SNAPSHOT

GDPR

Data strengthens its defences.

BCS CONSULTING

Expect **Excellence**

What is GDPR?

The General Data Protection Regulation (GDPR) is an EU-wide initiative designed to strengthen individuals' data rights by introducing tougher standardised data protection laws across all industries throughout the single market. The regulation aims to put us, as individuals, back in charge of our personal data and stop organisations having the ability to profit from this data without our knowledge or there being a legitimate legal reason. The regulation covers all EU personal data and will go live on 25th May 2018.

Data legislation is certainly due an overhaul as the current legislation in Europe was implemented in the late 1990s following an EU directive in 1995. Since then, the way organisations and individuals use personal data has changed dramatically. The likes of Google, Facebook and Amazon are now able to harness personal data in a way that the current legislation could not have planned for. To illustrate this, 2014's global data volume was 85 times larger than that of 2000 and 90% of today's data volume was created in the last two years.

GDPR will come into force prior to Brexit, hence the UK must comply with the regulation regardless. Moreover, the UK will introduce a new Data Protection Bill, clearly signalling the UK's intent to be closely aligned with the EU on data protection in the future.

Why is it important to the financial services industry?

GDPR affects banks and insurance firms who process huge volumes of client and employee personal data on a daily basis. The sheer complexity and scale of change required for firms cannot be underestimated and will see them focusing sharply on managing their compliance functions, embedding the regulation and creating business value out of the process.

GDPR is both very broad and deep. It covers organisations of all sizes, across all industries. Even organisations outside the EU who process the personal data of EU citizens must comply.

Programme scope and subsequent implementation costs can quickly surge when reviewing GDPR elements such as data encryption and anonymisation, or when managing individuals' requests to receive all personal data an organisation holds on them.

In the event of serious data breaches, fines of up to 4% of global turnover can be issued and, as a result, our teams are seeing nervousness in the market. To calm the waters, the UK's GDPR regulator, the Information Commissioner's Office (ICO), has repeatedly stated that the purpose of the regulation is not to enforce penalties, but to ensure that proper thinking and design is applied to the processing of personal data.

What's the BCS view on it?

This is BCS's area of expertise and we are in a strong position to help clients here. GDPR offers an opportunity for organisations to go further than just complying. For example, those that have got the basics right could start to think about how to build further trust with their clients, improve the client experience and assure clients that their personal data is safe.

At the other end of the spectrum, organisations that need to catch up on necessary IT investments could use the GDPR as a good argument to finally do what was previously neglected, e.g. cyber security, encryption (encoding data so only authorised staff can read it).

In any case, a cultural change with regards to the treatment of personal data is fundamental to the successful implementation of the regulation.

Another point to consider is the role of the Data Protection Officer. All banks and financial institutions will be required to have a DPO, who will be responsible for monitoring compliance with the GDPR and other data protection laws. The DPO must report to the board, indirectly as a minimum, and be sufficiently independent with regards to decision-making (similar to the Internal Audit department). The key challenge for financial institutions will be in deciding how to position and structure this role to satisfy the regulation requirements, while enabling them to fulfil their responsibilities.

Finally, the GDPR is being introduced concurrently with other regulations such as MiFID II and PSD2. Whilst MiFID II seeks to improve transparency by encouraging data gathering, data retention and data sharing, GDPR mandates more stringent controls around the same activities.

Who should you speak to about it?

For more information, please contact Alastair Hegarty, Principal Consultant, at Alastair.Hegarty@bcsconsulting.com or Richard Stearn, Principal Consultant, at Richard.Stearn@bcsconsulting.com

SNAPSHOT