OON & BAZUL

ASIAN EXPERTISE·GLOBAL REACH

Towards a Safe Digital Banking Future: How Singapore balances Cybersecurity and Data Protection Laws

Oon Thian Seng
Partner
Banking & Finance

Angeline Woo
Senior Associate
Banking & Finance

Towards a Safe Digital Banking Future: How Singapore balances Cybersecurity and Data Protection Laws

With increasing data breaches and evolving cyber threats and internet scams, the importance of integrating stringent legal and technological measures cannot be overstated.

This article explores how the Personal Data Protection Act 2012 (“**PDPA**”), cybersecurity regulations, and banking law interact in Singapore’s financial industry. It aims to provide examples of how institutions are navigating this complex and evolving ecosystem.

1. The Role of PDPA in Singapore’s Banking Sector

The PDPA governs the use, disclosure and collection of personal data in Singapore. Banks, being custodians of sensitive customer information, are subject to stringent obligations under the PDPA. In summary, PDPA has 11 obligations that organisations must comply with[1]. These include the consent obligation, notification obligation and transfer limitation obligation.

Out of these 11 obligations, these are the following provisions which are relevant to banks:

(i) Consent Obligation

Banks must obtain consent before collecting or using personal data unless an exception under the PDPA applies. As an illustration, banks cannot use customer data for marketing purposes without explicit consent, even if the data is already collected for account operations.

(ii) Purpose Limitation Obligation

Furthermore, data collected must only be used for purposes that customers are informed about. For example, if a bank collects data for a home loan application, it cannot share this data with third parties unrelated to the loan process.

(iii) Retention Limitation Obligation

Another obligation which banks must comply with is the retention limitation, which states that data must not be retained longer than necessary. To elaborate, if a bank closes a dormant account, it must delete customer data once the legal retention period expires.

[1] https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act/data-protection-obligations

2. Cybersecurity and Singapore's Banking Industry

Cybersecurity is critical in banking as the sector is a prime target for cybercriminals. There is a framework in the form of the Cybersecurity Act 2018 and the Technology Risk Management Guidelines implemented by the Monetary Authority of Singapore ("**MAS**") in 2021 to mitigate technology-related risks[2].

2.1 Technology Management Guidelines

Some of the key provisions include (i) risk assessment, (ii) risk treatment and (iii) incident response.

(i) Risk Assessment

Banks must regularly assess cybersecurity risks and vulnerabilities. This may include a structured framework for risk identification, which includes identifying all assets (i.e. IT systems, customer data), mapping assets to potential threats and vulnerabilities and quantifying potential consequences under various threat scenarios. The diagram below is a sample to risk prioritisation criteria.

Risk Scenario	Likelihood	Impact
Phishing attack targeting staff	High	Medium
Data breach from vendor system	Medium	High
Natural disaster affecting IT headquarters	Low	High

(ii) Risk Treatment

Thereafter, banks can develop a risk scoring system and assign numerical values to likelihoods and impact for each identified risk. Then, banks can calculate overall risk scores to prioritise resource allocation for mitigation. To elaborate, a phishing attack (likelihood: 5, impact: 3) with a score of 15 (5 x 3) would rank higher than a natural disaster affecting the IT headquarters (likelihood: 2, impact: 5) which will have a score of 10 (2 x 5).

(iii) Incident Response

Banks are required to implement a cyber response and management plan. This plan mist include procedures to isolate affected systems to prevent further spread of the attach and neutralise the threat by using appropriate technical measures such as disabling compromised accounts. For example, during a ransomware attack, the bank should immediately disconnect the affected network from external connections to contain the malware.

[2] https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf

2.2 Cybersecurity Act

The Cybersecurity Act 2018 focuses on critical information infrastructure ("**CII**"), including financial services. In the banking sector, CII refers to essential systems, such as ATMs or online banking platforms, whose disruption could severely impact national security or the economy[3]. Banks must conduct regular cybersecurity risk assessments, comply with codes of Cyber Security Agency of Singapore ("**CSA**")[4] and report cybersecurity incidents affecting CII to CSA. For example, a distributed Denial of Service (DDoS) attack targeting a bank's online banking platform must be reported immediately to the CSA. In the event of failing to report, the bank will face penalties under the Cybersecurity Act 2018.

3. Intersection of PDPA, Cybersecurity, and Banking Law

Singapore's legal framework seeks to integrate PDPA, cybersecurity measures, and banking law to create a system that ensures data protection and regulatory compliance.

Banks in Singapore have implemented a few measures to aim to create a harmonious ecosystem.

For example, DBS Bank has invested heavily in cybersecurity[5]. Its AI-Driven Fraud Detection:

DBS deploys machine learning algorithms to detect and prevent fraudulent transactions.

Through a rule-based transaction surveillance system powered by AI and machine learning, DBS analyses transaction data to identify unusual patterns or deviations from expected norms. This system generates a probability score to assess the level of suspicion, allowing analysts to review flagged cases before reports are made.

Furthermore, DBS also engages in regular campaigns and emails to educate customers about phishing and secure online practices.

Another illustration is OCBC's Cybersecurity Programme[6].

OCBC has established a Group Information Security and Digital Risk Management Committee and the Board Risk Management Committee to oversee risk management practices and information security. In addition, it has introduced an anti-malware security feature in its digital banking application. This feature detects and blocks access to the application if malicious software is present on a user's device. Within the first month of its implementation, this measure prevented scammers from stealing over S$2 million from customer's accounts.

4. Challenges in Compliance

With the rise of cloud computing, blockchain, and artificial intelligence, banks face difficulty ensuring compliance with PDPA and cybersecurity laws while leveraging these technologies.

[3] https://sso.agc.gov.sg/Acts-Supp/9-2018/

[4] https://www.csa.gov.sg/

[5] https://www.dbs.com/artificial-intelligence-machine-learning/artificial-intelligence/ai-the-future-of-banking-and-finance.html

[6] https://www.ocbc.com/group/sustainability/responsible-business/our-cybersecurity-programme

Moreover, overly stringent security measures may hinder customer experience. Banks must balance strong cybersecurity with seamless services.

5. Recommendations for Banks

To navigate the intersection of PDPA, cybersecurity, and banking law effectively, banks should adopt the following strategies.

5.1 Invest in Customer Awareness

Banks can educate customers about their rights under PDPA and the importance of protecting their data in the form of talks and campaigns.

5.2 RegTech Solutions

Furthermore, banks can utilise Regulatory technology ("**RegTech**") tools to automate compliance. Automated systems identify where personal data is stored, processed and shared. Alerts are generated for unauthorised access or transfers. For example, a RegTech tool flags that customer data is being transferred to an external vendor without proper consent, enabling the bank to fix the issue. This complies with the accountability obligation under the PDPA, which requires banks to maintain oversight of data handling. Data mapping ensures compliance by providing full visibility.

6. Conclusion

To conclude, the intersection of PDPA, cybersecurity, and banking law highlights the complexity of operating in Singapore's financial sector. While stringent regulations ensure robust data protection and cybersecurity, they also present challenges for banks striving to innovate. Banks like DBS, OCBC, and UOB provide practical examples of how to balance innovation with legal frameworks.

This article was authored by our Founding Partner and Head of Corporate Oon Thian Seng and Senior Associate Angeline Woo.

Oon & Bazul LLP's Banking & Finance Practice has established a strong reputation with financial institutions in Singapore, particularly with merchant and trade banks. Our expertise in trade and asset finance in shipping and international trade is highly regarded. Our work includes advising on all forms of finance including syndicated, club and bilateral debt financings as well as leasing, export credit financings, seller's credits, derivatives and other credit enhancement products, bond issues and other forms of capital raising. We are also capable of advising in specialty matters relating to conveyancing, projects & real estate and private client services.

The team has capabilities in both non-contentious and contentious matters, and also assists banks with compliance and regulatory advice in the quickly developing AML/KYC compliance environment.

You may visit our Banking & Finance page to learn more about our practice.