

## DOES BUSINESS REALLY NEED TO **WORRY ABOUT GDPR?**



Replaces existing Data Protection Act 1998

Affects every one of your clients

Increases fines to €20,000,000 or 4% global group turnover (if higher)

85% of your clients do not comply according to Information Commissioners Office

This is a question I have been asked a lot recently. It is a good question and throws up a lot of issues. I think it is probably useful to set a little context first so my answer has some useful substance.

### Some **background**

The current legislation which the GDPR is replacing is the Data Protection Act 1998 (the DPA).

Essentially, the DPA requires anyone who collects names and other details of any living individual (business, retail, patient, subscriber or member) on computer or other electronic means or in an organised paper filing cabinet, and uses it for more than just providing the goods they sold or the services they provided, has to register. That means anyone who was more than a window cleaner or corner shop keeper should register. These days even those businesses should register.



The startling fact to note is that according to the Information Commissioners Office only 8% of the United Kingdom's 5.4 million businesses have registered. If you limit that to the 2.45 million registered for PAYE or VAT then it is about 16%. Whichever way you look at it the vast majority of businesses have totally ignored these laws.



Number of UK businesses



Number of businesses registered with Information Commissioner



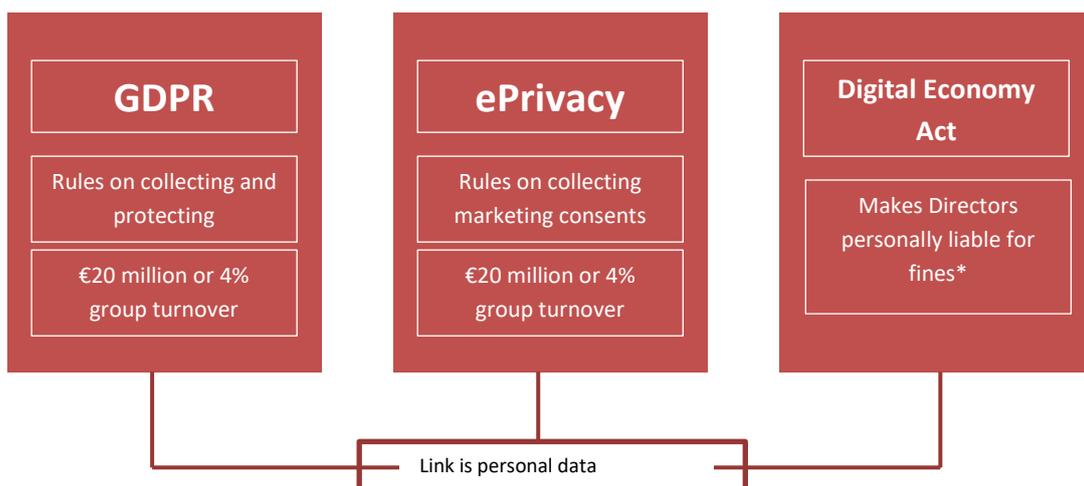
Percentage of UK businesses that suffered a data breach last year according to UK Government

The Data Protection Act is a most inappropriately named piece of legislation, because it is founded on 8 principles or rules – only 1 of which is about protection.

The other 7 (8 when you include the marketing rule) are about how to lawfully collect and use that personal information in the first place. The reasons for that imbalance is simple - information is where the value lies: protection is just something you have to do once you have it. You don't add value to information by protecting it; but huge losses lie in not protecting it.

If you aren't protecting your computer systems, as we know now, you are in danger of losing a lot of money, but if you don't collect it lawfully in the first place you are now in danger of losing your entire business, even your home. I will cover this in the next article.

### First, it is not just about the GDPR



Collecting personal data whether that is B2B or B2C is governed by the above rules. Both sets of fines under the GDPR and ePrivacy rules can apply at the same time, exposing businesses to €40,000,000 or 8% group turnover in fines.

In light of the fact that 92% of the businesses you currently coach are not currently compliant the chances are they will face a fine at some point for the reasons I will set out below.

It has just been confirmed that the Information Commissioner has won the argument and the Digital Economy Bill which will **\*make Directors personally liable for fines** levied under the ePrivacy regulations (fines the ICO also administers).

## **Second, it's the new norm**

Business these days lives online or in their computers, there is no alternative these days. Compliance with the rules that cover these areas has to be observed. I know it has not been the case so far, but consumers are increasingly aware of their online safety and privacy, as surveys have consistently shown.

Business will have to demonstrably comply in order to keep and attract new business, which is why the GDPR contains requirements for business to display Privacy Seals to show they are compliant. Any business that does not have one of these seals will suffer in the next few years as customers go elsewhere, to businesses that do display these marks of trustworthiness.

## **Summary**

It is now a core feature of business that it has to comply with the rules that apply to the collection and use of personal information, including for marketing, as well as its protection.

Failure to realise this will see regulators force businesses out, as they pose a risk to the creation of a safe online environment.

So does business need to worry about the GDPR? In my view it is a clear yes, and not just about the GDPR as you will discover in the next in the series.

Ian Sinclair-Ford

DataGuardz

May 2017