GDPR Post 25 May - So what now?

- Published on June 4, 2018

So, 25 May has come and gone and we are now living in a “GDPR world” - but what does that mean and what has actually changed?

Well, to a degree nothing has really changed - unless of course you are Facebook, WhatsApp, Instagram or Google, facing billion dollar claims by the campaign group Noyb (Max Schrems) in Austria, Belgium, Germany and France, respectively! For the rest of us, as long as personal data has been properly obtained, is being properly protected and is not being misused, you will be most of the way there.

What has changed, apart from a tightening of the processes to be followed and an extension of the rights of individuals, is the need for transparency, and for confirmation that the processing of personal data is lawful and justified (and that this has all been explained to the personal data subjects in clear and plain language). Importantly businesses are going to have to make sure that their business partners with whom they share personal data are also GDPR compliant, and if you are not able to provide this confirmation then you may find that your business partners are no longer prepared to deal with you. Similarly, if your business partners are not GDPR compliant, then if you continue to deal with them then you will find that you are also in breach.

So the key question is how do you know if the steps you have taken, or are in the process of taking, are GDPR compliant? The best way to measure this is to review your “Information Register” and keep it under review. You have to make sure that all appropriate technical and organisational measures are in place for the processing of personal data, taking into account the nature, scope, context and purpose of processing, and the rights of individuals (*see Article 24* of the Regulations). But what does this actually mean, and how do you know whether you have adopted the correct measures? Unfortunately, there is no universal standard. It will depend on the type of business you have and the reasons you have for collecting personal data. However, if you have considered and made reasonable provision for all aspects of the new regulations and you have in

your Information Register a paper-trail in which the justification for the decisions you have taken is recorded, then you are in a good position for maintaining that you have taken all reasonable and appropriate steps.

As a general guide your Information Register should contain the following:

1) contact details of your data protection officer, or data protection manager (*Articles 37-39*).

2) a list of all the different types of personal data you hold, and where it comes from (*Article 4*).

3) a list of the lawful reasons you have for holding / processing the different types of personal data, and confirmation that this has been explained to the data subjects (*Articles 6, 13, 14*).

4) details of where the personal data is held, who has access to it, and the measures which are in place to ensure that it is kept securely and only available for the purposes permitted by the data subjects (*Article 32*).

5) a list of third parties with whom personal data is shared – and an agreement or written confirmation with each of them that those third parties have the necessary safeguards in place (*Article 28*).

6) details of any automated processes involving personal data (*Article 25*).

7) a list of all the policies which are in place (e.g. privacy policy, retention policy, notification of breach policy, responding to subject access request policy etc.).

8) a record of when annual training is provided to all staff (*Article 39*).

9) provision for recording any “data protection impact assessments” (*Article 35*).

If your Information Register is complete, then it will be difficult for the Information Commissioner's Office ("ICO") to find fault. In the event the ICO does become involved then your Information Register will be key to demonstrating the steps you have taken and why you considered that to be appropriate and adequate. Even if the ICO does not agree that you have taken the requisite steps, if you have demonstrated a reasonable approach

to GDPR compliance then it will be difficult for the ICO to do anything more serious than issue directions for corrective steps to be taken.

GDPR is not a bear trap. All it has done is ensure that the ever increasing volumes of personal data in this technology driven era are properly protected. It has made personal data an even more valuable commodity that it already was, and anyone who doesn't have the GDPR compliance "kitemark" in place will not be able to conduct business on the back of that commodity.

-------- If you have any queries about GDPR then you do need to take specific advice. If you want to contact me, Carl Robinson, CMR Advisory Ltd please visit www.cmradvisory.co.uk--------