GDPR - What should you be doing?

- Published on April 12, 2018

Personal data is very much in the headlines at the moment - you just need to ask Mark Zuckerberg about that - and as a result individuals are becoming more aware and protective about their personal data and their rights. Data protection is not therefore something to be brushed aside and to be looked at only if something bad happens. At that point it is too late.

However, despite such sensational incidents like Facebook / Cambridge Analytica, and despite a lot of scaremongering over the past 6 months to a year, the reality is that the General Data Protection Regulations is just a means of updating the Data Protection Directive which the EU introduced some 20 years ago. Of course businesses do still need to be very much aware of the implications of the rights and obligations under the GDPR.

There are now just over 6 weeks before the EU's GDPR comes into force. Companies should already have processes in place for the safe handling of all personal data, so adapting to the new regulations should not be too onerous. If your business operates in England and you have not already registered with the Information Commissioner's Office (ICO) and are not aware of your obligations under the current Data Protection Act 1998, then you will have more to do to be compliant, but the way you go about assessing what needs to be done is exactly the same, namely you need to conduct an audit of your processes, policies, contracts and systems. As a result of GDPR companies do need to be more vigilant on the processes and policies they have in place, and to make sure that the personal data they hold is secure and not open to abuse, either by them or a third party.

So, for example, if you are transferring personal data to a third party you need to make sure that that company has the appropriate safeguards in place. You also first need to make sure that the data subjects have been made aware of (in clear and intelligible language) and have approved all the different types of processing which will take place. You will probably have a justifiable purpose for processing personal data, so it is just a case of making sure that this is explained to the data subjects. Crucially, if you are going to implement a new system or automated process which uses

personal data, then you will need to determine whether a data protection impact assessment needs to be conducted. Similarly, if you are going to process personal data in a different way from the purpose for which the personal data was originally collected, then you may have to obtain fresh consent. And remember, if you are dealing with 'sensitive personal data' then extra care needs to be taken. There are also some minor changes, such as the time limits for responding to a Subject Access Request, and the need to notify the ICO of a breach within 72 hours. Also, after 25 May 2018 (when your current registration with the ICO expires) you will have to keep your own records of the personal data you process and the reasons for doing so, but you will still need to pay an annual 'data protection fee' to the ICO .

So with the introduction of GDPR you do need to be very careful with personal data as the consequences can be severe (in the most serious of cases) - not just in terms of increased fines but damaging PR. You therefore need to make sure that you will comply with all your obligations arising from the GDPR, but it is something which is very manageable. This article is not meant to provide a short-cut to what you need to do, but hopefully it will put in perspective the size of the task you may face, and the reality is that it may not be as big a task as you imagine. To know how compliant you will be you should conduct a full audit of how you handle personal data, as well as all the contracts, policies, processes, and systems you have in place, and then implement any changes which might be identified. If you do that, then breaches of personal data should only be something you read in the papers.