



Hogan
Lovells



Data Privacy Regulation
Comes of Age in Asia

2014

Data Privacy Regulation Comes of Age in Asia

A Sea Change

There has been an explosion of new data privacy regulation across the Asia Pacific region in recent years.

Australia, New Zealand, Hong Kong and Japan were the region's earliest movers, passing comprehensive data privacy laws in 1988, 1993, 1995 and 2003, respectively. The Privacy Framework agreed by the Asia-Pacific Economic Co-Operation (APEC) member economies in 2005 has been the formal catalyst for continued regulatory development across the region. The policy rationale for APEC is decidedly economic and trade-related, as Asian governments seek to continue the impressive growth of e-commerce across the region and to provide businesses both regionally and globally with greater confidence in processing their data in Asia's offshore and regional service hubs.

APEC members **Singapore, Malaysia, the Philippines, South Korea and Taiwan** have now all passed comprehensive data privacy regimes. **India** has also enacted an IT law tracking a similar principles-based approach to data privacy. Perhaps most significantly, **China** has passed a whole raft of legislation in this area in recent years, both industry specific and of more general application including a set of internet and telecommunications industry rules drawing from the APEC model which came into force in September 2013. Amendments to China's consumer protection law effective in March 2014 have expanded these same principles into a much wider sphere of application that now takes in all business operators in China.

It is now clear that data privacy compliance is a critical business issue across the Asia-Pacific region. Failure to comply can have consequences that go far beyond simply monetary fines and other regulatory sanctions: very often reputational issues are also in play.

The New Compliance Challenge

Although Asia's data privacy laws draw from a common set of guiding principles, each law is unique. Moreover, as freshly minted regulators come to grips with these new laws, differences in interpretation and underlying policy are becoming apparent. As a consequence, there is a "patchwork" of compliance requirements across the region. For example, some laws have data export controls, some do not. Some laws have "opt in" requirements for direct marketing, some are satisfied by "opt outs", others are vague on the issue. Health information is specifically regulated in some jurisdictions, while in others it is not. Depending on the jurisdiction, sector specific laws, consumer protection laws, employment laws and laws in emerging areas such as cyber security also complicate the compliance picture for Asia, and there is no common framework for any of these laws.

The challenge for multi-national businesses operating in the region is to find practical compliance solutions that effectively and efficiently manage risk. The objectives of the APEC Privacy Framework – the promotion of easier cross-border data transfers and the encouragement of public confidence in data processing - should mean that the regulatory reforms lead to effective outcomes for business. However, we are not yet at a stage where Asian governments are focused on harmonisation that would help achieve this end. Careful analysis is required.

Asia's New Laws are Being Enforced

While it is fair to say that enforcement rates in the data privacy space have historically been low in the region, it is clear that this picture has changed and is changing still.

As is the case elsewhere in the world, public awareness of data privacy in Asia is often "event driven". Data security and data privacy issues are routinely front page news and this fosters individual awareness of and concern for privacy rights. Asia is no exception.

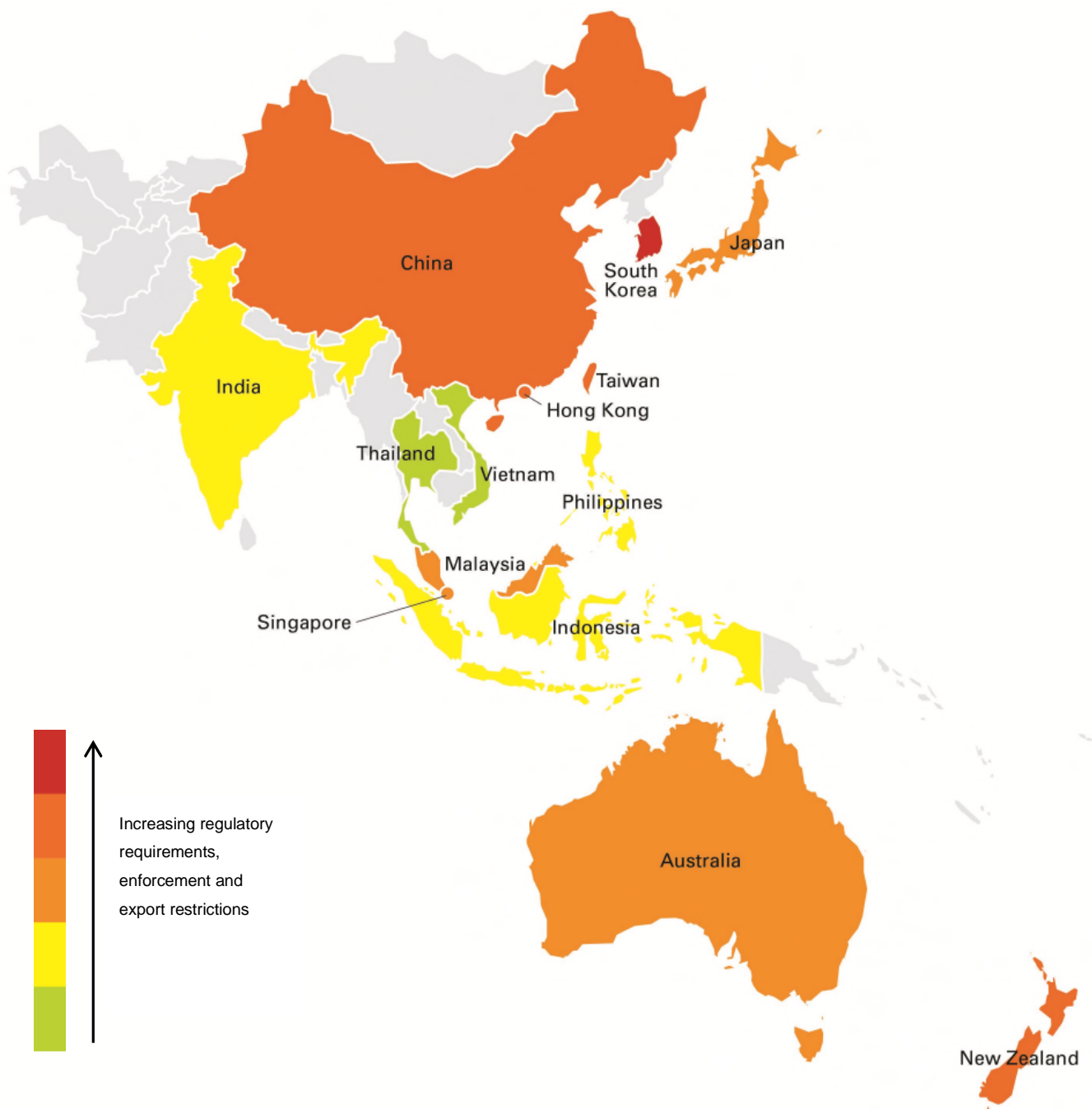
A poignant illustration is Hong Kong's experience in 2010 when the regulator found a reward card programme to be unlawfully selling personal data to other businesses for marketing purposes. The press reports triggered legislative reforms that have made Hong Kong's direct marketing laws amongst the world's most challenging and precipitated a stepping up of the available penalties. In his latest published figures for 2013¹, Hong Kong's regulator reported a 48% per cent increase in complaints and a doubling of enforcement notices. Moreover, the incident and investigations that followed showed a greater willingness by Hong Kong's privacy regulator to "name and shame" businesses that he believes have fallen foul of the law, making the consequences of non-compliance far greater than in the past.

As regulators across the region develop policy requirements and test their enforcement tools, the risk of failing to comply with data privacy laws in Asia can no longer be ignored.

¹ Hong Kong Corporate briefing "Privacy Complaints Up 48% in Hong Kong in 2013: Are you Prepared?" March 2014.

Asia-Pacific Data Privacy Regulatory Heat Map

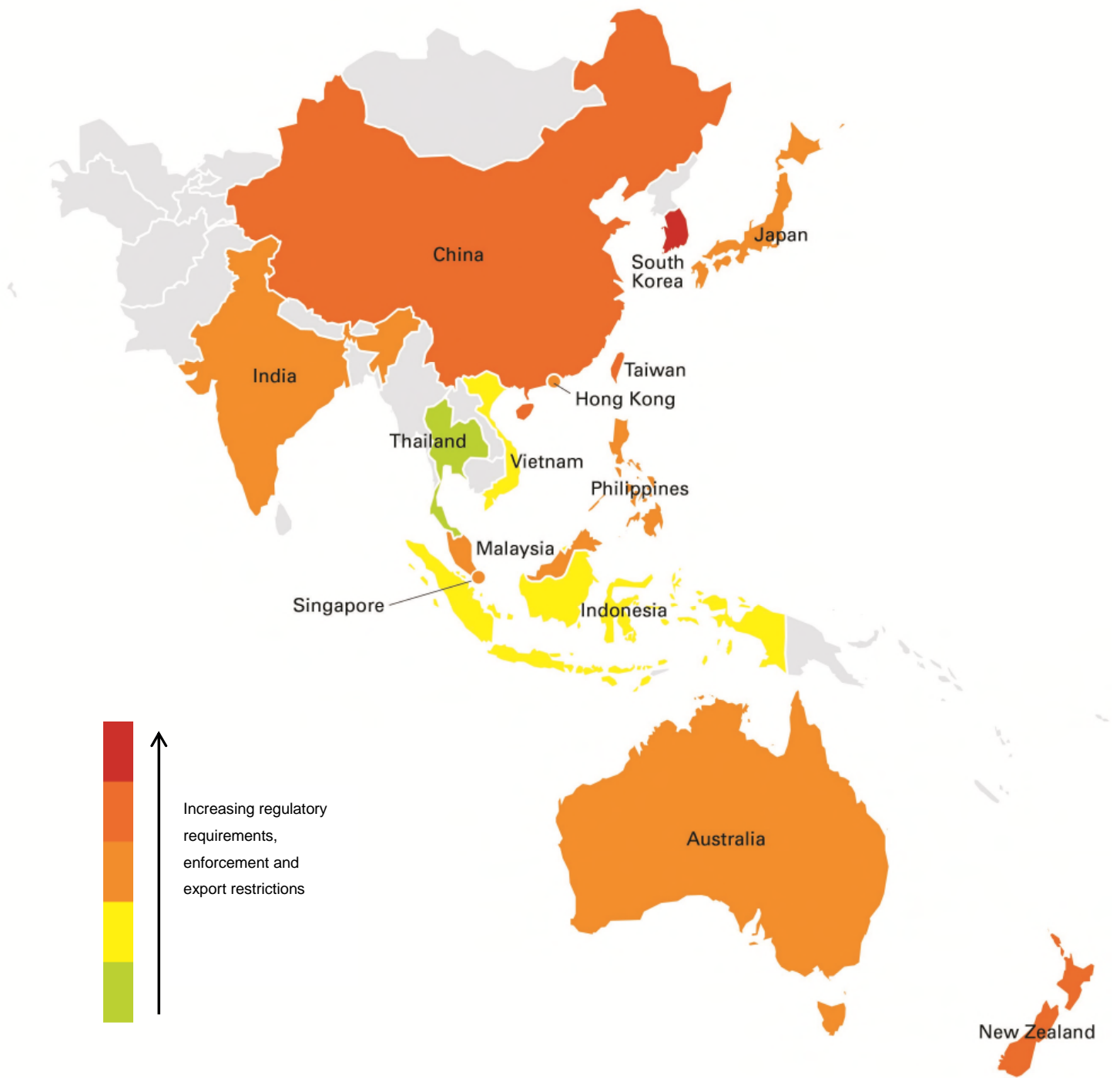
Our Asia-Pacific Data Privacy Regulatory Heat Map illustrates the differences in approach to regulation in Asia. The map below compares the various regimes in Asia by grading jurisdictions against four criteria: 1) data management requirements; 2) direct marketing regulation; 3) data export control; and 4) aggressiveness of the enforcement environment. The map is intended to show the relative strictness of the regulatory and enforcement environment across the region.



In the maps below, each jurisdiction has been scored separately against each of the four criteria above to highlight the more challenging regimes from a business perspective:

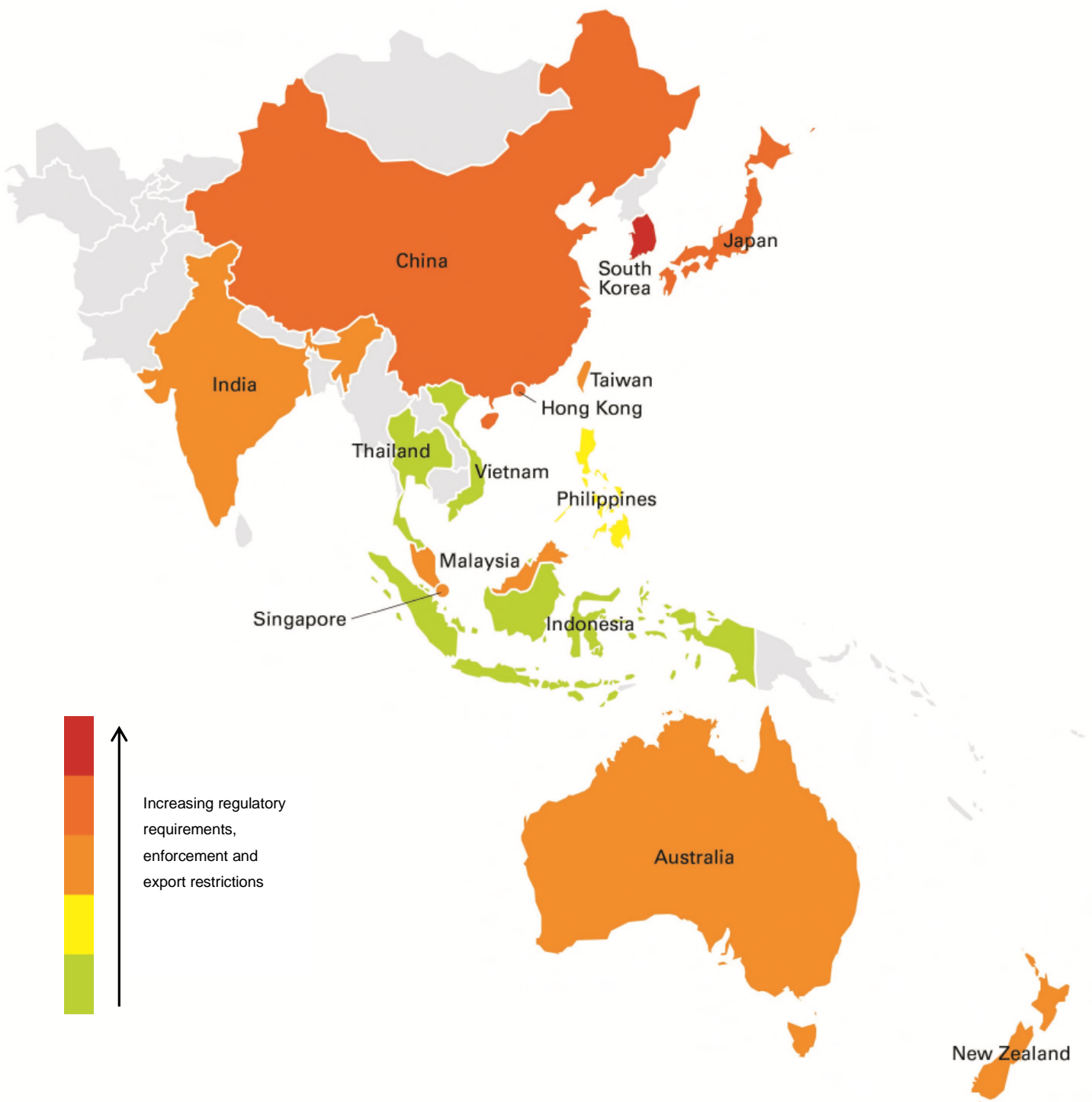
Data Management Requirements:

How prescriptive is the regulation in terms of steps that businesses must take towards data security and disclosure of processing arrangements? Is sensitive personal data regulated more stringently? Are businesses obliged to disclose breaches to regulators and/or data subjects?



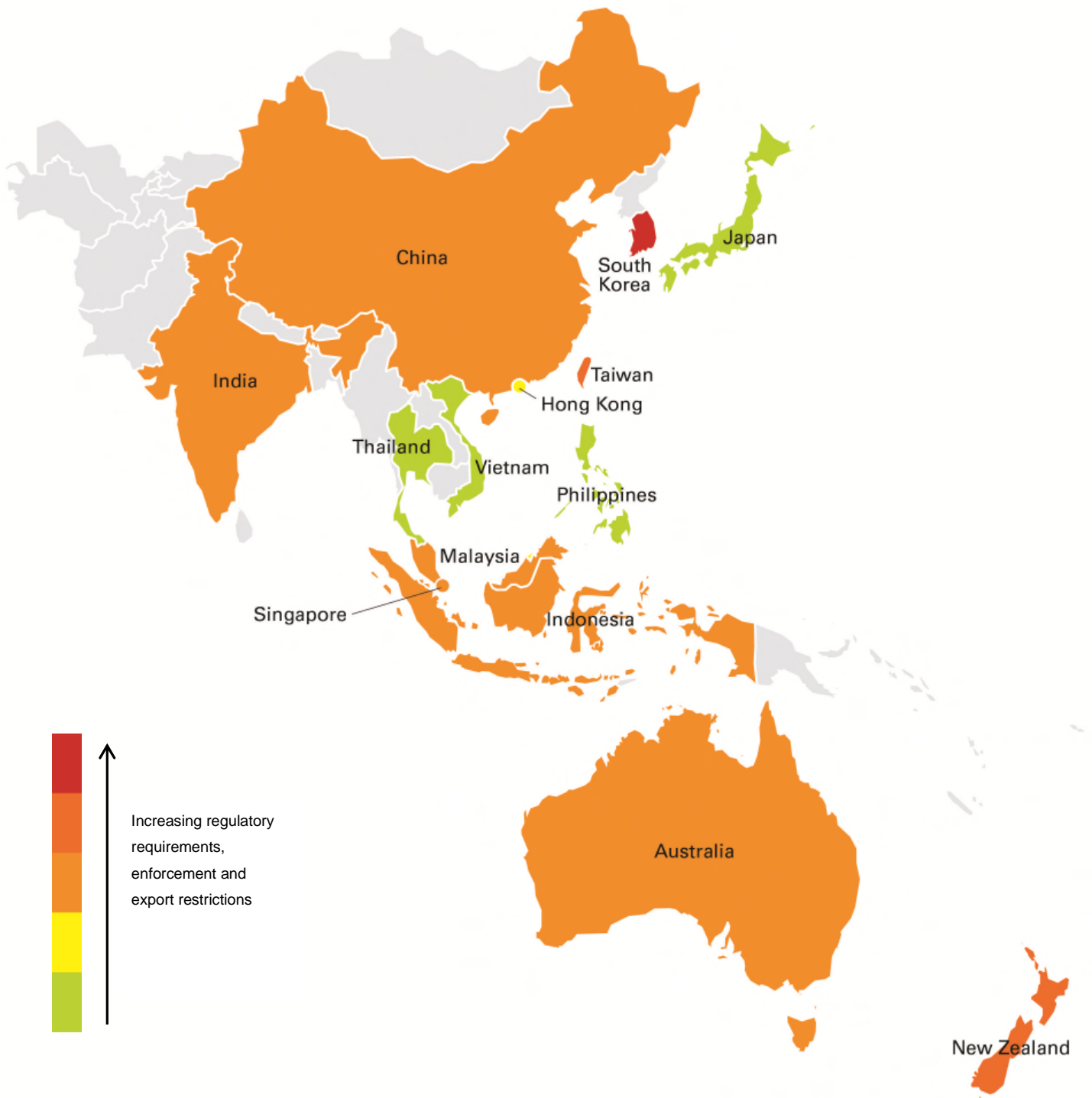
Direct Marketing Regulation:

Does an "opt in" standard apply? Will an "opt out" suffice? Are there other measures that must be taken before direct marketing may commence?



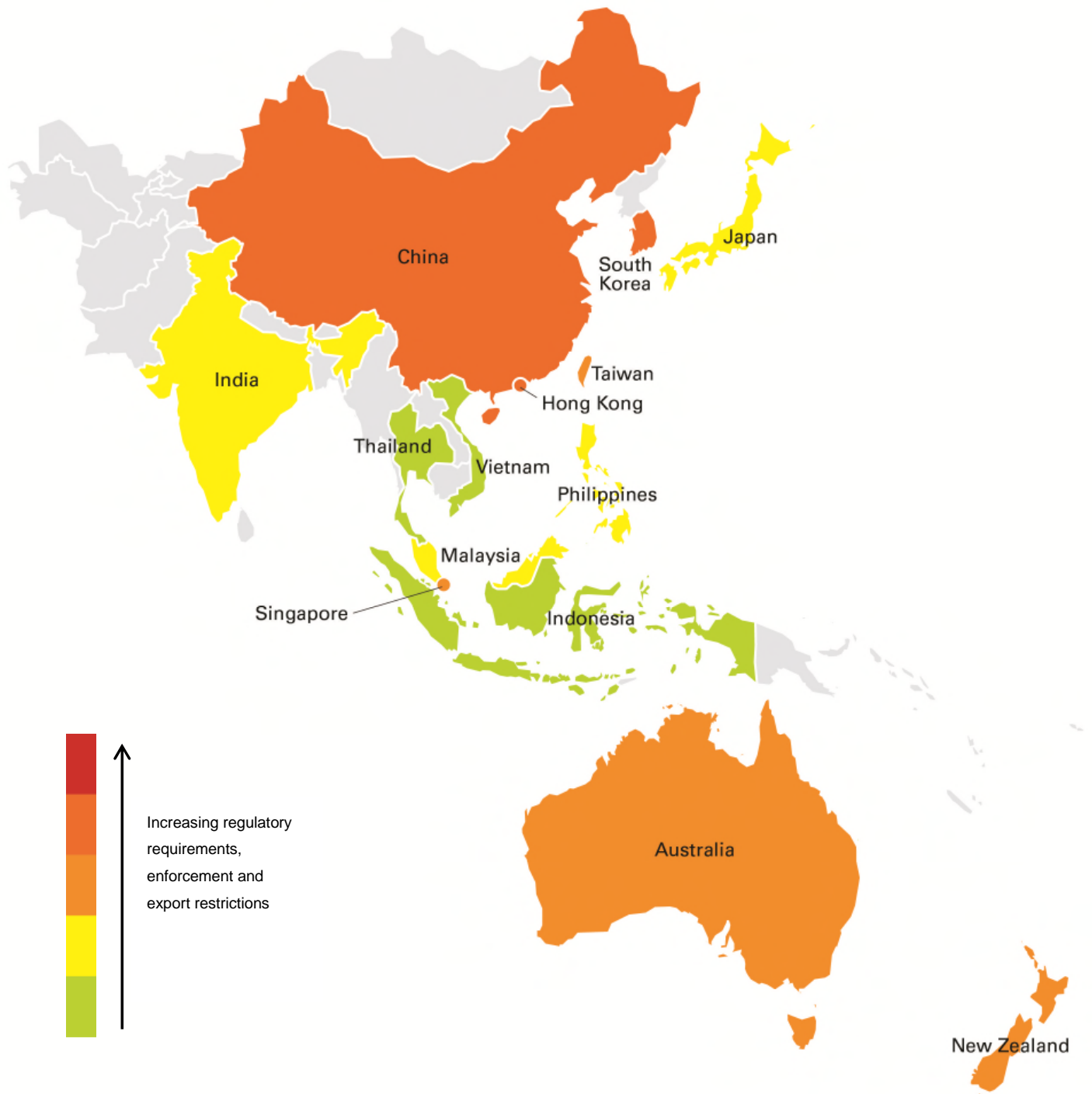
Data Export Controls:

The ability to move data across borders is increasingly important to doing business in Asia. Is data subject consent or other regulatory measures required in order to transfer personal data from the jurisdiction?



Aggressiveness of the Enforcement Environment:

How aggressive is the regulator in terms of initiating investigations and pursuing enforcement? How likely is it that the regulator imposes the full extent of fines and penalties available and how significant are these penalties? What is the regulator's attitude towards "naming and shaming" offenders?



Individual Country Spotlights

China

Perhaps against expectation, a rapid sequence of legislative reforms in China in recent years show a serious resolve to move the country towards a more comprehensive data privacy regime². However, without the unifying force of a law to provide a framework, there has been a tendency to approach the issue in a somewhat piecemeal fashion.

Specific offences in relation to misuse of personal data were introduced to the criminal law in 2009. The next year saw the introduction of specific privacy-related torts. Since then the pace has accelerated, with a series of legislative developments commencing in 2011 concerning the processing of personal data collected through the provision of internet and telecommunications services. The most significant reforms directed at the processing of electronic personal data came into force in March 2012, followed in February 2013 with non-binding general guidelines and in September 2013, with further rules specifically addressed at telecommunications and internet content providers. March 2014 saw the first significant set of amendments to the consumer protection law in the last 20 years, many of which relate to data privacy and which apply the rules to a much wider universe of all business operators in China.

The general shape of the new requirements draws from the same principles-based regulation that underlies other Organisation for Economic Co-operation and Development ('OECD') model-inspired laws, but analysing data privacy issues in China now requires a very careful assessment of various overlapping laws, decisions and guidelines against the specific type of personal data involved and the circumstances of its collection and processing. The thicket of potentially relevant laws, regulations and guidelines that has grown up in a rather piecemeal fashion around this area cannot be viewed in isolation. There is a need to consider industry-specific regulation and intersections with certain very sensitive areas of regulation, such as anti-bribery laws and state secrecy laws, not to mention potential reputational issues where an issue becomes publicised in the media.

While the hardest thrust to legislative reform has been directed at curing abuses of personal data by online fraudsters and data merchants, recent high profile prosecutions have underlined the growing importance of data privacy in the Chinese legal and regulatory landscape. Multi-national businesses can no longer afford to put data privacy regulation in China on the back burner.

South Korea

South Korea is now widely understood to be amongst the most challenging jurisdictions in Asia in terms of data privacy regulation.

Provisions of the over-arching Personal Information Protection Act and the IT Network Act (which regulates the collection and use of personal information by any commercial enterprise that sells or markets its goods or services online) are supplemented by sector-specific laws, creating a very difficult compliance environment.

South Korea has extensive registration and disclosure requirements and a need for separate specific data subject consents in areas such as the processing of sensitive personal data, data transfers and data exports. From November 2014, data subject consent will also be required by any business transmitting advertising information by email. Businesses are obliged to disclose the identities of third party data processors and must report all data security breaches to data subjects and the authorities. The legislation is backed up with extensive enforcement measures, including provision for data subject class action suits against offenders.

Businesses seeking to integrate their South Korean operations into global and regional operating platforms are finding the requirements to be difficult to meet in practice. Some requirements, such as the obligation to disclose the identities of third party data processors, appear to many to be counter-productive to achieving data security in fact.

The official view is that these requirements must be met and substantial public resources are now being spent on official investigators. Any business with operations in South Korea needs to take these regulations into account.

² Hogan Lovells briefing "China Turns up the Heat in the Battle Against Abuses of Personal Data" Corporate China Alert 20 August 2013 (updated in March 2014).

Singapore

Singapore is one of Asia's most recent movers towards comprehensive data privacy regulation, with the Personal Data Protection Act fully in force with effect from 2 July, 2014.

Singapore's new law draws heavily from the OECD model, with general requirements for data subject consent, data export controls and other measures which are now increasingly common across the region. Singapore's new Personal Data Protection Commission has been very active in taking public consultations about specific requirements under the law and publishing extensive explanatory guidance for businesses and consumers alike.

There are economic motives informing the new law.

Singapore has gone so far as to draw an explicit link between the implementation of data privacy regulation and its national ambitions to be a leading high tech hub in the region, including in areas such as data analytics. While these statements should be somewhat reassuring to businesses, the law has been enacted with some of the stiffest penalties for data privacy offences in the region, with fines of up to S\$1 million (USD800,000). It is clear that the new Commission will be resourced to enforce the law. With a strong culture of compliance in Singapore, we expect to see the island state at the fore of policy development across the region going forward.

Hong Kong

Data privacy regulation has a relatively long history in Hong Kong, with the Personal Data (Privacy) Ordinance (the PDPO) dating back to 1995. However, after many years of relatively lax enforcement, recent times have seen a regulatory environment substantially in flux.

In 2013 Hong Kong introduced one of the world's most challenging direct marketing regulatory regimes. Much of the complexity relates to requirements that direct marketing notifications be increasingly specific as to the kinds of personal data that will be used and the classes of goods and services that will be marketed. The "opt out" standard adopted by Hong Kong also requires that data subjects affirmatively indicate that they have opted out. Silence is not sufficient. The new regime has come forward backed up by substantially increased fines and an increased willingness by the authorities to "name and shame" offenders.

Hong Kong's Privacy Commissioner for Personal Data is very much an activist regulator. He has published a substantial volume of guidance on topics as diverse as data security breach notifications, cloud computing, mobile app development and public domain data. He publicly comments on developments in privacy law abroad and continues to press for wider ranging regulation and heavier enforcement powers under the PDPO. It is very likely that Hong Kong will see further development in coming years, as consumer awareness of privacy issues continues to grow.



Our Asia Practice

At Hogan Lovells we bring an international perspective to advising clients on Asia's data privacy laws and the ongoing development of policy across the region. Our Asia team based in Hong Kong, Beijing, Shanghai, Singapore and Tokyo include practitioners who practised data privacy law in Europe, and so bring a depth of experience to interpreting Asia-Pacific laws that have a common origin in the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. At the same time, our experts are on the ground in the region and rooted in the local law and language, sensitive to the important emerging local nuances.

Our Asia team is closely integrated with our international team of data privacy practitioners, and so benefits heavily from a wider team of market-leading lawyers who are at the forefront of policy developments in Europe and the United States, advising clients on the most critical mandates on a world-wide basis.

Where Hogan Lovells does not have offices in the Asia-Pacific region, we have strong working relationships with local counsel experts. These relationships have developed over the course of the effective lifetime of these emerging laws, supporting the delivery of a uniformly consistent and high quality work product and practical solutions for business.

Our wide network in Asia and elsewhere means that we can provide joined-up thinking on all aspects of data privacy compliance, including:

- Conducting data privacy compliance audits and developing data privacy policies, including integrating Asia policies with existing international policies;
- Helping clients structure and allocate risk in relation to cross-border data transfers, including as part of outsourcing, shared services and cloud arrangements;
- Advising on the acquisition of personal data as an increasingly important part of merger and acquisition and joint venture activity;
- Advising on commercial arrangements, such as marketing, distribution and sponsorship agreements, where securing rights to use personal data is a key business objective;
- Advising on data breach notification requirements when data is hacked or lost;
- Advising on data subject access requests;
- Defending companies against enforcement actions; and
- Bringing to bear the knowledge and experience of our extensive and market-leading privacy and information management team across the world in finding solutions that work in Asia based on lessons learnt elsewhere.

Key Contacts

Hong Kong



Mark Parsons, Partner
mark.parsons@hoganlovells.com
T: +852 2840 5033

Japan



Eiichiro Kubota, Partner
eiichiro.kubota@hoganlovells.com
T: +81 3 5157 8247



Peter Colegate, Associate
peter.colegate@hoganlovells.com
T: +852 2840 5961

Singapore



Stephanie Keen, Partner
stephanie.keen@hoganlovells.com
T: +65 6302 2553

Shanghai



Andrew McGinty, Partner
andrew.mcginty@hoganlovells.com
T: +86 21 6122 3866

Beijing



Jun Wei, Partner
jun.wei@hoganlovells.com
T: +86 10 6582 9501



Philip Cheng, Partner
philip.cheng@hoganlovells.com
T: +86 21 6122 3816

Vietnam



My Doan, Associate
my.doan@hoganlovells.com
T: +84 8 3829 5100

www.hoganlovells.com

Hogan Lovells has offices in:

| | | | | |
|------------------|------------------|-------------|-------------------|----------------|
| Alicante | Dusseldorf | London | New York | Silicon Valley |
| Amsterdam | Frankfurt | Los Angeles | Northern Virginia | Singapore |
| Baltimore | Hamburg | Luxembourg | Paris | Tokyo |
| Beijing | Hanoi | Madrid | Philadelphia | Ulaanbaatar |
| Brussels | Ho Chi Minh City | Mexico City | Rio de Janeiro | Warsaw |
| Budapest* | Hong Kong | Miami | Riyadh* | Washington DC |
| Caracas | Houston | Milan | Rome | Zagreb* |
| Colorado Springs | Jakarta* | Monterrey | San Francisco | |
| Denver | Jeddah* | Moscow | São Paulo | |
| Dubai | Johannesburg | Munich | Shanghai | |

"Hogan Lovells" or the "firm" is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses. The word "partner" is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.

For more information about Hogan Lovells, the partners and their qualifications, see www.hoganlovells.com.

Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney Advertising.

©Hogan Lovells 2014. All rights reserved. #1160455

*Associated offices