GDPR QUICK GUIDE

SUMMARY

The EU's General Data Protection Regulation ('GDPR') dramatically increased potential penalties for failing to properly protect customer data and businesses need to be prepared.

WHAT DO YOU NEED TO KNOW?

- It took effect on **25th May 2018**
- It applies **to all businesses who offer goods and services to data subjects located in the EU** – even if **you** are not EU based. This includes post Brexit Britain
- It applies **to businesses of all sizes and scales**
- GDPR focuses on the **rights of data subjects** and ensuring there are appropriate processes in place for **identifying and responding to data breaches**

There are simple steps you can take to prepare for GDPR and ensure you are well on the way to being compliant.

DATA BREACH RESPONSE

GDPR introduced EU wide mandatory breach notification requirements, meaning you must report certain types of data breaches to the relevant EU regulator within 72 hours at the latest. In more severe cases, you may also be required to notify all your impacted customers.

You should ensure that you have thought about what you would do in the event of a data breach, including identifying where you can go for assistance if you need it. Those employing third party processors should ensure that contracts require processors to notify you of a breach within a set timescale, ideally allowing you sufficient time to comply with your own notification obligations.

Depending on breach severity, you may need help from legal specialists, forensics experts and public relations gurus. CFC provides these as a component of our cyber cover.

RIGHTS OF DATA SUBJECTS

With all the fuss about cyber security and having an appropriate data breach response plan in place, it's easy to forget that the GDPR is just as concerned with the rights of data subjects. What does this mean?

You need to know what types of customer data you collect and how you process this data. You must also ensure that you have either an appropriate legal basis for collecting the data or that you obtain your customers' specific consent to collect and process their data. Customer data is not limited to personal information – names, address, dates of birth, etc. – but also includes other identifying information like biometric data or CCTV images of your customers.

Where you outsource aspects of your business to third parties, and you provide them with access to your customer data, you need to ensure that you have in place a contract with these parties. This contract should contain certain key clauses governing how they may process and use this data.

GDPR QUICK GUIDE

You must ensure that you have in place a data registry or data map – a listing of all the customer data you collect and where it is stored. This is because the GDPR creates new rights for data subjects and strengthens existing ones. For example, EU customers will have expanded rights to request copies of their data from you, request that you amend the data you hold on them, and lastly will have the 'the right to be forgotten', whereby you will have to erase all the data you hold on them.

HOW CAN YOU GET STARTED?

1) Have you done a self-assessment of your GDPR readiness? If **no**, a template is available.
2) Have you created a data map of the data that your organisation holds, the legal basis of that audit and who is processing that data on your behalf?
3) Have you reviewed your privacy statement to ensure compliance? If **no**, useful guidance from the Information Commissioners Office including good and bad privacy notice examples can be found on the ICO web site: https://ico.org.uk/