Why does my website need to be GDPR compliant?

Your website is often the first contact a potential client has with your business, and as such it is vital that it gives the right impression. You may have engaged a great web developer, who has designed a clean, modern looking site, with SEO optimisation that brings you to the top of any web searches. You may also have lots of relevant content and regularly update it to keep it interesting. Isn't that enough?

It might be, but how are you fulfilling your GDPR obligations on your website? This is a vital part of how you present yourself to your clients, and if you don't get it right then you could be inadvertently telling your clients that you don't handle their personal data (information) correctly so they won't be confident enough to use your services.

In my role as a Data Protection Officer, I have found that the general public is generally more aware about their data protection rights, and very willing to exercise them. If there is the slightest hint that you have obtained and used their data without their consent, then they will complain. And if you haven't told them how you will use their data and keep it safe through a suitable notice on your website, they will click away from your site and will not use you.

As well as running the risk of lack of willingness of clients to engage your services, a website that is not GDPR compliant also risks enforcement action or fines from the UK's data protection regulatory body, the Information Commissioners Office [ICO]. Under the Data Protection Act 2018 they have the power to fine companies 4% of its annual global turnover or £17.5 million (whichever is higher) if you're found to be failing in your data protection obligations. Could your company afford to lose 4% of its turnover?

If your company holds Director and Officer or Cyber Liability insurance, you should check your policy wording to see if these policies will cover you for any ICO fines, as well as your defence costs or costs incurred as a result of a data breach. But three years on from GDPR implantation, we are still waiting to see if these policies would cover you for any ICO fine, as there still isn't any case law to give a clear ruling on this. Surely it's better to get your GDPR compliance correct instead of running this risk to your business?

And finally, if you are subject to enforcement action or fines from the ICO, they publish the action that they take and it is available to anyone via their website. This could risk significant reputational loss to your business. You might 'get away with' individual clients not realising that this had happened, unless the story appears in the national press, and so your client base may be unaffected. But what about if you want to sell your business in the future? Any due diligence process would pick this up and it might be enough to reduce the valuation or even prevent the sale.

With all of this in mind, isn't it time that you reviewed your website for GDPR compliance?

About



Sarah Hodgkin-Bates is a qualified GDPR Practitioner and director of Fintect Limited www.fintect.co.uk If you have any comments or questions about this article or GDPR in general, please email her at sarah@fintect.co.uk

© Fintect Limited