asifma

Growing Asia's Markets

Implications of Data Privacy for Financial Technology in Asia

October 2018

asifma
Growing Asia's Markets

Disclaimer

The information and opinion commentary in this ASIFMA – Implications of Data Privacy for Financial Technology ('Paper') was prepared by the Asia Securities Industry and Financial Markets Association (ASIFMA) to reflect the views of our members. ASIFMA believes that the information in the Paper, which has been obtained from multiple sources believed to be reliable, is reliable as of the date of publication. As estimates by individual sources may differ from one another, estimates for similar types of data could vary within the Paper. In no event, however, does ASIFMA make any representation as to the accuracy or completeness of such information. ASIFMA has no obligation to update, modify or amend the information in this Paper or to otherwise notify readers if any information in the Paper becomes outdated or inaccurate. ASIFMA will make every effort to include updated information as it becomes available and in subsequent Papers.

asifma
Growing Asia's Markets

ASIFMA is an independent, regional trade association with over 100 member firms comprising a diverse range of leading financial institutions from both the buy and sell side including banks, asset managers, law firms and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative and competitive Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the GFMA alliance with SIFMA in the US and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region.

asifma
Growing Asia's Markets

Table of Contents

I. Balancing Innovation With Data Privacy 2
II. Impact/Considerations of Data Protection Regulations on Fintech for Personal Data 3
a. Defining 'Personal Data' 3
b. Consent and Notice Regimes 4
c. Sharing Data & Export Controls 5
d. Impacts and Limitations on Innovative Technology 6
i. Distributed Ledger Technology 6
ii. Artificial Intelligence 7
iii. Big Data 7
iv. Cloud Computing 7
III. Importance of a Principles-Based Approach 8
a. Promoting Innovation 8
b. Meeting Regulatory Needs 8
IV. Fundamentals of a Principles-Based Approach 9

I. Balancing Innovation with Data Privacy

Over the last three decades the global flow of digital data has risen dramatically from close to zero to more than a zettabyte (one trillion gigabytes) globally. A 2017 paper by the International Data Corporation estimates that by 2025, the world "will create and replicate 163ZB of data," which would be a tenfold increase over 2016.[1] The exponential growth of data has occurred simultaneously with an exponential growth of the value of utilizing that data in products and services. All organisations create and use data and the most successful are those that are best able to process it into meaningful forms.

The free flow and utilisation of data are particularly important to the proliferation of financial technology ("**Fintech**"). Emerging technologies such as distributed ledger technology ("**DLT**"), big data, machine learning, artificial intelligence and the cloud have the potential to drive innovation in the industry and to catalyse greater financial inclusion. The World Bank estimates that there are about 1.1 billion unbanked adults globally, but in countries such as China where over 80% of unbanked adults have a mobile phone, Fintech can present an avenue to gain access to financial services. Jurisdictions across the Asia-Pacific region are understandably keen to promote the development of Fintech ecosystems that can support economic growth and opportunity.

Despite the rising importance of data, relevant regulatory structures have not adapted or been optimised for use in commerce and Fintech. Until recently some countries were using laws and regulations meant for managing risks from information on paper and/or locally, rather than for data that can be shared around the globe in moments. Meanwhile, many jurisdictions that have acted to introduce new regulations and requirements have created a patchwork of legal and regulatory barriers that impose varying, and at times conflicting, obligations on firms. Over 100 countries have national and/or sectorial laws and regulations across applicable areas, particularly privacy, information security, cybersecurity and data localisation.

As countries across Asia update their personal data protection regulations, it is essential that they avoid placing barriers that would prevent the flow of information or the innovative use of data, as such impediments can impose real and substantial economic costs. A report released in 2017 by the Information Technology & Innovation Foundation estimated the costs to national GDP of data localisation and other barriers to data flows for certain countries as "reducing U.S. GDP by 0.1-0.36 percent; causing prices for some cloud services in Brazil and the European Union to increase 10.5 to 54 percent; and reducing GDP by 0.7 to 1.7 percent in Brazil, China, the European Union, India, Indonesia, Korea, and Vietnam."[2]

The privacy regulations across the region directly impact where an institution or business decides to make the relevant product available, and in some circumstances even influences where they or their applicable subsidiary will be incorporated. The difference in regulations across the Asia-Pacific region also means that some countries in the region are 'left behind' in terms of innovation and financial inclusion due to their localisation requirements, effectively excluding them from the advances and innovation enjoyed by others and creating a

[1] "Data Age 2025: The Evolution of Data to Life-Critical," International Data Corporation, April 2017, https://www.seagate.com/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf

[2] "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?," Information Technology & Innovation Foundation, May 2017, https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost

fragmented geographical area.

While this paper specifically focuses on personal data, it is important to remember that other types of data are similarly important, such as financial data or client information that is not typically considered personally identifiable in many jurisdictions. Additionally, non-data-specific requirements such as Know Your Customer ("**KYC**"), anti-money laundering ("**AML**") and counter-terrorism financing, trade reporting, and cybersecurity requirements can all necessitate the collection, sharing and processing of information with public and private organisations, as well as within a company across borders. Different types of data are impacted directly and indirectly by requirements from a variety of bodies including financial regulators, data privacy commissions and other government agencies. Each of these should consider the implications and interplay of their requirements, both in the Fintech space and across industries, as the complexities of overlapping regulations and obligations can represent substantial costs to firms and act as a barrier to expansion in new or different jurisdictions.

In keeping with their support for Fintech, governments and regulators should keep in mind that these technologies are exponentially more powerful and effective when they have access to larger pools of information. While there should be protections around personal data, the regional harmonisation of definitions, requirements and expectations for data protection would provide a level of legal certainty that could help facilitate the continued growth of the use of these new technologies and of innovative Fintech ecosystems across the region. This harmonisation would also generally broaden the appeal of the region for all businesses and boost economic growth.

II. Impact/Considerations of Data Protection Regulations on Fintech for Personal Data

Data protection rules have a fundamental impact on the uptake and development of financial technologies. These financial technologies are being developed by companies ranging from start-ups through to existing, global financial institutions. Without exception, these companies rely on some measure of processing of personal information and this can be core to the relevant product. Different interpretations of data protection definitions and rules can cause confusion, as these rules directly impact the innovative technologies and products being developed, and the confidence of the business to make a product available across markets in Asia.

Some key areas where different regulations across the region have complicated the adoption or expansion of Fintech include the definition of 'personal data,' unclear and disparate consent and notice regimes, and restrictions on the sharing or export of data to third parties.

Defining 'Personal Data'

The central tenet of data privacy regulation is that such laws govern the practices and activities relating to 'personal data' or 'personal information'. However, the definition of personal information is not consistent across Asia and the interpretation of such terms also varies across the regulatory landscape.[3] In addition to this, certain jurisdictions go a step further and include additional rules for 'sensitive' data (such as biometric data, which can be a desired method of authentication as it can be considered more secure than traditional

[3] E.g., Vietnam leverages cybersecurity regulations rather than any specific privacy laws, meaning the 'data' regulated is not personal in the way it is understood in Singapore and Hong Kong. In Thailand, requirements on processing of data stem from computer systems regulations, which deal with 'computer data' rather than data which has any connection to an individual.

methods or which may be combined with another authentication method, such as a password, for increased security). However, not all jurisdictions have a subset of rules for sensitive data.[4] As a result, the use of biometric data, for example, by a company in one jurisdiction may not be practical or even permitted in another, even though it may be a more secure method of authenticating a user.

Whether encrypted data and IP addresses are personal data has been hotly debated.[5] In certain jurisdictions such as Australia, it can be argued that encrypted data is sufficiently obfuscated that it no longer constitutes 'personal information', while in others, such as in the European Economic Area (even before the entry into force of the General Data Protection Regulation), it remains personal data in its encrypted form. Encryption is at the heart of many emerging financial technologies and not knowing whether data is subject to regulation even when it is encrypted can hamper a firm's ability in many jurisdictions to take a dataset and obfuscate in a way that allows it to be useful while still complying with privacy requirements. A harmonised approach to the status of encrypted data and IP addresses would be a boost to innovation and the growth of Fintech ecosystems.

Consent and Notice Regimes

Jurisdictions across Asia have varying rules governing consent, with some common themes but no single, fixed rule that a firm can leverage to treat Asia as a whole. In certain jurisdictions, express consent, or 'opt in' is required[6] for personal data, whereas in others, an implied consent will suffice.[7] Indeed, certain jurisdictions, such as Cambodia, have no explicit rules at all, and therefore firms must look to obscure legislation or general international treaties to determine what rules might apply to obtain consent for the use of personal data in that jurisdiction. If firms are subject to financial regulation, additional consent requirements may apply to personal and non-personal data (taking as an example, banking secrecy consents under the Banking Act in Singapore).

As such, there is no "one size fits all" approach that can be taken by companies looking to comply with data protection rules, meaning they and their partners need to have a tailored approach to consents: determining where they are actually relevant and meaningful and drafting up different consent clauses for different jurisdictions. This presents an additional costly barrier to entry to new markets and can especially factor into decisions on the value proposition whether of entering a smaller market or rolling out a new product in an existing market.

Some firms have resorted to asking for explicit consent from consumers whenever they collect personal data, under the misconception that doing so is the simplest way to ensure compliance with data protection regulations. This is an erroneous view, for multiple reasons. In many instances, consent is not a meaningful basis for processing, as the processing is necessary or required in order to provide the goods or services (for example, AML or KYC processing, or consent from employees to outsource payroll functions to a third party where there is no alternative internal function). Furthermore, individuals must be able to withdraw

[4] E.g., Singapore.
[5] Case C-582/14: *Patrick Breyer v Bundesrepublik Deutschland*.
[6] For example, Indonesia requires express "approval". See MOCIT Reg 20/2016. 'Express consent" is required in the Philippines under the Data Privacy Act of 2012.
[7] Singapore affords some flexibility where organisations are tasked with determining whether a person "has sufficient understanding of the natured and consequences of giving consent", and to obtain such consent accordingly.

their consent at any point. This means that companies must have mechanisms to remove personal data from their database upon an individual's request. For companies that use personal data collected for machine-learning, this might create complex problems such as ensuring that the algorithm can "reverse" any learning from a specific data set at any point in time. In addition, sometimes the very act of requesting consent through the use of personal data like email addresses is still a violation of data privacy regulations.

The multitude of laws across Asia that deal with the requirements for notice has also led to wide variation in privacy policies in the market. Start-ups favour simple, template-based notices while more sophisticated firms generally adopt more precise and detailed privacy policies. Privacy notices also vary in detail, from policies that provide a high-level overview to others that go into more granular detail (the latter driven by regimes such as those in Korea and Europe). The problem of regulatory fragmentation is compounded for multinational companies, whose products and services are offered in multiple jurisdictions. In those scenarios, companies usually adopt lengthy, and often convoluted, privacy policies with multiple annexes that only serve to confuse, rather than inform, users.

To add to the confusion, regulators across Asia have historically not proactively policed privacy notices, so until something goes wrong (for example, in the event of a data breach), an entity generally does not know if its privacy notice is considered compliant or appropriate by the regulator.

While there has not been definitive guidance on what is required to satisfy notice requirements, Asia has a great opportunity to learn from the experiences in the US and EU where privacy notices have become long and complex and are rarely read or understood by users, thereby inhibiting the user experience and creating an unnecessary bureaucratic burden. Instead, notices should be brief, to the point, and relevant to the type and risk of processing, and the means of delivery of the service (e.g. mobile phones versus websites versus paper etc.).

Sharing Data & Export Controls

The storage of data, and many processing operations, are in the modern environment outsourced to a third-party service provider that specialises in and may be better suited to securing such data (notwithstanding that institutions maintain control of the data even where the infrastructure is managed by a third party).

The 'controller', 'processor', 'co-controller' and 'joint controller' distinctions (to the extent these European-centric concepts have commensurate meanings in Asia), and the definition of what constitutes a 'transfer' of data, are difficult to align with the models of service delivery that are emerging. In traditional models of service delivery for software or infrastructure, it was reasonably clear who had responsibility for what personal information. This is not the case with hybrid solutions that mix, for example, Platform/Software as a Service with DLT. Where privacy laws have created specific roles for entities, the laws are not as amenable to accommodate hybrid models of service delivery. The result is that either: (i) the parties to the transaction artificially assign themselves roles required by law that are not reflective of the nature of the service; or (ii) the parties have to try and backwards engineer the service to reflect the law (such as adding special permissions in a permissioned blockchain to allow an administrative account to have master control of the ledger – which is the antithesis of the security and integrity afforded by the technology). Such efforts to accommodate prior

concepts and roles further have the adverse effect of impeding innovation and the ability to improve efficiencies.

Vagaries in interpretation of data protection laws also has an impact on the increasing volume of collaborations and joint ventures between established financial institutions and start-up firms. The aim of many of these relationships is that the parties can share information and pool resources to better service existing customers and attract new clients, and in doing so develop innovative new financial technologies and products. However, the challenges outlined above, including what conditions should be satisfied before data can be shared, whether such data can be encrypted or anonymised and therefore be used flexibly, and what role each party has given the traditional privacy frameworks, presents a significant barrier to rapid development and adoption of Fintech solutions by financial institutions, and consequently the growth of Fintech ecosystems.

Impacts and Limitations on Innovative Technology

Data privacy rules are playing a key role in influencing future innovations such as digital ID, big data, artificial intelligence and cloud-based systems, all of which play a significant role in the development of new financial technology and will be critical to the growth of Fintech firms and applications in the Asia-Pacific region. Policymakers should take care that their rules are technology neutral, such that the requirements do not unduly impede technologies that could otherwise present great opportunities in meeting the financial needs of their citizens.

Distributed Ledger Technology

A pertinent example is blockchain and DLT, which do not pair well with privacy regimes that mandate specific roles for entities that process data, such as the regimes in Korea and Europe. A permissionless blockchain stores (personal) information in multiple locations with permanency. Although it is possible to find creative arguments to align the technology with the law – for example, arguing that obfuscating the data is adequate to satisfy 'deletion' requirements; or to twist the technology to comply with the law (such as allowing a 'super user' on a permissioned blockchain to delete data; or having the personal data stored outside of the blockchain itself with the blocks storing mere reference files) – each of the arguments or technical solutions runs contrary to the intention of the technology itself, as they increase the overall complexity of fetching and storing data on a blockchain, and in some cases actually increases the risk to the integrity and security of the data. In particular, the benefit of transparency with blockchain is reduced since, by storing data outside the blockchain, there is no way of knowing who accessed the data, and who has access to the data.

As noted above, the way DLT processes personal data is challenging the established paradigms that underpin many data protection regimes, such as the notion of a 'processor' and a 'controller'. The difficulties presented by the underlying conceptual framework, along with inconsistencies in data export, transfer and localisation laws across the region (for example Hong Kong has 'soft' export restrictions[8] that are not yet in force but considered "guidance," while localisation restrictions are already in place in Indonesia[9] and Vietnam[10]) makes it difficult for financial institutions to address Asia as a whole and reduces their ability to use promising technologies like DLT. This is compounded by issues in managing data subject rights (e.g., How do you delete information that is un-deletable? How can data be corrected if the

[8] See section 33 of Cap 486 Personal Data (Privacy) Ordinance.
[9] Regulation 82.
[10] Decree No. 72/2013/ND-CP of the Government of Vietnam dated 15 July 2018.

ledger is immutable?).

Artificial Intelligence

Another example of new technology that does not fit neatly into the existing data privacy framework is artificial intelligence and machine learning. This includes robo-advisors and robo-solutions where systems are automated and the owner of the platform (i.e., the technology firm or financial institution) does not have interaction-by-interaction control over the system. Technology firms are offering up these types of platforms to financial institutions to use in test environments and in some cases with dummy customer data. It is unclear in these cases who would be the data controller and who would be the data processor. While robo-advisors or robo-solutions typically require user input of personal information in order to generate results, should a user decide not to proceed, data may be deleted, and therefore, may not technically be used or controlled by the entity that offers the platform. This makes it problematic for the parties involved with the platform to determine what their obligations are to users under data privacy rules. AI solutions are also challenging one of the founding notions of most transparency requirements under data privacy regimes: telling users what their data will be used for. The core benefit of AI is that it may have the ability to perform tasks and offer products and services to a customer that are perhaps not contemplated by a human being tasked with the same role. Does this mean that the AI is using personal data in a way that is not technically articulated as the purpose for which data was collected in the relevant privacy notice?

Big Data

Further, use of large databases of customer data with data sourced from different places (i.e., 'big data') is a helpful tool for start-ups seeking to experiment with products and train products to better address customer needs. However, the use of big data, particularly enriching data from multiple sources, presents a significant challenge: users may not be aware that certain data may be mixed with data sourced from a third party in order to create custom products.

Cloud Computing

Use of cloud solutions presents its own challenges for regulated financial institutions. Multiple regimes with varying degrees of expectation with regards to control, access, audit and transfer, make it difficult to economically leverage cloud services. For example, Korea, Singapore and Europe each require some form of contractual control for data export, whether or not data is accessed by a third party. This means that use of a cloud service provider, even where the master encryption key may be held by the customer itself and not the service provider, is treated no differently than a traditional software-supply set-up. To contrast, a jurisdiction such as Australia arguably allows an entity to leverage cloud services and the law instructs that provided certain controls are in place such use of cloud is treated as if it is the clients' own infrastructure (i.e., as a 'use' rather than a disclosure' for the purposes of the Australian Privacy principles).

The varied nature of data protection laws across Asia, together with a lack of clarity on how such laws fit with emerging technologies results in significant uncertainty for innovative firms, large and small, developing financial technologies for the benefit of consumers. Compared to other regions, Asia would disproportionately benefit from harmonisation of approach and interpretation of data protection laws in order to boost innovation and strengthen its position as a centre for developing and bettering Fintech solutions.

III. Importance of a Principles-Based Approach

ASIFMA recommends the adoption of a principles-based approach to regulation as a guide to develop tools for ensuring privacy of personal data. Broadly, a principles-based approach means moving away from reliance on detailed, prescriptive rules and instead designing high-level rules or principles that are results-oriented and focuses on "what" rather than "how". Regulation should define the desired outcomes (i.e. results) rather than setting out an exhaustive and prescriptive list of the means that must be taken by a data controller or a data processor to achieve the desired outcomes (i.e. technical details). Such an approach should also be technology-neutral, to allow principles to preserve their relevance and applicability in the context of continually changing and emerging technologies, particularly in the Fintech space.

Principles-based regulation generally contains terms that are more qualitative than quantitative in nature, and uses evaluative terms (e.g. fair, reasonable, suitable) rather than bright line rules. This enables a risk-based approach to compliance, which is particularly important in the Fintech space as it does not stifle innovation with rigid requirements while still meeting regulatory needs in an area of rapid change and growth.

Promoting Innovation

A principles-based approach affords firms the flexibility and space to innovate, recognising the shortcomings of a one-size-fits all model. It gives firms, whether they are large, well-established institutions or new start-ups, the flexibility to take a risk-based approach to compliance that is tailored to their own business models, needs and practices. For start-ups with limited resources, this flexibility is particularly critical as it permits them to focus more on their products and services rather than diverting precious, limited resources towards complying with prescriptive rules unfit for their risk profiles.

Following principles rather than prescriptive rules also makes it easier for firms to operate confidently across borders and enter new markets, a consideration that is especially important if the disparate markets of the Asia-Pacific region are to benefit from Fintech. Harmonised principles can apply effectively throughout the region in ways that let firms access consumer bases internationally. When firms are more comfortable working across borders, they are more likely to confidently enter new markets, encouraging beneficial competition among firms that ultimately results in better solutions for clients and consumers.

Meeting Regulatory Needs

Regulators applying prescriptive rules to the industry face significant headwinds in a time of unprecedented innovation. Rules are just best guesses as to the future, and new technologies and applications make it likely that regulators will encounter unexpected situations where previously drafted rules cannot be effectively applied. Innovation is simply moving too quickly for backward-looking regulation and prescriptive rules serve only to stifle the potential of innovation. Principles-based and technology-neutral regulations, on the other hand, allow for a greater degree of “future-proofing” where the regulatory regime does not need to be updated or amended with every new technology or application. They can also continue to apply well even in situations where regulators have not yet been able to understand a new technology, lessening the risk of a delayed (or rushed) regulatory response that could bring about vulnerabilities in the regulatory framework.

A principles-based approach can also provide a solid basis for open and ongoing dialogues

between regulators and firms using new technology solutions. This dialogue can in turn facilitate a more cooperative and educative approach to supervision, and industry buy-in to the flexibility of a principles-based approach can end a "tick-the-box" mindset to compliance that ultimately yields more substantive compliance and better results.

Principles that focus on operational results rather than technical details can be more effective because firms and their management are better placed than regulators to determine what processes and actions are required to best achieve regulatory objectives. Rather than prescribing specific processes or actions, regulators can simply define desired outcomes and check for compliance through normal supervisory mechanisms.

IV. Fundamentals of a Principles-Based Approach

Taking into consideration the issues discussed in this paper, we would recommend that policymakers take the following into consideration when developing their own principles-based regulatory frameworks for personal data privacy:

1. Focus on outcomes rather than processes

The definition of desired outcomes by regulators, rather than prescription of "one size fits all" processes for all firms and business models, allows firms to apply a risk-based approach to compliance that is best-tailored to specific business models and activities. Firms are better positioned to understand their own systems and vulnerabilities than regulators and should be empowered to leverage this understanding to make informed decisions on how to best meet regulatory objectives.

2. Ensure technology neutrality of regulation

Principles afford a degree of technology neutrality that is necessary in the ever-changing Fintech space. A regulatory framework, even with broadly principles-based, can be undermined if it does not account for the possibility, and indeed likelihood, of innovation and new technologies. Policies with specific technology requirements are inherently reactive to threat environments and become quickly outdated.

3. Ensure consistency with existing international best practices

As a means of ensuring regulatory harmonisation governments can turn to both international and regional frameworks to guide their efforts. This approach will provide a foundation for globally synchronised regulatory approaches and mutual recognition which would facilitate similar protections and also facilitate better access for individuals to protect their data rights.

The OECD Guidelines on the "Protection of Privacy and Transborder Flows of Personal Data" were developed by OECD member states over four decades ago through engagement with a wide cross section of stakeholders and focus on personal data. Notably, the OECD's guidelines specifically warn against restrictions on cross-border data flows that could "cause serious disruption in important sectors of the economy, such as banking and insurance."

The APEC Privacy Framework, which is partly based on the OECD Guidelines, is also an important resource for Asian governments. All of the member governments of APEC have signed the Privacy Framework which "promotes a flexible approach to information privacy protection across APEC member economies, while avoiding the creation of unnecessary barriers to information flows." It includes a set of principles and implementation guidelines that form the basis of the APEC Cross-Border Privacy Rules System (CBPR), an international

framework that could be used to help harmonise the requirements for cross-border transfers. Currently, one of the key limitations of CBPR is that certification does not in itself mean that personal data can be transferred from any other APEC economy. The law in each other economy must permit such transfers. Currently, no laws in APEC economies clearly provide that exports to APEC CBPR-compliant companies are allowed. This is an area that the Asian governments and privacy regulators may want to work on.

4. Focus on how data is stored, not the geographic location

There is a trend in the region of governments instituting data localisation and cybersecurity laws that require data be stored onshore to ensure its accessibility to local authorities. However, the geographic location of data is less important than how it is processed, as regional data centres can more effectively monitor and react to threats than can localised national data centres that segregate data. Differing requirements across jurisdictions also cause legal tensions that undermine the coordinated multijurisdictional approaches necessary to make cybersecurity, sanctions and AML enforcement effective. Governments and regulators should instead focus on how data is processed to ensure minimum protections are met regardless of the physical location of data centres.

5. Allow for mechanisms to facilitate cross-border sharing

The regulatory regimes that govern the financial sector must allow for mechanisms to facilitate the cross-border sharing of specific information that allows the private and public sectors to work together more effectively to ensure investor protection and combat financial crime. One such mechanism that has seen success is the global network of Financial Information Sharing Partnerships (FISPs). More than 20 countries have committed to developing public–private financial information-sharing partnerships (FISPs) that bring law enforcement and other public agencies together with groups of major financial institutions to tackle money-laundering and terrorist-financing risks more effectively. It would be helpful for local privacy laws to contain an exception to allow information sharing and cross-border transfer under such mechanisms.

In 2017, three new FISPs were launched in the Asia-Pacific. This includes the Fintel Alliance in Australia, the Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership (ACIP) in Singapore; and the Fraud and Money Laundering Intelligence Taskforce (FMLIT) in Hong Kong. In the first four months of FMLIT's operation, public–private information sharing through FMLIT is credited with contributing to the arrest of 65 persons and the restraint of HK$1.9 million worth of assets. FISPs must act within existing laws, however, and laws that develop barriers to information sharing threaten the development of these tools to fight financial crime more effectively. Further, there are many firms, large and small, using technology to come up with innovative solutions in the area of financial crime. Barriers on the movement of data across borders limits the efficacy of such solutions and therefore discourages innovation.

6. Preserve ability of firms to outsource functions to third-parties

As innovative firms in the financial sector grow, they often need to rely on a network of other firms to provide services that they are unable to accomplish effectively in-house or to leverage third-party expertise. These might include customer service, KYC screening or even some back-end IT functions. Through outsourcing, firms can achieve greater consistency of approach, leverage established expertise and reduce operational costs while maintaining high levels of efficiency. We recognise that an effective data protection regime must include requirements related to outsourcing and the engagement of personal data processors, but to

avoid unnecessary complications or barriers and make local companies less competitive than those located outside, regulators should be mindful of how requirements might limit access to critical third-party providers.

This successful application of a principles-based approach could serve as a good model for other jurisdictions in the Asia-Pacific region that protects data privacy without unduly burdening start-ups and financial institutions. It is worth noting that a purely principles-based approach is not always necessary, and indeed there will be some limited instances in which more prescriptive rules or guidance are necessary. As with any regulatory action, the best results are achieved through robust consultation with industry and other stakeholders. ASIFMA stands ready to offer industry views to inform the development of frameworks that serve the best interests of firms, customers and policymakers.

Authors

ASIFMA would like to extend its gratitude to all the individuals and member firms who contributed to the development of this paper.

Paul Hadzewycz
Senior Associate, GFMA

Kieran Donovan
Registered Foreign Lawyer (New South Wales)

Peggy Chow
Senior Associate

Dan Warelis
Government and Regulatory Affairs, Asia-Pacific

About Refinitiv
Refinitiv is one of the world's largest providers of financial markets data and infrastructure, serving over 40,000 institutions in over 190 countries. It provides leading data and insights, trading platforms, and open data and technology platforms that connect a thriving global financial markets community - driving performance in trading, investment, wealth management, regulatory compliance, market data management, enterprise risk and fighting financial crime.

About Latham & Watkins
Latham & Watkins delivers innovative solutions to complex legal and business challenges around the world. From a global platform, our lawyers advise clients on market-shaping transactions, high-stakes litigation and trials, and sophisticated regulatory matters. Latham is one of the world's largest providers of pro bono services, steadfastly supports initiatives designed to advance diversity within the firm and the legal profession, and is committed to exploring and promoting environmental sustainability

About Herbert Smith Freehills
Operating from 27 offices across Asia Pacific, EMEA and North America, Herbert Smith Freehills is at the heart of the new global business landscape providing premium quality, full-service legal advice. We provide many of the world's most important organisations with access to market-leading dispute resolution, projects and transactional legal advice, combined with expertise in the global financial services sector. With a 30-year history in Asia, Herbert Smith Freehills has over 300 lawyers and legal professionals in the region, advising clients on complex corporate, disputes and finance matters from offices in Bangkok, Beijing, Hong Kong, Jakarta*, Kuala Lumpur, Seoul, Shanghai, Singapore and Tokyo.

*In Jakarta, Herbert Smith Freehills' international counsel practise alongside its affiliate firm, Hiswara Bunjamin & Tandjung, one of Indonesia's leading commercial and corporate law firms.

UNIT 3603, TOWER 2

LIPPO CENTRE

89 QUEENSWAY

ADMIRALTY

HONG KONG

TEL +852 2531 6500

WWW.ASIFMA.ORG