GDPR - General Data Protection Regulations

LOSE CUSTOMER DATA

LOSE YOUR BUSINESS*

Kent County Council
kent.gov.uk

GDPR

General Data Protection Regulations

The new General Data Protection Regulations (GDPR) come into effect on 25th May 2018 and replace the Data Protection Act. This will affect every business that handles customer information, how they process it, how they gain consent and how they keep it safe. Here is some information to help you prepare your business for GDPR.

***** Pay €20 million or 4% of global turnover for a breach of the GDPR. Also, if you fail to notify the ICO of a breach it can result in a fine of up to €10 million or 2% of your global turnover.

DEFINITIONS

Personal data is "any information relating to an identified or identifiable natural person" so name, address, date of birth, telephone number, email address, photograph etc. of an individual.

Data controller decides what will be done with the data. GDPR checklist for data controllers.

Data processor is responsible for processing the data for the controller. GDPR checklist for data processors.

Information Commissioners Office (ICO) independent authority who uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. ICO Website.

UNDER GDPR YOU MUST:

1. **Tell your customers how you will use their information (data).**

   Example: If you keep your customers name, address, email and telephone number to send them a reminder about their annual central heating service, make sure you clearly inform them of this.

   Visit ICO for more information on Lawful basis for processing

2. **Tell your customer who you share their information (data) with.**

   Example: If you do not, ever give your customer details to anyone else, tell them that you do not share their data but if you do then you must tell them who you share it with and why.

   Visit ICO for more information on Right to be informed

3. **Make sure you have their agreement to process their information (data).**
   You must have a lawful reason to process your customers data and clearly state this in your privacy notice. A lawful basis means that collecting processing is 'necessary', if it isn't necessary, then it won't be lawful.

   Visit ICO for more information on Lawful basis for processing and Special category data

4. **You must show how you got their agreement and what was agreed.**
   Consent requires a positive opt-in, don't use pre-ticked boxes or any other method of default consent and you must keep evidence of consent – who, when, how, and what you told people.

   Visit ICO for more information on Consent

5. **Individuals have the right to access their personal data and you must allow your customers to ask for their information to be deleted.**
   Often called 'the right to be forgotten'.

   Visit ICO for more information on Right to erasure

6. **You cannot charge a fee when your customers ask what information you have on them and you must reply, in most cases, within one month.**

   Visit ICO for more information on Right of access

7. **You are responsible for making sure your customers' information is safe – you must take reasonable steps to prevent theft and access.**

   Example: Storing data in a notebook, phone or tablet represents a risk because the personal data for which you are responsible could be stolen, lost or hacked. Equally if you store data in the cloud, the data leaves your network and is processed in systems managed by your cloud provider. You therefore need to assess the security measures that the cloud provider has in place to ensure that they are appropriate.

   Visit ICO for more information on Security

8. **If you lose your customers' information or your systems are hacked you must tell the ICO within 72 hours as well as the customer whose information has been lost or stolen.**

   Visit ICO for more information on Data breaches

9. **If you process the data of children, you will need to obtain consent from the parents or guardians.**

   Visit ICO for more information

10. **Pay €20 million or 4% of global turnover for a breach of the GDPR.**
    Also, if you fail to notify the ICO of a breach it can result in a fine of up to €10 million or 2% of your global turnover.

NEXT STEPS

- Carry out an audit of what data your business holds on its customers.
- Delete any unnecessary data. Don't store data for any longer than necessary.
- Do you use subcontractors and share personal data with them? Don't forget to consider the risks in sharing data and make sure any contractors (as a data processor) are storing the data securely.
- Assess any potential risks to the data, for example customer credit card details could be vulnerable if your system is hacked, or if you lose your smart phone where personal data is stored.
- Review your security.

Online resources

An Introduction to GDPR - Click here for a free overview course.

Cost effective online learning – The essentials of GDPR use code KENTGDPR20 for £5 off until 30.04.18

Further Advice

Find out how GDPR will affect your business and what you need to do.

A dedicated advice phone line is available for small businesses from the ICO (Information Commissioners Office).

This information is intended for guidance; only the courts can give an authoritative interpretation of the law. More information can be found on the ICO Website.