NORTON ROSE FULBRIGHT

IS Summit 2021

Cybersecurity Regulation in Asia: New developments and lessons learned

Anna Gamvros
Asia Pacific Head of Data Protection, Privacy and Cybersecurity

10 March 2021

Agenda

- APAC overview
- Recent developments in APAC
- Lessons learned
  - Investigation Steps & Protocols
  - Privacy Gaps
  - Security/ Technical Gaps
- How do the regulators investigate and what are they asking

APAC overview

APAC overview

India: Draft Personal Data Protection Bill issued in December 2019. Currently provisions spread across the IT Act 2000, the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 and the IT (Intermediaries Guidelines) Rules 2011 (draft amendments proposed in 2018)

Thailand: Cybersecurity Act effective from May 2019; Personal Data Protection Act passed in February 2019, effective from May 2021

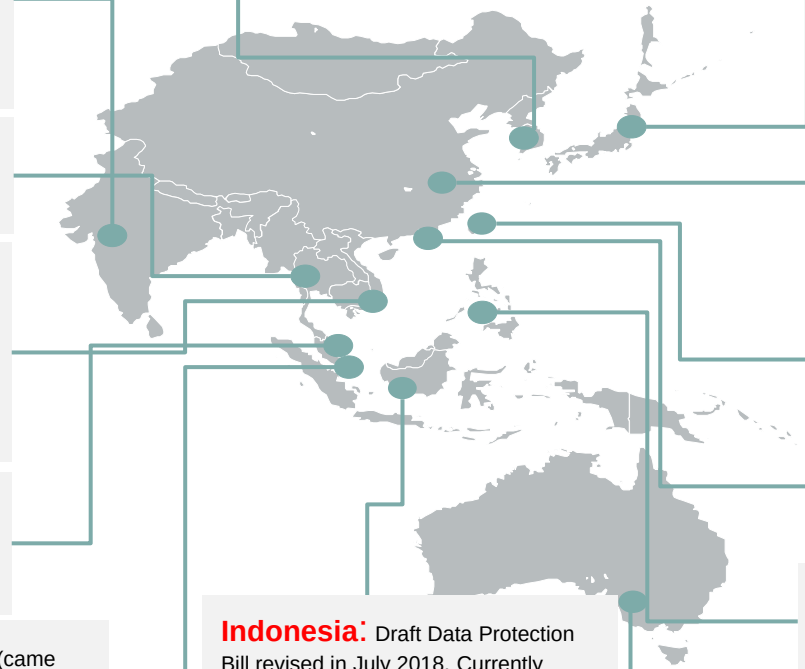
Vietnam: Draft Decree on Personal Data Protection issued in December 2019. No comprehensive data protection law – provisions spread across Civil Code, the IT Law, the Penal Code, and the Telecommunications Law. Cyber Security Law was passed in June 2018 and effective from January 1, 2019

Malaysia: Personal Data Protection Act 2013 (Personal Data Protection Standards effective from 23 Dec 2015). Consultation on data breach notification requirement published in February 2020

Singapore: Personal Data Protection Act 2012 (came into full force on July 2, 2014). Amendments to the Personal Data Protection Act 2012 were passed on November 2, 2020. Certain sections (including the mandatory data breach notification regime) took effect from 1 February 2021. Most of the Cybersecurity Act provisions have come into force as of August 2018.

South Korea: Personal Information Protection Act 2011, Act on Promotion of Information and Communications Network Utilization and Information Protection and Credit Information Use and Protection Act. Amendments to all three acts passed in Jan 2020, effective from August 2020.

Japan: Act on Protection of Personal Information 2013 (amendments passed in June 2020, to be effective by 2022), Basic Act on Cyber Security 2014 (amended in December 2018)



China: No comprehensive data protection law. Spread across laws and regulations, including Cybersecurity Law (effective June 1, 2017), Personal Information Protection Law (draft October 21, 2020), Personal Information Security Specification 2020 (effective October 1, 2020), Measures for Cybersecurity Review (effective June 1, 2020), Measures on Administration of Data Security (draft May 28, 2019), Measures on Security Assessment of Cross-Border Transfer of Personal Information (draft June 13, 2019) and Cryptography Law (effective January 1, 2020)

Taiwan: Personal Data Protection Act 2010 (amendments came into force March 2016). Information and Communication Security Management Act was passed in May 2018 and effective from 1 January 2019

Hong Kong: Personal Data (Privacy) Ordinance (under review)

Indonesia: Draft Data Protection Bill revised in July 2018. Currently provisions spread across Electronic Information and Transaction Law 2008 and Government Regulation on the Implementation of Electronic Systems and Transactions.

The Philippines: Data Privacy Act 2012 (Implementing Rules and Regulations effective September 9, 2016)

Australia: Privacy Act 1988 (amendments in full effect on March 2014). Notifiable Data Breaches scheme effective Feb 2018

Cybersecurity - Tighter regulation

China 

- Cybersecurity Law 2016, effective June 1, 2017
- Measures for Cybersecurity Review, effective June 1, 2020
- Cryptography Law, effective January 1, 2020
- Issuing of regulations on security regulations and assessments regarding cross border data transfers and critical information infrastructure

Hong Kong 

- SFC and/or HKMA issued various cybersecurity circulars and initiatives and conducted on-site examinations
- SFC issued Guidance to reduce hacking risks associated with internet trading in October 2017

Taiwan 

- Information and Communication Security Management Act passed in May 2018 (and in effect on January 1, 2019)

Vietnam 

- Cybersecurity Law passed in June 2018 (and in full effect on January 1, 2019)

Indonesia 

- National Cyber and Encryption Agency established in 2017

Japan 

- Cybersecurity Strategy announced in July 2018
- Cybersecurity Act was amended in December 2018

Malaysia 

- Draft Cybersecurity Bill announced in 2017

The Philippines 

- National Cybersecurity Plan 2022 unveiled in May 2017

Singapore 

- Most of the Cybersecurity Act provisions came into effect on August 31, 2018

Thailand 

- The Cybersecurity Act, published on 27 May 2019, is now effective

5

Data breach notification

	Hong Kong	China	Taiwan	Singapore	Malaysia	Australia	Japan	South Korea	Philippines	India	Indonesia	Thailand	Vietnam
Mandatory Breach Notification	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓
Requirement to notify data subjects	✗	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗
Requirement to notify authorities	✗	✓	✗	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓

Recent developments

Recent developments

Singapore

Personal Data Protection (Amendment) Bill was introduced read in Parliament on 5 October 2020. Certain sections (including the mandatory data breach notification regime) took effect from 1 February 2021.

China

Draft Personal Information Protection Law published on October 21, 2020.

Hong Kong

Discussion paper regarding proposed changes to the Personal Data (Privacy) Ordinance was published on January 13, 2020. Mandatory data breach notification proposed.

Lessons Learned

Summary

- Investigation Steps & Protocols
  - Attorney Client Privilege
  - Teams
  - Communications
  - Notification
- Privacy Gaps
- Security/ Technical Gaps

Lessons Learned

Investigation Steps & Protocols

Attorney Client-Privilege

Issues

- Timely engagement of legal counsel – days/weeks delay
- Alerting/normal BAU/IR response – harmful to privilege claim
- IR retainers triggering – no counsel
- Other 3rd parties: MSPs, vendors, vendors, etc. – comms going out regularly
- Work product – deliverables and written work product from any 3rd party requested.
- Communications happening rapidly, expansion of “tent”, lawyers not involved
- May not be recognized depending on jurisdiction and/or not as strong
- Note: consider privilege claims over previous assessments, testing, etc.

NRF

Attorney Client-Privilege

Lessons Learned

- Ensure counsel brought in before any 3rd party substantively engaged {consider SOC plug-in} (even if alerting comes from 3rd party)
- Establish terms of reference setting out the following:
  - Who the investigation is being led by (external advisors have been instructed by Legal)
  - Objectives of the investigation (to inform legal analysis of obligations, liability, risks, and/or in contemplation of anticipated legal/regulatory proceedings
  - Key workstreams and purpose of workstreams (e.g., assessing legal risk, reporting obligations, etc.) Note: even when pertaining to containment, eradication and remediation.
  - The investigation team
  - Reporting lines
  - Steps taken to preserve data. Note: issue legal hold early
  - Protocols for communications and protecting ACP
- Assert privilege and proceed as in place everywhere

Team

Issues

- Team composition too large (keep small and tight as possible)
- Roles and responsibilities unclear
- Governance structure and decision making authority unclear
- Dependencies on IT for investigation
- Dependencies on 3rd parties for investigation

Lessons Learned

- Identify key people to be involved (core team) from:
- Legal, IT, Ops, IS, Asset protection/Security, Comms/PR, Gov Affairs, HR
- Set up Steering Committee (use existing structure) as decision making body

Communications

Issues

Internal

- Escalation/reporting: board and senior leaders not being informed
- Employee comms
- Being prepared early for leaks

External

- Reporting to and from forensic firms, PFI
- Law enforcement– very different around the world
- Acting quickly on threat Intel
- Managing other 3rd parties (IT providers, vendors, business partners, corporate accounts)
- Public response
- Too quickly and too late
- Statements harmful to litigation defense (compensation, harm)
- Statements harmful to regulatory defense (improvements, concessions)
- Poor word choices (numbers, sophistication, attribution, victim)

Communications

Lessons Learned

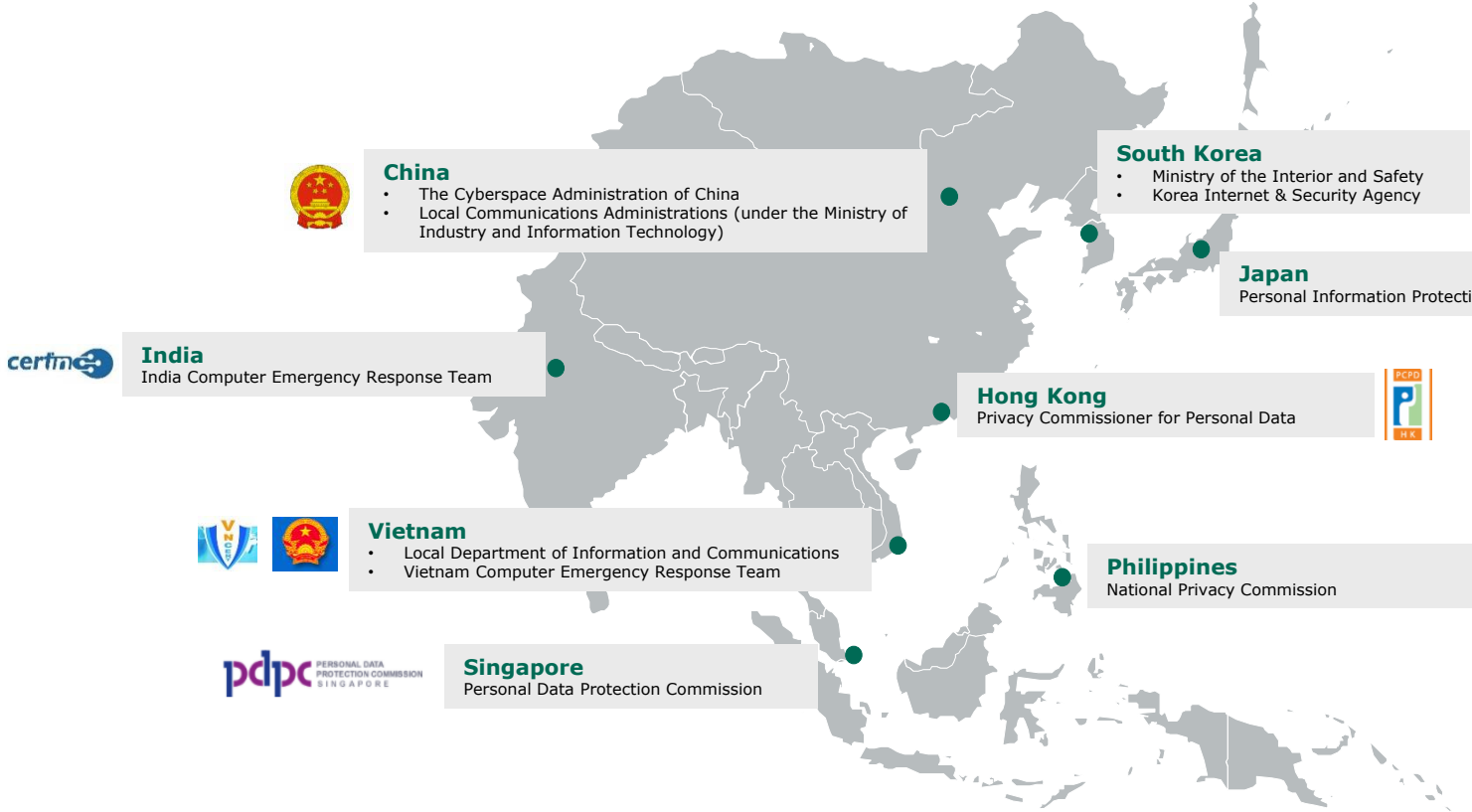
- Establish protocols on:
  - Internal comms for SIRT (only factual comms, mark documents and emails as *privileged and confidential*, copy lawyers)
  - Internal comms for employees outside tent
  - External comms (limit to need to know basis; no comms without lawyers, including LE)
  - PR
  - ACP/Work Product
  - Evidence preservation/legal hold
  - Escalation
- Note: Forensic reporting should be carefully considered due to legal challenges (historic approach should be amended when possible)

Notifications

Issues

- Global strategy needs to be balanced with strict compliance objectives
- Approach different across the globe
- Lack of vendors (call center, mailing, credit monitoring)
- Notice content
- Local language
- Formats for regulators vary significantly
- Questions vary
- Different timing requirements
- Cultural differences
- Geopolitical issues

Notifications – APAC privacy regulators



China
- The Cyberspace Administration of China
- Local Communications Administrations (under the Ministry of Industry and Information Technology)

South Korea
- Ministry of the Interior and Safety
- Korea Internet & Security Agency

Japan
Personal Information Protection Commission

India
India Computer Emergency Response Team

Hong Kong
Privacy Commissioner for Personal Data

Vietnam
- Local Department of Information and Communications
- Vietnam Computer Emergency Response Team

Philippines
National Privacy Commission

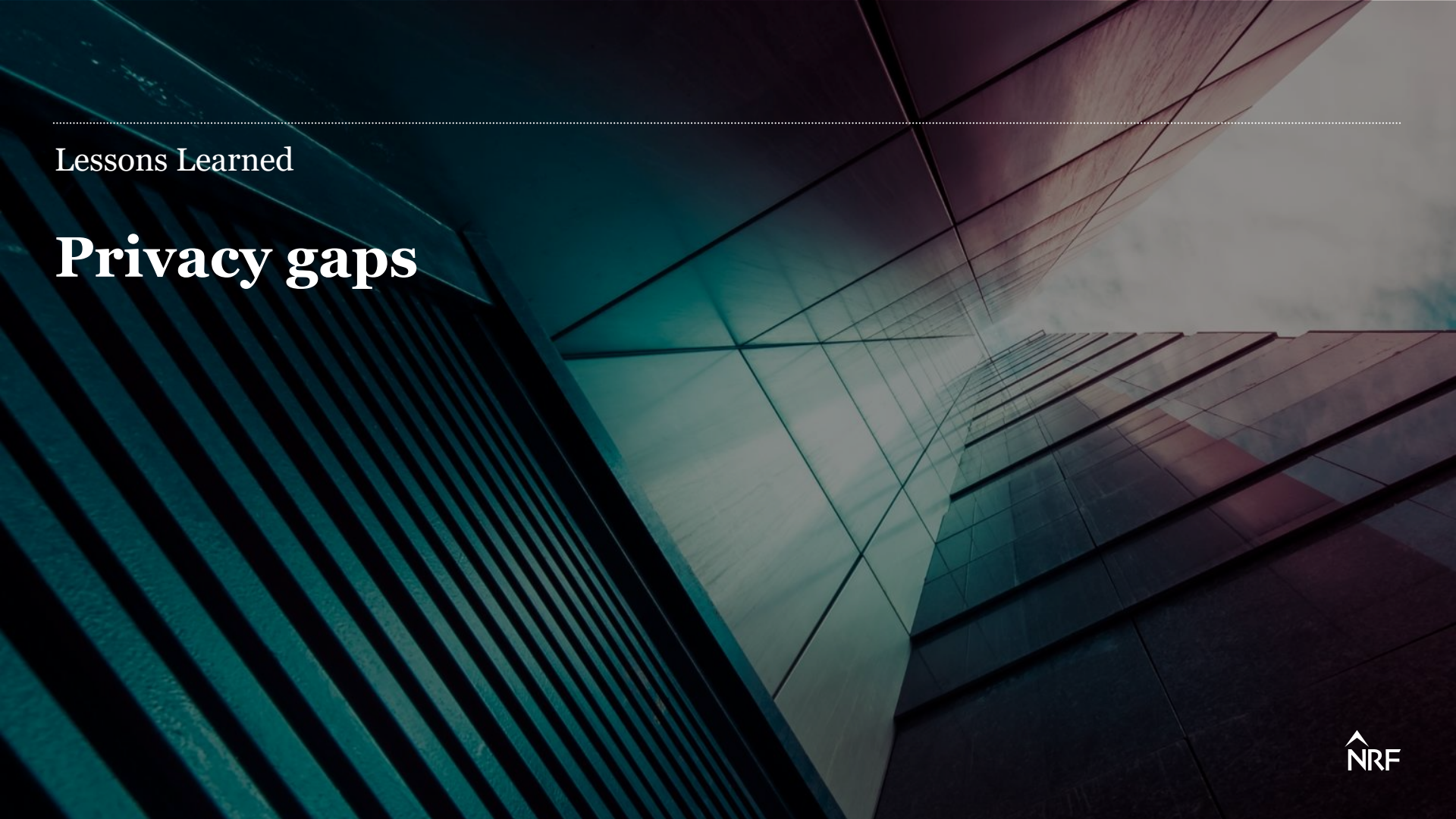
Singapore
Personal Data Protection Commission

Notifications – APAC law enforcement agencies

Notifications: Global

Lessons Learned

- Plan in advance
- Identify vendors
- Execution strategy
- Understanding hot spots (GDPR, China, Philippines)



Lessons Learned

Privacy gaps

Privacy Gaps

Issues

- Excessive collection of data
- Excessive retention of data
- Using production data in non-production database for testing
- Saving database back-ups on production server for data migration
- Lack of/inadequate encryption
- Data everywhere (and not known)

Lessons Learned

- Up to date data inventory
- Evaluate encryption
- Testing data policy
- Retention policy being followed

Lessons Learned

Security/Technical gaps

Security/Technical gaps

Issues

- Poor vulnerability/ patch management
- Poor identity management/ access controls
- Lack of adequate monitoring/detection – poor management of same
- AV/malware detection capabilities – inadequate detection/response; inadequate coverage
- Network segmentation
- Unsupported systems (difficult to defend)
- 3rd party management (contractual requirements – don't waive, cooperation, awareness of control/responsibilities, oversight of vendor compliance with contractual requirements)

Lessons Learned

- Key: risk management, defensible position
- Evaluate tools and capabilities and people
- Get rid of unsupported systems – if must keep mitigations in place and documentation re justification (and obtain appropriate level of approval based on articulated risk)
- Stronger vendor management
- Key: how are service providers performing
- Key: audit/oversight

How the regulators investigate

Investigation Process

- Very short turnaround time
  - Prompt response required (e.g., ~80 complex technical questions in less than 10 days)
- Very thorough and highly technical
  - The depth and technical complexity of the questions is increasing
- Questions coming from regulators all over the world and not the breached party's primary regulator
  - Number of regulators asking questions at the same time
  - Similar questions but not identical – very challenging
  - European regulators increasingly active and aggressive

Example

- 26 data privacy regulators notified globally/7 regulators investigated across 4 continents
- Well over 500 questions asked in total, over 20 question sets.

Questions being asked: Key Themes

Governance – cybersecurity program and privacy program

Priority – budget and resources and preparation

Board of directors – including decisions made and when informed

Risk Management function and decisions

Privilege assertions/ challenges

Supporting evidence

- Controls
- Policies, procedures, contracts
- Prior risk assessments/tests
- Investigation materials: timelines, forensic reports, correspondence, minutes…

Questions being asked: Key Topics

- Timeliness (reporting and responding)
- Appropriate technical and administrative measures
  - Monitoring and detection
  - Identity management
  - Patch and vulnerability management
  - Remote access and Multi-Factor Authentication
  - Asset management
- PCI – credit cards
- Privacy
- 3rd party vendors

Example Board and Senior Management Questions

- What did the board/senior management know and when
- Who told them and when did senior management know/assess exposure to fines/penalties
- What were they told
- What decisions were made and when
- How were the decisions made
- What controls in place and documentation re all of the above

Takeaways

Takeaways

- Ensure the security team have a basic knowledge of legal obligations
- Legal complexity with multi-jurisdictional breach
- Ensure communications protocol to protect privilege
- A breach is an exponential drag on productivity
- Regulator focus on security and data governance
- Lawyers will help to defend decisions and prioritization
- Get ready now – incident response plan

Key contact

Anna Gamvros

Asia Pacific Head of Data Protection, Privacy and Cybersecurity, Hong Kong
+852 3405 2428
anna.gamvros@nortonrosefulbright.com

Anna Gamvros is a partner at Norton Rose Fulbright, Hong Kong and is the Head of Data Protection, Privacy and Cybersecurity for Asia Pacific. Anna has been based in Asia for the last 18 years and her practice focuses primarily on data protection, incident response and technology and communications related issues. Anna has worked on numerous cybersecurity incident and data breaches involving a variety of threats and threat actors including some of the largest and most high profile breaches in Asia. She has experience in dealing with regulators across multiple jurisdictions in terms of both notifications and investigations. Anna has a wealth of experience in multi-jurisdictional projects assisting clients with data protection compliance and advisory projects both globally and across the Asian region. Anna sits on the Asia Advisory Board and the Women Leading Privacy Board for the International Association of Privacy Professionals.

Questions

Law around the world

nortonrosefulbright.com