“Don’t Panic”, it’s only GDPR

On May 25th 2018, a new piece of legislation comes into force which will, to a greater or lesser degree, affect every one of us. It places new duties on all types of organisations, whether a commercial company, a non-profit organisation, statutory sector etc., and gives new rights to individuals concerning their “personal data”.

Depending on who you listen to, the General Data Protection Regulation (GDPR) is either absolutely terrifying or a load of hot air. The truth is (as is so often the case) somewhere between the two extremes. GDPR certainly deserves to be taken very seriously but, in essence, it enshrines in law the sort of principles that most decent people would regard as common sense and courtesy.

The current legislation covering personal data is the Data Protection Act 1998, devised 6 years before Facebook was born, when twitter was something that birds did. Since then, the world of social media has resulted in an explosion of sharing of personal information, which unscrupulous people have sought to use to their own advantage. The concepts of identity theft, SPAM and cyber-bullying have all arisen in just one generation.

GDPR seeks to restore the ownership of personal data to the individual to whom it relates. It won’t stop bad people from trying to do bad things, but it should make it just a little bit harder for them, and a little easier for individuals to protect themselves.

What is Personal Data?

Personal data is anything that is used to identify an individual; names, address, e-mail, date of birth, NI number, memberships, bank details and so on. The individual that the information relates to is known as the Data Subject. Generally, one piece of information by itself will be of limited value to a crook. It is when a number of pieces of data are collected together that they can become useful.

Of course, it is essential that data is collected and used for legitimate purposes. An employer, for instance, has to be able to identify his/her employee, and will need bank details to effect payment and NI details to account for what is due to HMRC. What GDPR aims to do is to;

a) discourage bodies from keeping more information that they really need, nor for longer than they need it,
b) ensure that such information that is necessary is kept securely and used only for legitimate purposes,
c) encourage the keeper of personal data to securely dispose of the same when it is no longer needed,
d) give the owner of the information the right to inspect any information held about them and, under certain circumstances, to demand its destruction.

I think most people would agree that these principles are entirely reasonable, and it is probably true to say that most cases of loss of sensitive data are due to carelessness (a laptop left on a train, a data stick mislaid, or an e-mail sent in error to the wrong person) rather than deliberate action. So the purpose of GDPR is, perhaps, simply to force organisations to give a higher priority to the subject of data security than they have done to date.

What if I ignore it? Will it go away?

Afraid not. The Data Registrar can impose severe penalties for non-compliance (although you probably don’t need to fret about the maximum penalty of 20m Euros unless your name is Mark

Zuckerberg). If you run a small organisation holding only a small amount of personal data, a few simple measures to assess and address any risks will be sufficient, but you must be able to demonstrate that you have given the matter appropriate thought and have taken "reasonable" measures to comply.

So what does my organisation have to do?

Here is a brief checklist.

- Conduct an internal audit of all the personal data that you hold.
- Do you have a legitimate reason for holding it?
    - It is necessary to enable you to perform a service for your client
    - There is a legal requirement to retain it for a given period (i.e. tax & payroll)
    - The data subject has given explicit consent
- Is it stored securely?
- Who do you share it with?
- How is transmitted?
- Do you hold it longer than you need it?

The answers to these questions will almost certainly prompt some actions, which might include;

- Seeking consent where existing consent cannot be evidenced (note - the new regulations demand a positive "opt in" rather than failing to opt out)
- Taking measures to improve security
    - Password protection
    - Data sticks (unless encrypted) are a really bad idea
    - Are you happy with the security/privacy of e-mail networks?
    - Do staff understand how to use (and the importance of using) the BCC facility?
- Instigating policies for a regular clean-up of personal data and secure disposal thereof.
- You should also plan what to do in case of a data breach (breaches must be reported within 72 hours).
- And know how you will respond to an individual's request to inspect his/her personal data.

In many cases there are no right or wrong answers, but you must be able to show that you have taken "reasonable" measures. If you can truthfully say that you treat all personal data with the same care that you would wish to be taken with your own, you probably won't go far wrong.

A vast amount of information is available through the Information Commissioner's website and elsewhere to help you in addressing this issue, and we at HVA hope to be able to make further resources available very soon to our members. It is most certainly a subject which must be taken seriously, but just remember … Don't panic … it's only GDPR.

Note – this article was compiled for the benefit of members of Hastings Voluntary Action. It is not intended to be a comprehensive guide to the subject, nor an exhaustive list of the measures that you should consider, but rather a gentle introduction to stimulate further discussion.