The GSMA Data Privacy Survey

The Evolution of Data Protection law across ASEAN Member States

In 2004 APEC adopted the APEC Privacy Framework promoting a flexible approach to information privacy protection across member economies. Many of the privacy principles set out in the framework are reflected in national regulation, however, differences in interpretation still exist and several countries still have not incorporated general privacy principles into national law.

More recently three important factors are influencing the development of national data protection legislation:

- A desire to look to the European Union's newly passed General Data Protection Regulation (GDPR) as a basis for national legislation;
- An increased interest in the APEC Cross Border Privacy Rules system to enable data flows, and;
- The 2016 ASEAN Framework for Personal Data Protection - with its objective to "strengthen the protection of personal data in ASEAN and to facilitate cooperation among ASEAN countries, with a view to contribute to the promotion and growth of regional and global trade and the flow of information."

ASEAN now has an opportunity to build on this foundation and shape how future data privacy laws in the region can benefit consumers and trade.

Background

In October 2016, and in-line with AIM 2020, the GSMA prepared a White Paper presenting a series of policy proposals for the promotion of pan-regional digital trade. The White Paper was presented to TELSOM in November 2016. 'Consumer Trust' was identified as the pre-eminent policy topic, with the ASEAN secretariat inviting GSMA to TELSOM 2017 to present further research and continue dialogue.

The GSMA Data Privacy Survey

From May-July 2017, and in collaboration with ASEAN, the GSMA surveyed ASEAN Member States to gain a clear picture on the implementation of national data privacy laws.

At the same time the GSMA also surveyed its own member organisations across the wider Asia Pacific region to better appreciate the impact of national data privacy laws and cross border data restrictions, as well as ascertain what operators considered to be good, or 'smart', data privacy regulation.

Key Findings from the Survey of ASEAN Member States

1. Mixed regulatory landscape for data privacy

Singapore and Malaysia have comprehensive data privacy laws in place, Thailand has draft laws and Cambodia and Vietnam have no plans for general data privacy laws. However many address privacy concerns in their constitutions, civil codes or laws aimed at e-commerce or cybersecurity.

2. Discrepancies regarding which principles are incorporated into data privacy laws and how they are implemented

Malaysia allows certain exceptions to the duty to obtain consent, whereas in Indonesia consent in writing must be obtained for all data processing and data must be kept for five years. This contrasts with Singapore where organisations must delete data once the original purpose is no longer being served.

3. Some laws applicable to a specific sector, technology or type of data

In Thailand privacy is protected in relation to telecommunications users and in relation to children. Before Singapore passed its recent data privacy law privacy was protected by reference to sectors. Malaysia's law applies to data collected in commercial transactions which are further divided into 13 classes of sectoral activity.

4. Different approaches to cross-border data transfers

The Philippines data privacy law considers the "controller" to continue to be responsible for data once the data has been transferred, whereas Malaysia allows transfers to countries based on certain exceptions. Indonesia has strict localisation requirements so that transfers can only be made in consultation with the ministry.

Key Findings from the Survey of GSMA Members

1. **National data privacy laws and cross-border data restrictions have a significant impact on operators**
2. **National data privacy laws foster trust and innovation, but there is room for improvement**
3. **The ability to use personal data responsibly is important to operators**
4. **Good data governance is seen as a potential competitive differentiator**
5. **Operators believe smart data privacy regulation should:**
    - Enhance consumer trust and enable innovation and investment
    - Be principles-based
    - Be technology and sector neutral
    - Be based on risk of harm to individuals
    - Be based on accountability
    - Encourage transparency and control
    - Allow personal data to flow freely across borders provided users are not disadvantaged

Conclusions

The ASEAN Member State survey provides clear evidence of the differences that exist between national legislative frameworks and highlights the fragmented approach to pan-regional data privacy regulation.

The GSMA operator survey outlines the need for principles-based data privacy laws to allow businesses to take full responsibility for data privacy, demonstrate a culture of good corporate digital governance, protect consumers, and maintain a relationship of trust.

The results of both surveys have proved extremely useful in determining what is required, both from a national government and an operator perspective, to create an environment of trust and enable responsible data-driven innovation.

Based on the results of both surveys, the GSMA makes the following policy recommendations:

- Apply the ASEAN Personal Data Protection Framework and implement data privacy rules based on common principles
- Focus data privacy laws on the risk of harm to individuals
- Apply data privacy laws horizontally rather than to a particular sector, technology or type of data, and remove such specific requirements from national licence conditions
- Instil data privacy laws with the idea of accountability or "corporate digital responsibility" to incentivise responsible data governance
- Avoid unnecessary restrictions on cross-border data flows and encourage Member States to join the APEC Cross Border Privacy Rules system or establish an equivalent mechanism for ASEAN