PROTECTING ONE OF YOUR COMPANY'S MOST IMPORTANT ASSETS

By: Tom Kelly & Chris Eaton

New rules governing data protection come into effect on May 25, 2018 with the implementation of the General Data Protection Regulation (GDPR) by European Privacy regulators. This represents the biggest change in regulations relating to data protection in more than 20 years. Bermuda is following suit with the introduction of the Personal Information Protection Act, PIPA, which received Royal Assent on July 27, 2016 and is due to come into force in late 2018. Regulators have made it very clear that they intend to enforce the new rules with fines and penalties for non-compliance. For the GDPR, it could mean potential fines to corporations of up to 4 per cent of annual global revenues.

In an age when personal information is a key advantage and a business driver, getting your privacy strategy right can give you a competitive edge.

Perhaps the most important mind-shift relates to perceptions of ownership of personal data that companies collect. In this new world, according to the European Union, personal data still effectively belongs to the person it identifies. A core value of the GDPR for example is that: "Natural persons should have control over their own personal data" and that person has the right to control how it is processed.

How can you turn GDPR & PIPA into an advantage?

It starts with recognising that personal information is one of your organisation's most valuable assets.

Managing this data requires a careful strategy to ensure that it's reliable, that customers understand what you are doing with their personal information and, where required, that you have obtained their consent. This will ensure the insights it delivers are actionable, and reduces the risk that organisations won't be perceived as intrusive as customers see more targeted offers for products, pricing or services.

Five steps to ensure compliance

Since the impacts of the new privacy regulations are universal for organisations regardless of industry sector or geography, the following five-step approach is recommended. These steps could be used specifically for the purposes of the GDPR or as a broader privacy strategy approach to cater to PIPA.

1. Define your privacy strategy

Be realistic when developing your privacy strategy. Consider what levels of privacy risk your organisation is prepared to accept? Where do you want to be compared to your peers? Which aspects of the GDPR and/or PIPA are most critical for you and your customers? How are you gaining buy-in from senior management? Who is accountable on the board?

2. Where are you now?

In order to establish the size of the task ahead and what specific areas need addressing, you need to assess your organisation's current maturity. This is not a tick-box exercise but a pragmatic, focused process to really understand the privacy risk exposures that exist across your business and how to reduce them.

In undertaking these first two steps, you will also need to consider what aspects of the GDPR and/or PIPA, and privacy in general, are the key drivers for your organisation. What matters most?

3. Take a pragmatic approach

You need to build a plan that will help you manage your risk to an appropriate level, in line with your overall business strategy. This does not necessarily mean taking a leading position in every single respect — but a clear view of what success looks like for you.

Where you start depends on your risk appetite but here are some areas you could focus on: governance, inventory and risk; individuals rights; incident management and breach notification; third party diligence, contracts and assurance.

4. Coordinate and deliver

You need to ensure that a privacy compliance programme is embedded as part of day-to-day business operations. This will require coordination across the business to design and implement robust privacy processes, policies and controls. Make sure you have the right blend of input from legal, IT, HR and marketing as well as enough resources to execute. Don't underestimate the level of effort — personal information is everywhere in your organisation. Once your programme is implemented, processes need to be in place to maintain and monitor your performance privacy regime and operationalise the ongoing support of your privacy framework.

5. Embed into business as usual

Complying with the privacy regulation is about defining, implementing and then sustaining compliant processes. Post 2018, you will be required to demonstrate, on an ongoing basis, how you collect, use, retain, disclose and destroy personal information in line with the GDPR and PIPA requirements. This impacts everything you do relating to personal information and may be a significant transformational activity for your organisation going forward.

In short, the privacy best practice has to become business as usual. It's about embedding the accountability principle. This requires you to show how you comply with the privacy principles —by documenting the decisions you take about a processing activity.

The time to act is now.

Every business process using personal information should be seen as an opportunity to gather and refine data that drives a better understanding of your customers, your organisation's performance and the broader marketplace. Managing this data requires a careful strategy in-line with a business's risk appetite and future business goals and objectives. With the first implementation date just a few months away, are you GDPR and PIPA ready?

The KPMG privacy team has deep experience in helping clients to address the challenges posed by privacy risk, with a structured and flexible approach to meet the needs of diverse organisations. We support clients around the globe in resolving complex privacy issues, from niche challenges specific to certain organisations to end-to-end privacy compliance programmes in complex and highly-regulated industries.

About Tom Kelly: Tom is a Managing Director with KPMG in Bermuda. For more than 20 years, he has provided audit and advisory services primarily to insurance and reinsurance companies. This has included risk management, regulatory advice, IT architecture and cyber security maturity assessments.

About Chris Eaton: Chris is a Senior Manager with KPMG in Bermuda. He holds the CIPP/E qualification from the International Association of Privacy Professionals and is the Cyber Security Lead for the KPMG Islands Group. Chris joined KPMG in 2014 and is a Senior Manager and the Service Line Lead for IT Advisory in Bermuda. He has been principally involved in providing Information Protection, Attestation and IT Risk Consulting to a wide variety of clients including SEC registrants and large public and non-public entities.