What is GDPR – and what must I do?

This month sees stronger rules take effect on consumer data protection right across Europe, including the UK. The regulations affect ALL businesses, whatever their size, with potentially huge fines for non-compliance. Here, Registered Gas Engineer sets out what you need to know – and do.

At first glance, the EU General Data Protection Regulations (GDPR) might seem scary and onerous, but the actions you need to take are more straightforward than you might think, especially if you're a small business.

The rules are aimed at making sure that people have more control over their personal data, and GDPR should boost consumer confidence – and, in turn, business – says the European Commission.

What your company must do
Protect the rights of people who give you their data.

Communication
- Use plain language
- Tell them who you are when you request their data
- Say why you are processing their data, how long it will be stored, and who receives it.

Consent
Get their clear consent to process their data.

Access and portability
Let people access their data and give it to another company.

Warnings
Inform people of data breaches if there is a serious risk to them.

Erase data
- Give people the right to be forgotten
- Erase their personal data if they ask you to do so.

Marketing
Give people the right to opt out of direct marketing that uses their data.

Safeguarding sensitive data
Use extra safeguards for information on health, race, sexual orientation, religion and political beliefs.

Do data protection by design
Build data protection safeguards into your services.

Keep records
Small businesses only need to keep records if data processing is regular, a threat to people's rights and freedoms, or deals with sensitive data or criminal records.
Records should contain:
- Your customer's name and address
- The reason for data processing
- Description of the categories of data subjects, and personal data
- Any transfer of data to another organisation or country
- Time limit for removal of data, if possible
- Description of security measures used when processing, if possible.

Do I need to appoint a data protection officer?
Not always: it depends on the type and amount of data you collect, and what you do with it. If you're a sole trader or small business that contacts your customers infrequently to promote your business, you're unlikely to need a data protection officer and you don't need to register your company with the ICO.

What are the penalties for non-compliance?
The Information Commissioner's Office monitors compliance, co-ordinated at EU level. The cost of breaking the rules on GDPR can be high:
- Warning
- Reprimand
- Suspension of data processing
- Fine – up to 20 million euros or 4 per cent of turnover.

Further reading
The European Commission has produced a simple illustration about what GDPR is, and how it could affect you. It's what we based this article on. You can read it here:
http://ec.europa.eu/justice/smedataprotect/index_en.htm
More information here:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
https://www.hubspot.com/data-privacy/gdpr-checklist

Are you ready?

Our friends at Commusoft have created a useful checklist designed for small field service businesses – like many registered gas engineers. Here are some of the main actions and points to check to make sure that you're complying with GDPR.

What data do you collect about your customers or prospects?
- Name
- Address
- Phone number
- Email address
- IP address
- Date of birth
- Banking information
- Details about a customer's home, such as boiler details
- Other.

How do you collect this information?
Is it online, by email, phone, text, in person?

Why do you collect the data?
- For marketing
- To complete a job
- To accept or track payments
- To send reminders and notifications.

Where do you store the data?
- In physical files
- In a database
- In an online database
- In an app.

With whom do you share this data?
- Our employees
- Our suppliers
- Outside agencies
- Others.

Data protection practices
Make sure that any data you hold or collect is secure. Have firewalls and internet gateways in place; update passwords and create separate user names and passwords for each user; remove unused software from desktop computers, tablets and phones; cancel system access for former employees.

Get consent
You must ask for permission before you collect and use your customers' data. Any permission form must easy to understand. Ask people to opt in and explain how you will use their information. People must agree to or opt out of different types of processing – they can opt in separately for newsletters and service reminders. You must tell them how they can opt out later if they change their mind.

If you already have a database of people from whom you haven't received consent, you don't need to contact them again if you can prove that you complied with the Data Protection Act when you gathered their information in the first place. If you don't know whether you've complied with the Act, it would be wise to contact them again to get their explicit permission to store and use their data.

Data breach
You should create an action plan for how you will deal with a data breach that might result in a risk to your customers – for example, if your customer's credit card details are compromised.
You also need to tell the Information Commissioner's Office within 72 hours and notify the people affected.

Create a privacy policy
This should be written in clear language and include information about what data is collected, and how it's used, how long it's kept and the fact the people can complain to the ICO if they think their data is being mishandled.

You can find out more and download The Complete GDPR Checklist for Field Service Businesses at:
https://blog.commusoft.co.uk/business/field-service-businesses-gdpr