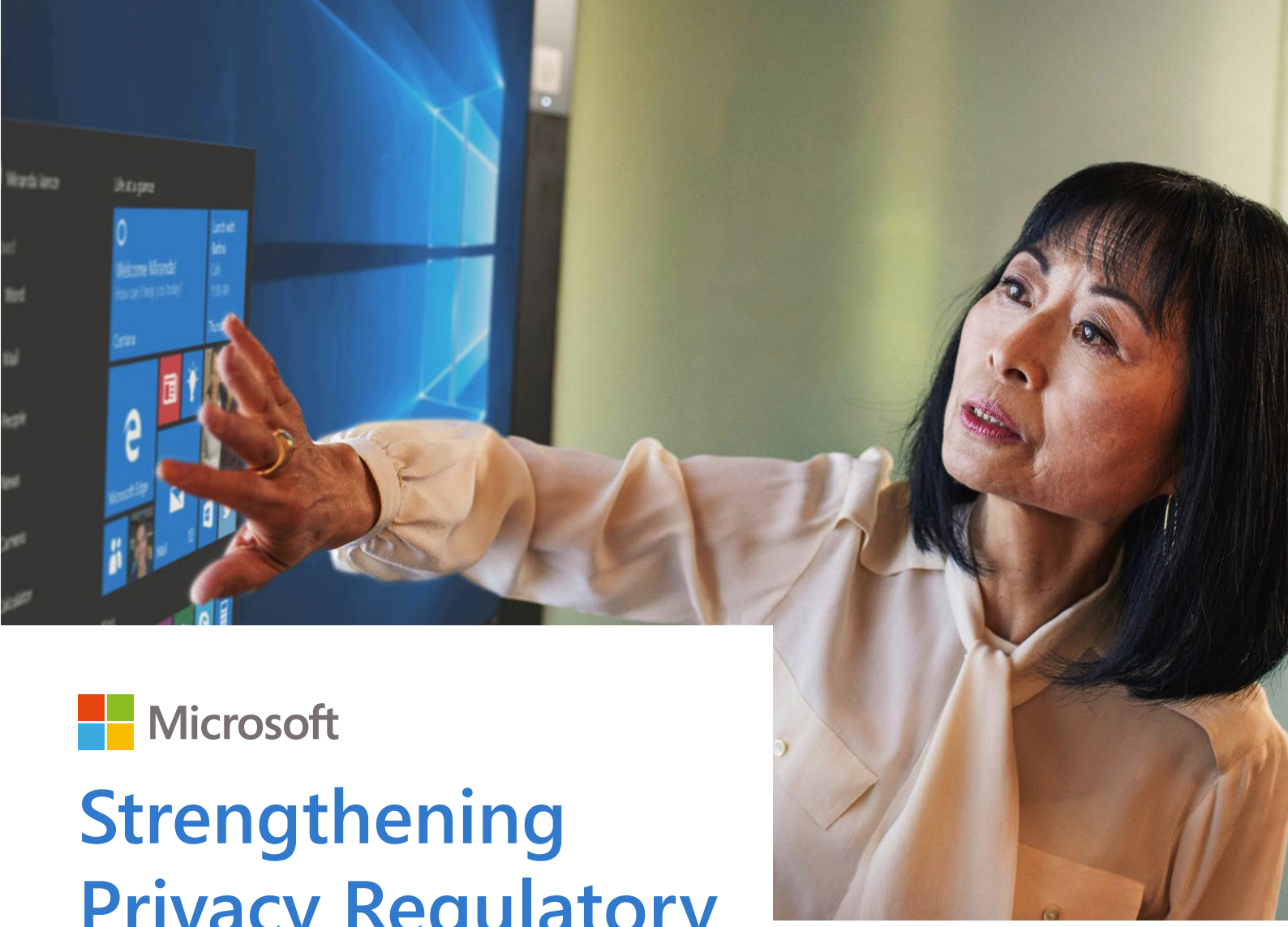
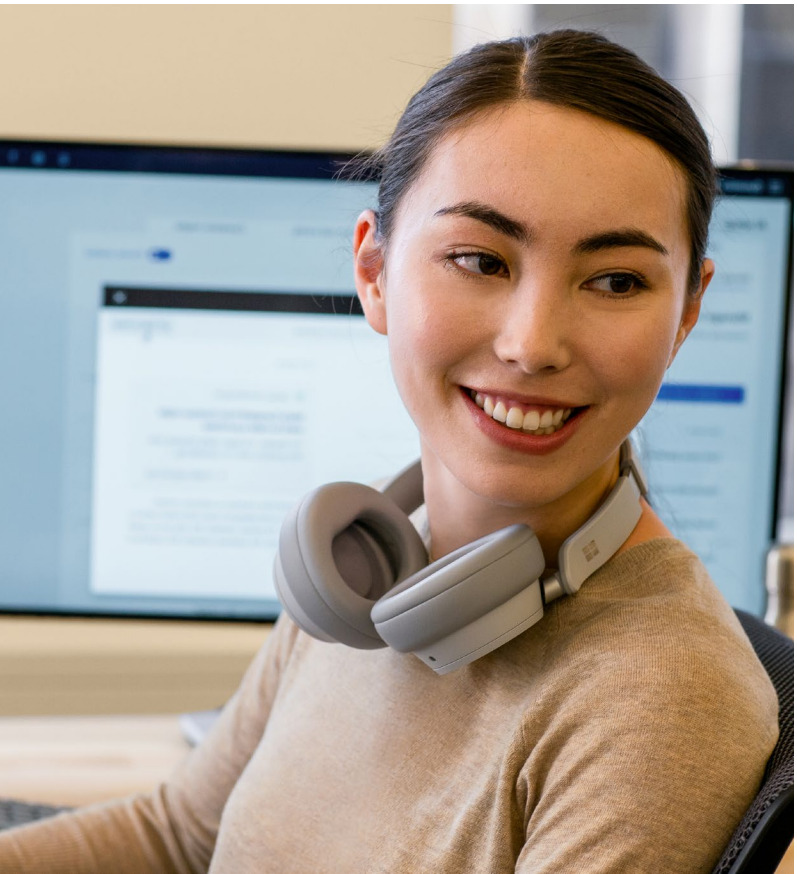


Microsoft

Strengthening Privacy Regulatory Coherence In Asia



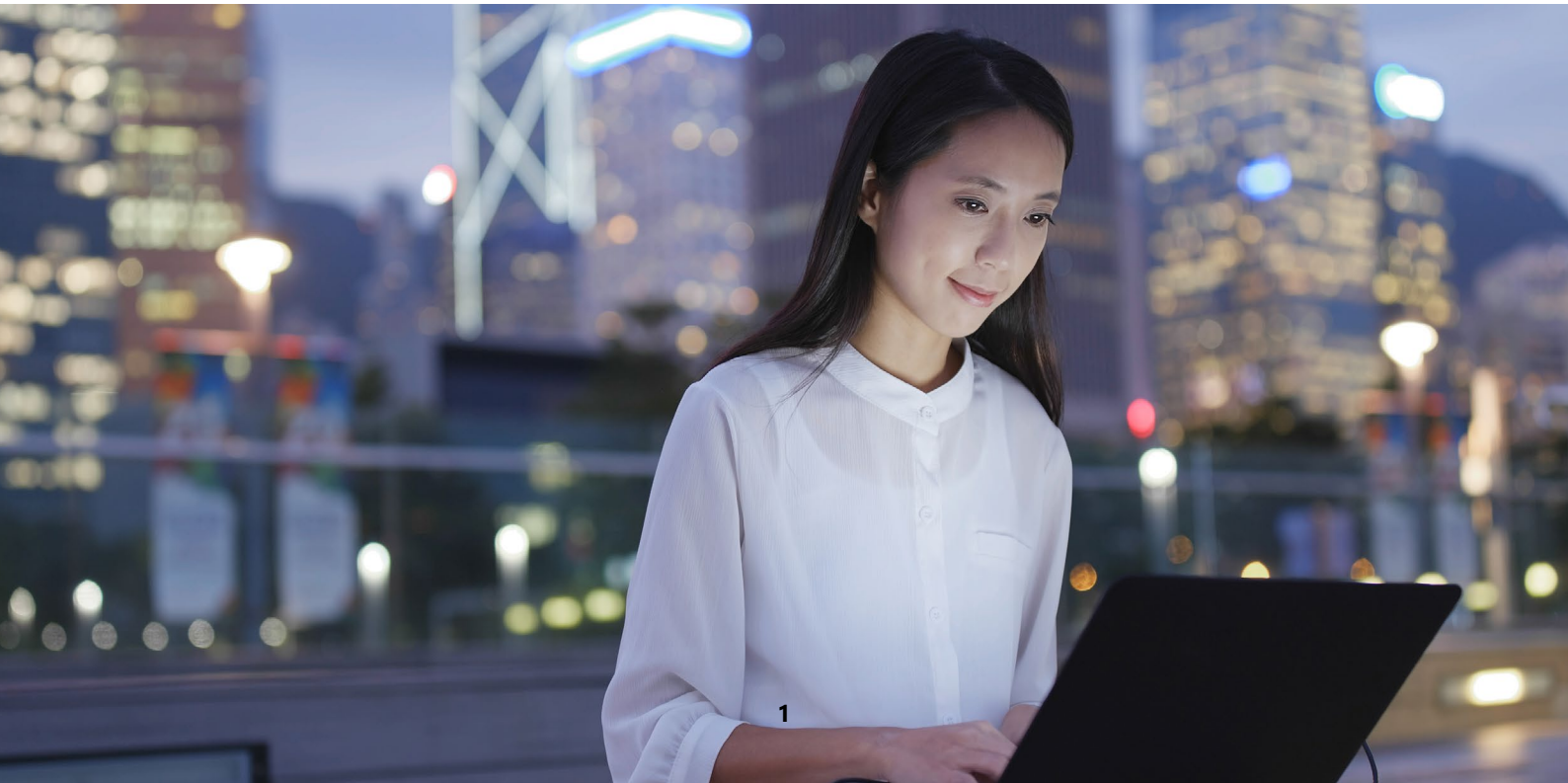
"People will only use technology if they trust that their privacy is being protected. In Asia, as in other regions around the globe, we are seeing a rapid pace of reform to amend or put new privacy laws in place in order to enhance trust, especially as society recovers from COVID. Increased cooperation between Asia's economies is needed to ensure that these reforms lead to stronger regulatory coherence, instead of increased complexity. This will give individuals more clarity on how their data is being protected when it moves across borders, while also allowing businesses to thrive. Stronger regulatory coherence will help companies expand into new markets, while ensuring companies are accountable for how they protect their users' data."

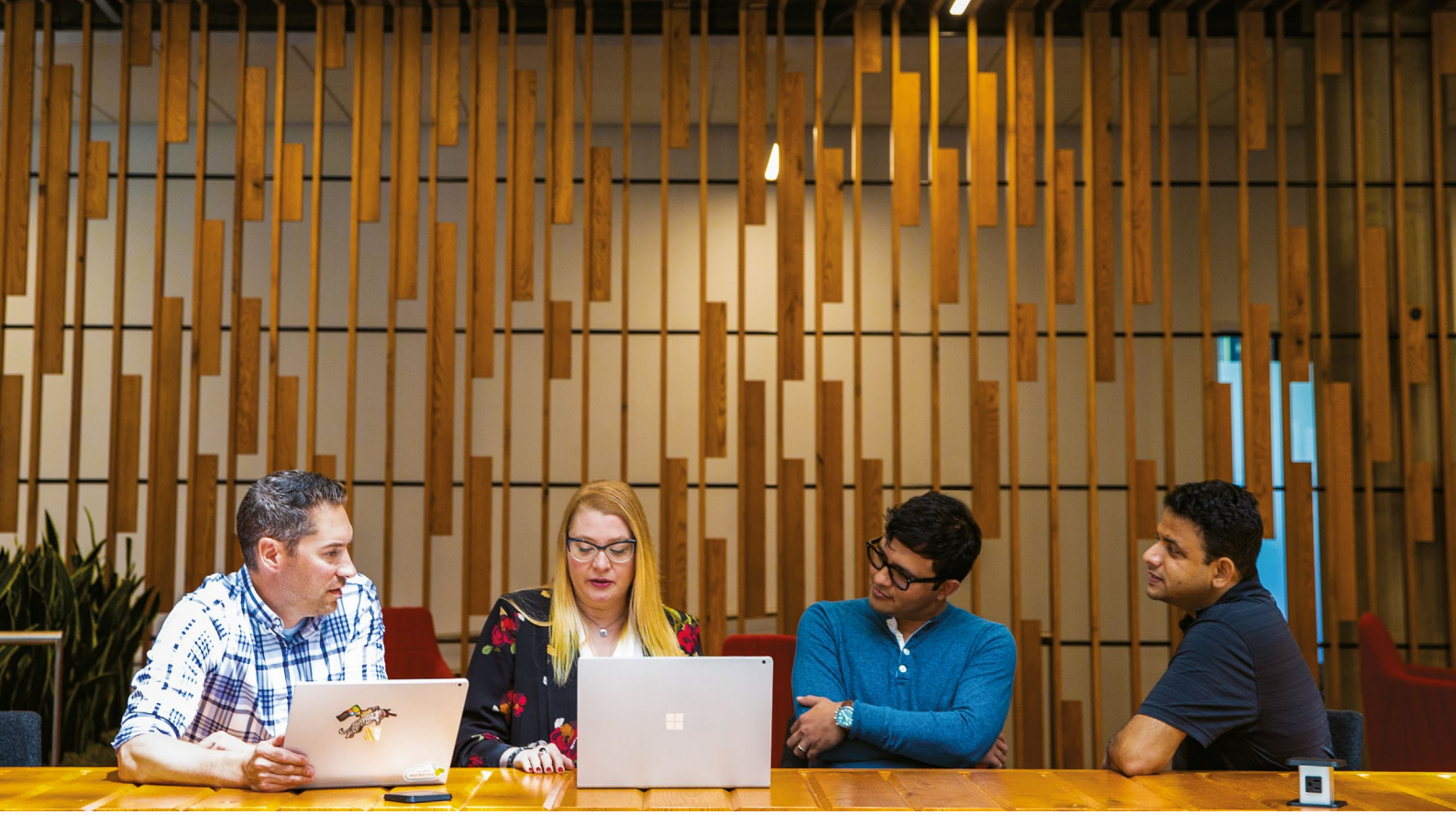
– Julie Brill, Chief Privacy Officer, Microsoft Corp.

Asia's Privacy Context

Asia is a dynamic privacy regulatory environment. Over the last two years, almost every economy in the region has worked to put a new or amended privacy law in place. A key driver of this is growing consumer and business expectation that personal data will be handled appropriately. At Microsoft, we are seeing clear evidence of these expectations across the region. For example, in the first 12 months following implementation of the EU General Data Protection Regulation (GDPR) in May 2018, when Microsoft rolled out new privacy transparency tools globally, there were 10 million users of these tools across the APEC region – more than in Europe. Individuals are increasingly choosing online services based on trust: a 2019 survey of more than 6000 consumers across the region highlighted that more than half of consumers would switch services if their trust was breached, with around half saying they would stop using the service altogether. There is a growing demand from trading partners for the privacy of personal data moving offshore to be protected, and the awareness of costs of trust being breached.

While these growing expectations of privacy protection have spurred domestic reform, with at least ten economies actively amending or establishing new laws, there has been little progress in Asia towards improving coherence between the rapidly changing privacy regimes across the region. As an economically-integrated region where trade and investment is of critical importance for all economies, it is essential to couple the reform of domestic laws with improvements in regulatory coherence.





Why is regulatory coherence important?

Privacy laws in the region draw inspiration from similar reference points, including the Organisation for Economic Co-operation and Development (OECD) Privacy Principles; regional frameworks like those agreed in Asia Pacific Economic Cooperation (APEC) or Association of South East Asian Nations (ASEAN); or developments in other regions like GDPR. At a high level, many laws in the region share common features, including, among others:

- **a similar scope of application, comprising a single omnibus privacy law and a single regulator;**
- **applicability to both public and private sectors;**
- **a category of sensitive personal data that requires additional protections;**
- **provisions for cross-border transfers of personal data; and**
- **data subject rights, and access, erasure, and data portability.**

While legal regimes may look similar at a high level, there is much more variation at the level of technical requirements that affect their implementation. Examples include:

- **the specific definition of "personal data", and whether it includes the data of deceased persons, or whether it includes pseudonymized data;**
- **the respective responsibilities of the "controller" and "processor", noting that in some cases the distinction is not made in the law;**
- **the available legal grounds for processing personal information, including whether legal bases beyond consent are available for different circumstances, e.g. executing a contract, in an emergency;**
- **the technical requirements for data breach notification;**
- **the personal liability of data protection officers; and**
- **the range of transfer mechanisms to facilitate cross-border trade and promote interoperability.**

As the pace of privacy law reform across Asia picks up, it is likely the regulatory complexity created through these variations will grow. This underlines the need for an effort to promote increased regulatory coherence. The goal need not be a full harmonization of laws, which is unlikely to be achievable for the foreseeable future given the wide variations that exist across the region. However, more coherence in key aspects of privacy laws and their implementation would have a number of positive impacts.

First, it would increase consumer trust that data is being appropriately protected when it moves offshore, because less complexity would result in greater transparency and comprehensibility on what rules apply across different jurisdictions. It would also result in fewer gaps in the protection of personal data, by addressing the variations in the levels of protection across the region. Second, greater engagement between regulators across borders would reduce the complexity they face, by facilitating the transfer of know-how from one jurisdiction to another, encouraging the co-development of frameworks and guidelines, and supporting more transparency on cross-border enforcement. Finally, organizations that operate across multiple jurisdictions in the region will be able to navigate their compliance obligations more effectively. Organizations can avoid unnecessary duplication of compliance efforts from one jurisdiction to the next, streamline their accountability measures internally and better negotiate and enable data transfer with other organizations. This is a particularly important consideration for SMEs and start-ups who do not have the resources and experience to deal with complex regulations, as large MNCs do. In this sense, regulatory coherence would promote a more inclusive digital economy in Asia, helping to level the playing field. This would also support greater regional trade and investment, as well as encourage digital transformation and innovation.

The way forward

The good news is that many of the frameworks to support greater privacy regulatory coherence in Asia are in place. Various platforms exist for greater cooperation between governments, like the Asia-Pacific Privacy Authorities (APPA) Forum, APEC's Data Privacy Subgroup, or the ASEAN Data Protection and Privacy Forum. Trade agreements like the Regional Comprehensive Economic Partnership, as well as digital economy agreements like those between Singapore-Australia, or New Zealand-Singapore-Chile, all contain commitments to cooperate on privacy regulation. These mechanisms provide varying levels of engagement with the broader Asian privacy community, including industry, and it is important to explore ways of increasing transparency and stakeholder consultation in their work.

Aside from government-to-government cooperation, institutions like the Asia Business Law Institute (ABLI), through its Data Privacy Project, are building the evidence base across the region on areas for improved coherence. Industry associations like the Business Software Alliance or US-ASEAN Business Council are increasingly engaging on regional privacy issues. The growing numbers of participants at regional meetings of groups like the International Association of Privacy Professionals (IAPP) demonstrates the strong interest from the privacy community in these issues.

The frameworks are in place, and there is interest in moving towards greater regulatory coherence. Given the complexity of the issues involved, it will be important for the region's governments to start making tangible progress towards improved coherence. "Quick wins" in some areas would help build support for more sustained efforts. Microsoft strongly supports this effort, and will continue working with regulators, industry, and the broader privacy community both on domestic efforts to strengthen privacy protection, and on efforts to promote regional coherence. This should be implemented in ways that promote not just regional, but global interoperability – for example, through the use of international standards.

There are many areas where concrete progress could be made. This paper highlights three of these many areas:

1. Mechanisms for facilitating cross-border data transfers;
2. Data breach notification; and
3. Grounds for processing personal information.

There are many other potential areas for fruitful cooperation to build regulatory coherence – the goal of this paper is to highlight only three among these many areas, in the hope that this contributes to more concrete progress on regulatory coherence. We look forward to engaging with regulators and others committed to improving regulatory coherence in Asia on these ideas.

For further information

Marcus Bartley Johns, Asia Regional Director, Government Affairs and Public Policy, Microsoft
Laura Gardner, Director, Global Privacy Policy, Microsoft
Privacy.microsoft.com

Practical options for strengthening privacy regulatory coherence in Asia

There are many potential areas for strengthening privacy regulatory coherence in the region. This paper outlines three of those areas, to illustrate the concrete options that exist for moving this agenda forward.

Issue 1: Cross-border data transfer mechanisms

- Greater recognition across jurisdictions on comparable approaches to data transfers, including in specific circumstances or sectors
- Increased recognition through law or guidelines of international certifications as a basis for transfers
- Joint or coordinated data transfer agreement guidelines

Issue 2: Data breach notification

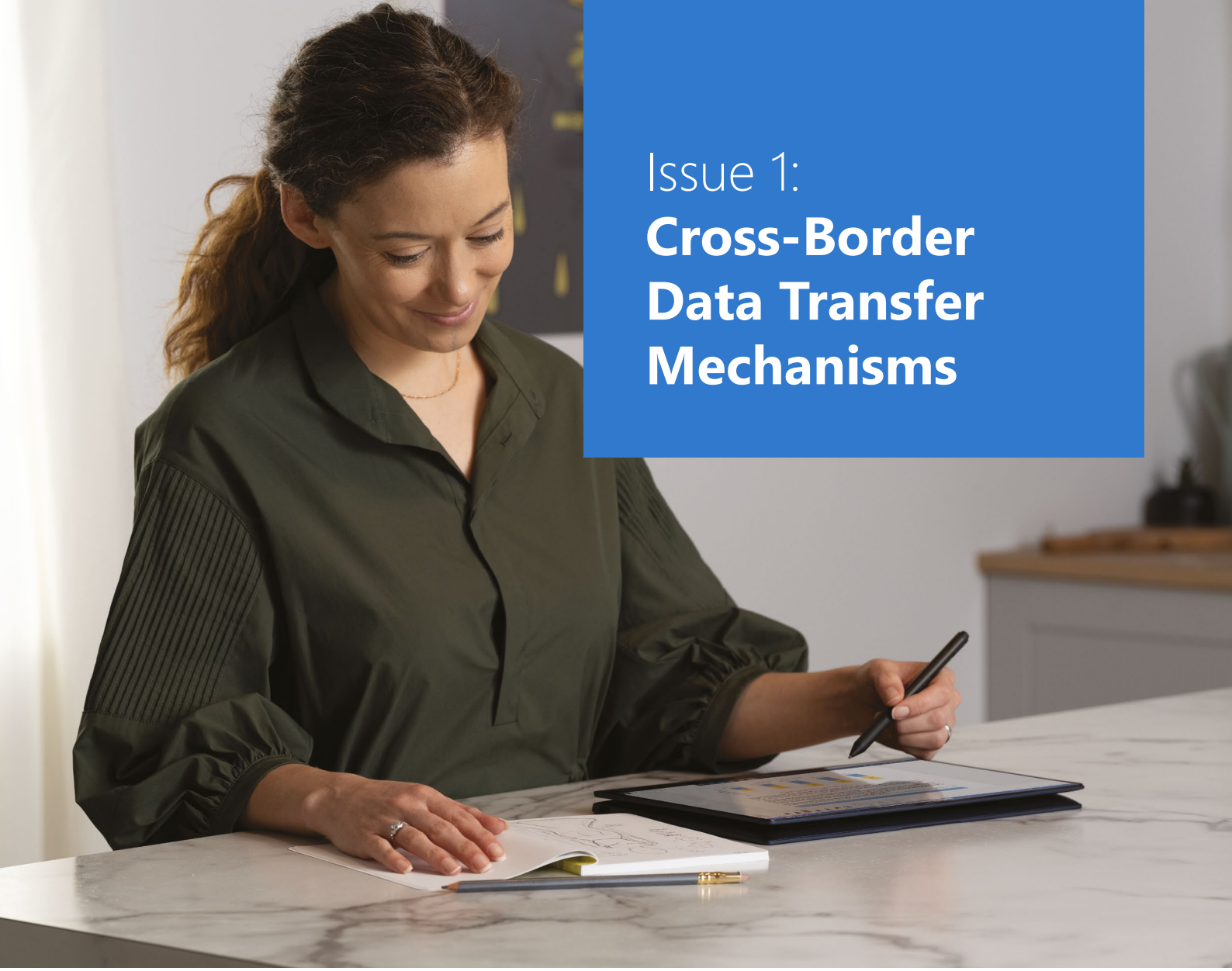
- Adoption in all privacy laws of mandatory data breach notification, aligned with areas of regional convergence, e.g. on thresholds, allocation of responsibilities, and timelines for notification
- Greater information exchange between regulators on notification requirements, including with sectoral regulators
- Joint or coordinated guidelines from regulators to build organizations' understanding of when a breach has occurred and what notification requirements may be triggered
- Exploring a regional data breach notification mechanism

Issue 3: Alternative grounds for processing data, notably legitimate interest

- Adoption across more privacy laws of alternative grounds for processing personal data, notably legitimate interest
- Regulator guidelines – referring to other jurisdictions – on implementing the legitimate interest approach
- Greater information sharing on implementation of the legitimate interest approach
- Agreement between regulators on key elements of the legitimate interest approach, e.g. assessment of legitimate interest in one jurisdiction being recognized in another

Implementation principles

- Building on existing regional privacy frameworks and groups, including APEC, ASEAN and APPA, as well as trade/digital economy agreements
- Strengthening dialogue on regional coherence between regulators, industry and the privacy community broadly
- Combining ambitious initiatives with ones that can deliver "quick wins"
- Assessing the impact of current processes and mechanisms and adjusting where necessary
- Supporting progress towards global interoperability



Issue 1: **Cross-Border Data Transfer Mechanisms**

Asia is a dynamic region for cross-border trade, investment, and people flows. Many individuals and companies in Asia today use services that involve cross-border transfers of data. McKinsey Global Institute estimates that the international flow of data could contribute US$11 trillion to global GDP by 2025. This underlines the importance of effective mechanisms for the transfer of personal data across borders in Asia to maintain an appropriate level of protection of privacy.

All jurisdictions in Asia allow cross-border data transfers in principle, and at a high level there is commonality in the mechanisms available for transferring data offshore across privacy laws. However, there is considerable variation at the technical level of implementation. This creates a dual challenge. First, organizations operating across borders face a significant compliance burden due to variations in requirements, which can be prohibitive for SMEs and start-ups. Second, the complexity reduces transparency, making it harder for regulators and individuals to understand how privacy protection is maintained when data moves overseas. These challenges are evident in two of the most common bases for transferring data in Asia's privacy laws: consent, and the use of data transfer agreements. These two examples underline how from a regulator and consumer perspective, the technical or procedural variations in what is required from one jurisdiction to another do not necessarily raise the level of data protection. The main impact is to increase the level of complexity, without having a substantive impact in most cases on how privacy is protected.

Variations in the "consent" method

Almost all privacy laws in Asia permit data to be transferred offshore with the consent of the relevant individual. However, the specific consent requirements vary significantly from one jurisdiction to another, as demonstrated by the requirements in Australia, South Korea, Thailand and Vietnam (see table).

Australia	South Korea	Thailand	Vietnam
Data can be transferred across borders with the individual's consent.	Data can be transferred across borders with the individual's consent.	Data can be transferred across borders with the individual's consent.	Data can be transferred across borders with the individual's consent.
Entity obtaining consent must: (a) inform the individual of the potential consequences of not providing consent; and (b) explain that, if the individual consents, the data controller will not be accountable under the Privacy Act.	Entity obtaining consent must inform the individual of: (a) the identity of the recipient; (b) the purpose for which the recipient will use such data; (c) particulars of the personal data to be provided; (d) the period for which the recipient retains and uses the personal data; and (e) the fact that the data subject is free not to give his or her consent (and any negative consequences for the data subject resulting from his denial to consent).	The entity obtaining consent must inform the individual of the inadequate personal data protection standards of the destination country.	The entity obtaining consent must inform the individual of the: (a) form; (b) scope; (c) place; and (d) purpose of the collection, processing or use of their personal data.
Opt-in consent is not required.	Opt-in consent is required.	Opt-in consent is required.	Unclear whether consent must be express (i.e. opt-in) or whether a notice and lack of objection would suffice (i.e. opt-out).

Variations in the "data transfer agreement" method

Another mechanism for transferring data offshore is through data transfer agreements. Almost all laws permit the transfer of data offshore where a contractual arrangement is put in place with the recipient (i.e. a data transfer agreement). This confers a level of protection that is commensurate with the level of protection under the data protection laws in the originating country. However, there are significant technical and procedural variations in what is required in data transfer agreements from one jurisdiction to another, as well as an absence of approved model clauses for data transfer agreements. This is highlighted in the requirements in Singapore, Australia, and South Korea (see table). These variations increase complexity, making it challenging to have data transfer agreements that can be used across multiple jurisdictions in the region. The costs involved in negotiating new agreements to meet the technical requirements of multiple jurisdictions can be prohibitive for many organizations, and the complex web of contractual requirements can reduce transparency for individuals.

Singapore	Australia	South Korea
Data can be transferred across borders where an appropriate data transfer agreement is put in place.	Data can be transferred across borders where an appropriate data transfer agreement is put in place.	Data can be transferred across borders where an appropriate data transfer agreement is put in place, in specific instances.
The data transfer agreement must: (a) provide for a standard of protection that is at least comparable to the protection under the Personal Data Protection Act; and (b) specify the jurisdictions and territories to which personal data may be transferred under the contract.	The data transfer agreement must: (a) include obligations substantively similar to the Australian Privacy Principles; (b) specify the minimum technical and organizational measures that will apply to the use of the personal data; (c) specify the agreed procedures for providing access to personal data on request and for making any necessary corrections; (d) include a requirement that the recipient implement a data breach response plan which includes a mechanism for notifying the data controller where there are reasonable grounds to suspect a data breach; and (e) specify appropriate remedial action and a mechanism that enables the data controller to monitor compliance with the arrangement.	The data transfer agreement must contain the following: (a) purpose and scope of outsourced work; (b) restrictions on re-outsourcing; (c) prevention measures designed for ensuring that the personal data is processed solely for the outsourced purpose; (d) technical and managerial safeguards to ensure security of personal data; (e) measures ensuring security of personal data, including restrictive access to personal data; (f) matters concerning the supervision and inspection of the management of personal data retained for the outsourcing purpose; and (g) matters concerning liability, such as the compensation for damages caused by the offshore entity's breach of the outsourcing agreement.

Options for Strengthening Regulatory Coherence

As the law stands, individuals, regulators and organizations face significant complexity in navigating the variations across the region in how cross-border transfers are facilitated – with consent and data transfer agreements being two demonstrations of these challenges. An ability to effectively transfer data across borders generates positive outcomes for multiple stakeholders. Organizations can expand their business in a cost-effective manner by relying on globally distributed cloud computing technologies, which can increase the resilience and security of their IT systems. Individuals can also benefit from more competitive prices, accessing a wider range of services, and relying on world leading privacy and security practices. For these reasons, cross-border transfers are an area with great potential for improving regulatory coherence. The issues involved are complex, but we propose three options for making progress in the short to medium-term, in collaboration with industry, the privacy community, and other stakeholders.

1. Greater recognition of certifications as a basis for transfers

Data privacy laws in Asia could potentially follow in the footsteps of GDPR and recognize certifications such as the international standard ISO/IEC 27001 or ISO/IEC 27701 or regional standards like CBPR as a lawful mechanism for cross-border data transfers. Certification schemes are recognized in the EU under the GDPR and already operate in key jurisdictions like Japan and Singapore, but have not yet been widely adopted in Asia as a basis for cross-border transfers.

International standards, as opposed to regional standards, would have the most profound benefits as they have global coverage and reduce the high cost of certification against multiple local or regional standards. This is particularly important for SMEs or start-ups seeking to operate across many markets. Practically, this would not require jurisdictions to amend their laws as it could be achieved through regulator guidance that promotes the adoption of such certifications. This could take the form of confirmation that certifications can be read as meeting the general provisions of the data privacy law on protecting data when it moves offshore. For example, Singapore's 2019 Advisory Guidelines on Cloud Services notes that organizations processing personal data through Cloud Service Providers (CSPs) can transfer data offshore through CSPs, if the CSPs are certified against relevant international standards. There may be an opportunity for groups like APEC or APPA to promote more widespread acceptance of such certifications, as well as share lessons on the implementation of certification schemes already in place.

2. Model data transfer agreements and regional data transfer agreement guidelines

Data transfer agreements are the most widely recognized transfer mechanism in Asia's privacy laws. They provide legal certainty, and are widely seen as one of the most promising avenues for increasing compatibility of data transfer requirements in Asia.

One practical step for improved coherence in transfer mechanisms would be for regulators to issue joint or coordinated guidelines on data transfer agreements. Such guidelines would set out key elements to be reflected in a compliant data transfer agreement. This would provide greater clarity and certainty to companies and consumers on what regulators see as key steps. This could complement more ambitious regional efforts like the ASEAN Model Contractual Clauses, while retaining the benefit of flexibility in how the specific contents of data transfer agreements reflect the guidance developed by regulators. This is particularly important if more jurisdictions develop model or standard contractual clauses. If there are variations between these standard clauses, but an expectation that they are reflected in their entirety in each data transfer agreement, this would result in greater fragmentation and regulatory complexity. This underlines the importance of greater regulatory cooperation, to avoid such fragmentation.

3. Recognition of compatible data privacy regimes

The greater use of "safe" lists of jurisdictions to which data can be transferred would strengthen regulatory coherence. At the same time, it needs to be recognized that formal "adequacy" decisions between jurisdictions take many years to negotiate and have not been extensively used in Asia. Japan has already designated EU Member States in this way through a mutual adequacy decision with the European Commission; New Zealand has obtained adequacy status with the EU; and talks between the EU and Korea have reportedly made progress. The benefit of such arrangements is that they provide legal clarity and could make substantial contributions towards improved coherence.

However, formal adequacy decisions remain a relatively long-term objective, and more pragmatic steps could be taken in the short term. For example, the development of Memoranda of Understanding (MOUs), through the collaboration of pairs or small groups of regulators, could be used to give clear guidance on the acceptable basis for transfers between jurisdictions and streamline cross-border data transfers. These could be developed in a step-by-step manner, based on specific circumstances and sectors. Promising signs of such cooperation is evident in the Singaporean and Australian regulators recently entering into an MOU to jointly promote the APEC Cross-Border Privacy Rules (CBPR) System.

Issue 2: Data Breach Notification Regimes

Cyber-attacks and data breaches are on the rise in Asia. In response, privacy laws increasingly require the notification of data breaches. The basic premise of data breach notifications – in which the organization must notify the relevant regulator and/or those affected by a data breach – is to increase transparency of an organization's security measures, promptly inform affected individuals, and ensure corporate accountability of organizations involved in data breaches.

Variations

Despite requirements to notify data breaches becoming commonplace in Asia, the region has not taken a coherent approach. Significant variations exist in how data breach notification is implemented. This is demonstrated, for example, by the contrasting approaches of Singapore, the Philippines, South Korea and India (see table). This becomes a problem when a single data breach impacts an individual's data in several jurisdictions and triggers varying notification requirements. Rather than prioritizing remediation efforts, organizations may instead divert their attention towards legal gap analyses and compliance reporting to meet requirements of different jurisdictions.

	Singapore	Philippines	South Korea	India
Who must report the data breach and what types of data/security breaches are notifiable?	An organization must notify of data breach where it: (a) results in, or is likely to result in, significant harm to the affected individual; or (b) affects no fewer than the minimum number of affected individuals prescribed.	The controller must notify the National Privacy Commission ("NPC") and the affected data subjects of a personal data breach data breach is notifiable where: (a) it is reasonably believed that an unauthorized person has acquired sensitive personal information or any other information that may enable identity fraud; and (b) the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.	The personal information controller must notify: (a) an affected data subject where the data subject's personal data has been divulged; and (b) the Minister of the Interior and Safety ("MOIS") if the data breach involves more than 1,000 data subjects.	Cyber security breaches that must be notified to CERT-In include: • targeted scanning or probing of critical networks and systems; compromise of critical systems or information; • unauthorized access of IT systems or data; • defacement of a website or intrusion into a website; • malicious code attacks including attacks on servers; • identity thefts, spoofing or phishing attacks; and • Denial of Service or Distributed Denial of Service attacks.
When (e.g. within a certain time period) must the data breach be notified?	Notification must be made as soon as practicable, but in any case, no later than 3 days.	Notification must be made within 72 hours upon knowledge of, or when there is reasonable belief.	Notification must be made without delay.	Notification must be made as early as possible (by any individual, organization or corporate entity); and within a reasonable time of occurrence or noticing the incident (by service providers, intermediaries, data centers and body corporate).
Can a notification of a data breach be delayed?	None provided.	Delay may be permitted only where necessary to determine the scope of the breach, prevent further data breaches, or secure the underlying system. Postponement may also be permitted where it may hinder criminal investigations related to a serious breach.	Delay may be permitted to enable the controller to take contingent measures necessary to prevent the dissemination of the divulged personal data and additional divulgence.	No exception is provided under the CERT-In Rules. Under the PDP Bill, the controller can provide information to the Authority in phases where it is not possible to provide all the required information at the same time.
Are there any exceptions to notifying a data breach?	Exceptions exist if the organization has taken remedial action or implemented technological protection, or if the organization is instructed by a prescribed law enforcement agency or the PDPC to not disclose, or if the PDPC waives the requirement.	Exceptions exist if it would not be in the public interest or the interests of the data subjects; or the controller had complied with the security requirements and acquired the personal data in good faith.	None provided.	None provided.
What format should notification take?	Submission via an online form or, if urgent, by contacting the PDPC directly by phone.	Submission via a report in written or electronic form.	Submission via writing and post the matters to be notified for at least seven days on the personal information collector's website or, at easily noticeable places of his/her workplace.	Submission of incident report form via email or by fax or calling the helpline.

Benefits of a more coherent approach

More coherent notification requirements across the region would help address the significant complexity organizations are facing under the current laws. First, organizations would face reduced compliance burdens, by no longer being required to undertake country-by-country analysis and develop systems to cater for technical variations in requirements. Second, organizations would have an increased familiarity with the compliance requirements. This would allow them to have faster and more accurate responses to data breaches, improving the quality of notifications sent to regulators. Third, it would also improve transparency by making information comparable across markets, making it easier to quickly assess the scale, impact, and lessons learned from data breaches.

Options for Strengthening Regulatory Coherence

For the above reasons, data breach notifications are a key area for improving regulatory coherence.

1. Universal inclusion of mandatory data breach notification in the region's privacy laws

We support all markets in Asia adopting a mandatory requirement for data breach notification. Mandatory breach notification requirements lead to improved transparency and accountability, incentivize organizations to strengthen security measures to prevent potential security breaches, and provide a baseline for regulators to improve coherence. There is increasing convergence in the region's laws on several key elements of data breach notification provisions, including:

- **Threshold** – adopt a risk-based approach rather than a quantitative threshold whereby a data breach will only be notifiable if it is likely to result in serious harm to the affected individual. This will help prevent regulatory authorities and individuals from being overburdened with notices of trivial breaches.

- **Responsibilities of Controller/Processor** – The controller is the stakeholder responsible for notifying the regulator and data subject, given the controller holds the relationship with the data subject and is accountable for personal data under its control. The processor is only responsible for notifying controllers of a breach.

- **Timeframe for notification** – Both the data subject and regulator are notified without undue delay, where feasible, after the data controller assesses there is a notifiable data breach. Delays of notifications are allowed for justifiable reasons. This timeline does not impose an unnecessary, aggressive deadline and enables organizations to prioritize breach mitigation measures rather than meeting reporting and administrative burdens.

2. Practical steps to improve coherence through regional cooperation

The universal adoption of a data breach notification requirement across the region's privacy laws would be complemented by regional cooperation to improve coherence among breach notification regimes.

Increased cooperation on data breach notifications could be considered in a number of areas, including:

- Developing guidelines across jurisdictions that assist entities in understanding when a breach has occurred, providing practical guidance and illustrative examples of events that would trigger the notification requirements;

- Identifying commonly required elements of data breach notifications as a basis for identifying potential for improved coherence;

- Developing a harmonized breach notification template(s) across multiple jurisdictions; and

- Working towards a regional data breach notification mechanism, through which a data breach notifiable in various Asian countries would only need to be disclosed to a single regulator in the region, who would then share the notification with other relevant regulators as appropriate. This would also significantly improve transparency, while lowering compliance costs.

These steps could be implemented through bilateral or small group cooperation among regulators, as well as through regional bodies like APEC, ASEAN or APPA.

Issue 3: **Alternative Grounds For Processing Data**

There is increasing awareness of the challenges in relying on consent alone to process personal data. Individuals can be interrupted, overwhelmed and fatigued if constantly presented with privacy choices, especially if these involve lengthy and complex notices to consent to the processing of data. It can also be difficult to obtain valid consent where there is some power imbalance which means that an individual may not be able to give voluntary consent in certain circumstances (e.g., in an employment relationship), as noted in GDPR. Finally, it may not always be possible or practical to seek consent every time data is collected or if data is used for a new purpose. Although the basic principle of seeking consent from individuals for the use of the personal data continues to be highly relevant, there is a growing recognition that, in some contexts, mechanisms other than consent may be more suitable for effectively protecting individual privacy rights.

This is driving greater discussion in Asia and beyond on alternative approaches to consent for processing personal data – notably the "legitimate interest" approach. In general, this allows processing to occur when there is a legitimate interest for doing so, based on a robust and documented assessment. In Asia, four jurisdictions allow personal data to be processed based on the legitimate interest approach, and others (including Indonesia and India) are considering whether to include the legitimate interest approach in the amendments to their data privacy laws. While there is some regulatory guidance available across the region on applying the legitimate interest approach, there is generally no prescribed list or limitation on the circumstances in which it can be applied. The table below highlights some of the similarities and variations across four jurisdictions.

Variations in current and proposed implementation of the legitimate interest approach

	Singapore	Thailand	Philippines	India
Are "legitimate interests" (or similar concept) an acceptable ground for processing personal data?	Personal data can be collected, used or disclosed if: (a) it is in the legitimate interests of the organization; and (b) the benefit to the public or any section of the public is greater than any adverse effect on the individual.	Personal data can be processed for legitimate interests unless overridden by the fundamental rights of the data subject.	Personal data can be processed for legitimate interests unless overridden by the fundamental rights and freedoms of the data subject.	There is currently no "legitimate interest" concept for processing personal data under the IT Act. However, the PDP Bill allows personal data to be processed without consent if such processing is necessary for "reasonable purposes": and some include: • prevention and detection of unlawful activity including fraud; • network and information security; and • recovery of debt.
Any specific obligation to notify data subjects that legitimate interests is being used?	The individual must be informed in a reasonable manner of his/her personal data that is being collected, used or disclosed.	The data subject must be informed of the purpose of the collection/use of the personal data, including where personal data is to be processed for the legitimate interests of the controller and collected without the data subject's consent.	The data subject must be informed of the basis of processing, when processing is not based on the consent of the data subject.	Notice will depend on whether such provision will substantially prejudice the relevant reasonable purpose.
Does data subject have specific right to object to legitimate interests being used?	No.	The data subject has the right to object at any time unless the controller can demonstrate that there is a compelling legitimate ground to do so.	No.	No.
Any other the conditions for using the "legitimate interests" ground to process personal data?	The organization must conduct an assessment to determine that the benefit to the public is greater than any adverse effect on the individual. Some of the matters to be included are: (a) the identification of any adverse effect on the individual; (b) the identification and implementation of any measure to eliminate the adverse effect.	The collection of the personal data must be necessary for the lawful purpose of the controller.	The processing of personal data must not be otherwise prohibited by law.	There is discretion for the regulations to specify any safeguards that are appropriate to ensure the protection of the rights of data principals.

Benefits of a more coherent approach

More coherent notification requirements across the region would help address the significant complexity organizations are facing under the current laws. First, organizations would face reduced compliance burdens, by no longer being required to undertake country-by-country analysis and develop systems to cater for technical variations in requirements. Second, organizations would have an increased familiarity with the compliance requirements. This would allow them to have faster and more accurate responses to data breaches, improving the quality of notifications sent to regulators. Third, it would also improve transparency by making information comparable across markets, making it easier to quickly assess the scale, impact, and lessons learned from data breaches.

Options for Strengthening Regulatory Coherence

While there is no one prescribed approach to strengthen regulatory coherence in this area, Microsoft proposes potential avenues to facilitate progress in the short-to-medium term.

1. Increasing the adoption of the legitimate interest approach across Asia

The baseline for improved coherence would be the more widespread adoption across Asia of alternative grounds for processing personal data, notably the legitimate interest approach. As noted above, there is already growing momentum towards its increased adoption. As this approach becomes increasingly widespread, there will be a clear benefit of regulators issuing guidelines on how it should be implemented. Such guidelines would help promote coherence if they directly reference other jurisdictions with developed legitimate interest regimes. Examples include the Philippines, which follow the guidelines published by the ICO and applies the principles established in the GDPR recitals; Singapore, which in November 2020 published draft guidelines addressing implementation of the legitimate interest approach; as well as global jurisdictions like the EU, with its growing body of case law regarding the application of the test. We believe the guidelines should be flexible and non-binding in nature, and would deliver benefits for industry and the privacy community more broadly if they:

- detail what assessment an organization must undertake (including the factors to consider);
- provide non-exhaustive examples; and
- detail the records companies must keep.

2. Increasing regional dialogue on the legitimate interest approach

Building on the baseline set through increased adoption of the legitimate interest approach, there would be clear benefits in increasing regional dialogue on its implementation. As noted in the Executive Summary, the mechanisms for such dialogue through bodies like APEC or APPA already exist. Although each jurisdiction would adopt an approach suitable for its own context, greater dialogue could identify shared views among regulators on aspects of the legitimate interest approach, such as the Philippines NPC's three-part test for assessing legitimate interest (which is comparable with that in GDPR). This could pave the way for significant improvements in coherence, like regulators recognizing an assessment of legitimate interests in one jurisdiction as meeting the requirements in another.

This paper is not intended to be a comprehensive analysis of all regulations and their requirements, nor is it legal advice. It is intended to provide a summary for discussion purposes for companies, regulators and other stakeholders interested in building privacy regulatory coherence in Asia.