Extra-territorial scope of the GDPR

The Impact of the GDPR on Organisations in Asia

1. Background on the GDPR for Asian organisations

The General Data Protection Regulation (GDPR) poses challenges for organisations with customers in the European Union. Entering into force in May 2018, the GDPR requires to undertake a root and branch review of how they handle, process and govern the use of customer data across their entire organisation. Organisations who do not make the necessary operational and technology changes are looking at fines up to 4 percent of their annual turnover. Many organisations admit they will not be ready in time and that they are struggling to find the right expertise to guide the transition.

2. Extraterritoriality of the GDPR: When does the GDPR apply to organisations in Asia?

Territorial scope of the GDPR

In general, the GDPR applies to (1) individuals that are EU residents, (2) organisations that are based in the EU, or (3) organisations based outside the EU, that target EU citizens.

Targeting EU citizens

Asian organisations and their subcontractors will have to adhere to the GDPR in case they have the intention to offer their services to individuals residing in the EU or monitor their behaviour.

Examples:

- **Offering services:** An organisation that has a website, accessible by EU individuals, providing them the option to sign up for its services. Whether the targeted EU citizens have to pay for this service, is irrelevant.
- **Monitoring behaviour:** Where an Asian organisation "tracks" individuals in Europe by use of cookies or logging IP addresses, the GDPR will be applicable. Incidental collection of EU IP addresses might not be interpreted as the trigger for GDPR compliance.

Indirect application of the GDPR through contractual obligations

In light of the data controller – data processor relationship, Asian companies might be obliged to adhere to GDPR requirements by their suppliers or contracting partners. This is where these other organisations themselves (and by extension, their data processors or co-data controllers) fall under the scope of the regulation.

For Singapore, the organisations will be affected by the GDPR as Singapore is the EU's largest commercial partner in ASEAN, accounting for slightly under one-third of EU-ASEAN trade in goods and services[1].

3. What are the general requirements of the GDPR?

The 99 articles of the GDPR can be summarised in the following nine requirements for organisations and their subcontractors:

- Legal basis and lawfulness of processing
- Data governance
- Contractual obligations
- Risk assessment and mitigation
- Data breach notification
- Records of processing activities
- Data protection officer
- Data subject rights
- Data transfers

4. What are the consequences of non-compliance?

Powers of supervisory authorities

Next to the specific requirements and enforcement for subcontractors, organisations can be held accountable in case a subcontractor does not comply with the requirements. This is because the organisation has the obligation to contract solely with subcontractors that provide sufficient guarantees of their abilities to implement the technical and operational measures to comply with the GDPR. Or in other words: organisations cannot outsource their risk.

[1] European Commission, Directorate-General for Trade, "European Union, Trade in goods with Singapore", May 2017, http://trade.ec.europa.eu/doclib/docs/2006/september/tradoc_113443.pdf (as on 20 November 2017).

Supervisory authorities can levy fines up to 4 percent of the global annual turnover of an organisation. Besides, supervisory authorities can conduct audits, access premises and equipment, and order organisations to bring their operations into compliance with the GDPR. Ultimately, the supervisory authorities can impose a ban on data processing, or require organisations to rectify or delete personal data.

Complaints and claims by individuals

In case an Asian company does not comply with the GDPR, and consequently breaches the rights of individuals, these individuals have two options: One is to file a complaint against the organisation at the Supervisory Authority. The Supervisory Authority can investigate the complaint and use its powers to enforce compliance and/or to sanction the organisation. The other option is to claim damages in front of a European court. The GDPR also opens the door to potential class actions. Many expect that this mechanism will be used where data security breaches affect a large number of individuals or where an organisation disregards the new rights of individuals.

Reputational damage

Enforcement by supervisory authorities or courts might not be the only compelling reason for organisations in Asia to comply with the GDPR. The potential reputational damage that comes with refusing to comply with GDPR requirements is equally daunting.

5. How can the GDPR be enforced in Asia?

There remains significant doubts regarding the enforceability by European supervisory authorities and courts on organisations in Asia:

Representatives based in the EU

The GDPR requires overseas data controllers or processors falling within the scope of the GDPR to designate a representative based in an EU Member State to act as the point of contact for the relevant DPAs. This representative should be subjected to enforcement actions in case of non-compliance by the organisation in Asia.

International cooperation

The DPAs may have limited enforcement powers against overseas entities without representatives based in the EU. The DPAs might seek to coordinate with overseas regulators in taking any enforcement action.

6. What can organisations do in order to prepare for the GDPR?

A. Gap assessment

The first step organisations are taking is to understand how compliant they are with existing legislation, including a gap analysis to identify potential holes in their compliance with the provisions of GDPR. For some banks, this will amount to a sober assessment of what elements they can comply with in the remaining time available.

B. Prioritise

Although achieving 100 percent compliance is not achievable for most companies, figuring out where the compliance focus is, is a good start. Organisations can adopt a risk based approach and implement protective measures corresponding to the level of risk of their data processing activities.

For example: organisations with over hundreds of thousands of contracts should prioritise the revision of the contracts involving the processing of large volumes of personal data.

Organisations can opt to prioritise with article 30 of the GDPR, on the creation and maintenance of records of processing. This is a core article of the GDPR, enabling organisations to track data and demonstrate compliance.

C. Executing the Data Protection Roadmap

As May 2018 is the kick off date where Data Protection Authorities (DPAs) can enforce their powers, organisations might face fines because of the delay. Organisations that are just starting to look into GDPR compliance, will probably not be fully compliant by May 2018. However, being able to demonstrate the implementation of a Data Protection Roadmap will help mitigate the implications of non-compliance. Planning priorities ahead for the next year will be necessary to gradually achieve GDPR compliance.

Contact us

Daryl Pereira
Head of Cyber Security
KPMG in Singapore
T: +65 6411 8116
E: darylpereira@kpmg.com.sg

Alban Perrin
Manager, Cyber Security
KPMG in Singapore
T: +65 6411 8274
E: albanperrin@kpmg.com.sg

Emma Haenebalcke
Senior Associate, Cyber Security
KPMG in Singapore
T: +65 6411 8569
E: ehaenebalcke@kpmg.com.sg

KPMG
16 Raffles Quay
#22-00 Hong Leong Building
Singapore 048581
T: +65 6213 3388
F: +65 6227 1297

Find out more about our services at **kpmg.com.sg**

kpmg.com.sg/socialmedia