APPLEBY

News Alert
April 2018

Comparing GDPR and PIPA – is there a difference?

Investors in offshore financial centres increasingly require and demand data privacy. Obligations to collect personal data resulting from new international data sharing regimes, combined with cybersecurity concerns and innovative technology deployments, are making the regulation of personal data more complex than ever before.

The latest addition to the data protection legislative canon is the European Union's (**EU**) General Data Protection Regulation (**GDPR**) which is due to come into effect from 25 May 2018. The GDPR is designed to allow individuals to better control their personal data and to establish one single set of data protection rules across the EU, making it simpler and cheaper for organisations to do business. So far, so sensible. The sting in the tail however is that organisations outside the EU may also be subject to the GDPR. With fines of up to €20 million or 4% of the entity's global gross revenue, organisations in Bermuda need to understand their obligations under the GDPR as reputations and criminal liability will soon be at stake.

The good news for entities in Bermuda comes in the form of the new Personal Information Protection Act 2016 (**PIPA**). Anticipated to come into full effect in December 2018, the PIPA will regulate the future processing of all personal data in Bermuda. Drafted around a set of internationally recognised EU-style privacy principles, Bermuda's new law provides a framework of rights and duties designed to give individuals greater control over their personal data. As a result, many of the compliance obligations under the PIPA and the GDPR dovetail to a large extent. This means achieving compliance with one regime puts an organisation well on the way to achieving compliance with the other.

Am I caught by the GDPR?

The GDPR will extend to data controllers and data processors located outside the EU where data is processed in connection with the offer of goods and services to individuals in the EU or who monitor their behaviour. Monitoring would include, for example, the tracking of individuals on the internet to profile them for the purposes of analysing them or predicting their personal preferences.

The GDPR therefore extends the scope of current EU data protection regulations. Technology companies in particular, who may currently locate their servers outside of the EU and therefore be out of scope of the existing EU data protection regime, may now find themselves subject to the GDPR if they are targeting EU customers.

PIPA and GDPR – compliance similarities

Definitions

The PIPA doesn't adopt the "data controller", "data subject" or "data processor" nomenclature of the GDPR, referring instead to "organisations" "individuals" and "third parties". However, the Act does retain the principle that the "organisation" – defined as any individual, entity or public authority that uses personal information - is responsible for ensuring compliance with the law at all times. Pure processors of personal information are not directly regulated under the PIPA.

"Personal data/information" in both the PIPA and the GDPR means any information relating to an individual who can be identified, directly or indirectly, from that data. So online identifiers including IP addresses, cookies and other anonymised data sets may now qualify as personal data if they can be (or are capable of being) linked back to the data subject – the individual who is the subject of the data.

Rights of Data Subjects

There are various themes running through both the PIPA and the GDPR. One such theme relates to the rights of data subjects and transparency with respect to the processing of their personal data. Under both laws, organisations are required to provide a significant amount of information to individuals at the time of collection of their data including the purposes and detail behind the processing, details of transfers of data outside Bermuda, and any security and technical safeguards in place to protect the data subject's personal data. The expectation under both laws is that this information will be provided in a separate privacy notice.

Both laws give data subjects the right to obtain confirmation that their data is being processed and to access that personal data. Organisations have one month under GDPR or 45 days under PIPA in which to respond to a subject access request, although this time period can be extended where necessary, taking into account the complexity of the request and the number of requests. Under the GDPR, a copy of this information must be provided free of charge. The PIPA permits a prescribed fee to be charged.

Under both the PIPA and the GDPR, personal data should not be kept for longer than is necessary to fulfil the purpose for which it was originally collected. Prescribed data retention periods are not set out in either law but an analysis will need to be undertaken to determine how long different types of personal data should be retained. Under the GDPR, controllers must inform data subjects of the period of time (or reasons why) data will be retained on collection. This is not a requirement under the PIPA but as the retention analysis is required, a notification to data subjects would be easy to achieve.

Under both laws, should the data subject subsequently wish to have their data removed, and the data is no longer required for the reasons for which it was collected, then it must be erased. Note that there is a "downstream" responsibility for controllers under both laws to notify processors and other downstream data recipients (such as third party processors or sub-contractors) of such requests.

International transfers

Both the PIPA and the GDPR permit international transfers of data, provided certain criteria are met. Contracts can be put in place to control data transfers with third party processors or between members of the same group of companies.

The PIPA was drafted with the specific aim of achieving adequacy status in the eyes of the EU to allow personal data to flow freely between EU member states and Bermuda without additional mechanisms being put in place. The GDPR now provides for adequacy designation, and decisions can apply to specific processing sectors or territories within a country, as well as to a country as a whole. This could result in future adequacy decisions finding specific industry sectors or states to provide adequate protection for data. Bermuda has already confirmed its intention to apply to the EU for adequacy status in due course.

Data security

The PIPA requires that "appropriate" technical and organisational measures are taken to prevent unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data.

The GDPR is slightly more prescriptive than the PIPA about what organisations need to have in place from a security perspective but not overly so, and certainly not as prescriptive as earlier drafts had suggested. For example the GDPR lists security measures such as:

- pseudonymisation and encryption of personal data;
- ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services;
- ability to restore the availability and access to data; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational security measures.

These are all basic measures that organisations should already have in place. However, it is worth noting that under the GDPR the security requirements are now legally extended to data processors as well as data controllers, putting processors on the hook for regulatory liability. There is no similar liability for processors under the PIPA.

Data breach notification

Under the PIPA, in the event of a personal data breach, the organisation must, "*without undue delay*", notify the Commissioner and any affected data subjects of the breach.

The GDPR also introduces a requirement for data controllers to notify the regulatory authority of personal data breaches without undue delay and, where feasible, not later than 72 hours after having become aware of a breach. The only exception to this rule is in cases where the breach is "*unlikely to result in a risk for the rights and freedoms of individuals*."

Both the PIPA and the GDPR require the notification to describe:

- the nature of the breach;
- the consequences of the breach;
- the measures proposed or taken by the data controller to address the breach; and
- the measures recommended by the data controller to the data subject to mitigate the possible adverse effects of the breach.

Right to be forgotten

There has been much confusion around the new "right to be forgotten" under the GDPR. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. The right does not provide an absolute "right to be forgotten." Individuals have a right to have personal data erased and to prevent processing in specific circumstances, for example when the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.

The PIPA contains a similar right, although this is expressed as a general right of "erasure". As with the GDPR, if there is no compelling reason for an organisation to retain personal data, a data subject can request its secure deletion.

Appointment of a data protection officer (DPO)

The PIPA requires the appointment of a designated "privacy officer" within an organisation. The GDPR provides that the appointment of a data protection officer will only be mandatory where the data controller is a public authority or the core activities of the data controller consist of processing operations which require: (i) regular and systematic monitoring of data subjects on a large scale; or (ii) processing on a large scale of sensitive personal data. For all other organisations, the appointment of a DPO will be voluntary.

Navigating the differences

Direct marketing and consent

Under both the PIPA and the GDPR, a data subject has the right at any time to require an organisation/data controller to stop processing their personal data for the purposes of direct marketing. There are no exemptions or grounds to refuse. An organisation/data controller must deal with an objection to processing for direct marketing at any time and free of charge.

Under the GDPR, the controller must inform individuals of their right to object "*at the point of first communication*" and in a privacy notice. There is no such requirement under the PIPA but including an unsubscribe facility in each marketing communication would be recommended best practice.

Where things get slightly complicated is the issue of consent. Under the PIPA, consent can be implied from the actions of the data subject. If a data subject continues to accept the services of the organisation without objection, consent can be implied. With the GDPR, for any consent to be valid it needs to be obvious to the data subject what their data is going to be used for at the point of data collection and the controller needs to be able to show clearly how consent was gained and when it was obtained.

For marketers in particular, there has been much debate about the type of consent that might be required under the GDPR. In the context of financial and professional services, many businesses currently rely on the data protection clauses within their terms and conditions of business as the basis upon which consent has been given. Existing consents will therefore need to be reviewed to understand if they remain valid. Where personal data is held on a marketing database, it is questionable now whether that would be considered "freely given" so a separate marketing notice should be issued seeking explicit consent for marketing directed at individuals in the EU.

The other point for marketers targeting individuals in the EU is the requirement to comply with a number of other EU regulations. Some of these apply to unsolicited electronic messages sent by telephone, fax, email or text, while others apply to marketing material sent by post.

Treatment of data processors

The GDPR sets out more detailed statutory requirements to apply to the controller/processor relationship and to processors in general. The GDPR also makes data processors directly subject to regulation for the first time and directly prohibits data processors from processing personal data except on instructions from the data controller. The GDPR also extends data security obligations to data processors. Under the PIPA, recommended best practice would always be to put in place a contract between an organisation and third party processor to ensure that any personal data is processed only for authorised purposes, that all data is stored and transmitted securely and that disaster recovery practices are in place in the event of a data breach. Essentially, the contract should require the third party processor to level-up its policies and procedures for handling personal data to ensure compliance with the PIPA. Use of subcontractors by the third party processor should be prohibited without the prior approval of the organisation for whom they are processing the data.

Fines and penalties

The GDPR will provide for two tiers of sanctions, with maximum fines of up to €20 million or 4% of annual worldwide turnover, whichever is greater.

Under the PIPA, refusal to comply or failure to comply with an order issued by the Commissioner is an offence. A corporate entity is liable on conviction to a fine of up to BMD$250,000. Individuals found in breach may be subject to a fine of up to BMD$25,000, or imprisonment for a term of 2 years, or both.

Conclusion

As personal data develops into an increasingly valuable business asset, data protection and cybersecurity are now board level issues. Although questions remain regarding the effective enforceability of the GDPR against non-EU controllers, there is no doubt that the long arm of EU data protection law is seeking to reach beyond EU borders.

For more information, feel free to get in touch with Steven Rees Davies or Peter Colegate.

Key Contacts

Steven Rees Davies
Partner
Corporate
Bermuda
+1 441 298 3296
sreesdavies@applebyglobal.com

Peter Colegate
Senior Associate
Corporate
Cayman
+1 345 814 2745
pcolegate@applebyglobal.com