Link to Article on website

GDPR and Singapore Companies

Pan Min, Ingenia Consultant's GDPR specialist, looks at the implications of the GDPR on Singapore companies and why we should care.

BY:
Pan Min, Partner
INGENIA CONSULTANTS

MOST OF US HAVE HEARD OF THE GENERAL DATA Protection Regulation (GDPR), an EU law on data protection and privacy for all individuals within the European Union and which addresses the processing of personal data in the EU and export outside the EU. The GDPR came into effect on Friday 25 May 2018, but many of us outside the EU will wonder what it has to do with us.

'The fines, of course', he tells us. How much are the fines? A breach will make the company liable for a fine of twenty million Euros or 4% of a company's annual revenue, whichever is greater - certainly not a token slap on the wrist. This is not a small fine for any company, much less SMEs. The GDPR will affect companies in Singapore in various way. For example, you may have a European employee and his data was collected when he was in Europe, but if he is in your company now - you are affected by the GDPR. Alternatively, if you have any current or previous clients who are based in the EU or are EU citizens, you are also affected.

You might think that in the case of Singapore-based companies with a minimal EU presence, the EU might not be able to enforce disciplinary fines. We do not know yet how the EU plans to enforce the GDPR, but 4% of your revenue is at stake. The first wave of companies that are targeted for enforcement and breaches are likely to be big data mining companies - such as Facebook, Google, LinkedIn, and so on. After that, perhaps schools, hospitals, and government agencies, followed by privately-owned companies in the EU. Once all that has settled, they may start to go after companies outside the EU. In a sense, there are likely to be several waves before the enforcement tide hits us in Asia. It is better to be prepared, of course.

PAN MIN
INGENIA CONSULTANTS

"If you have any current or previous clients who are based in the EU or are EU citizens, you are also affected."

How much is this going to cost?

Not much. Let us examine it from another angle. Financial institutions in Singapore are already required to be compliant with various regulations stipulated by the Monetary Authority of Singapore. These regulations include Technology Risk Management and Anti Money Laundering. They also have to comply with Singapore's Personal Data Protection Act (PDPA) from the Personal Data Protection Council, and so the GDPR by the EU is just another related internal control component.

In some ways, when comparing the PDPA and the GDPR, they are quite similar - both contain wording that can be somewhat vague. Both state that relevant protections must be in place, but without defining these relevant protections. Is compliance going to be a headache? For companies that already have various policies and procedures in place, this is not going to be a hassle - only a matter of some time and effort.

"Financial institutions in Singapore are already required to be compliant with various regulations stipulated by the Monetary Authority of Singapore."

Some key challenges are to define who the controllers or processors of the data are. Once those definitions have been made, it is relatively straightforward to follow procedures and policies that have been established. A data inventory map needs to be created to know where data is stored, who has control, how much control, the risks involved in leaks etc. A fair bit

of work is involved but not much cost. Usually an IT person will be doing this part, so if you are a small company that already outsources your IT, your IT service provider should be able to provide this. If you are big enough and have your IT team, the IT team can work with your compliance team to do that. We at Ingenia can work with your IT team on this front.

"Some key challenges are to define who the controllers or processors of the data are. Once those definitions have been made, it is relatively straightforward to follow procedures and policies that have been established. "

How long will GDPR compliance take?

The good news is that nobody will be starting from a zero state, so to speak. There are already various sorts of controls in place if you are using - password controls, folder access controls, for example, that limit folder access to certain people. The first step is to do an assessment - we have a look at their policy documents and examine it for gaps. Then we go onto the company premises to see if they follow these policy documents in their data storage and processing procedures. This may take perhaps two weeks for a small company, or up to two months for a large company. We will then make recommendations for improvement in data security, and the company then needs to implement these changes and procedures. Speed of implementation is not something we can control, of course, but if the gaps are not major, a month or two should be sufficient for most companies.

After this is done, we aim to come in quarterly or so to check if the policies and procedures are being followed. Once this is done, we can say they are GDPR compliant. The on-going work of a Data Protection Officer (DPO) can be as little as two hours per quarter for small companies, or some eight hours per quarter for large companies. One concern many clients and potential clients have is that they would like a legal opinion on whether they are GDPR-compliant, and not being a law firm, we cannot offer a legal opinion.

To this end we are collaborating with law firms to provide such a service. After our assessment, the law firm can sign off to give the client a greater sense of assurance. Why are Ingenia ideal for handling the GDPR compliance of financial institutions? A law firm can do GDPR compliance, certainly, but they may not be familiar with the finer details of how financial institutions work, resulting in a top-down style of working. As we are a consultancy for the financial industry, our compliance team are intimately familiar with the processes, challenges, and needs of the industry, meaning that we can give a bottom-up approach. ■