Management Consultants in Big Data

BigData4 Analytics

The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years

By Jackie Down

Companies operating in Europe are dramatically underestimating the impact of new data protection regulation that comes into force in May 2018 and many are failing to prepare adequately for it. The EU's General Data Protection Regulation (GDPR) will require many companies to adopt much stricter processes in dealing with customer data.

The GDPR rules will mean companies must provide more information on how customer data are collected and retained, allow customers the "right to be forgotten", and implement special rules protecting children. Data breaches will have to be notified within 72 hours to the EU's Information Commissioner's Office.

While the growing inventiveness and sophistication of cyber security threats and attacks has made compliance and security top of mind for most organisations. We are all aware of the high-profile breaches that have happened, for example TalkTalk, Yahoo, and of course the recent ransomware attacks on the UK National Health Service, Telefonica, Renault etc. GDPR legislation has heightened this focus.

It appears that very few organisations have as yet started implementation, and this is with less than 12 months to go until organisation need to comply with the new rules. According to a recent survey by IDC of 700 European companies of various sizes, almost 80% of IT decision-makers have a poor understanding of GDPR's impact of or have not even heard of it. Of the 20% surveyed who said they were aware of GDPR, only 20% said that they already meet the new requirements.

There are many issues to deal with that will have long lead times, where development is needed to legacy IT systems. GDPR is not a tick-box compliance exercise. Organisations must start working hard to get ready for the new legislation or pay the consequences. Non-compliance can lead to an administrative fine up 4 per cent of the previous year's annual global turnover, or €20m, whichever is the higher.

Big data complicates the process of maintaining compliance for GDPR regulations, as well as other privacy rules. GDPR guidelines apply to all the data that is gathered throughout the big data analytics ecosystem, whether it is willingly provided by customers or gathered by automated systems.

Managing of all this data may seem like an insurmountable task! Whilst GDPR builds on the existing Data Protection Act, it's a sizable piece of legislation. But with closer regulatory oversight anticipated, especially on the SME community, it's important to get going now and have a comprehensive governance action plan in place.

A major challenge with GDPR compliance is dealing with the untold amounts of data that is hidden in unstructured content, and possibly within unsearchable documents stored as image formats, across an organisation. If this data includes sensitive information such as payment information, passport information, health information, or other Personally identifiable information (PII), it needs to be identified.

The first phase of any plan will be the discovery phase – 'The Data Audit'- the discovery process which is critical to identify all characteristics of the private data that is managed under GDPR compliance. This requires extensive exploration of data assets to understand if any rights (consent) have been given to use the data.

The data exploration process is far broader than simply identifying the private, personal data. It also includes identifying:

- How it is used (or will be used) — Seeing how the data is transformed, what processes use the data or derivatives of the data and what actions are taken because of the data.
- If consent is granted — Determining if the person gave consent to use the data and in what manner they allowed use of the data.
- Where it came from — Tracing the data back to its sources and how it was moved to different systems and different forms within the organisation.

Once private personal data is catalogued, categorised and split, it can then be secured and governed. Then the ongoing monitoring and managing process of all the data need to ensure on-going compliance.

Don't wait, start now on your GDPR action plan.

The UK's Information Commissioner recently commented: "*The digital economy is primarily built upon the collection and exchange of data, including large amounts of personal data - much of it sensitive. Growth in the digital economy requires public confidence in the protection of this information*." Therefore, it is in the best interests of businesses to ensure they get their act together when it comes to the new legislation.

Useful Links

http://www.eugdpr.org/

https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

https://dma.org.uk/gdpr