
MAYER | BROWN
GLOBAL PERSPECTIVES
CYBERSECURITY AND DATA PRIVACY LANDSCAPE

OUR SPEAKERS

PARTNER

ANA BRUDER

FRANKFURT +49 69 7941 1778
ABRUDER@MAYERBROWN.COM

PARTNER

GABRIELA KENNEDY

HONG KONG +852 2977-1790
GABRIELA.KENNEDY@MAYERBROWN.COM

PARTNER

OLIVER YAROS

LONDON +44 20 3130 3698
OYAROS@MAYERBROWN.COM

AGENDA

1. Europe (EU and UK)
    - Data Developments
    - Privacy Enforcement Trends
    - Cybersecurity Developments
2. Asia – Pacific
    - Evolution of Regulatory Landscape
    - Issues and Trends in Privacy
    - Key Updates in Privacy and Cyber
    - Privacy Enforcement Trends

01

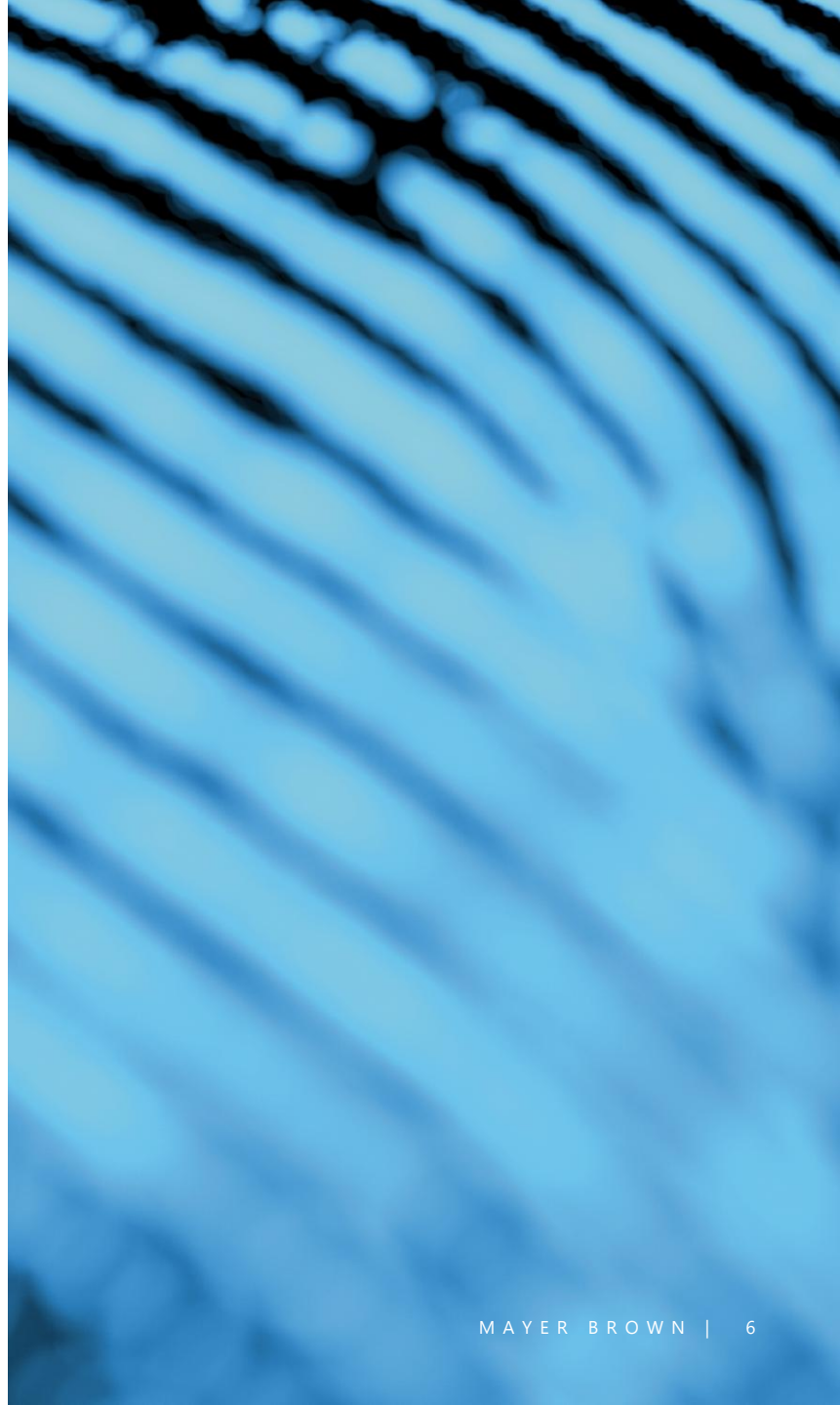
EUROPE

1a

DATA DEVELOPMENTS

EU DATA DEVELOPMENTS

- **EU Data Act** came into force on 12 September 2025
  - Obligation for data holders (e.g., **manufacturers of connected products**) to share user-generated 'product data' or 'related service data'.
    - Obligation to provide 'readily available data' and metadata with user or a third party upon user's request in force since 12 September 2025.
    - Obligation to make 'product data' or 'related service data' and metadata directly accessible to user, where feasible, from 12 Sept. 2026, relating to products placed on the market after that.
  - Obligation for **providers of data processing services** (such as cloud service providers) to facilitate customers switching to a different provider, for instance, by providing transitional services and ensuring 'functional equivalence'.
  - The European Commission has published **guidance** specifically **relating to data sharing obligations in the automotive industry** and announced that further tools to assist with implementation of the EU Data Act are in progress.
- **EU Digital Services Act** came into force in November 2022. Data aspects:
  - Prohibits platforms from using **targeted advertising** based on the use of minors' personal data.
  - Limits on the **presentation of advertising** and on use of sensitive personal data for targeted advertising, including gender, race and religion.



UK PRIVACY & DATA DEVELOPMENTS

2003
ePrivacy Regulation

2018
UK GDPR – Sits alongside EU GDPR

2023
The Online Safety Act

2024
Data Protection and Digital Information Bill

2025
Data (Use and Access) Act

1b

PRIVACY ENFORCEMENT TRENDS

EU REGULATORY TRENDS: SOCIAL MEDIA

Case 1: Irish DPC imposed a fine of €251 million on social media company because of **a data breach**.

- Arose from the exploitation by **unauthorised third parties of user tokens** on the social media platform. The breach was remedied shortly after its discovery.
- The fines were for:
  - Not including **all relevant information** in the breach notification;
  - Failing to **document the facts** relating to each breach;
  - Failing to ensure that **data protection principles were protected** in the design of processing systems; and
  - Failing to ensure that, by default, only personal data that are **necessary for specific purposes are processed.**

Case 2: Irish DPC imposed a fine of €310 million on social media company because of **data analysis** and **targeted advertising**.

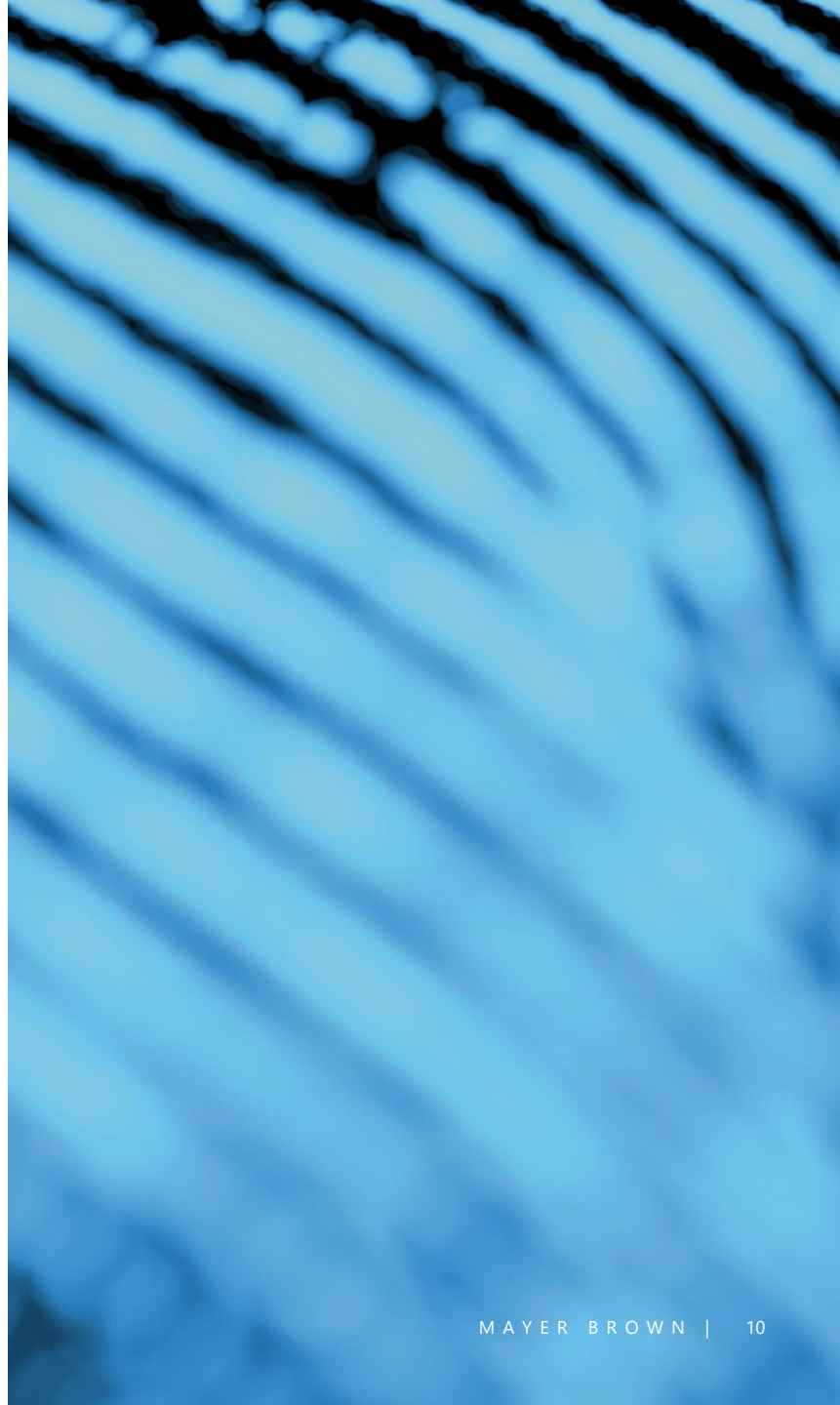
- Processed certain personal data relating to data subjects, for the purposes of behavioural analysis and target advertising without a **valid legal basis**, and in an **unfair** and **non-transparent manner**.
- **Consent was not freely given** as the wording implied that if the user did not provide consent, this would **negatively impact** their ability to interact with the platform.

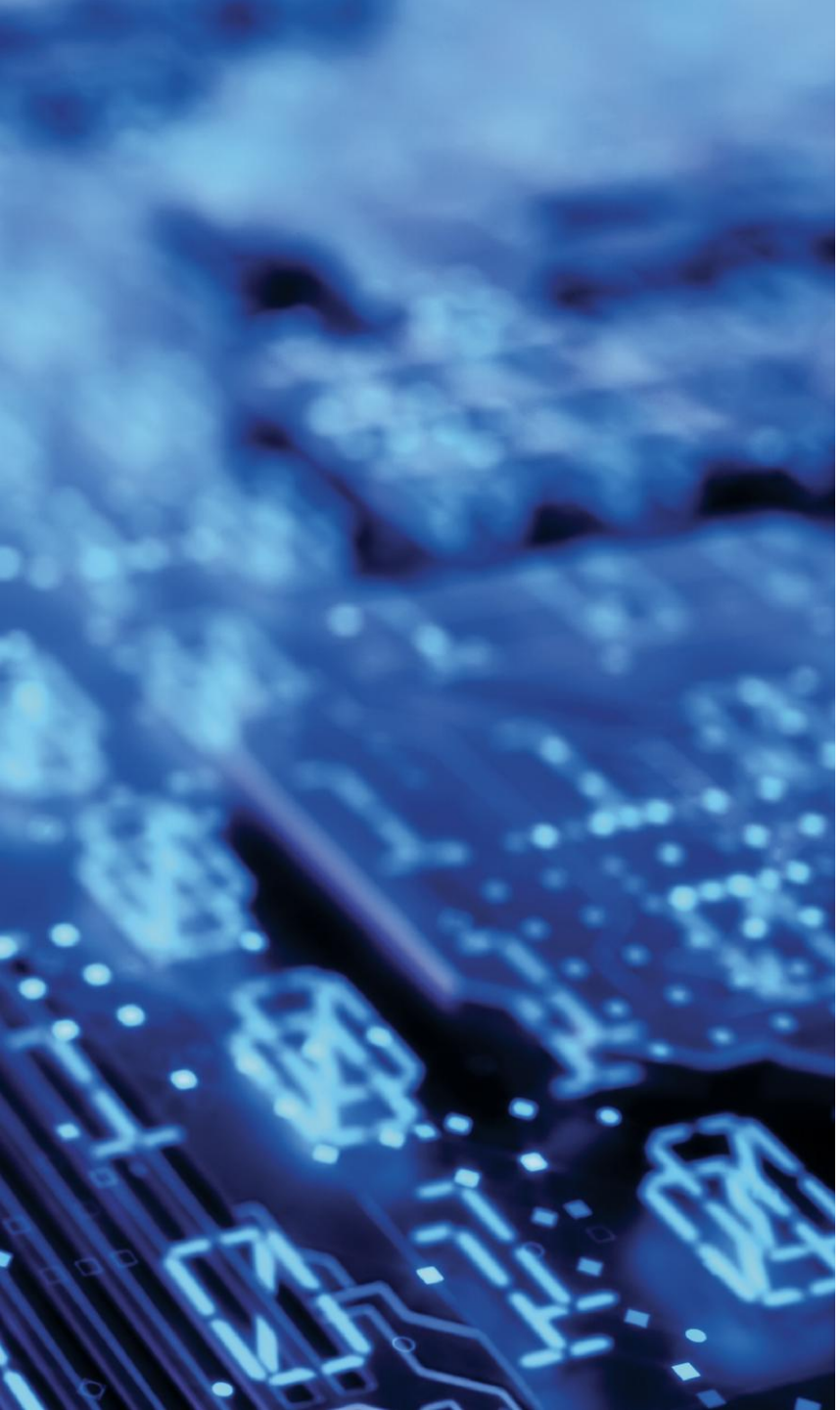
Case 3: Irish DPC imposed a fine of €530 million on another social media platform because of **transfers** of users' data to China.

- Failed to verify, guarantee and demonstrate that the **supplementary measures** and the Standard Contractual Clauses were effective to ensure that the personal data of EEA users transferred were afforded a level of protection essentially equivalent to that guaranteed within the EU.

EU NOTABLE CASES: CJEU

- **Social Media Platform -** The CJEU decided that:
  - The **indiscriminate use of all of the personal data** held by a social media company for advertising purposes, irrespective of the level of sensitivity of the data, was not proportionate
  - The fact that the data subject had made his sexuality known to the public outside of his social media, did not mean that he gave his **consent to the company processing other data** relating to his sexuality that came from outside the platform with a view to aggregating and analysing the data, in order to offer personalised advertising.
- **EDPS v SRB –** The CJEU determined personal data that has been processed so that it can **no longer be linked to a specific person** without additional information, isn't always personal data "in all cases and for every person"
  - **Pseudonymized data** shared by one party with another won't be considered personal data for the receiver of the information, provided that the recipient doesn't have the **legal means to re-identify** the individuals behind the data
  - The identifiable nature of the data subject must be **assessed at the time of collection** of the data and from the point of view of the controller



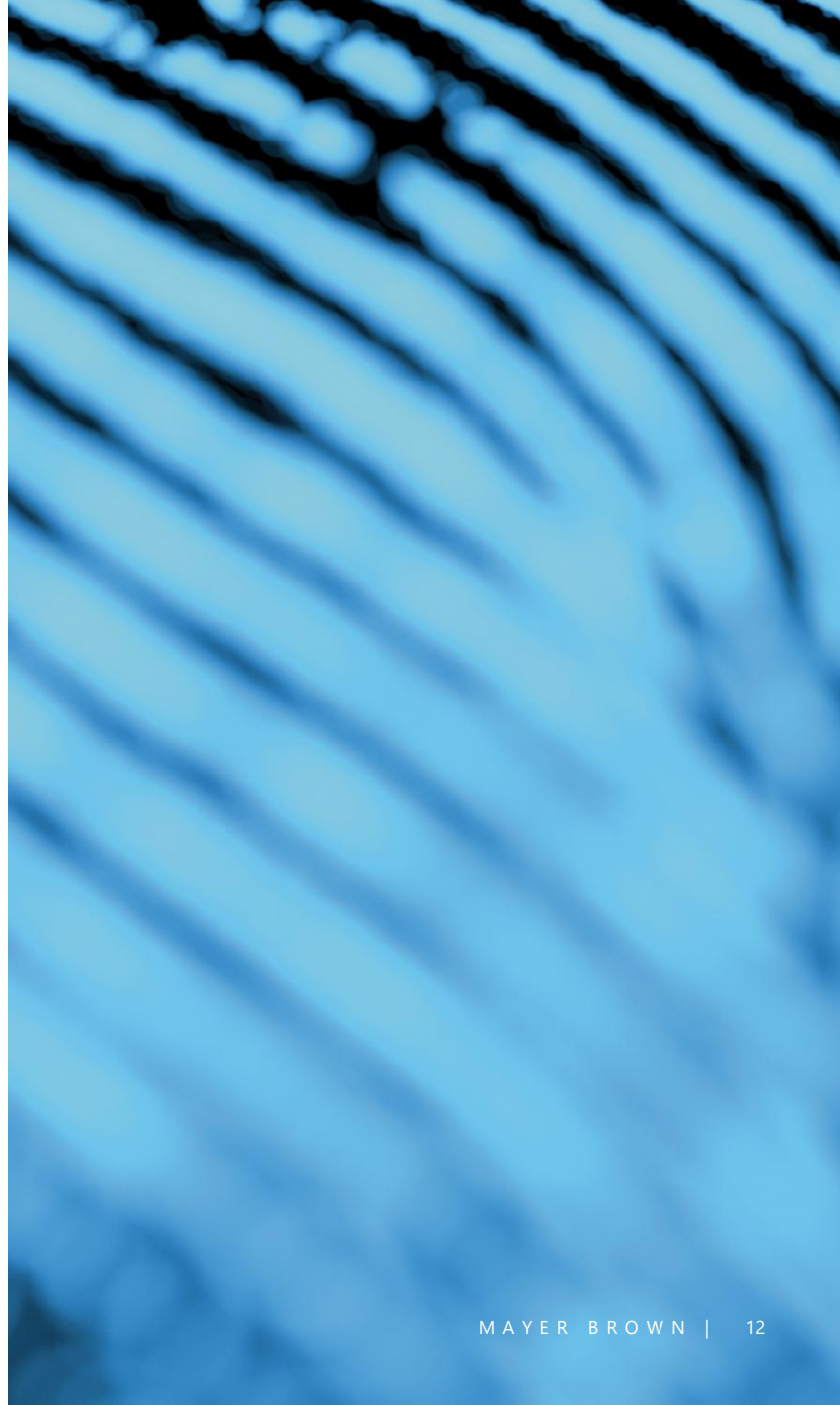


UK ICO'S ACTIONS

- **Afghan Data Breach** – In July 2025, the High Court lifted the super injunction allowing journalists and ministers discussing the case publicly.
  - The ICO stated that the government had already taken significant steps to fix the damage, and that further action by the ICO wouldn't add much
  - The ICO faced significant backlash as the lifting of the injunction exposed the failings of the ICO, namely:
    - ICO's failure to engage in any enforcement action in response to such an egregious breach; and
    - ICO did not mount any independent investigation into this matter and that it did not maintain any contemporaneous record of its decisions.
- **ICO Guidance** – the ICO has released guidance in response to cyber incidents including '**Disclosing documents to the public securely**: hidden personal information and how to avoid an accidental breach'.

UK ICO'S ACTIONS

- ICO focus on **transparency**, **legal grounds**, **data breaches**
- "Consent-or-pay" – EDBP decided against it, the ICO said it can be operated compliantly.
- High fines in the UK for data breaches (£20m is the highest fine).
- The ICO recently made a provisional decision to fine a data processor – a contractor of the NHS that suffered a data breach in 2022. The provisional fine is set at £6 million.
- The ICO continues its work on genAI – recently launched fifth call for evidence on allocating data controllership across the AI supply chain
- The ICO has recently taken action in relation to biometric data:
  - In February 2024, the ICO ordered a leisure company to stop all processing of biometric data for monitoring employees' attendance at work, as well as to destroy all biometric data that they are not legally obliged to retain.
  - On 25 June 2025 , the ICO issued its AI and biometric strategy which identified three high-risk areas:
    - **Foundation models development**– the ICO will scrutinise developers of large-scale AI systems, particularly regarding personal data protection in training processes and compliance with lawful data processing requirements.
    - **Automated decision-making**– special focus on AI use in recruitment processes and public services, with the ICO working with early adopters to establish best practices and regulatory expectations.
    - **Facial recognition technology**– specific emphasis on police force usage rather than commercial applications, with planned audits and guidance on lawful, proportionate deployment following public concerns about privacy rights.



1c

CYBER DEVELOPMENTS

NEW EU CYBER RULES

- **Cyber rules for essential and important entities**: **NIS2** started applying on 18 Oct. 2024. National laws transposing NIS2 have been adopted by 16 EU Member States. Commission Implementing Regulation adopted for providers of digital infrastructures and services.
- **Cyber rules in the financial sector**: **DORA** came into force in January 2025.
  - Substantial cybersecurity obligations applying to banks, insurance companies, investment firms and other financial entities, and service providers that are in the process of being designated as 'critical' by competent authorities.
- **Cyber rules for products with digital elements**: the **Cybersecurity Resilience Act (CRA)** entered into force in December 2024. It is set to become fully applicable in the fall of 2027, except for the reporting obligations, which will apply in September 2026.
  - Cybersecurity and vulnerability handling requirements;
  - Products with digital elements: wired or wireless products connected to the internet, including software or hardware components placed on the market separately.
    - Broad definition covers a wide range of **IoT devices**, including laptops and mobile devices, and **stand-alone software** like identity, privileged access and mobile device management software, firewalls, mobile aps, video games and desktop applications.

UK LEGAL DEVELOPMENTS

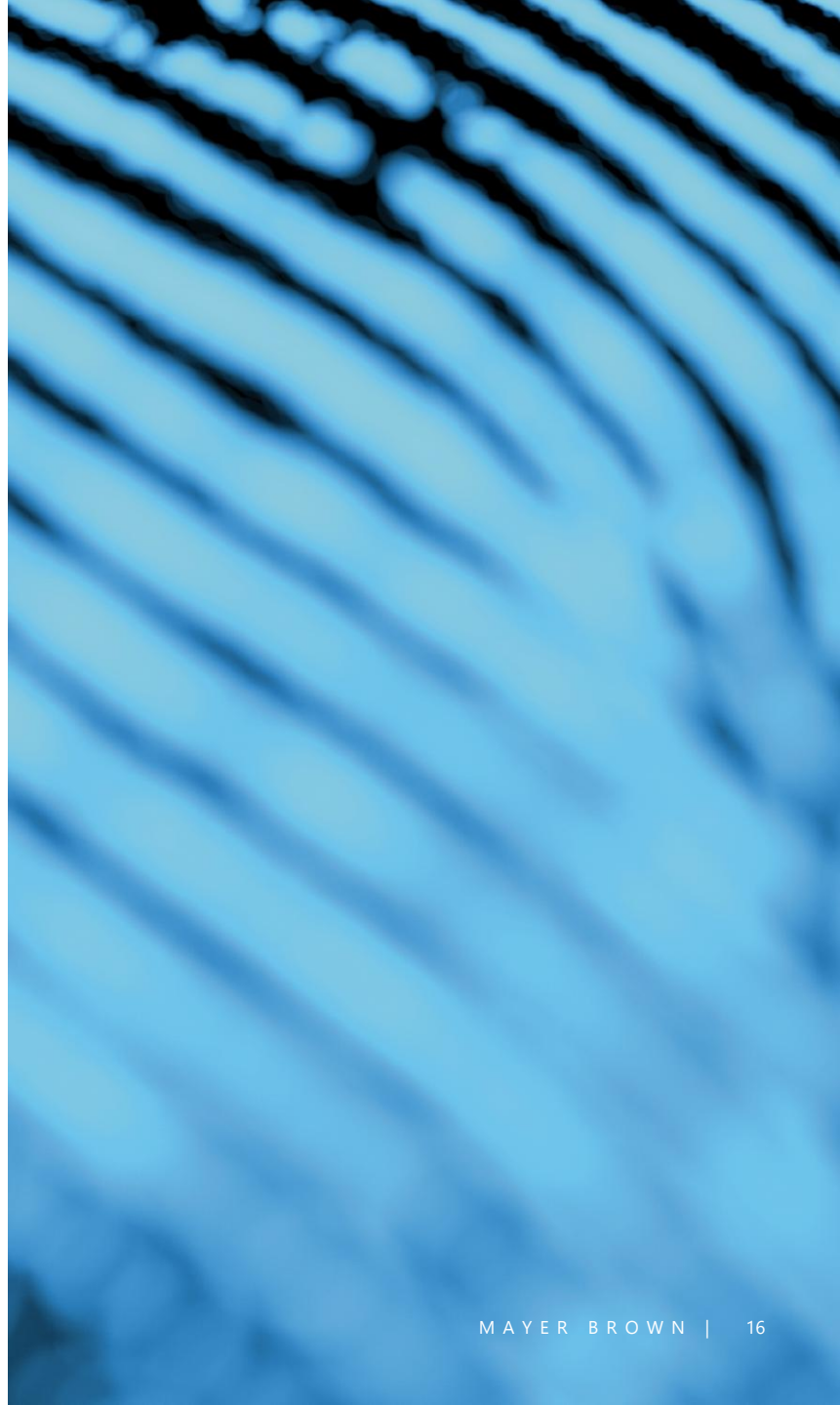
- **The Network Information Systems Regulation 2018**
  - The NIS1 Directive was transposed into UK Law as The Network and Information Systems Regulations 2018.
- **Cyber Security and Resilience Bill**.
  - Legislation aiming to increase cyber resilience of UK economy
- **ICO and the National Crime Agency (NCA) sign Memorandum of Understanding**
  - Aim to improve the UK cyber resilience by sharing information, enhancing security measures and encouraging the reporting of cyber-crimes.

UK FUTURE DEVELOPMENTS

- In research by Gartner, they predict that

  "by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021."

- The ICO identified
  - Misconfiguration is one of the top 10 security issues
    - Generative AI is a method to reduce human error and enable faster responses
  - Machine learning is likely to play a part in future mitigation strategies, as well as attack techniques
  - Attackers are targeting:
    - software development systems; and
    - open-source artefacts to compromise software supply chains



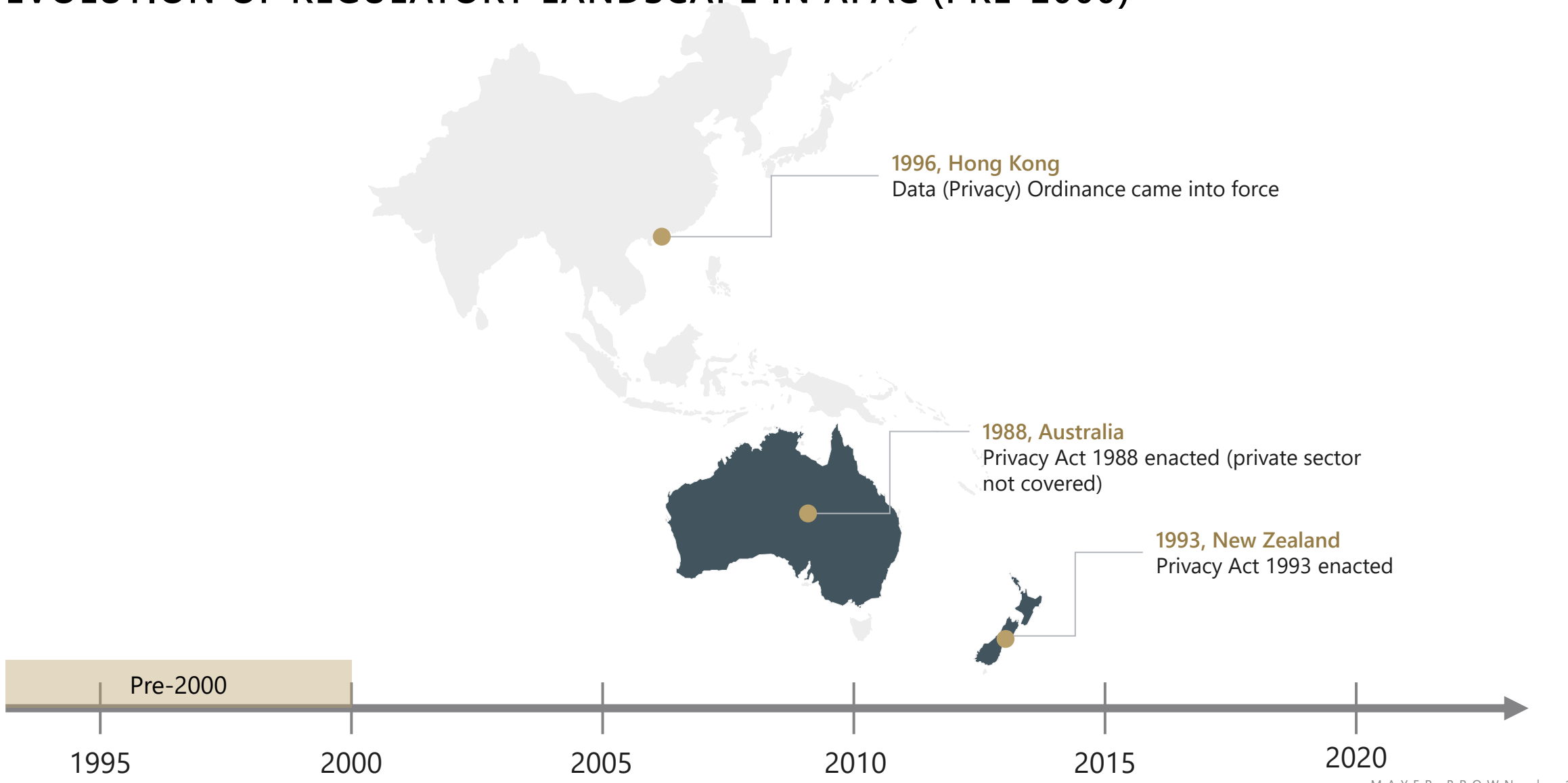
02

ASIA PACIFIC

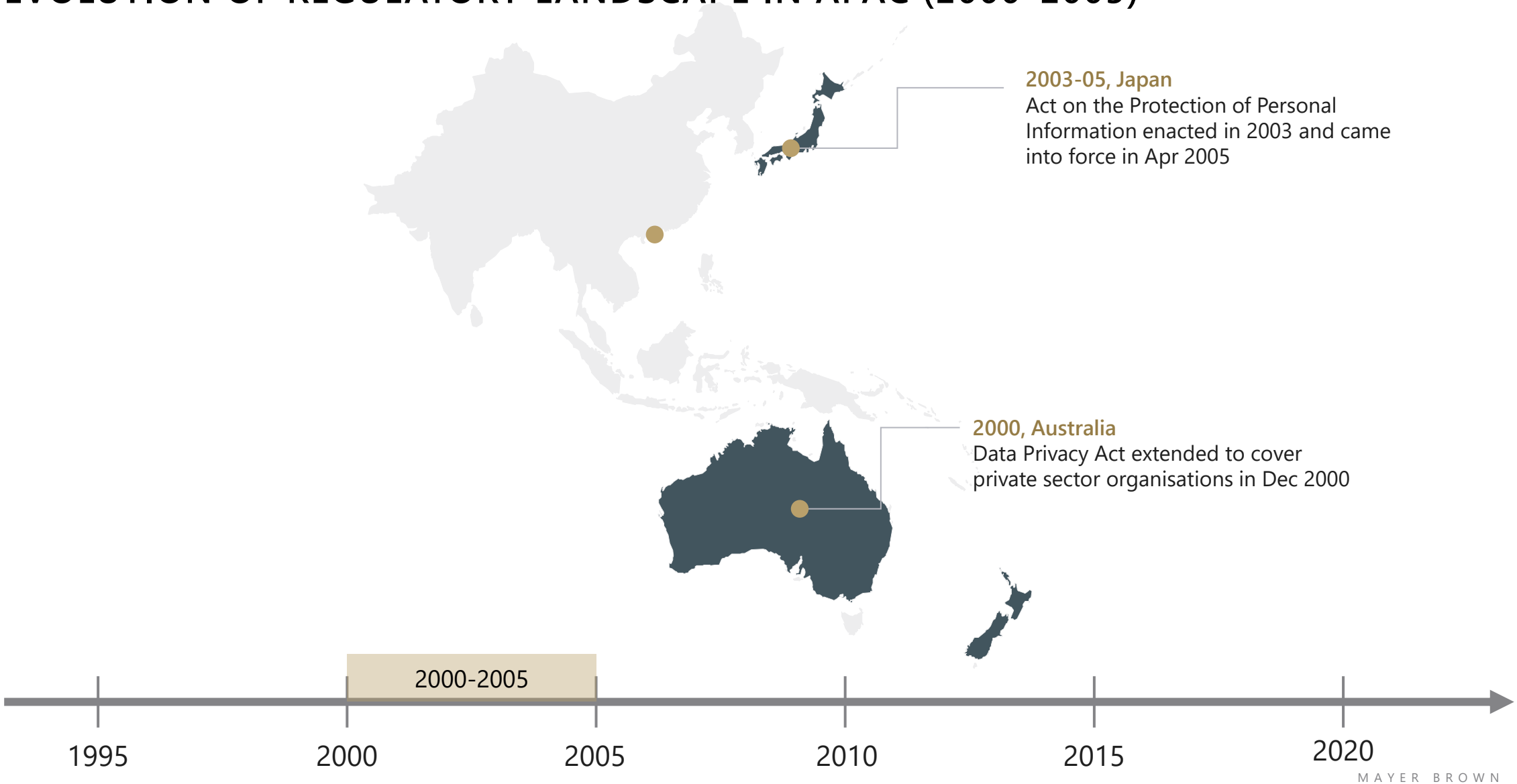
2a

EVOLUTION OF REGULATORY LANDSCAPE

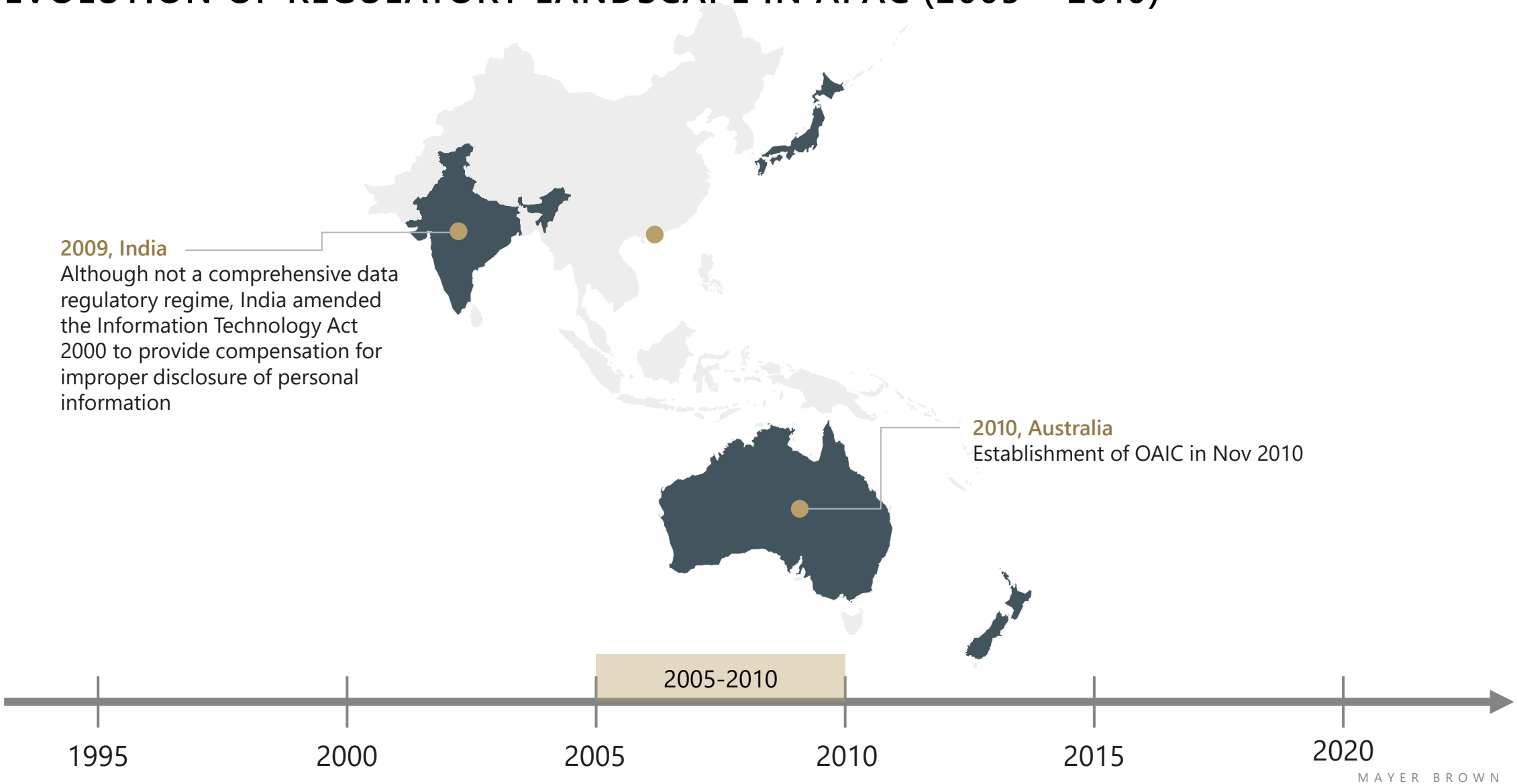
EVOLUTION OF REGULATORY LANDSCAPE IN APAC (PRE-2000)



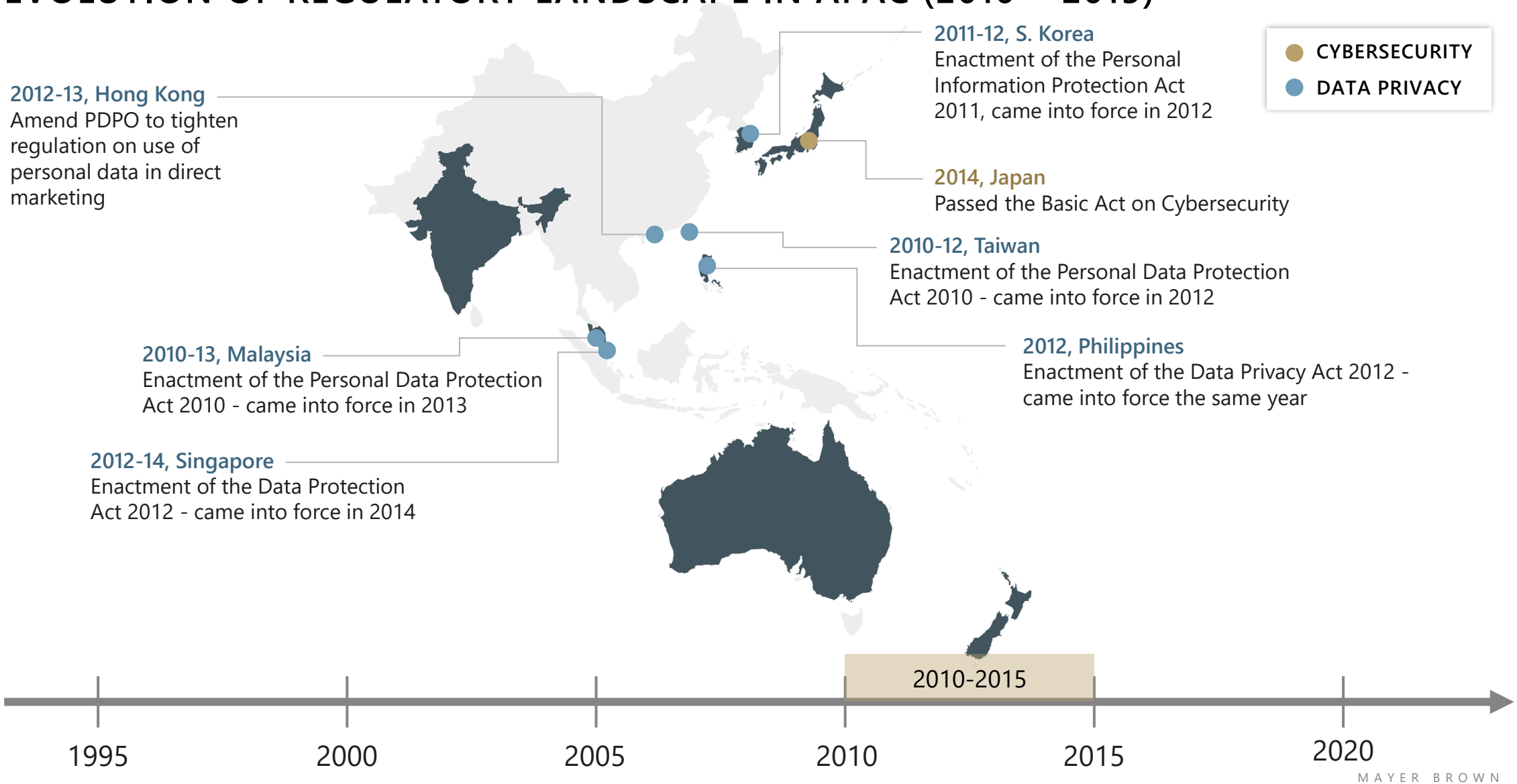
EVOLUTION OF REGULATORY LANDSCAPE IN APAC (2000-2005)



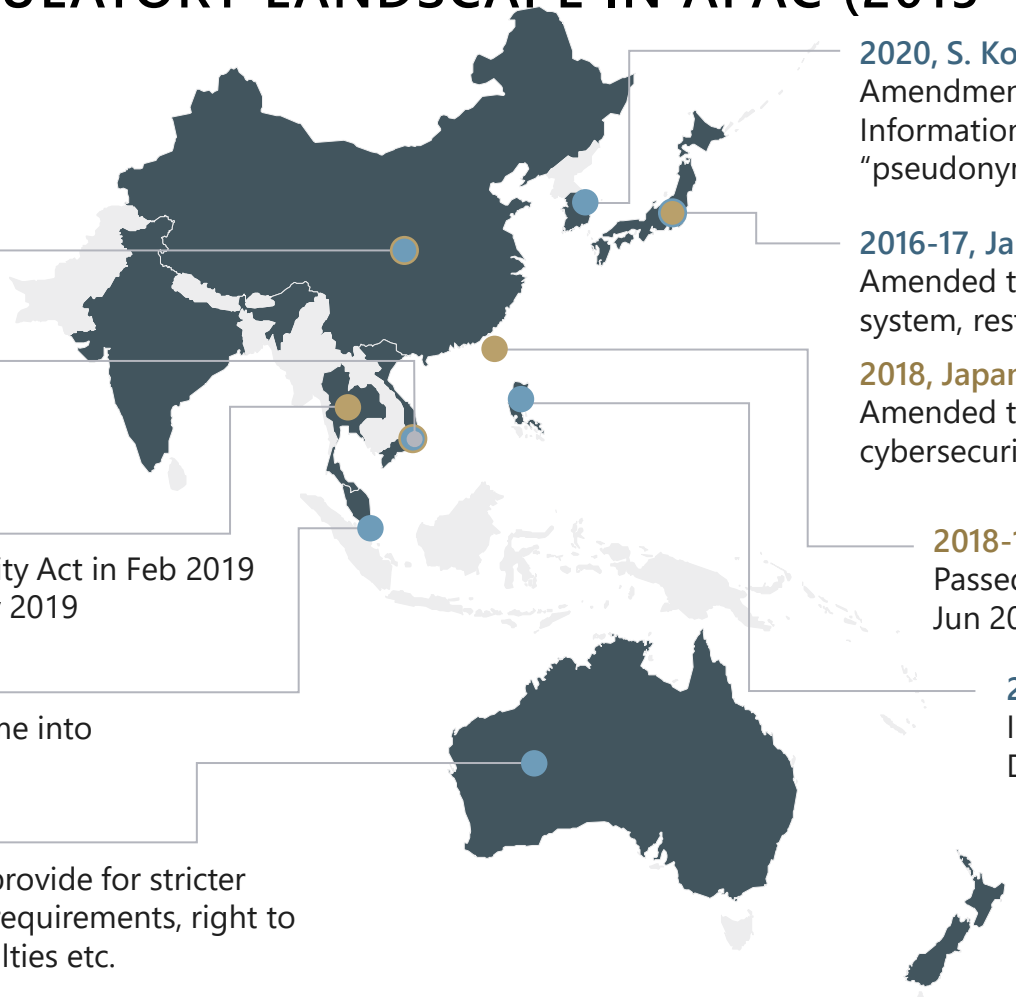
EVOLUTION OF REGULATORY LANDSCAPE IN APAC (2005 – 2010)



EVOLUTION OF REGULATORY LANDSCAPE IN APAC (2010 – 2015)



EVOLUTION OF REGULATORY LANDSCAPE IN APAC (2015 – 2020)



CYBERSECURITY
DATA PRIVACY

2017, China
The Cybersecurity Law came into force in Jun 2017, regulates both data privacy and **cybersecurity**

2019, Vietnam
Law No. 24/2018/QH14 on Cybersecurity came into force in 2019 data privacy and **cybersecurity**

2019, Thailand
Passed the Cybersecurity Act in Feb 2019 came into force in May 2019

2018, Singapore
The Cybersecurity Act came into force in Aug 2018

2018, Australia
Amended Privacy Act to provide for stricter notification and consent requirements, right to be forgotten, higher penalties etc.

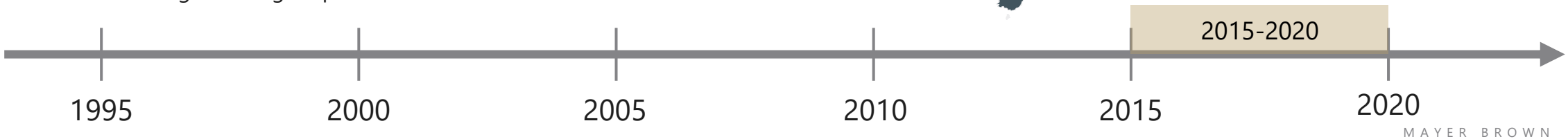
2020, S. Korea
Amendments to Personal Information Protection Act – "pseudonymised data"

2016-17, Japan
Amended the APPI – pre-emptive disclosure required for opt-out system, restriction on cross-border transfer

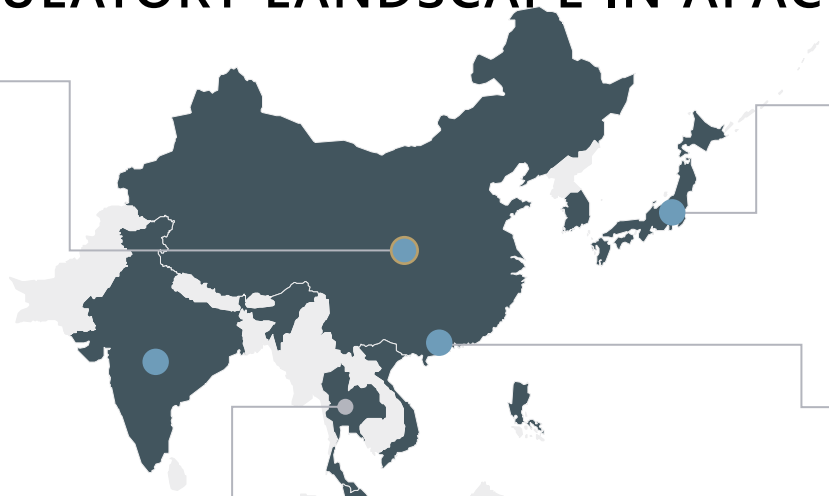
2018, Japan
Amended the Basic Act on Cybersecurity – established a cybersecurity council for info-sharing and discussions

2018-19, Taiwan
Passed the Cybersecurity Management Act in Jun 2018 which came into force in Jan 2019

2016, Philippines
Implementing Rules and Regulations of the Data Privacy Act came into force in Sept 2016



EVOLUTION OF REGULATORY LANDSCAPE IN APAC (2020 – 2022)



2021, China
Data Security Law and Personal Information Protection Law came into effect

2020, China
National Standards on Information Security Technology came into force

2022, Japan
Amendments to Act on the Protection of Personal Information came into effect – mandatory notification requirements, "pseudonymously processed information"

- CYBERSECURITY
- DATA PRIVACY

2021, Hong Kong
Amended provisions in PDPO (doxxing offences) came into effect

2022, Thailand
Personal Data Protection Act came into full force in 2022

2021 – 2022, Singapore
Personal Data Protection (Amendment) Act 2020 – mandatory breach notification, exceptions to consent, increased fines

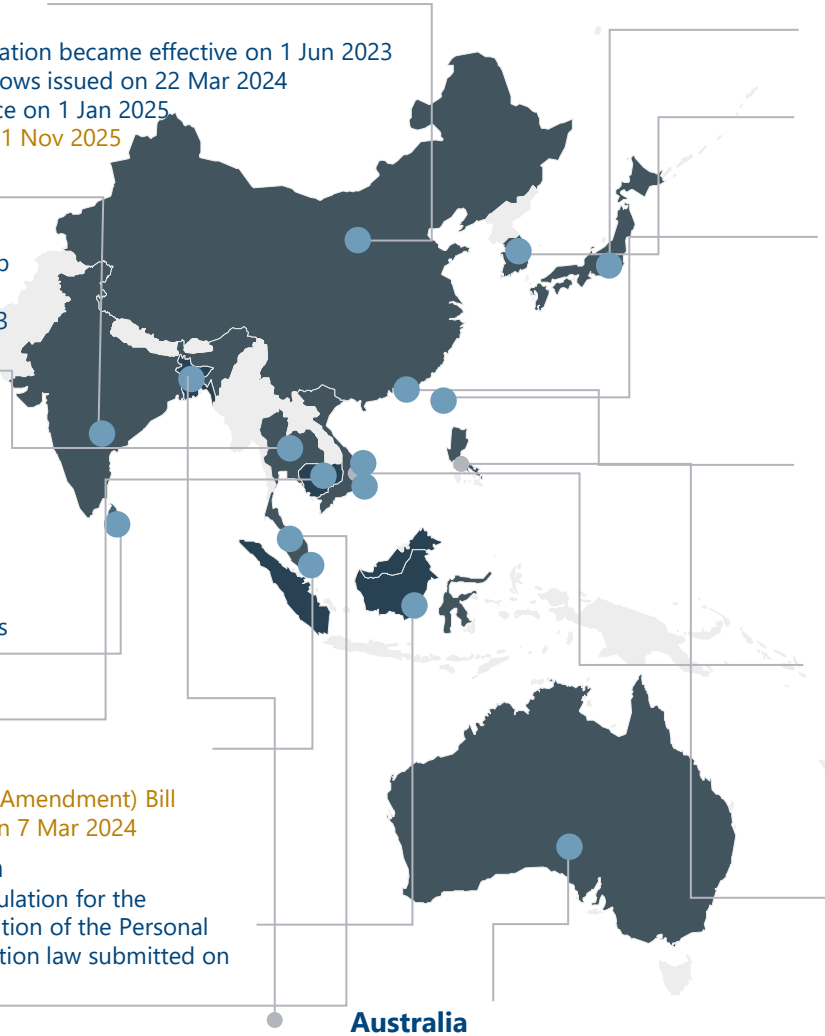
2022, Indonesia
Personal Data Protection Law came into effect

2020, New Zealand
Privacy Act 2020 came into force

1995 2000 2005 2010 2015 2020

CURRENT REGULATORY LANDSCAPE IN APAC

CYBERSECURITY
DATA PRIVACY



China
2023 – Standard Contract for Cross-Border Transfer of Personal Information became effective on 1 Jun 2023
2024 – Regulations on Promoting and Regulating Cross-Border Data Flows issued on 22 Mar 2024
2025 – Network Data Security Management Regulations came into force on 1 Jan 2025
2025 – Cybersecurity Incident Reporting Regulations effective from on 1 Nov 2025

India
2023 – Digital Personal Data Protection Act enacted on 11 Aug 2023
2024 – FAQs on Digital Personal Data Protection Act published on 8 Feb 2024
2025 – Draft Digital Personal Data Protection Rules 2025 published on 3 Jan 2025

Thailand
2023 – Notification requirements for the appointment of a data protection officer came into effect on 13 Dec 2023
2023 – Regulation on international data transfers under the Personal Data Protection Act ("**PDPA**") came into effect on 25 Dec 2023
2024 – The Royal Decree outlining exceptions to data controller obligations under the PDPA came into force on 14 Jan 2024; Personal Data Protection Act Centre set up on 29 Jan 2024
2025 – Public consultation on effectiveness of PDPA and secondary laws initiated on 20 Dec 2024

Cambodia -
Draft law on personal data protection published on 23 Jul 2025

Sri Lanka -
2023 – Parts of the Personal Data Protection Act came into effect on 17 Jul 2023 and 1 Dec 2023, other Parts to come into effect on 18 Mar 2025
2025 – The Personal Data Protection (Amendment) Bill published

Malaysia
2024 – Cyber Security Bill 2024 passed on 27 Mar 2024
2024 – Data Sharing Bill passed on 12 Dec 2024
2025 – PDPA Amendment Act came into effect on 1 Jun 2025; Data Sharing Act came into effect on 28 Apr 2025; Guidelines for Cross Border Personal Data Transfer
2025 – Cybersecurity (Exemption) Order 2025 came into effect; Online Safety Bill published on 22 May 2025

Singapore
2024 – Cyber (Amendment) Bill 2024 passed on 7 Mar 2024

Indonesia
2024 – Regulation for the Implementation of the Personal Data Protection law submitted on 3 Apr 2024

Bangladesh
2025 – Draft Personal Data Protection Ordinance published on 19 Jan 2025
2025 – Cybersecurity Ordinance came into effect on 21 May 2025

Australia
2022 – The Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022 effected on 13 Dec 2022
2024 – Privacy and Other Legislation Amendment Bill 2024 and Online Safety Amendment (Social Media Minimum Age) Bill 2024 pass on 1 Dec 2024; receive royal assent on 12 Dec 2024

Japan
2025 – The Active Cyber Defence Law passed on 16 May 2025

South Korea
2024 – Several Guidelines on personal data processing published; Amendments to the Enforcement Decree of the PIPA (PIPA Enforcement Act) took effect
2025 – Amendments to Personal Information Protection Act ("PIPA") came into effect on 2 Oct 2025

Taiwan
2023 – Amendments to Personal Data Protection Act ("**PDPA**") came into force on 2 Jun 2023; Personal Data Protection Committee ("**PDPC**") Preparatory Office set up on 5 Dec 2023
2025 – The Executive Yuan approved draft Personal Information Protection Commission Organization Act and the draft amendments to PDPA
2025 – Amendments to Cyber Security Management Act passed on 29 Aug 2025

Hong Kong
2023 – The Office of the Privacy Commissioner for Personal Data reported to the Legislative Council on specific proposed amendments to the PDPO on 23 Nov 2023
2025 – Protection of Critical Infrastructures (Computer Systems) Bill passed on 19 March 2025

Vietnam
2023 – Law on Personal Data Protection came into force on 1 Jul 2023
2024 – Data Law passed on 3 Dec 2024
2025 – Provisions of the Law on Telecommunications came into force on 1 Jan 2025; The Personal Data Protection Law (PDPL) passed on 26 June 2025; Data Law came into effect on 1 July 2025
2025 – Protection Decree on Core and Important Data came into effect in July 2025

Philippines
2023 – Circular on registration of data protection officers and data processing systems became effective 11 Jan 2023
2024 – Circular Amending 2021 Rules of Procedure released on 26 Jan 2024

New Zealand
2025 – Proposed Privacy Amendment Bill received royal assent on 23 Sep 2025

2b

ISSUES AND TRENDS IN PRIVACY

ISSUES RELATING TO DATA PRIVACY IN ASIA

A patchwork of laws

Different requirements around consent/notification and direct marketing

Mandatory vs voluntary breach notification

Cross-border data transfers

Data processors

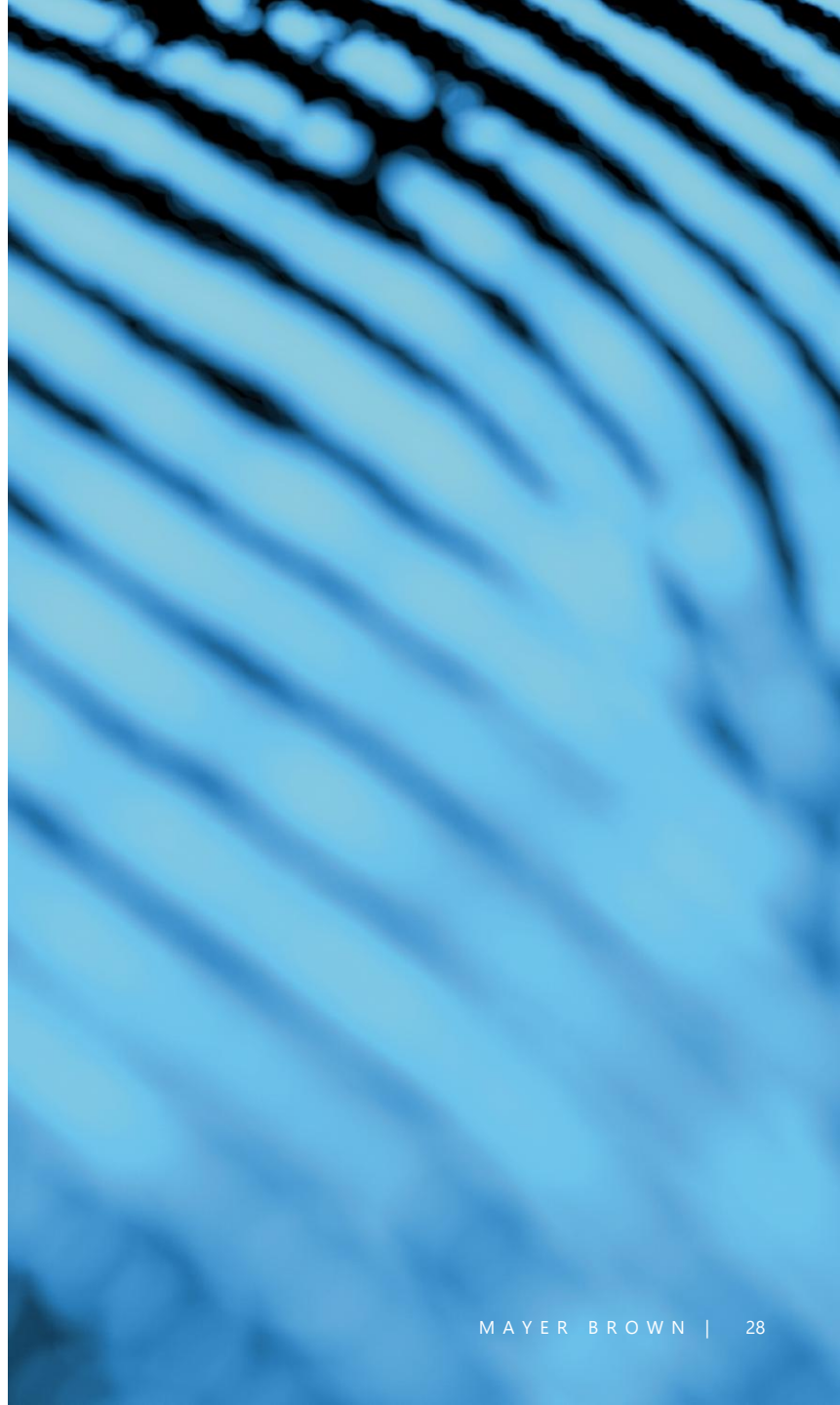
Data retention

Definition of data (sensitive data; biometric data)

Data privacy regulators

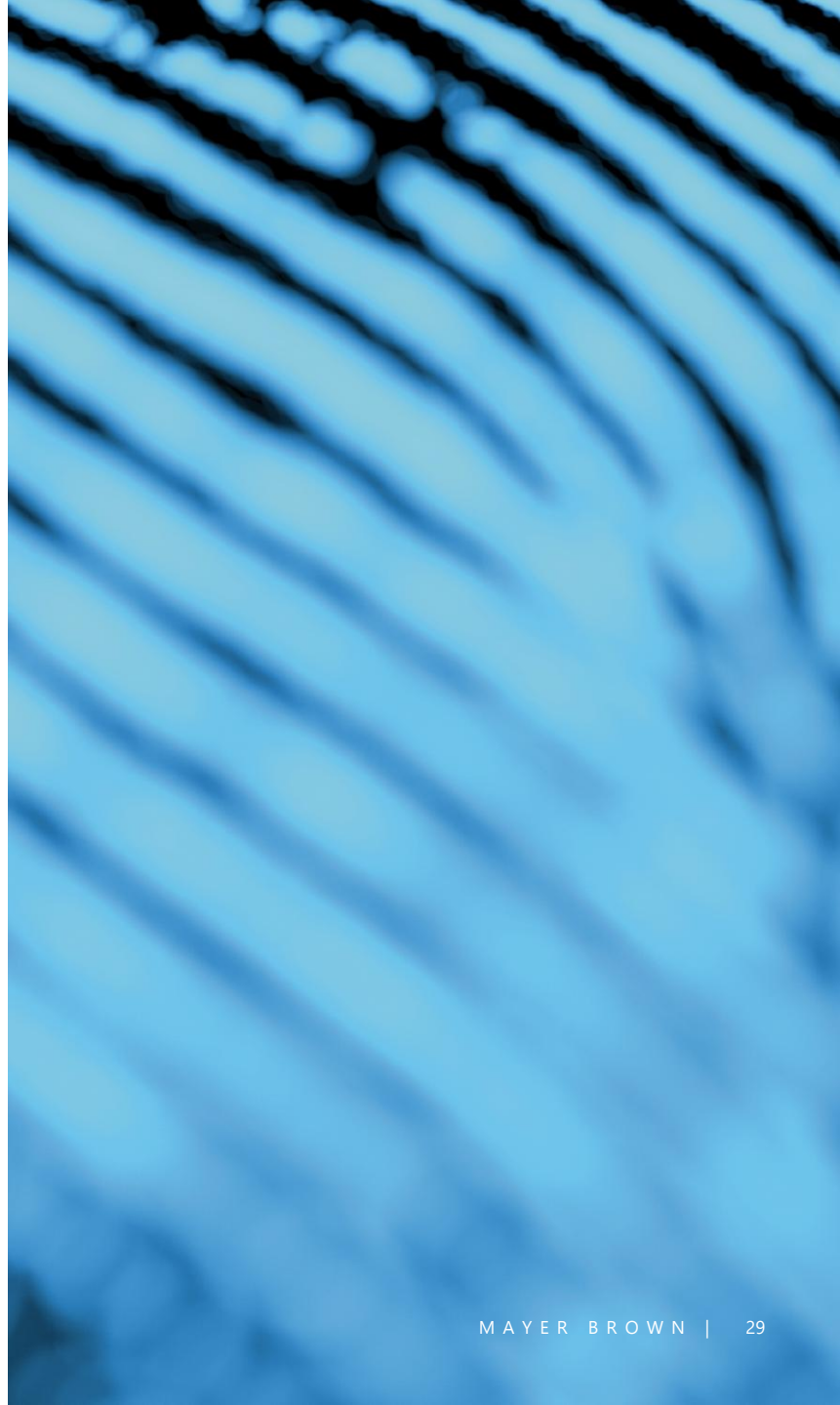
TRENDS / THEMES IN APAC

- Alignment in standards across Asia - gradual shift towards a GDPR-esque standard
- Mandatory Breach Notification
- Increasing penalties (revenue based)
  - China, Singapore, Australia, Philippines, South Korea, Vietnam
- Greater emphasis on accountability-based frameworks
- Cross-Border Transfer Restrictions
- Guidelines / Recommendations
  - Privacy by design and PIAs
  - Regular (at least annual) reviews of processes and procedures (e.g. tabletop exercises, validation of BCP plans)



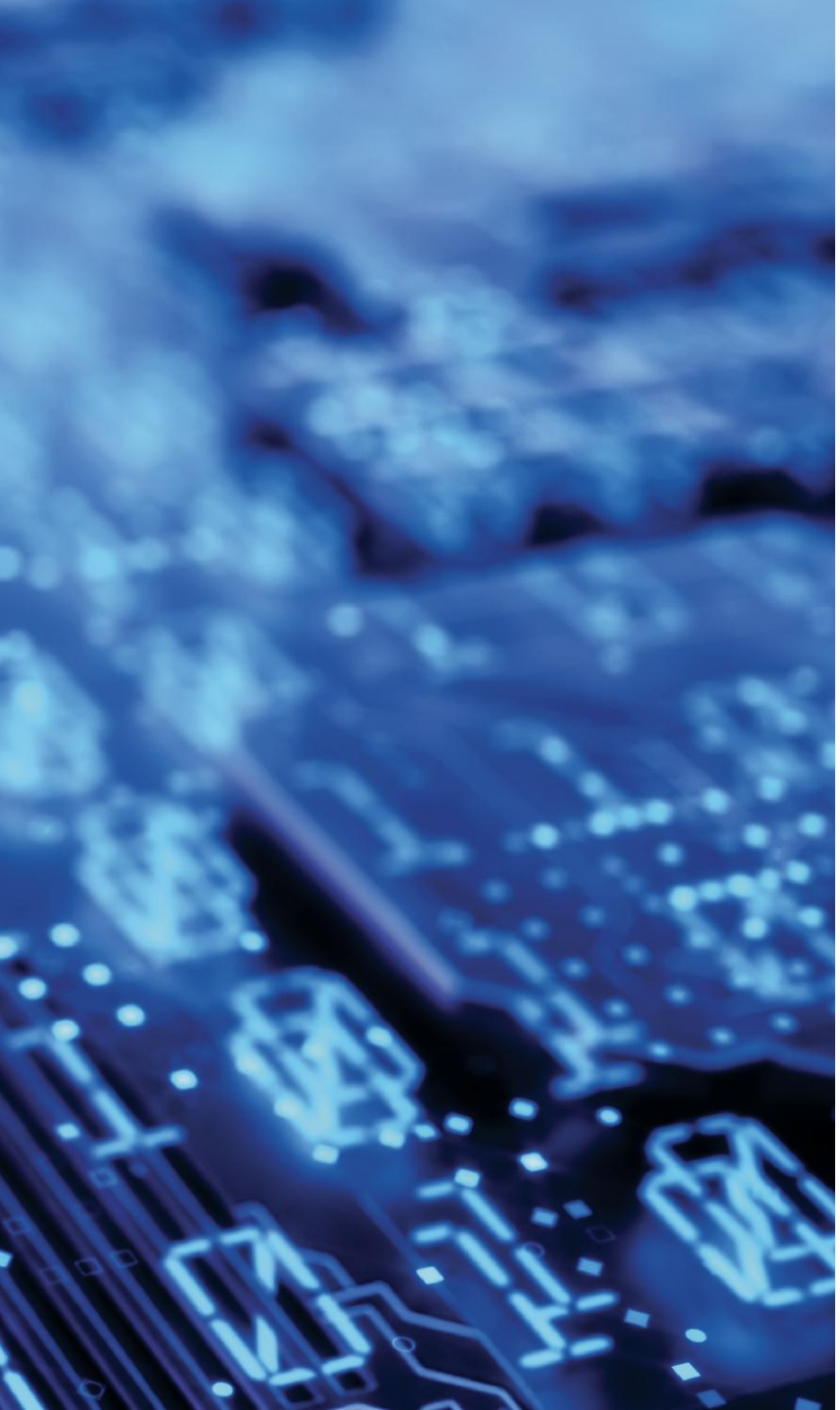
TRENDS / THEMES IN APAC

- Increased awareness of privacy rights
- Increased adoption of overarching data privacy laws – trend towards more regulation
- Increased enforcement through constant updating of laws and regulations (Hong Kong, Australia, South Korea, Singapore, Japan, New Zealand, Malaysia, etc.)
- Increased focus on cross-border data transfers
- Jurisdictions with no overarching legislation currently in force have issued draft data privacy laws (e.g. Cambodia)



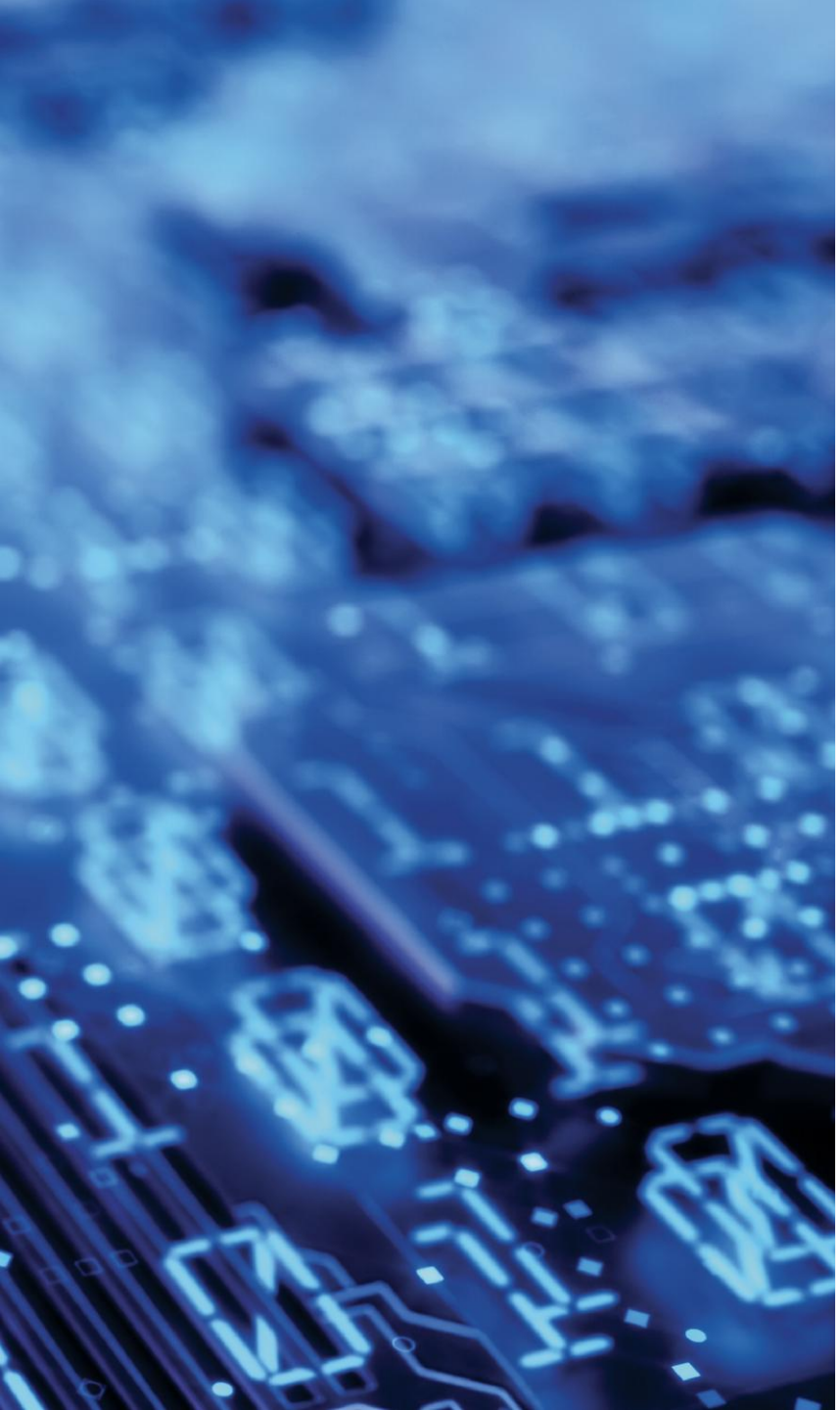
2c

KEY UPDATES IN PRIVACY AND CYBER



PRIVACY – KEY UPDATES IN ASIA IN 2025

- **China** - Network Data Security Management Regulations came into force on 1 January 2025
  - Covers all electronic data processed and generated over a computer network (including but not limited to personal information and "important data")
  - Provide more clarity on the key network data security requirements under CSL, DSL and PIPL
- **Vietnam** - Personal Data Protection Law (PDPL) passed on 26 June 2025
  - Updating the predecessor, Personal Data Protection Decree (PDPD). PDPL will come into effect on 1 January 2026
  - Maximum fines for violations of cross-border data transfer rules: 5% of revenue in previous financial year
- **Malaysia** – Phased implementation of the Personal Data Protection (Amendment) Act 2024 and official launch of the Guidelines for Cross Border Personal Data Transfer
  - Mandatory data breach notification (within 72 hours)
  - Mandatory appointment of DPO
  - Revised cross-border transfer regime to remove the previous "whitelist" approach and replace with a risk-based framework



CYBER – KEY UPDATES IN ASIA IN 2025

- **China** - Cybersecurity Incident Reporting Regulations will come into effect on 1 November 2025
  - CIIOs are required to report cyber incidents classified as "relatively serious" (or above) within 1 hour after the incident occurred. For non-CIIO operators, the required timeframe is 4 hours.
  - Obligation to notify regulators of details of ransom payments
- **China** – **DRAFT** amendments to Cybersecurity Law (CSL) issued on 28 March 2025
  - Introduce higher penalties for breaches of key cybersecurity obligations - align with DSL and PIPL
  - Network operators that proactively rectify or mitigate the adverse consequences of their violations, or first-time offenders with minor violations, may receive a lighter penalty
- **Hong Kong** - Protection of Critical Infrastructures (Computer Systems) Ordinance will come into force on 1 January 2026
  - Mandatory cyber incident notification obligations for CIOs (reporting timeframes depends on severity of incident, 12-48 hours)

2d

PRIVACY ENFORCEMENT TRENDS

OPTUS

Reuters

World Business Markets Sustainability Legal More

Australia's privacy regulator sues Optus over 2022 data breach

By **Reuters**

August 8, 2025 10:42 PM GMT+8 · Updated August 8, 2025

Aa

Australian Government
Office of the Australian Information Commissioner

Search...

News > Media centre >
Australian Information Commissioner takes civil penalty action against Optus

Australian Information Commissioner takes civil penalty action against Optus

Listen

Published: 08 August 2025

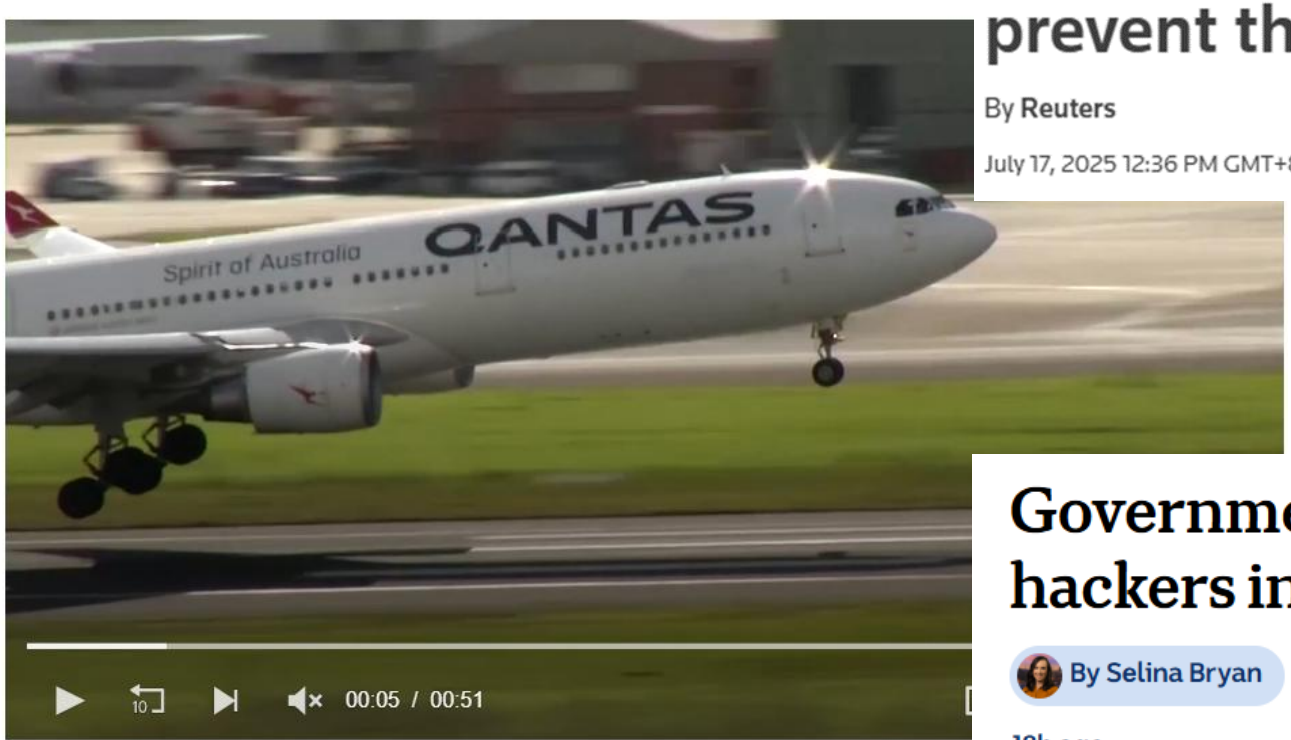
4 min read

TOP

Qantas confirms personal data of over a million customers leaked in breach

By **Reuters**

July 10, 2025 6:06 AM GMT+8 · Updated July 10, 2025



Australia's Qantas obtains court order to prevent third-party access to stolen data

By **Reuters**

July 17, 2025 12:36 PM GMT+8 · Updated July 17, 2025

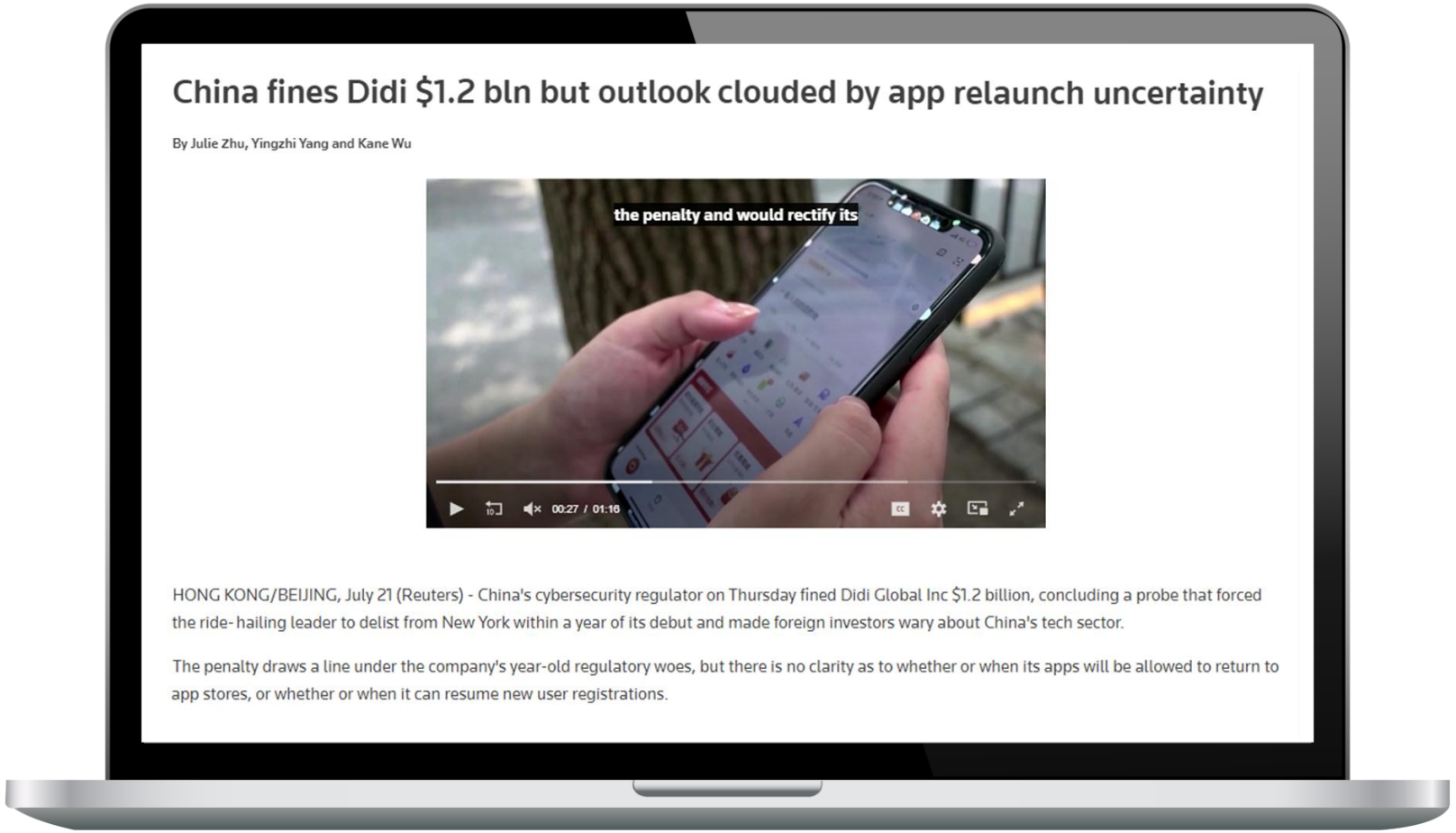
Aa

Government holds firm on not negotiating with hackers in wake of Qantas breach

By Selina Bryan | Cyber Crime | ABC NEWS

18h ago

DiDi

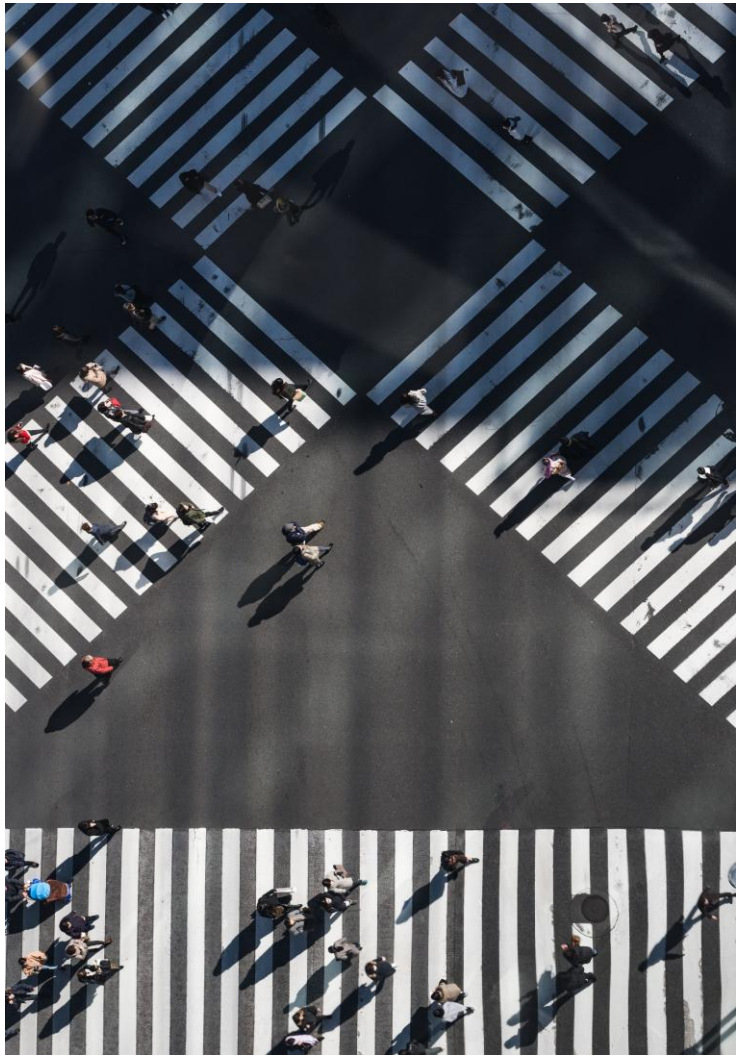


The violations included:

- Illegally collecting screenshots
- Collecting information in excess of scope necessary for its processing
- Lack of notification to customers re: collection and processing of information
- Failure to accurately and clearly explain the purpose for processing 19 types of personal information including user device information

CHINA'S FIRST DECISION ON CROSS-BORDER TRANSFER OF PERSONAL DATA UNDER PIPL

- The Guangzhou Internet Court (the "Court") in 2024 issued its first judgment involving the cross-border transfer of personal data under the PIPL
- An international hotel group was accused of unlawfully transferring the Plaintiff's personal data to various overseas entities in the course of processing a hotel reservation
- Order to provide a written apology, pay RMB 20,000 (approx. USD 2,800) in damages, and delete the Plaintiff's personal data



DISCLAIMER

These materials are provided by Mayer Brown and reflect information as of the date of presentation.

The contents are intended to provide a general guide to the subject matter only and should not be treated as a substitute for specific advice concerning individual situations.

MAYER | BROWN