The industry is failing to address the GDPR compliance challenge

DARREN WRAY

I spend a fair bit of my time speaking with senior people across the insurance sector, and when it comes to GDPR there are some common misconceptions that the market is suffering from. In this article I will explore some common GDPR fallacies and explain what steps insurance firms should be taking to ensure that they're on the path to international data privacy compliance.

Firstly, what are some of the headlines for GDPR?

This may dispel some of the myths or misunderstandings that some firms have developed.

The Fines; the potential fines that can be levied by GDPR are indeed large numbers. At their extreme they can be as great as €20m or (and this makes it important to companies of all sizes), 4% of global revenue, whichever is the greater.

The Scope; GDPR applies to a (re)insurance firm no matter where it is based so long as it is processing (collecting, storing or otherwise using) personal data of EU residents. For additional clarity, GDPR applies to UK based companies irrespective of Brexit, with the UK's Data Protection Bill 2017 on its way to becoming law at this time.

The Timeline; GDPR comes into enforcement from May 25th, 2018.

Where is the insurance market failing to address the GDPR challenges

The first driver of likely non-GDPR compliance is procrastination. In some cases this has been a result of not recognising the scale of the GDPR challenge, which in some cases resulted in insufficient resources being allocated. Regardless of the reasons, GDPR programmes did not make the progress they needed to in 2017. My observations are further borne out by a recent survey by the Law firm Paul Hastings, in which they find that only 39% of UK and 47% of US firms have an established GDPR programme.

What are the causes of those failures?

Delusion - Many insurance carriers and brokers that have implemented GDPR programmes believe that they don't have too much to do because they're compliant with the EU data protection directive (the Data Protection Act in the UK). This is a false assumption for many insurance businesses as their processes and systems have all changed significantly since most firms last looked at data privacy. As a result, their GDPR programmes need to have a larger scope than was initially assumed.

Under-investment – According to the Paul Harvey survey, only 10% of UK companies have allocated a budget for GDPR compliance. In my experience, the number of insurance firms allocating a budget is higher than 10%, however, these budgets are not always based on correct assumptions (as described above) therefore the project teams are likely to be asking for additional investment, or changing the scope to meet the budget. This often isn't the best approach for compliance projects.

Some (re)insurers are also falling into the trap of thinking that GDPR is a "one and done" project (this is why some firms didn't maintain their DPD compliance as tightly as they should have). For the GDPR some firms will require a data protection officer (in some cases they may need to be a full-time position but others might look at a DPO service offered by specialist third party contractors). This means that GDPR is likely to feature on most organisations' budgets in some form going forward.

+44 (0)20 7193 1966 enquiries@fifthstep.com www.fifthstep.com

Getting on the path to compliance

If your firm is one of those that has not formed a GDPR programme team this should be a priority. In putting together your team, look for the support of a trusted advisor, ideally a firm that works closely with the insurance market and helps others to implement and to become GDPR compliant. I have seen examples of firms looking to staff to be part-time members of projects teams whilst still having to fulfil their regular duties.

This approach is short sighted, not only will some duties suffer as a result of such an approach, but GDPR non-compliance is a real possibility because of the complexities of the regulation. Remember that GDPR is not just about compliances and fines; in today's world of social media wildfires, reputation is a major consideration.

If your firm already has a GDPR programme underway, then it is worth having it checked over to ensure that it is going to deliver the expected results. There are many different approaches to this; a GDPR assessment to confirm your organisation's current position can be very useful in ensuring that limited resources are directed appropriately and that the programme is on the right track.

Having the right resources in your GDPR programme can make a massive difference, either to supplement existing internal resources or playing a larger role. Indeed, having resources with access to the right experience right now could be the difference between a successful programme and one that is still running in January 2020.

If you need help with changing your organisation's ability to become compliance then please speak with Fifth Step. You can find outmore about us and our current thinking at www.fifthstep.com or by following us on with either Twitter @FifthStep and on LinkedIn.

+44 (0)20 7193 1966 enquiries@fifthstep.com www.fifthstep.com