4 June 2017

Boomerang Funding

Do Data Protection by Design – or Face a Fine!

Jun 4, 2017 | Blog | 0 comments

All businesses large and small must be aware of major changes to data protection law coming in May 2018 and should be preparing now, says Paul Motion of BTO Solicitors LLP who has represented organisations under investigation for data breaches.

Most small businesses and start-ups share the same worries. Finding premises, paying the rent (and the bills), dealing with paperwork, staff issues and employment law, the good leavers and the bad. Then there are such trifling matters as making things, or providing services, getting out and selling, differentiating your product, winning and keeping customers and ultimately, with a bit of luck, even making a profit. Data protection law isn't generally high on the mangement radar. But it should be. After 24 May 2018, it absolutely must be.

Existing data protection fines (up to £500,000) are bad enough but start-ups and SMEs will not be able to afford the new upper limit from May 2018, which will be a fine of €20 million. However, the eye watering new fines are being sensationalised by too many commentators in my opinion and shouldn't be the reason your business complies with the new General Data Protection Regulation (GDPR). You should be building data protection in to everything you do, as of now. From May 2018 the law will require you to run your business on the basis of "data protection by design". This will be particularly important where you need to obtain and prove consent, typically where you use customer data for direct marketing and where you have bought in customer lists or used a direct marketing agency to promote your business. Contrary to what many commentators are prone to suggesting about the GDPR, as with the current data protection law, consent *isn't* always required. There are many situations where data processing can be carried out without consent. However, where consent *is* required, the bar will now be far higher and the penalties for not being able to demonstrate that the new "explicit" level of consent has been obtained will be much greater from 2018. So you will need to think about your terms of business, your contracts, your privacy policies, your website forms and your sign-up pages. These will have to be in clear language without small print. It will be illegal to obtain consent using pre ticked boxes: that simply won't be treated as 'consent'.

If your business processes personal data on behalf of another organisation then at the moment you are classed as a Data Processor and don't need to worry too much about data protection law. This will change in May 2018. Both the Data Controller and the Data Processor will have obligations under the GDPR and Data Processors will also be subject to enforcement action including fines and compensation.

Compensation claims are going to increase. People are becoming more aware of their privacy rights and their right to compensation even under existing data protection law. Get data protection wrong and compensation can be awarded for "distress" caused by your error.

The law will also change in 2018 so that a data breach has to be reported to the National Regulator within 72 hours where "the breach is likely to involve significant risks to data subjects' rights and freedoms".

Let's not forget about Brexit – What difference will this make? In my opinion, none. The GDPR will come into effect well before the Brexit negotiations are concluded. It seems inconceivable that if it wishes to do business with the remaining 27 member states, Britain would create a radically different data protection regime.

What this looks like in practice for your business is over to you. There is a lot of useful guidance on the ICO website for example their GDPR Self Assessment tool. Given recent cyberattacks on the NHS and elsewhere, you should be keeping security of personal data at the forefront of your thinking. SMEs should consider signing up to the Government's "Cyber Essentials" programme.

We are seeing an increase in data protection distress claims and one commentator has described data protection as "the new health and safety". Make sure its not your business which trips up!

Blog by Paul Motion