INSIGHT

JANUARY 2018

ASIAN INSTITUTIONS MUST START TO TACKLE EU DATA PROTECTION RULES INTRODUCED BY GDPR

ASSESSING THEIR CURRENT DATA PRIVACY FRAMEWORK SHOULD BE ONE OF THE ITEMS ON THE AGENDA OF THE ORGANISATIONS IN ASIA

The European General Data Protection Regulation (GDPR) aims to protect individuals located in the EU by introducing new binding obligations for data controllers and data processors. This means any company holding personal data of individuals who are located in the EU, regardless of its operating location, needs to comply with GDPR. As a consequence, many institutions in Asia will fall within scope.

With less than six months to the enforcement date, companies are still unclear around how and when the European Commission will look at extra-territorial enforcement and how it will cooperate with local regulators to enforce GDPR outside of its borders.

The impacts of GDPR on Asian businesses depend on the gaps between the local law in force and GDPR. With a fragmented data privacy protection landscape across Asia, the workload associated to GDPR projects for each Asian country needs to be assessed on a case by case basis.

Sia Partners has conducted a thorough gap analysis study in Hong Kong and Singapore, where local companies have started to grasp the importance of GDPR following some announcements by their Privacy commissioners - respectively Stephen Wong and Tan Kiat How - to propose amendments of the privacy law and to uplift the standards. In this article, we present the key differences between GDPR, PDPO (HK Data Privacy Ordinance) and PDPA (SG Data Privacy Act).

The new obligations introduced by the GDPR

The notion of sensitive data

Sensitive data is special categories of personal data, such as information on medical conditions, financial situation, racial or ethnic origin, political opinions, religion or philosophical beliefs.

According to the GDPR, such data requires particular attention and appropriate security measures should be implemented to guarantee its security, such as:

- Pseudonymisation
- Data encryption

The PDPA has no definition of sensitive data. There is a non-binding guidance issued by the Hong Kong Privacy Commissioner for Personal Data (PCPD), in the context of biometric data, which indicates that higher standards should be applied as a matter of best practice to more sensitive personal data.

As a consequence, for companies handling sensitive data, a complete review and categorisation of special categories of data will be necessary to adopt enhanced security measures around the processing of this data.

The data breach notification to the regulator

The Data Protection Authorities (DPA) can only take appropriate enforcement actions in relation to data breaches if they are aware of those breaches. Therefore, the GDPR requires controllers and processors to report such breaches to the DPAs.

Under GDPR, any event leading to the destruction, loss/alteration, unauthorised disclosure of/ access to personal data must be notified to the regulator by the organisation holding such data, within 72 hours of the organisation becoming aware of it.

Although both the PDPO and PDPA encourage notification of data breaches to the Office of the PCPDs and relevant parties, there is neither binding obligation nor stringent timeframe to do so.

A substantial impact with an intense time pressure, can be expected on company's processes to identify, review and report data breaches. It will be necessary to implement data breach response plans, incident detection mechanisms and escalation processes.

We also recommend implementing robust security measures, such as personal data anonymisation or pseudonymisation by hashing data.

The appointment of a data protection officer

Under certain circumstances, GDPR imposes to the data controller the appointment of a Data Protection Officer (DPO) to deal with data privacy protection matters within the company and to face the Data Protection Authorities (DPA) in case of disputes.

Even if a company does not fall into the categories mentioned by GDPR, it should still appoint a DPO as best practice for its reputational value and to highlight the company's engagement towards data privacy protection matters.

The GDPR requirement is not covered by the PDPO but there is a non-binding guidance to advocate the development of a privacy management programme and the appointment of a DPO.

While appointing a DPO is mandatory under PDPA, only 50% of the companies have appointed a DPO[1]. The appointment of a DPO will require an overhaul of a company's internal structure, a review of its current job specifications to ensure its optimal reporting line.

The right to data portability

GDPR states that the data subject can request to transmit the personal data previously provided from one controller to another controller, without hindrance from the controller. The transmission process should be carried out by automated means if technically feasible.

There is no such requirement neither in PDPO nor in PDPA.

To comply, data controllers will have to restructure their data sets and implement processes to enable data exchange upon request.

The Privacy Impact Assessments (PIA)

GDPR introduces PIAs as a means to identify high risks to the privacy rights of individuals, when processing their personal data.

Where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

In PDPO, PIAs are encouraged when the processing activities are related to biometric data while in the "*Guide to Data Protection Impact Assessments*" issued by the PDPC of Singapore, PIAs are encouraged when creating new systems or processes that involve handling of personal data.
PIAs will be an additional compliance step for Organisations when they launch new projects or products, thus extra cost and time to be considered at the budgeting phase.

Existing standards in PDPO and PDPA strengthened with GDPR

The customer consents

Each and every personal data processing activity requires a lawful basis. Consent provides one such lawful basis.

The conditions to obtain a valid consent from individuals to use their personal data is stricter under GDPR. The consent must meet specific requirements to be deemed sufficient, it must be freely given, unambiguous, explicit (given by either a statement or clear affirmative action) and expressed by the data subject.

- Under PDPO, an indication of no objection is considered as consent but it is not sufficient under GDPR as not resulting from a positive action.
- PDPA considers deemed consent where personal data is voluntarily provided by data subject, therefore, in such case, the consent does not need to be expressed or verbalized at all.

Organisation will have to carry out a complete review of the way the customer consent is collected (contracts, online forms, etc.) to make sure it will meet the GDPR standards on being specific, granular, clear, opt-in, documented and easily withdrawn. This applies to both new and existing consents.

The Accountability principle

Data controllers are accountable for GDPR compliance, meaning not only they are responsible to enforce GDPR within the organisation, but they are obliged to demonstrate compliance to the regulator.

While the principles of accountability have previously been implicit requirements of data protection law, GDPR makes it mandatory.

Both PDPO and PDPA provide guidance on how to embrace the notion of accountability as a vehicle to drive privacy compliance without notion of mandatory accountability principle.

Accountability principles means additional compliance steps for data controller to:

- ✓ Keep a record of all processing activities
- ✓ Appoint a DPO when necessary

[1] (as of Jan 2017, according to PCPD)

- ✓ Implement measures that secure compliance with the data protection principles
- ✓ Use PIAs whenever appropriate

The right to rectification

The data subjects have the right to obtain from the data controller the rectification of inaccurate personal data concerning them, without undue delay.

The GDPR stipulates that personal data that is processed should be accurate and kept up to date, should the data subjects request to rectify their personal data, organisations must oblige within one month from the date of request. Moreover, if the personal data has been disclosed to third parties, the data controller must inform them of the rectification where possible.

Under PDPA, it is an absolute requirement only when the personal data in question is likely to be used by the organisation to make a decision that affects the individual to whom the personal data relates or if likely to be disclosed to a third-party.

To comply, organisations must implement reporting to monitor and control the quality of the personal data they hold and process about the individuals. They must be able to respond to personal rectification requests in a timely manner.

The right of access

Data subjects have the right to access their personal data held by an organisation.

Under GDPR, the request to personal data access should be processed without delay and at the latest within one month from the date of request. The copy of the information must be provided free of charge.

GDPR does not impose a time limit for personal data access while PDPA only requires to disclose information concerning the use or disclosure of personal data in the preceding one year from the date of request.

To comply with GDPR, organisations should respond to personal data access and rectification requests in a timely manner and maintain a record of processing activities to be made available to the data subject upon request.

The right to be forgotten

The right to erasure, also known as the right "to be forgotten", is to enable an individual to request the deletion or removal of personal data.

Upon the data subject's request, the data controller is obliged to erase personal data without undue delay where specific conditions are met.

PDPO states that all practicable steps must be taken to erase personal data held by the data user where the data is no longer required for the purpose but does not specify that a data subject has the right to request for personal data erasure.

In PDPA, data must be destroyed or deidentified only when there are no longer any legal or business and any other purpose for its retention.

To comply with GDPR, it will be necessary to upgrade IT systems to enable data deletion and to conduct regular review of data retention schedules to erase unused or obsolete data.

The right to object to profiling

Under GDPR, the data subjects have the right to object, regardless of the process purpose, at any time to processing of personal data, unless the data controller can demonstrate the legitimate ground.

Such right only applies to direct marketing for PDPO.

With regard to the consent process mentioned earlier, companies will have to review their privacy notices and implement a more comprehensive process to collect consents and objections.

Conclusion

The above study suggests that organisations in Hong Kong and Singapore need to make numerous changes to be compliant with GDPR, with impacts expected on governance, reporting, processes and information systems.

In addition to more stringent obligations under GDPR, business could be fined up to four percent of their global annual turnover or EUR20 million (USD23.35 million), whichever is higher. Statutory fines in Hong Kong are relatively low at HK$100,000 (US$12,780) – except for direct marketing offences – and in Singapore SG$1 million (~US$732,900) thus not acting as a deterrent in certain circumstances.

Finally, 25 May 2018 is the date to keep in mind, as the data privacy protection landscape will drastically change in the EU when GDPR comes into force, leading to some interesting developments outside the EU.

It is crucial for companies doing business with the EU to start assessing the comprehensiveness of their data privacy frameworks and kick off GDPR compliance exercises.

YOUR CONTACTS

JUSTINE LAPRUN
Manager
+ 852 5564 1228
Justine.laprun@sia-partners.com

Founded in 1999, Sia Partners is an independent global management consulting firm with over 950 consultants and an annual turnover of USD 150 million. The Group has 20 offices in 15 countries, including the U.S., its second biggest market. Sia Partners is renowned for its expertise in the Energy, Banking, Insurance, Telecommunications and Transportation sectors.

Sia Partners Asia operates out of three locations Hong Kong (Greater China), Tokyo (Japan) and Singapore (South-East Asia).

Abu Dhabi
PO Box 54605
West Tower #605
Abu Dhabi Mall - UAE

Amsterdam
Barbara Strozzilaan 101
1083 HN Amsterdam - Netherlands

Brussels
Av Henri Jasparlaan, 128
1060 Brussels - Belgium

Casablanca
14, avenue Mers Sultan
20500 Casablanca - Morocco

Charlotte
401 N. Tryon Street
10th Floor
Charlotte, NC 28202 - USA

Doha
PO Box 27774 Doha
Tornado Tower #2238
West Bay - Qatar

Dubai
PO Box 502665
Shatha Tower office #2115
Dubai Media City
Dubai - UAE

Hong Kong
23/F, The Southland Building,
48 Connaught Road Central
Central - Hong Kong

Houston
800 Town and Country Blvd, Suite 300
Houston, TX 77024 - USA

London
2nd Floor, 4 Eastcheap
London EC3M 1AE - UK

Luxembourg
7 rue Robert Stumper
L-2557 Luxembourg

Lyon
3 rue du Président Carnot
69002 Lyon - France

Milan
Via Gioberti 8
20123 Milano - Italy

Montreal
2000 McGill College, Suite 600
Montreal QC H3A 3H3 – Canada

New York
40 Rector St, Suite 1111
New York, NY 10006 – USA

Paris
12 rue Magellan
75008 Paris - France

Riyadh
PO Box 502665
Shatha Tower office #2115
Dubai Media City
Dubai - UAE

Rome
Via Quattro Fontane 116
00184 Roma - Italy

Singapore
137 Market Street
#10-02 Grace Global Raffles
048943 Singapore

Tokyo
Level 20 Marunouchi Trust Tower-Main
1-8-3 Marunouchi, Chiyoda-ku
Tokyo 100-0005 Japan