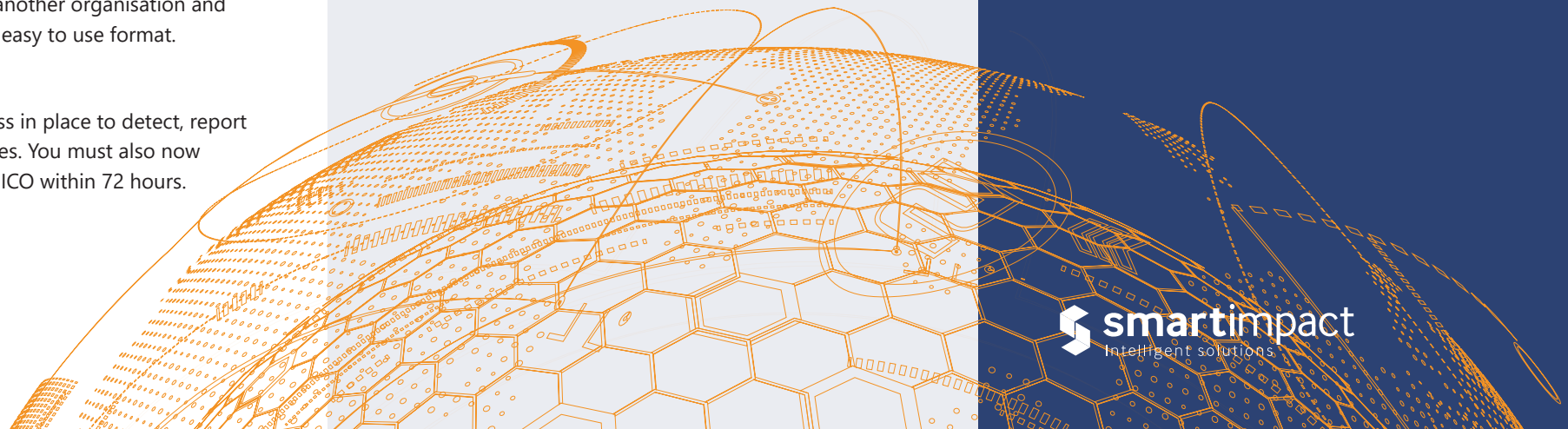
What's missing, what needs updating?

☑ Review your consent notices

Are you asking for consent at every point of data collection? Are you providing the opportunity to opt-out at each point (granular consent)?

☑ Ensure all your data system providers are compliant

Are all your data system providers compliant? You have a responsibility to make sure they are, or to not use them if they are not.



Getting ready

Here at **smart**impact, we work hard to make sure that all our CRM solutions comply with GDPR and continue to protect member data. We are working closely with our clients and third party partners, such as Microsoft, to ensure compliance is built into the very framework of each system we deliver.

This includes **the right to be forgotten**, **the portability of data** and **privacy by design** along with **consent tracking** and **granular preference services**.

We also believe in the close integration of your website, membership/marketing teams and CRM to provide a central repository with audit history on all members' consents captured.

You can get information on GDPR from:

The ICO website

https://ico.org.uk/for-organisations/guide-to-data-protection/whats-new/

Microsoft (check out their GDPR Trust Centre website) and we are here to help and advise.

Call us on 0845 544 2043.

smartimpact
Intelligent solutions