GDPR post-implementation – what next?

We explore the common themes and pitfalls of the General Data Protection Regulation (GDPR) implementation and highlight some key areas that require continual attention.

The General Data Protection Regulation (GDPR) came into force on 25th May 2018 following a two year transition period, which gave organisations time to prepare and implement the necessary changes.

In the months leading up to the deadline, there was an unprecedented level of activity in the market, which was a clear indication of the importance of data protection, the value of data to our working lives and the fear of getting things wrong.

Regardless of whether your firm has a tight grip on data protection, or is still getting its information governance into shape, one thing that we can all benefit from is a continual focus on the topic in an effort to promote and strengthen a culture of data protection.

As outlined in the previous GDPR article (Best practice), we have been involved in a great deal of consultancy with firms, both in the run-up to the deadline and post-implementation. In our experience, most firms shared similar concerns and almost every firm had the same weak links, regardless of size, structure or age.

In this article, we will briefly explore these common themes and pitfalls, as it may help to refocus our collective efforts and promote a data protection culture.

1 Training

Most firms hadn't paid serious attention to this in the run-up to implementation, with many stating that they found the technology and terminologies confusing and they didn't want to draw attention to their lack of knowledge. Others were of the opinion that their staff had fared well under the Data Protection Act 1998, so felt little need to invest in additional training.

A lack of training is a significant weak link, which every firm must address. If you visit the 'Action we've taken' section of the Information Commissioners Office website (https://ico.org.uk/action-weve-taken/), you will see that a large proportion of the fines and enforcement that have been issued can be traced back to a single individual, who unknowingly makes an error.

It is vital that every firm addresses their weak links before something preventable happens. Appropriate training programmes mitigates risk. It is that simple.

2 Subject Access Requests (SARs):

The prevailing initial opinions were, “that won’t happen to us”, “why would anyone be interested in what we hold – we only do insurance”, or, “our staff don’t have a problem with our HR so won’t make a SAR.”

Firms also commented about not having sufficient resources to attend to requests, not knowing how to recognise a request and not having relevant procedures or training programmes in place.

The bottom line is that it’s not optional - you can’t bury your head in the sand and hope that a SAR goes away. Once a request is made, which could be in writing, verbally, digitally, etc., the clock is ticking. If you don’t respond within the appropriate timescale, the ICO will take a very dim view of your approach to data protection.

Each firm must be proactive and put a policy and procedure in place for handling SARs. This policy should be strength tested regularly, to ensure that if it is ever needed, you don’t have to waste time working out what to do.

3 Lack of internal policies or procedures

The next common theme builds from the issues around training and SARs, and that is a distinct lack of policies or procedures. GDPR challenges each organisation to effectively ‘show their workings out’. What measures have you put in place and why? What systems do you operate and how have you determined their suitability? What steps do you take to protect the data you hold or process?

In addition to documenting decisions, the output of these decisions should be captured in policies and procedures which cover all of an organisations processing activity, security measures, staff responsibilities, technologies, etc.

The lack of procedures extends to the systems that brokers have in place to manage the data that they hold. For example, many firms did not have any way of identifying the consent statements that were in place when data was collected, or to segment data based upon its retention period.

Without an agreed policy or procedure, how do staff and stakeholders know what is required of them? Policies and procedures are a vital component in a firm’s overall governance structure.

4 Overall security

The ICO has long championed a ‘data protection by design and default’ approach, but many firms still routinely failed to tackle even the most fundamental issues, such as:

- **Clean desk policies and record handling -** a number of firms were storing personally identifiable information (PII) in paper form on desks, or in unsecured folders. This presents a significant issue as, not only is the information unsecured, but it is very difficult to identify if a breach has occurred and to determine the impact of any loss.

  The practicalities of active renewal or new business transactions mean that files are printed and left on a desk until completed. A few firms were still using faxes to send information but were not checking to see of if the fax machine was being manned at the recipient’s end, so were sending files without knowing if it was being left on a fax for days on end.

  A further issue was raised by a number of firms, who routinely stored client records in their cars between visits or even for extended periods of time.

- **Physical security -** this was largely satisfactory, with most brokers having appropriate security measures in place and sufficient lockable storage for client records. However, while most had the means to lock storage, not all storage was locked.

- **Digital security** - again, most of the IT systems in operation today had been well considered, but a number of firms hadn't paid attention to this in the context of security of portable data e.g. emails being sent with inappropriate attachments, confidential data being worked upon in public spaces which can be viewed e.g. on trains, loud telephone calls discussing clients whilst in a café, etc.

5 Data

Most firms had not conducted an information audit to identify the data they hold, to determine how it was obtained and to map the flow of information into and out of the organisation.

Without knowing what data they held, it was difficult to determine the existing consents or to document data processor agreements or which lawful base for processing would be relied upon under GDPR.

Furthermore, having not identified the data held, these firms also failed to consider breach detection. When asked, "could you identify a breach", the typical response was one of uncertainty.

Each firm must protect the data they process, they must document their data processor agreements, they must publish a privacy policy which documents their lawful base, and they must be able to identify a breach if one occurs.

Conclusion

Overall, there was a general lack of understanding of the GDPR regulations and confusion of how these would apply to the firm on a practical basis.

Thankfully, for those firms who tackled their responsibilities head on, they found that by taking the practical steps towards compliance, they were able to meet their obligations without too much disruption. For many, they also found that their business was more robust and operationally efficient as a result.

The one overriding theme was that firms hadn't thought about the extent of activity required and that by discussing it openly, it served to address their concerns around their own lack of knowledge and identify the practical steps they must take.

If you have any remaining GDPR hoops to jump through, my advice is to not delay any longer; there is little point in closing the stable door once the horse has bolted.

John Miller, Head of London Business, RWA Business Consultancy

John has more than 30 years' experience in the world of general insurance, working for some of the largest UK brands including Norwich Union and Aviva. His experience includes mergers and acquisitions, business development, marketing and propositions. At RWA John has responsibility for developing the business in London in addition to managing the relationship with several key clients.

For further information visit
www.ecclesiastical.com/broker

PD3028 1 10/18