Data Protection Laws– Important considerations for companies in Singapore, Thailand and India.

Whitepaper | March 2022

Author:
Dr Raghuveer Kaur
Regulatory and Compliance Analyst
Starfish Digital

"Data protection has become a mandatory requirement globally. As governments introduce privacy laws, it is necessary to understand how they impact businesses. This study presents a comparative view of personal data protection laws in three Asia Pacific countries – namely: Singapore, Thailand, and India. More so, it compares their regulatory environment with that of the European Union. Importantly, the study also highlights the importance of data protection and privacy for businesses operating in these countries."

– Dr Raghuveer Kaur Regulatory and Compliance Analyst Starfish Digital

Patrick Huang
CEO and Founder,
Starfish Digital

Foreword.

It is about Trust. Trust that businesses will protect the sensitive data of customers, partners, and staff such that we can enjoy services with confidence. These legal frameworks lay an important foundation to enable growth and innovation.

The fintech sector is ever evolving, finding new ways to disrupt traditional business models with data and products. That is why keeping these principles at the core is so important. The trajectory of growth in Asia will continue to accelerate. Governments are responding with greater clarity on the rights, use, consent, and access of sensitive data. Leading digital companies are data companies. With a digital-first approach, businesses may adhere to these frameworks with transparency, efficiency, and scale. This paper compares the current state of protection laws in three major economies and pinpoints the success and challenges of data management reforms.

At Starfish Digital, building trusted relationships is key to our driving innovations in corporate banking.

starfish DIGITAL

Contents.

Introduction.

Data protection and privacy are the nexus around which businesses operate. Every country in the world seeks to strike a balance between data protection and innovation. Multinational companies are working to adhere to compliance laws, best practices and obtain certifications like ISO27001 and SOC (Service Organisation Control) 1 & 2.

2018

In 2018 when the European Union (E.U) established the General Data Protection Regulation (GDPR), little did we know that it would shake business operations worldwide and pose such challenges. GDPR is the legal framework that states guidelines for collecting and processing personal information from individuals living in the European Union.

Globally, countries are now examining how to enforce data protection. While Singapore has a Personal Data Protection Act (2012) implemented and effective, Thailand has only enacted the law. In contrast, India has a privacy bill that is still to be enacted and enforced.

The study also looks at how these laws align and differ from the GDPR and its significance to financial institutions operating in those countries. State data protection laws play a crucial role in more regulated sectors such as banks. Thus, these institutions must pay attention to these laws as they deal with personal data.

There has been tremendous growth in API (Application Programming Interface) banking and open banking in these countries, compelling governments to institute regulations. Singapore has a Personal Data Protection Act (PDPA,2012) with amendments in 2020 making it more comprehensive and aligned to GDPR. While Thailand has passed the Personal Data Protection Act (not enforced it yet), India presents a different picture with data protection covered by the IT Act (2000 and 2008) at present and a future privacy law with the Personal Data Protection Bill (PDPB), The PDPB of India is in line with GDPR and is in some aspect broader than the scope of GDPR.

There has been tremendous growth in API (Application Programming Interface) banking and open banking in Singapore, Thailand and India, compelling governments to institute regulations.

i. What is General Data Protection Regulation (GDPR)?

GDPR is a vital data protection regulation. It is a humongous law that contains ninety-nine individual articles. The General Data Protection Regulation (GDPR) is a legal framework that details guidelines for the business on processing and collecting personal information from individuals of the European Union. The UK (United Kingdom) GDPR sets out seven fundamental principles: Lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality (security), and accountability.

GDPR

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- The rights to automated decision making and profiling

GDPR provides the framework for digital privacy legislation in Europe. It also serves as the source of inspiration for digital privacy across the globe and is a benchmark for countries globally.

ii. Comparative analysis of the laws across countries.

The next section of the article analyses significant headings of the law and how each country's bill and act cover them. It also discusses how each country's approach is similar or different to the GDPR.

iii. Scope of Applicability.

All companies, whether private or public, registered, or unregistered, which undertake activities involving personal data will fall under the purview of the law.

The scope of applicability has two aspects. One is in which country it applies. The other is the extraterritorial aspect, which implies the law's applicability outside one's own country. All companies, whether private or public, registered, or unregistered, which undertake activities involving personal data will fall under the purview of the law. The law covers business entities, whether incorporated inside or outside the country. However, in India, the government may reserve the right to exempt certain public sector agencies either partially or fully in the nation's best interest. The GDPR, PDPA Thailand, PDPA Singapore, and PDPB have extraterritorial reach.

iv. Notification of breach.

Breach refers to unlawful processing of personal data. Breach notification has become mandatory in all countries. Breach notification implies the intimation of the breach to the authorities (Data Controller or Data Protection Officer) and the data subjects within three days or 72 hours period. Breach notification has been from GDPR and is similar to GDPR in all three countries.

v. Consent requirement and withdrawal.

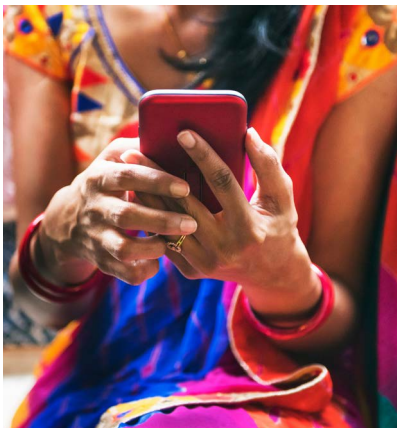
Consent requirement is the pivotal point around all data privacy laws. GDPR details an exhaustive list of how consent can be taken from data subjects, and other countries have followed suit. However, GDPR has dealt with consent management at considerable depth while these countries' coverage of the subject may not be as broad as GDPR.

Every regulation has mandated that consent should be sought from data subjects either in written or in any other form as per the applicable law of the land. All three countries have mandated that before processing personal data consent is to be taken from data subjects. Similarly, business entities must allow the data subject to retract or withdraw consent easily.

vi. Cross-border transfer of data.

The GDPR specifies that a cross-border transfer is allowed based on international agreements for judicial cooperation.

It refers to the transfer of personal data to other countries or international organisations. Transfer of personal data is allowed with certain constraints. It also states that the country to which data is being transferred should have rules to provide ample data protection. There are restrictions on the way sensitive data is transferred. The GDPR specifies that a cross-border transfer is allowed based on international agreements for judicial cooperation. Cross-border transfer is applicable in all three countries.



vii. Marketing.

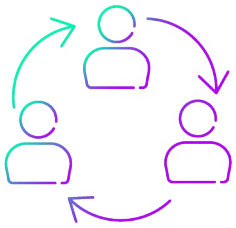
The rights of data subjects are safeguarded in the case of marketing. Whilst modes may differ, most countries make it mandatory for companies to obtain consent from data subjects to use their information for marketing purposes. For example, GDPR makes it compulsory to obtain approval for direct marketing reasons.

The “Do Not Call (DNC) Registry” permits individuals to opt out from certain marketing messages in Singapore. Thailand restricts marketing if it invades the rights and freedom of a data subject and allows data subjects to oppose the use of personal data for direct messages

viii. Right of data subject to request access and correction.

Data privacy is designed to empower individuals and protect their rights to privacy. GDPR defines a data subject as “any living individual whose personal data is collected, held or processed by an organisation.” GDPR has introduced eight such rights. Chief amongst them is the right of data subjects to request access to their data and update or correct the existing database.

In Singapore, individuals have the right to not only request access to their data but also rectifications. In India, data principles have the right to rectify any inaccurate or misleading personal data, complete any incomplete information and keep their data updated. In Thailand also, data subjects have the right to access personal data.



ix. Data Storage and Retention Policy.

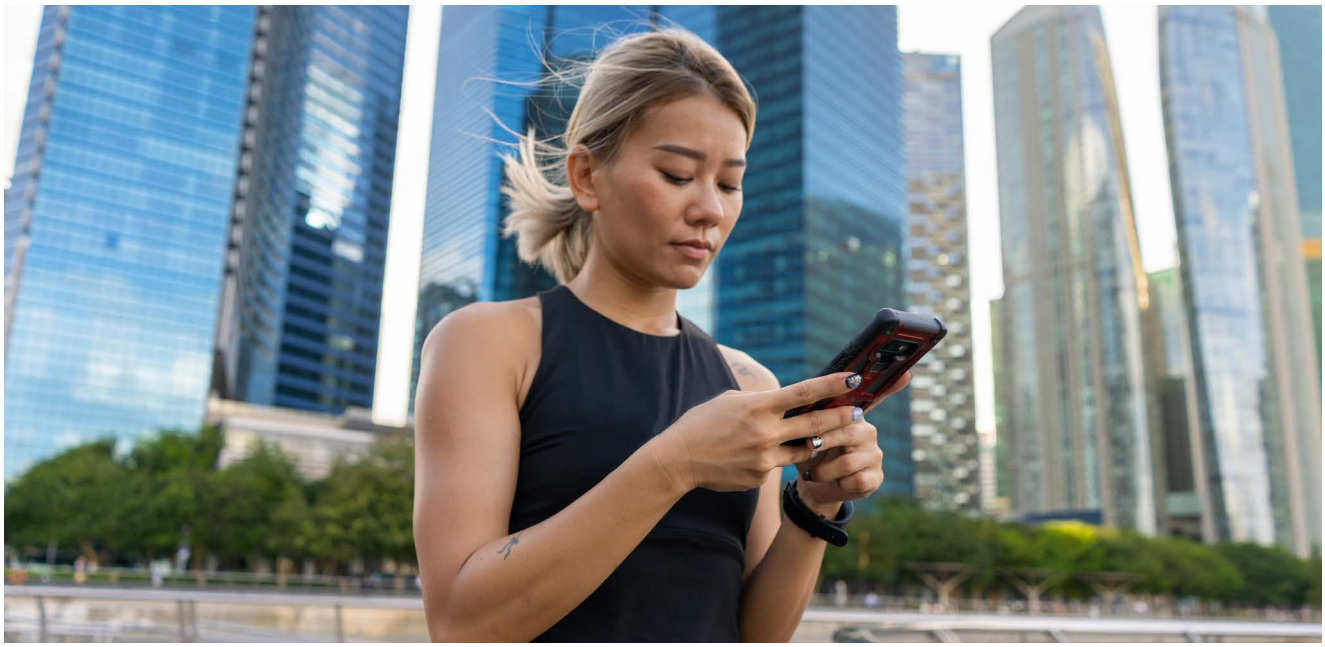
The storage of data uses up an organisation's space. It is better to erase/anonymise data once the purpose for which it was collected is fulfilled. The UK GDPR does not establish any predefined time limits for storing diverse data types. It is on the organisation to decide upon the period they need data for. On the fulfilment of purpose, either the data can be erased or anonymised.

In Singapore, an organisation should not hold personal data or remove the source through which the personal data can be linked with specific individuals when the purpose of data is fulfilled and is not required for any business or legal purposes.

In Thailand, the data controller needs to inform the data subjects in advance or at the time of collection of personal data, the period for which the data will be retained. If the period cannot be specified, the expected data retention period should be detailed. In India, as per PDPB, the time depends on the purpose.

Data can be retained till the time; it has fulfilled its purpose (at which point it must be expunged). In circumstances where the data is to be retained for a lengthier period, explicit consent is required.

Data can be retained till the time; it has fulfilled its purpose (at which point it must be expunged). In circumstances where the data is to be retained for a lengthier period, explicit consent is required.



x. Pseudonymisation.

The GDPR defines pseudonymised data as 'the processing of personal data in such a manner that the personal data that can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.'

Having said that, GDPR defines and has the provision of pseudonymisation

In India, the same has been dealt, under de-identification in PDPB. It states that de-identifying data is a compulsory security safeguard. It necessarily is implemented by data fiduciaries (anyone who determines the purpose and means of personal processing data) and processors (those who process personal data on behalf of a data fiduciary). The Data Protection Authority might issue a code of conduct on de-identification methods. Thailand PDPA and Singapore does not define pseudonymised data

xi. Anonymisation.

Anonymisation refers to the process of removing the identity of data.

Anonymisation refers to the process of removing the identity of data. It is an irreversible process of transforming or converting personal data so that an individual cannot be identified, which meets the standards of irreversibility stated by the DPA (Data Protection Authority).

However, some countries have listed conditions and allowed re-identification of data. In Singapore, the advisory guidelines define anonymised data, uses, and conditions under which it can be re-identified. In Thailand, the PDPA provides the right to request that personal data be anonymised.

The PDPA does not explicitly exclude anonymised data from its application. In India, the government may, in consultation with the DPA, direct a data fiduciary or data processor to disclose anonymised data or other non-personal data "to enable better targeting of delivery of services or formulation of evidence-based policies." Although not defined by the GDPR, anonymous data falls beyond the scope of the law (reasonable steps to re-identify). In practice, as per GDPR anonymisation is a high standard to put in practice.

€20m

xii. Penalties.

There is a penalty provision in all the laws being discussed in this article. The penalty ranges from civil, administrative, and criminal. All the penalties can be imposed on the defaulter in a few countries. As per GDPR, administrative fines up to the higher of twenty million Euros or four percent of a group of undertakings' annual global revenue can be imposed if there has been a violation of the law.

There are provisions of injunctive penalties, which include blocking processing, restricting international transfers, and requiring the deletion of personal data. Individuals may bring claims in court for compensation and mechanisms to exist for representative actions on behalf of a class of individuals. Singapore penalties range from fines of up to 10,000 Singapore Dollars or imprisonment for a term not exceeding three years, or both, depending on the offence. Officers and members of an organisation in breach of the PDPA may be held liable for breaches of that organisation.

In Thailand, civil, criminal, and administrative penalties are imposed on those who commit personal data breaches. A director or manager responsible for acts of a juristic person will be subject to criminal liability. In India, fines up to five crore rupees or two percent of total worldwide turnover, whichever is higher for lower-level offences. Fines up to INR15 crores or four per cent of total worldwide turnover, whichever is higher for more serious crimes. Any offence punishable under PDPB will be cognisable and non-bailable. INR 5000 per day for failure to address principal data requests, up to a maximum of INR10 lakhs for significant data fiduciaries and INR5 lakhs for other data fiduciaries.

A director or manager responsible for acts of a juristic person will be subject to criminal liability.

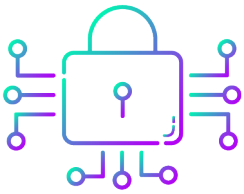
xiii. Important distinction:

There are few other rights that are applicable under GDPR, but other countries have not yet accepted them but are more likely to follow suit in near future. These are discussed below:

- **Right to object:** Under the GDPR, data subjects are provided with the right to object to processing their personal data in specific circumstances. This right is not applicable under PDPA Singapore. However, in Thailand and India individuals have this right.
- **Privacy of children:** The GDPR considers children as 'vulnerable natural persons' that merit specific protection about their data. Neither Thailand nor Singapore has such a provision. The Indian bill has certain sections dealing specifically with children's privacy.
- **Fines to government bodies:** The scope of GDPR is more expansive, and it provides for the application of penalties to government bodies. The PDPA in Thailand and Singapore does not apply to public authorities and bodies. In India, however, the bill applies to public agencies and private parties, but the central government can exercise its control to excuse any government agency from any or all provisions.

The Indian bill seems to be converging exactly in lines of GDPR, even at places broader than GDPR. The overreaching impact of the government is one of the concerns of Indian PDPB, but so is the concern with Thailand and Singapore.

The overreaching impact of the government is one of the concerns of Indian PDPB, but so is the concern with Thailand and Singapore.



952.8m

xiv. The importance of Data Security and Privacy.

A study revealed that in the first 11 months of 2021, a total of 952.8 million accounts were breached. It also revealed that one in five internet users each year are affected by data breaches, which is a worrying statistic. Data privacy is critical for every business organisation from the stakeholders' and management's viewpoints. Data privacy applies to every department of the organisation. It affects marketing, technical, human resource, product development. An entire organisation can be held culpable for the actions of a single department.

Many multinational corporations have received financial penalties for failing to meet privacy regulations. Amazon was fined a considerable sum of 746 million EU GDPR by Luxembourg's National Commission for Data Protection in July 2021. In 2020, the French Data Protection Authority (CNIL) imposed a fine of €35 million for Amazon's alleged failure to in providing cookie consent and associated information to users on its website.

In general, the areas where businesses fail, centre on the understanding and adhering to the data protection law, applicable in a country of operation. Another area, which is challenging for most companies is managing a data subject's rights. Another prone area is the technical and organisational measures offered by a company which sometimes do not provide sufficient levels of information security.

Today, data privacy and security are not just a compliance matter. There are other aspects included, like the growth and branding of the company. Breaches do not only cause harm to data subjects but also to the company that fails to protect security and privacy. The companies suffer monetary loss as well as legal complications. If a company does not provide data security in a digital world, it can very quickly (and publicly) admonish. Several companies are already taking data protection seriously and educating their employees through in-house training and education sessions. Simultaneously, they are adopting international standards, certifications and adhering to secure frameworks. It is also essential to understand that data security and privacy is not a one-time action; it is an ongoing process.

The road to adherence to various laws seems to be overwhelming. But the fact is it must be adhered to not just as a procedure but as a culture. The sooner the companies start to embrace the need to change business practices the better the outcomes will be.

Dr Raghuveer Kaur
Regulatory and Compliance Analyst, Starfish Digital

About the author.

Raghuveer holds a Ph.D. in management with a specialisation in finance from IIT Roorkee. She holds a double masters': business administration and commerce. Her areas of interest are data regulations and compliance and open banking. Since 2010, she has worked in the field of financial research and is the author of numerous published research papers. At Starfish Digital, Raghuveer is a Regulatory and Compliance Analyst.

About us.

Starfish Digital is a Financial Connectivity Platform. We digitise and deliver financial data between banks and companies. Our Starfish Universal Adaptor intelligently unlocks and integrates financial data from any source to any target. Starfish Connect provides an end-to-end managed service with the security and reliability demanded of critical B2B financial infrastructure. We understand the significance of Data protection. At Starfish Digital, data security is of utmost priority to us, our stakeholders, and our customers.

This working paper is a part of the **Starfish Digital Connect. Smart. Knowledge series.**

References:

1. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
2. https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act
3. https://www.dlapiperdataprotection.com/index.html?t=law&c=TH
4. https://www.dataguidance.com/resource/comparing-privacy-laws-gdpr-v-singapore-pdpa
5. https://www.dataguidance.com/sites/default/files/gdpr_v_thailand_updated.pdf
6. https://www.privacysecurityacademy.com/wp-content/uploads/2020/05/Comparison-Chart-GDPR-vs.-India-PDPB-2019-Jan.-16-2020.pdf
7. Data Breach Statistics for 2021 | The CISO Times
8. https://www.securitymagazine.com/articles/96667-the-top-data-breaches-of-2021
9. https://www.eqs.com/compliance-blog/biggest-gdpr-fines-2021/
10. https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/
11. https://www.lexorbis.com/key-features-of-the-personal-data-protection-bill-2019/
12. https://privacyterms.io/privacy/gdprcompliance/#:~:text=8.,profiling%20or%20automated%20decision%20making.
13. https://www.zicolaw.com/wp-content/uploads/2020/09/ASEAN-INSIDERS_PDPA-in-ASEAN-3.pdf
14. https://assets.kpmg/content/dam/kpmg/in/pdf/2020/01/data-privacy-day-infographic.pdf

About the publisher.

Starfish Digital is an Open Corporate Banking business.
We connect any company to any open banking service.

CONNECT. SMART.

starfish DIGITAL

www.starfish.digital/