

Why bother with GDPR now Britain has voted to exit the EU?



Over the past months, TrueSwift's clients have been taking a sharper interest in the General Data Protection Regulation (GDPR). It seems the message is getting through and has started to be taken seriously. However, one question I have been asked on several occasions is 'What will happen if Britain decides to exit Europe?'

On Friday 24th June, 2016 the result of the British electorate was confirmed and they chose to leave Europe. In light of this, should we still worry about GDPR? In my opinion, absolutely. If you are a company that processes data from any EU citizen, then you will still be liable under GDPR.

Even if you do not process EU data, I still suggest that GDPR is relevant. To start with, although Britain has elected to leave Europe, the process has not yet started and when it does start, can take 2 years. Initially David Cameron was going to invoke Article 50, the process to initiate the leave from the EU, immediately, but as he has decided to step down by October, the decision to invoke Article 50 will likely be after a new Conservative leader has been selected. Only then will the 2 year exit process start, and until this is finalised, Britain will still be under EU law including GDPR.

The second reason the GDPR process should be taken seriously is to do with the exit process. Each of the European laws will be evaluated and either written into British law (with or without modification), or removed. As the GDPR is a sensible law protecting citizens' identity and data, it is highly likely that the GDPR will be one of the laws taken into British law as is, or an updated version.

The data protection minister Baroness Neville-Rolfe has stated "All of us... need to consider carefully what might be done to replace [the GDPR] if and when it ceases to have effect or in the event that it never comes into force". According to 'Computing' she has also stated that "any country wishing to share data with EU member states or handles EU citizen's data will need to provide adequate protection".

Lastly, even in the unlikely event that Britain chooses not to adopt GDPR, the concept of understanding what data businesses have within their environment and protecting it is sound practice. At a minimum, regardless of whether GDPR is relevant to your organisation or not, preventing accidental data loss or even deliberate information extraction should be high on everyone's agenda. Encryption technologies and workstation port lockdowns can be used effectively in this regard.

For most organisations, step one is to gain an understanding of exactly what information the company is holding. Recent studies show that file servers are notorious for containing vast volumes of data, the majority of which is 'dark' and unknown to the business. New technologies exist to facilitate this task enabling intelligence and value to be drawn from the

results. From there, controls can be put in place to effectively manage (and even remove) stale, unused and redundant data. The benefits are very tangible – greater control, less storage, lower costs and streamlined legal searches – all positive and all relevant in the larger GDPR picture.

Author: Andrew Salmon
IT Director from TrueSwift Ltd.

TrueSwift is a world leading IT Consulting company in the area of Information Management. TrueSwift consultants have been involved with data archiving for more than 15 years and archive migrations for more than a decade.

TrueSwift further helps you manage your data by providing insight into the type and age of data stored in your environment, and providing legal disclosure experience from training to performing litigation discovery and review on behalf of clients.

TrueSwift clients range across all sectors. With UK Government security clearance TrueSwift clients include those from the Public Sector - Government, military, police, as well as the Private sector - banks, construction, retail

Published: 28th June 2016