INTERVIEW

WILLIAM LONG

William Long is a Partner and global co-leader of at Sidley Austin LLP's Privacy and Cybersecurity practice, and has been working on global data privacy and information security matters for a number of years. In particular, William advises international clients on a wide variety of General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), data protection, cybersecurity and financial services issues.

DataGuidance by OneTrust spoke with William about data protection issues in the financial services sector, and in particular about approaching compliance with the GDPR, sector-specific challenges, issues around Big Data, and cybersecurity.

What should financial services clients note in terms of approaching compliance with the GDPR?

The adoption of the GDPR is certainly something which is an evolution. It's not something which is sort of fixed in time on 25 May 2018, and that's something that clients need to recognise. They need to evolve as new guidance and cases come out on the GDPR, and as we have new enforcement actions. They need to really understand that this is not something which is static, and take on board that it's an evolving topic.

What has been interesting is some of the recent statistics that have come out about companies adopting the GDPR. One of those is an IAPP and Ernst & Young report, which included, for example, that 49% of the respondents felt that they weren't yet in compliance with the GDPR, and one in 20 of the respondents actually thought that it was impossible to adopt the GDPR. I think that demonstrates that it is very much an evolution.

At the same time, there are challenges that go with that evolution, and in particular, although we have seen an increase of 75% in the number of data privacy professionals or data protection officers, what we're also seeing is that the budgets that they have available have been significantly reduced, in some cases on average from $2 million to $1 million.

Are there any other major challenges that you see which are specific to the financial services industry that have come with the GDPR?

Absolutely. One of the biggest challenges for financial services clients is that they operate within a heavily regulated financial services industry. There are other regulators, such as the Financial Conduct Authority ('FCA') in the UK, and they of course have their own conduct of business rules as well as many other regulatory obligations in addition to data privacy. One of the big challenges for financial services companies is the fact that they have to balance sometimes potentially contradictory requirements. One the one hand, data privacy regulation, and on the other, financial services regulation. Sometimes those two come into conflict.

In particular, we've seen that quite recently with some issues with the U.S. Securities and Exchange Commission ('SCC'). They have expressed some concerns about whether they are able to carry on their oversight function, particularly for European fund managers, because of the GDPR. Will the GDPR prevent them from having access to documents and information? In some cases they have asked for a legal opinion from applicants to the SCC to demonstrate that the GDPR will not cause an issue for them as a financial regulator.

On the other hand, bringing it back to the UK, we have recently seen a Memorandum of Understanding being adopted between the Information Commissioner's Office ('ICO') and the FCA, which will allow for the exchange of information and set up a framework for cooperation between those two regulators.

So, although we are seeing some distinct challenges, we are seeing some movement towards solutions to those issues.

What kinds of issues are financial services operators coming up against in terms of Big Data?

I think the important point to note is that we are in a data century. This is the era of information and data. In fact, a recent report has indicated that we will see a doubling of existing amounts of data over the next three years. That is a huge increase in the actual amounts of data that are available, and that of course leads into emphasis on Big Data and the analysis that goes with it.

For financial services, they're very much involved in the Big Data world. There's use of algorithms within the financial services industry, whether it's for pricing products, understanding risk, or determining credit, so Big Data is something that is extremely relevant to financial services.

However, there are some challenges with that. In particular, there is an issue around transparency. How do you explain to consumers some of the logic that underlies some of the Big Data algorithms, and explain how their data is being processed and used? I think that is a challenge that all industries will need to address.

Another issue with Big Data is accuracy. Where you have large data sets, if there is a particular inaccuracy, then that will become quite profound in those data sets and can potentially lead to discrimination. That is something that always has to be guarded against.

There is also purpose limitation. With Big Data, typically you are looking at data sets some time after the data was collected, so you need to have a view as to whether the purpose for which you are using that data is really within the reasonable expectation of the individual when they first provided that information. Is there really fair processing of that information?

PRIVACY IN MOTION

FINANCIAL

William's interview is coming soon to DataGuidance by OneTrust's 'Privacy in Motion' video series.

To watch other video interviews filmed by DataGuidance by OneTrust, visit: www.dataguidance.com/resources/interviews/

continued

Finally, one of the other challenges with Big Data is the principle of data minimisation. Under the GDPR, you should only be collecting the minimum amount of data that you need to fulfil the purpose, which of course is the antithesis of Big Data, which is all about collecting as much data as possible.

So there are a number of challenges, but companies need to work their way through that and I'm sure they will. We will see an explosion of Big Data products and services.

What kind of emphasis do you see the financial services industry placing on cybersecurity?

I think this is probably the biggest and most significant risk that financial services companies face with the GDPR, and more generally in relation to use of information and data. In fact, the FCA recently reported that there has been a five-fold increase in the reporting of cybersecurity incidents involving financial institutions over the last year. That is a very significant increase, and I think is a concern for all financial institutions.

The other point to note is that the FCA recently came out with a report looking at cybersecurity, and one of the things it strongly emphasised was the need to develop a 'culture of cybersecurity' within institutions. This comes through training, through raising these issues and understanding these issues not just at the board level, but throughout the organisation. It really is a critical issue that companies need to focus on.

From a practical perspective, companies need to do a number of things, but essentially they need to develop a cybersecurity plan, and that has a number of elements to it. Key to that plan is first of all understanding where the data risks are. What kind of data do we have? Which data is most at risk and is susceptible to a cybersecurity attack? Obvious that can include personal data at a fairly mundane level, for example in terms of contact details, but can also be quite sensitive information, such as health data, or identification data such as a passport. One needs to understand what data you have.

In addition, particularly for financial institutions, they will typically have a lot of confidential business information, and that is extremely valuable and something that needs to be considered closely in any cybersecurity plan. In particular, there may be obligations when subject to a cybersecurity breach which involve confidential business information, to not only notify your counter-parties that there has been an incident where that data may have been compromised, but also having to inform financial regulators such as the FCA and the SCC as well. It's really important to understand what data sets you do have, to try and classify those, and ensure that you understand the risk for that information.

Another key area of that cybersecurity plan is to understand where the sources of that risk are. At the moment, we're seeing a lot of attacks emanating in relation to the use of ransomware, where malware which has a ransom element to it, will inflict itself on the system, and therefore you will have to actually pay a ransom to recover that data. Of course, if you have backed up your data, then your risk is significantly mitigated.

Similarly, we're seeing a lot of attacks in relation to phishing email attacks, where someone clicks on a link which gives a potential hacker access to the financial institution's system. Again, this can typically be dealt with, for example, through the use of multi-factor authentication.

So, there are a number of steps that companies can take, often they are common sense approaches, but it does require development of a plan to work through those kinds of assessments.

Then, of course, it is important to actually prepare for cybersecurity attacks, and that comes through training, but in our view, key to that assessment and preparedness for a cybersecurity attack is undertaking a tabletop exercise. You can bring in individuals from across the business, for example in IT, information security, legal, HR, and senior management, work through hypothetical experiences involving cybersecurity attacks, and actually be prepared when a cybersecurity attack occurs.

Finally, I would mention that you should develop an incident response plan. Work through your incident response plan so that you know exactly, if an incident should occur, how you deal with it, how you report it, whether it is notifiable under the GDPR, and who the regulators are that you will need to report to. That is a really keep document to have, and as a package and a plan, that should put companies in a good place to deal with cybersecurity incidents.