

Developments in Global Data Protection & Transfer: How They Impact Third-Party Contracts

Rebecca Eisner

Partner

+1 312 701 8577

reisner@mayerbrown.com

Gabriela Kennedy

Partner and Head of Asia IP & TMT

+852 2843 2380

gabriela.kennedy@mayerbrownjsm.com

Mark Prinsley

Partner

+44 20 3130 3900]

mprinsley@mayerbrown.com

Lei Shen

Senior Associate

+1 312 701 8852

lshen@mayerbrown.com

June 7, 2016

The Age of Disruption

HOW EMERGING TECHNOLOGIES AND CYBERSECURITY ARE TRANSFORMING SOURCING



Rebecca S. Eisner

Partner

Rebecca S. Eisner is the Partner in Charge of the Chicago office of Mayer Brown LLP and a member of the firm's Business & Technology Sourcing group. Her practice focuses on complex global cloud and emerging technologies, outsourcing and technology transactions, privacy, data protection and data transfers, Internet and e-commerce law issues. She is a frequent writer and speaker on outsourcing, cloud computing and privacy and data protection topics.



Gabriela Kennedy

Partner

Gabriela Kennedy is a partner of Mayer Brown JSM and head of the Asia IP and TMT group. She is also co-leader of Mayer Brown's global Intellectual Property practice. She is based in Hong Kong, practising intellectual property, privacy, media, information technology and telecommunications law. Gabriela advises extensively on technology and data protection issues in Hong Kong and throughout Asia, particularly in relation to business processing outsourcing, the cross-border transfer of data, data compliance and data breaches.



Mark A. Prinsley

Partner

Mark A. Prinsley is a partner of Mayer Brown and head of the Intellectual Property & IT group in London as well as the outsourcing practice. He is regularly named as a leading individual in the areas of business process outsourcing, information technology and intellectual property by *Chambers'* UK and Global guides. His practice involves acting for customers at all stages of outsourcing transactions with a particular focus on the financial services sector.



Lei Shen

Senior Associate

Lei Shen is a senior associate in the Cybersecurity & Data Privacy and Business & Technology Sourcing practices in Mayer Brown's Chicago office. Lei focuses her practice on data privacy and cybersecurity, technology and business process outsourcing, and information technology transactions. Lei is a Certified Information Privacy Professional in U.S. privacy law (CIPP/US) and a member of the International Association of Privacy Professionals (IAPP).

EUROPE: IMPLICATIONS OF THE GENERAL DATA PROTECTION REGULATION

EU General Data Protection Regulation

- Implementation
 - Regulation adopted and published 27 April 2016 and replaces existing EU data privacy regime in May 2018
- Key changes
 - Territorial scope/application
 - Compliance obligations
 - Rights of data subjects
 - Sanctions for breach
 - International transfers



Territorial Scope/Application

- New law is by way of EU Regulation – should result in a largely harmonised position throughout all EU countries
- Applies to processing of personal data
 - (a) in the context of the activities of a controller or processor established in the EU, irrespective of where the processing takes place;
 - (b) of data subjects who are in the EU by controllers or processors not established in the EU where the processing relates to offering goods or services to the data subjects or monitoring the behaviour in the EU of data subjects
 - NOTE: It applies to Data Processors and Data Controllers

Compliance Obligations

- “Privacy by design” concept builds on current technical and organisational security measures’ obligations on data controllers
- More sophisticated requirements for the contractual arrangements between a data controller and a data processor
- Formal record-keeping obligations on controllers and processors, records to be open to inspection by information commissioner
- Data privacy impact assessments for high-risk processing
- Data privacy officers required in some situations

Enhanced Rights of Data Subjects

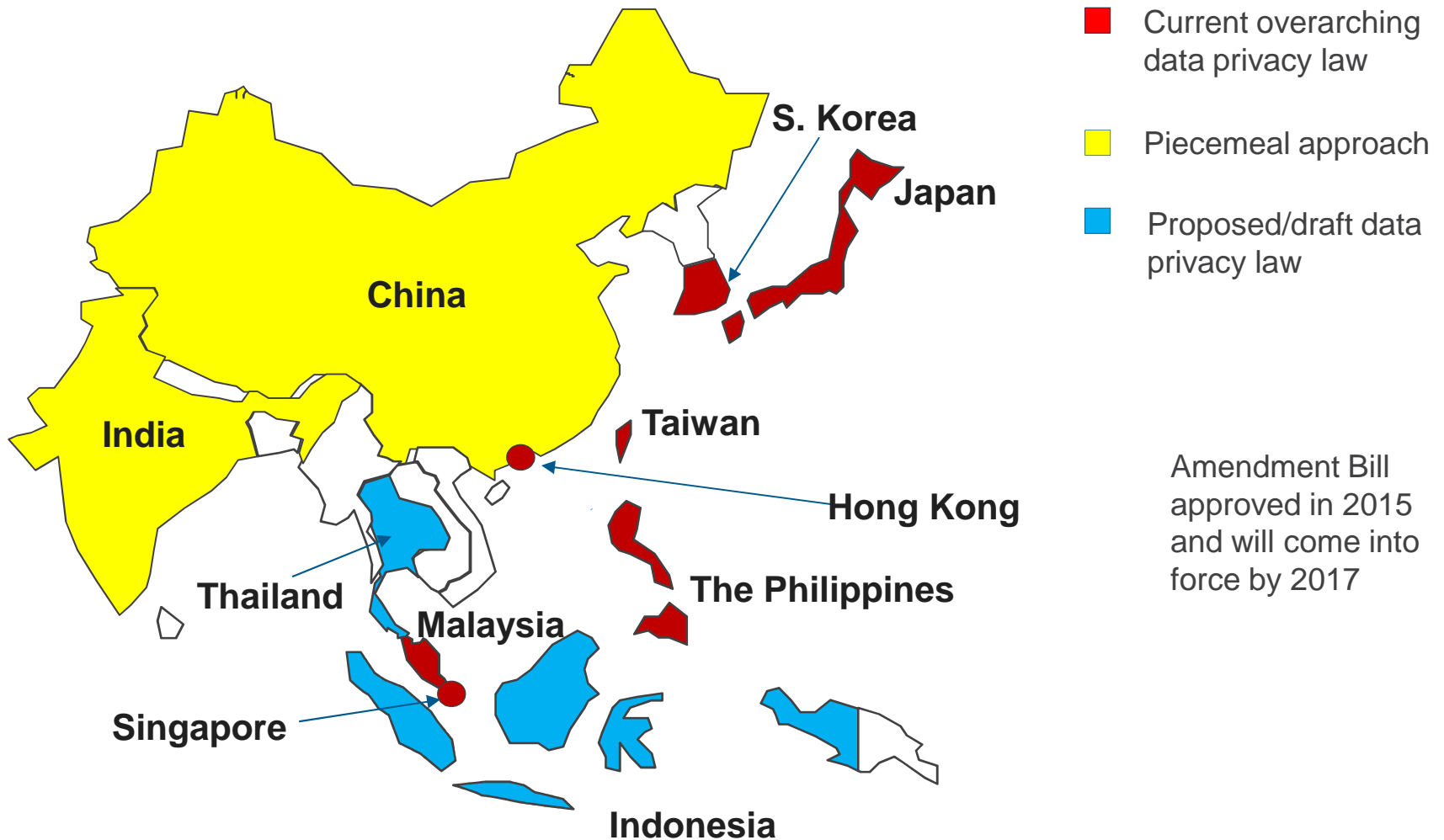
- Greater transparency of nature of processing
 - more information to be made available
 - clear and concise explanations required
 - likely emergence of “washing instructions” icons
- Right to be forgotten
 - impact on information made publicly available
- Data portability
 - for data an individual has provided to the data controller and where the processing is carried out by automated means
- Right to object to processing
 - potential impact on the “legitimate interests” ground for processing personal data
 - absolute right to object to processing for direct marketing

Data Breach and Sanctions (and International Transfers)

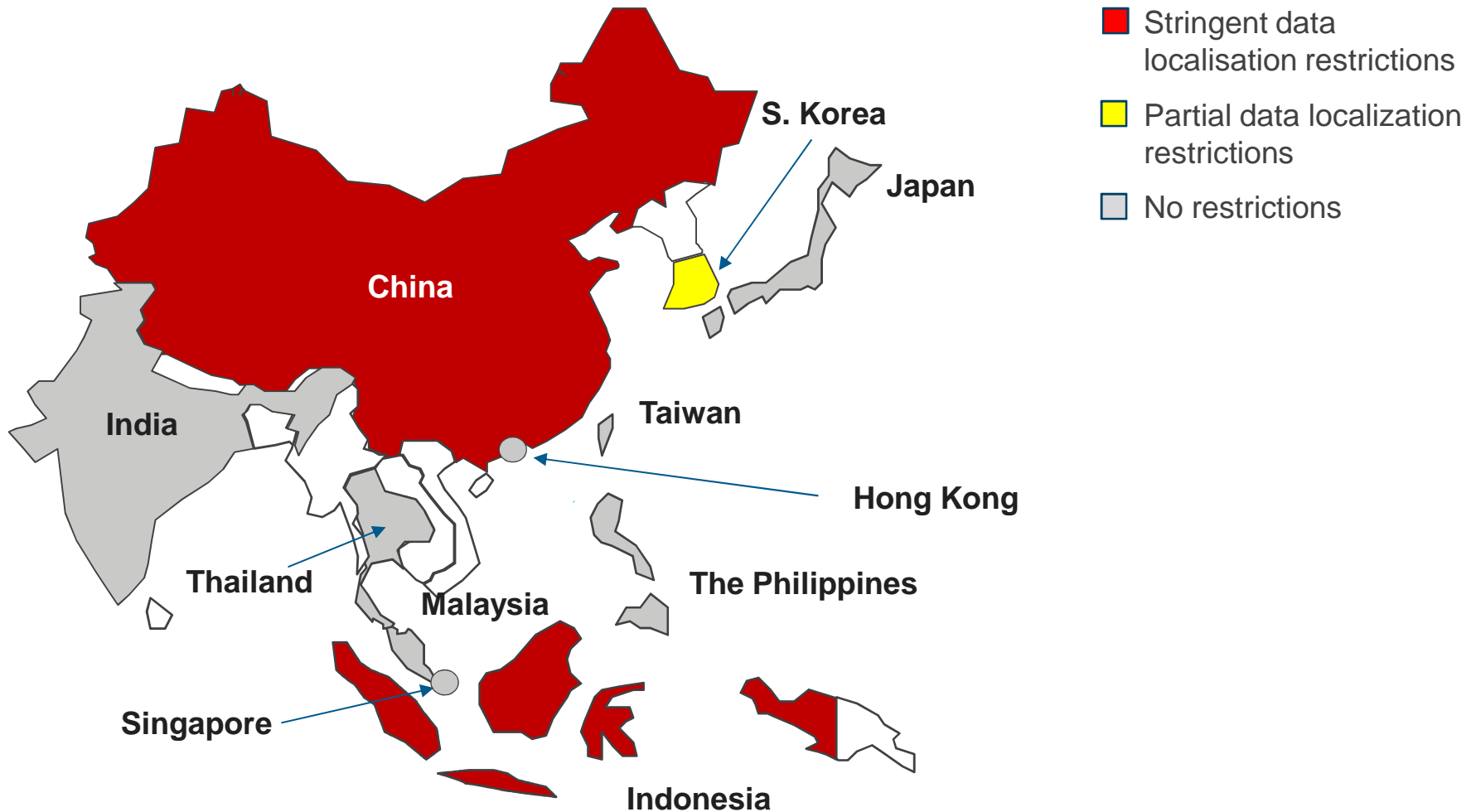
- Personal data breaches
 - presumption that Information Commissioner must be notified within 72 hours of the controller becoming aware of the breach
 - processor under obligation to notify the controller
 - notification of data subjects only required where there is a high risk to the rights and freedoms of the data subject
- Administrative fines
 - up to 4% of worldwide annual turnover or €20 million, whichever is the greater. **BUT** many qualifications on likely level of fines
- Direct legal remedies
 - greater clarity as to potential for direct proceedings. Consumer class actions possible
- International transfers
 - current regime continues – but that is not the whole story!

ASIA: CONSTANT CHANGE

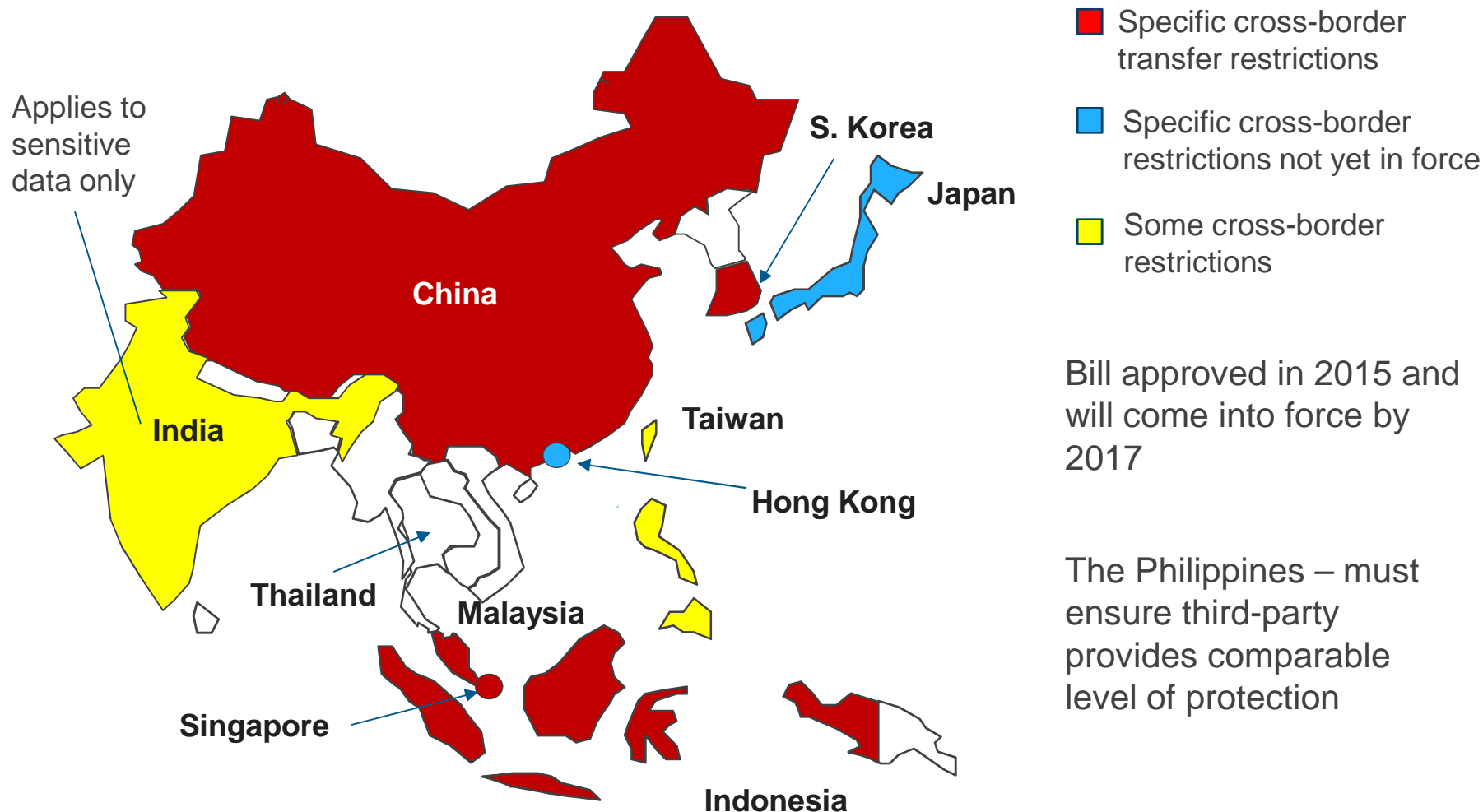
The Emergence of Privacy Legislation



Data Localisation



Personal Data Cross-Border Transfer Restrictions



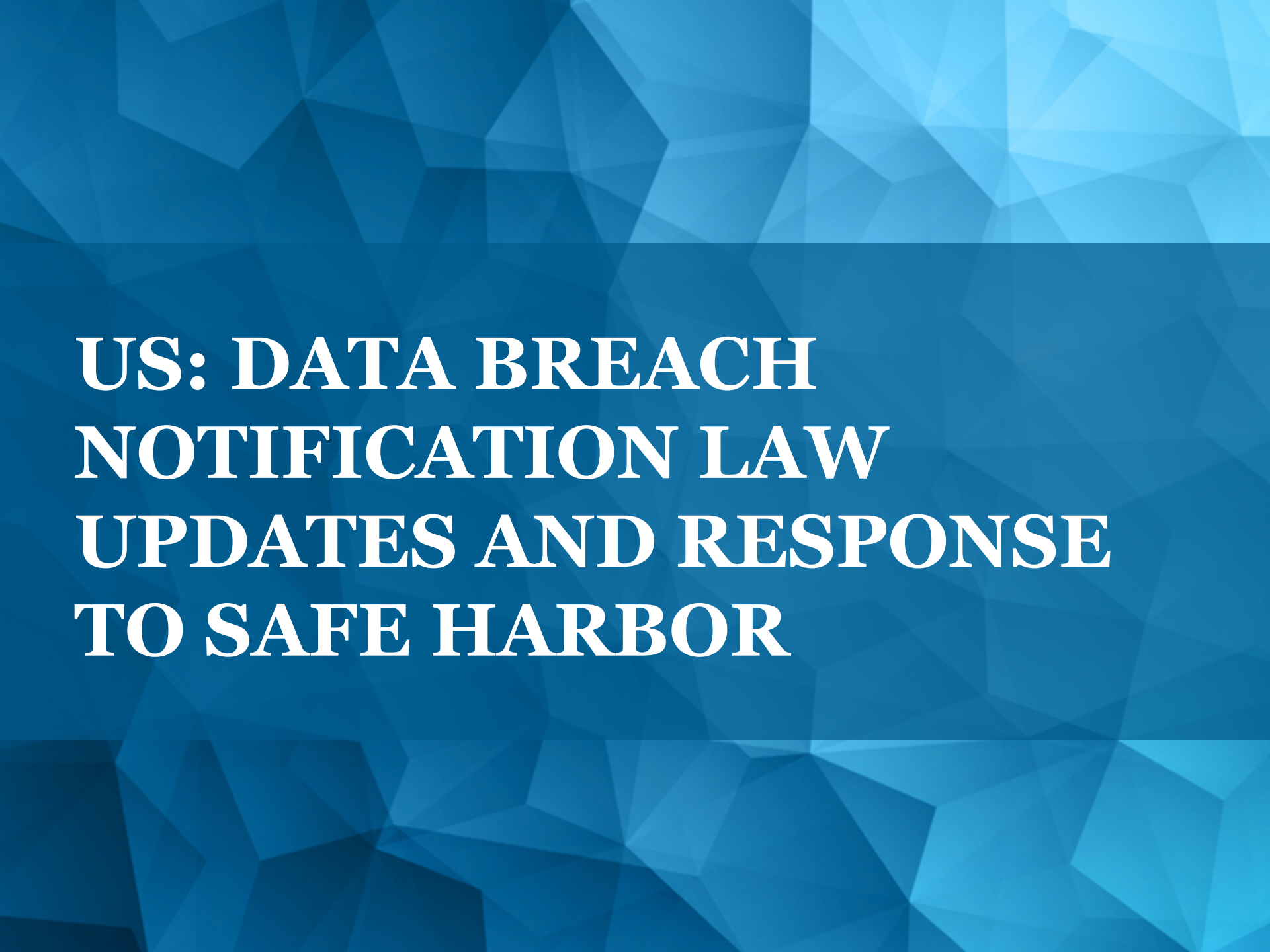
Marketing Restrictions



- Data localisation
 - China and Indonesia
- Cybersecurity
 - HK – HKMA initiated Cybersecurity Fortification Initiative in May 2016, SFC issued Circular on Cybersecurity in March 2016
 - China – draft Cybersecurity Law
 - Singapore – new Cybersecurity Act will be tabled in Singapore's parliament in 2017
 - Philippines – Sept 2015, National Cybersecurity Inter-Agency Committee and National Cybersecurity Coordination Centre formed

Emerging Trends (*Cont.*)

- Biometric / sensitive data
 - India – 25 March 2016, law passed enabling federal agencies to access Aadhaar database scheme
 - HK – Electronic Health Record Sharing System (March 2016); guidelines on handling biometric data in July 2015
 - Japan – 2015 amendments to introduce restrictions on sensitive personal data in PDPA (come into force in 2017)

The background of the slide is a solid blue color with a low-poly, geometric pattern of various shades of blue, creating a modern and professional look.

US: DATA BREACH NOTIFICATION LAW UPDATES AND RESPONSE TO SAFE HARBOR

- Recent Updates to US Data Breach Notification Laws
- Invalidation of Safe Harbor and Rejection of Privacy Shield



US Data Breach Notification Laws

- Recent updates to US Data Breach Notification Laws
 - Expansion of the Definition of Personal Data
 - Encryption Exceptions and Requirements
 - Notification Timeframes
 - Requirements for the Contents of Breach Notices



US Data Breach Notification Laws

- Expansion of the Definition of Personal Data
 - Additional elements added to scope
 - Outliers in recent updates:
 - California: data collected by an automated license plate recognition system
 - North Dakota: work ID number with security or access code
 - Wyoming: birth or marriage certificates



US Data Breach Notification Laws

- Encryption Exceptions and Requirements
 - Definition of encryption
 - Removal of encryption safe harbor
 - If encryption code is compromised
 - Regardless of whether data was encrypted or not



US Data Breach Notification Laws

- Notification Timeframes
 - Specific timeframes for notification of consumers
 - Data owner notification timeframe vs. data processor notification timeframe



US Data Breach Notification Laws

- Requirements for Contents of Breach Notices
 - California
 - Illinois



Safe Harbor Invalidation and Rejection of Privacy Shield

- Safe Harbor Invalidation
- Rejection of Privacy Shield
 - Article 29 Working Party
 - European Parliament
 - European Data Protection Supervisor

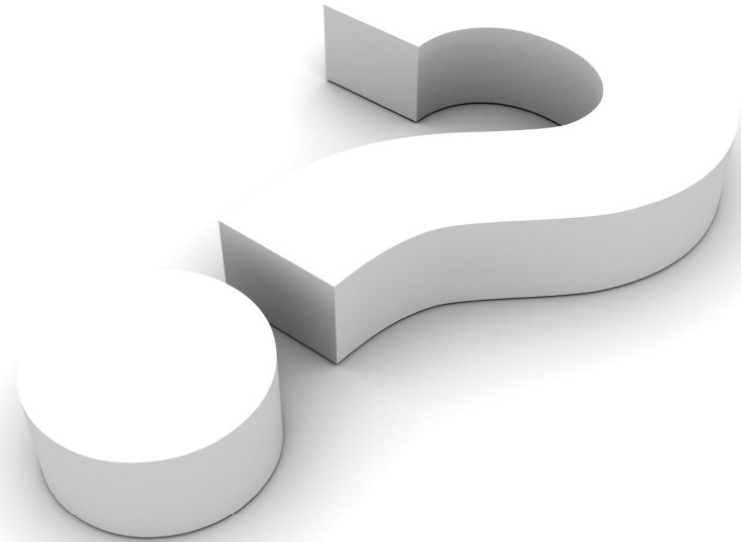


Other Transfer Mechanisms

- EU Model Clauses (but with caution)
- Binding Corporate Rules (BCRs)
- Derogations listed in Article 26 of EU Data Protection Directive
 - Data Subject Consent
- Approval from Data Protection Authority (DPA)



QUESTIONS



Rebecca Eisner

Partner

+1 312 701 8577

reisner@mayerbrown.com

Gabriela Kennedy

Partner and Head of Asia IP & TMT

+852 2843 2380

gabriela.kennedy@mayerbrownjsm.com

Mark Prinsley

Partner

+44 20 3130 3900]

mprinsley@mayerbrown.com

Lei Shen

Senior Associate

+1 312 701 8852

lshen@mayerbrown.com