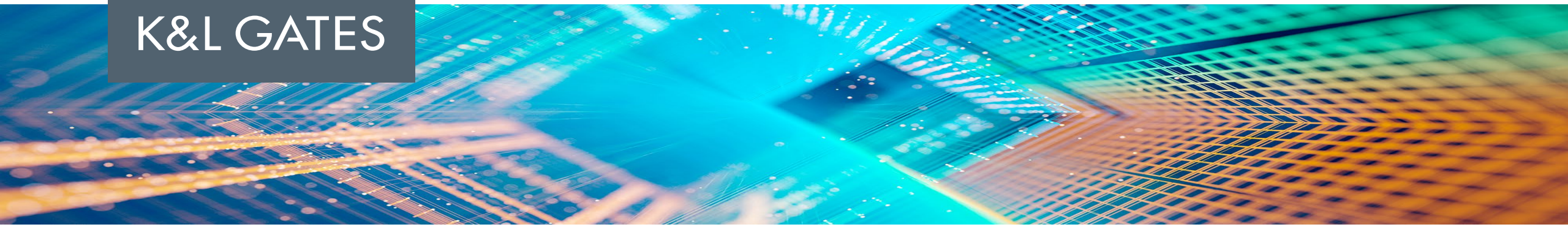
K&L GATES



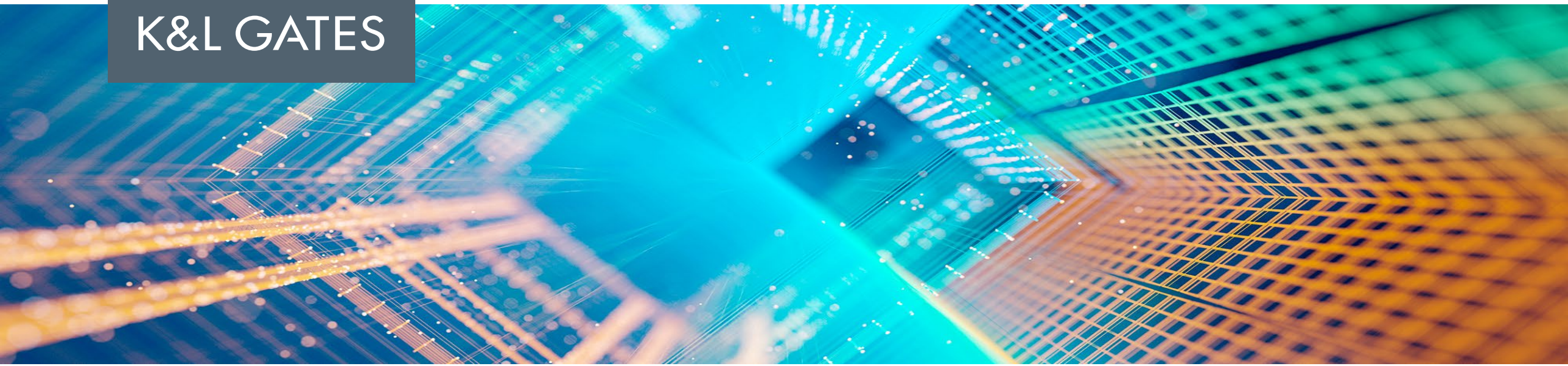
Session 2: Preparing for Privacy Law Shake-up and Staying Across Cyber Developments: Our Privacy and Cybersecurity In-Brief for 2024

Speakers: Rob Pulham, Special Counsel and Stephanie Mayhew, Lawyer
CPD Category: Substantive Law

10:00 AM – 11:00 AM (AEDT)

Everyone's lines are muted upon entry. We will open the lines up after the session for Q&A.	If you want to ask a question, use the chat icon (along the bottom of your screen) to send a message to the speakers.	This session is being recorded. The recording will be made available via the K&L Gates HUB.

K&L GATES



Wednesday 21 February 2024

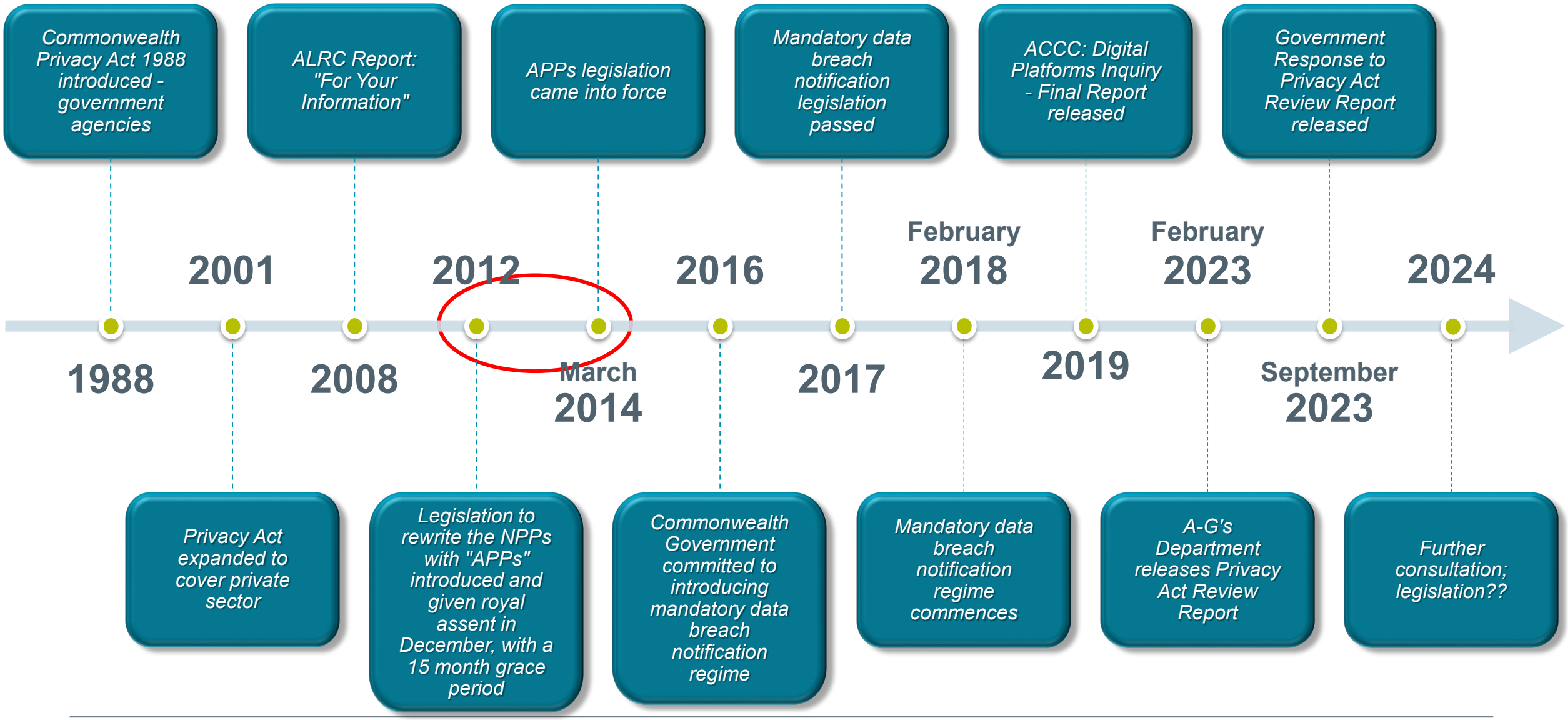
Preparing for Privacy Law Shake-up and Staying Across Cyber Developments: Our Privacy and Cybersecurity In-Brief for 2024

Rob Pulham, Special Counsel | Corporate
Stephanie Mayhew, Lawyer | Corporate

K&L GATES

Contents

Path to Reform


Commonwealth Privacy Act 1988 introduced - government agencies
ALRC Report: "For Your Information"
APPs legislation came into force
Mandatory data breach notification legislation passed
ACCC: Digital Platforms Inquiry - Final Report released
Government Response to Privacy Act Review Report released
1988
2001
2008
2012
March 2014
2016
2017
February 2018
2019
February 2023
September 2023
2024
Privacy Act expanded to cover private sector
Legislation to rewrite the NPPs with "APPs" introduced and given royal assent in December, with a 15 month grace period
Commonwealth Government committed to introducing mandatory data breach notification regime
Mandatory data breach notification regime commences
A-G's Department releases Privacy Act Review Report
Further consultation; legislation??

Path to Reform: What do we Expect to see in 2024?

- Targeted consultation – in particular on:
  - The employee records exemption; and
  - The small business exemption.
- Legislation drafted and introduced into Parliament, perhaps aiming for some ‘quick wins’ first
- Development of further guidance material by the OAIC
- If you’re interested in the detail on specific points, start with the Privacy Act Review Report which canvasses the issues in detail
- Expect further change and be patient – there may well be unexpected detours along the way

Expected Changes

Expected Changes: Employers and Small Business

Employee records exemption (Ch 7)

- To be significantly narrowed with enhanced protection for privacy sector employees:
  - Enhanced transparency;
  - More adequate security; and destroyed when not required
  - Breach notification.
- Balanced with ensuring employers have adequate flexibility, including addressing consent re sensitive information

Small business exemption (Ch 6)

- Government Response indicates agreement in-principle to removing the small business exemption
- But not until further consultation has been undertaken on the impacts on small business, to allow Government to:
  - Consider what obligations should be modified to easy the regulatory burden; and
  - Consider what support is required
- “In the shorter term”, activities posing significant privacy risks and trading in personal information should no longer be allowed to rely on the exemption

Expected Changes: Breach Response; Individual Rights

Data Breach Response	Government agrees in-principle that entities should be required to: (p 28) • notify the Information Commissioner as soon as practicable, and not later than 72 hours, after becoming aware that there are reasonable grounds to believe there has been an eligible data breach • notify individuals as soon as practicable, including providing information to individuals in phases if it is not practicable to provide the information at the same time • take reasonable steps to implement practices, procedures and systems to respond to a data breach Government agrees in-principle that entities should be required to set out the steps taken or to be taken in response to a data breach, including steps to reduce any adverse impacts on the individuals to whom the relevant information relates in their statement for an eligible data breach. Government agrees-in principle that further consultation should be undertaken on whether entities should be required to take reasonable steps to prevent or reduce the harm that is likely to arise for individuals as a result of a data breach.
Senior Privacy Role	Government agrees in-principle that entities should be required to appoint or designate a senior employee with specific responsibility for privacy (may be someone with other duties) (p 15.2)
Additional Rights for Individuals	Government agrees in-principle to introduce additional rights for individuals: • request an explanation of what personal information is held and what is being done with it through an enhanced right to access (p 18.1) • challenge the information handling practices of an entity and require the entity to justify how its information-handling practices comply with the Act (p 18.2) • require an entity to delete (or de-identify) personal information through a right to erasure (p 18.3) • request correction of online publications over which an entity has control (18.4) • require search engines to de-index certain online search results (p 18.5)

Expected Changes: Notices, 'Fair and Reasonable', ROPAs

Additional Privacy Policy Content	Privacy Policies will be required to include: • Retention periods for personal information the entity collects and holds (p 21.8) • Procedures for responding to requests to exercise individuals' rights, and (p 18.7) • Information about substantially automated decisions which have a legal or similarly significant effect on individual's rights. (p 19.1 and 19.2)
Additional Collection Notice Content	Collection Notices (APP 5) will be required to include: (p 10.2) • if the entity collects, uses or discloses personal information for a high privacy risk activity - the circumstances of that collection, use or disclosure • that the APP privacy policy contains details on how to exercise individuals' rights, and • the types of personal information that may be disclosed to overseas recipients. Collection Notices must also be clear, up-to-date, concise and understandable, and appropriate accessibility measures should also be in place. (p 10.1)
Standardised Templates	The Government has agreed in-principle to developing standardised templates and layouts for Privacy Policies and Collection Notices, with standardized terminology and icons. (p. 10.3)
'Fair and Reasonable' Test	Fundamental shift in onus of privacy compliance – away from reliance on notice and consent, and instead to require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances (an objective test to be assessed from the perspective of a reasonable person). (p 12.1 – 12.3)
PIAs for High Privacy Risk Activities	Mandatory requirement to conduct a Privacy Impact Assessment for activities with high privacy risks (before commencement) and provide to OAIC on request. (p 13.1)
Records of Processing Activities (ROPAs)	Entities must determine and record the purposes for which it will collect, use and disclose personal information at or before the time of collection, and record all secondary purposes. (p 15.1)

Expected Changes: Definitions, New Rights, New Penalties

Clarified Concepts	Government has agreed in-principle to introduce or amend definitions to cover: collection, disclosure, geolocation tracking data, de-identified, and consent.
Direct Marketing	Individuals will have the unqualified right to opt-out of receiving direct marketing, and there will be greater regulation around targeted advertising (e.g. online). However the Review Report's discussions around direct marketing and targeted advertising leave many questions to be fully answered. We also hope the Government follows through with its proposal to consider "providing clarity on what is meant by 'targeted advertising' as distinct from 'targeted content'."
Overseas Disclosures and Standard Contractual Clauses	• Government agrees a mechanism should be introduced to prescribe adequate countries with substantially similar privacy laws (p 23.2) • Government agrees in-principle to developing standard contractual clauses to allow transfers to countries not prescribed – voluntary to use and interoperable with other jurisdictions. (p 23.3)
Direct Right of Action	Government agrees in-principle that individuals should have more direct access to the courts to seek remedies for breaches of the Act through a direct right of action. (p 26.1)
Statutory Tort – Serious Invasion of Privacy	Government agrees in-principle that a statutory tort for serious invasions of privacy should be introduced, based on the model recommended by the ALRC in its Report 123. (p 27.1)
New Penalty Tiers	Government agrees to create tiers of civil penalty provisions, including: (p 25.1) • A new mid-tier civil penalty provision to cover interferences with privacy without a 'serious' element, excluding the new low-level civil penalty provision • A new low-level civil penalty provision for specific administrative breaches of the Act and APPs with attached infringement notice powers for the Information Commissioner with set penalties

How to Prepare

How to Prepare: Key Concepts

- Reform in this space is often S L O W
- Reform in this space can be unpredictable
- If you move too early, you risk:
  - Increased compliance costs between now and when reforms may ultimately enter into force;
  - Being out of step with industry peers;
  - Going further than legislation may ultimately require; and
  - Duplicating effort by having to re-assess changes you've made once the detail of legislation (once passed) becomes clearer.
- More than 20 of the proposals require further OAIC guidance

How to Prepare: What can you be Doing?

1. Know what personal information you collect and hold

2. Implement the appropriate steps to keep that information secure
3. Delete personal information you no longer need

4. Get your breach response planning sorted including:
    - Having steps in place to assess and respond efficiently.

How to Prepare: What can you be Doing?

1. Know what personal information you collect and hold and why you hold it (i.e. data inventory / ROPA as referred to in EU/UK)
2. Implement the appropriate steps to keep that information secure
3. Delete personal information you no longer need including about employees
4. Get your breach response planning sorted including:
    - Having steps in place to assess and respond efficiently; and
    - Creating and implementing a data breach response plan.
5. Improve your outward-facing compliance – Privacy Policy and Collection Notice

How to Prepare: Artefacts to Consider

Data Inventory / ROPA	Will enable: • Increased ability to respond to data breaches effectively and economically • Compliance with requirement to record processing activities • Responding appropriately to enhanced access requests and other individual rights • Underlies assessments of 'fair and reasonable' test purposes • Allows identification of automated decision making activities, for assessment of inclusion in Privacy Policy • Facilitates identification of high privacy risk activities, for undertaking PIA process and for inclusion in Collection Notices
Appoint Senior Employee with Privacy Responsibility	Will enable: • Cohesive response to privacy issues and clear accountability within the organisation • Compliance with requirement to appoint a senior employee with privacy responsibility
Data Breach Response Plan	Will enable: • More effective compliance with current obligations to take reasonable steps to secure personal information • Quicker and cheaper response to data breaches / incidents • More easily support notification within 72 hours • Allows quicker undertaking of reasonable steps to minimise potential harm to individuals • Compliance with requirement to take reasonable steps to implement practices, procedures and systems to respond to a data breach
Data Retention Policy	Will enable: • Quicker response to, and reduced loss from, data breaches • Clearer compliance with APP 11 (reasonable steps to secure personal information and to delete or de-identify once it's no longer needed) • Facilitates identification of retention periods for requirement to include them in Privacy Policy

How to Prepare: Artefacts to Consider

PIA Process	Will enable: • Entity to demonstrate reasonable steps to implement practices etc to comply with APPs (if it currently undertakes sophisticated or high risk practices with respect to personal information) • More effective consideration and mitigation of privacy risks • Compliance with requirement to undertake PIAs for high privacy risk activities
Cybersecurity Framework (e.g. NIST)	Will enable: • Compliance with APP 11 - reasonable steps to secure personal information • Reduce likelihood or frequency of data breaches and reduce severity of loss from incidents
Employee Privacy Policy and Collection Notices	Will enable: • Compliance with existing privacy obligations in Fair Work Commission's view in circumstances similar to *Lee v Superior Wood* • Clarity over ability to collect, use and disclose sensitive information and/or health information (in circumstances where other laws may apply which don't have an employee records exemption) • Compliance with new privacy obligations with respect to employee records, when the employee records exemption is narrowed
Privacy Policy and Collection Notices	Will enable: • Current compliance with APP 1 and APP 5 • Compliance with new legislation when enacted • Reduced risk of standing out for regulatory scrutiny and potential to be the target of 'low tier' civil penalties

Cyber Updates

Cyber Updates: Continued Incidents in the News

- We've seen continued reporting of data breaches in the news, including over the Christmas period:
  - Yakult, Court Services Victoria, St Vincent's Hospital.
- Clear that hackers are smarter than you'd like to give them credit for, and use inconvenient timings to increase stress and pressure on responders – no one wants to be dealing with this over the holidays!
- Application of waiver of privilege in investigation reports (Optus)
- Ongoing investigations into large scale incidents by the OAIC
- ASIC getting involved in enforcement

Cyber Updates: Resources Available

- Increased focus on assistance from Government and regulators:
  - Australian Government's 2023 – 2030 *Australian Cyber Security Strategy* (Nov 2023): https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf
  - Australian Government's *Overview of Cyber Security Obligations for Corporate Leaders*: https://www.cisc.gov.au/resources-subsite/Documents/overview-cyber-security-obligations-corporate-leaders.pdf
  - cyber.gov.au has some useful resources including on responding to ransomware: https://www.cyber.gov.au/report-and-recover/recover-from/ransomware/protect-yourself-from-ransomware and https://www.cyber.gov.au/sites/default/files/2023-03/ACSC_Ransomware_Emergency_Response_Guide_0.pdf
- Security of Critical Infrastructure regime continues to evolve

Cyber Updates: Minimising Risk

- We've presented in many of these sessions over the last 5-10 years on how to prepare for a data breach, and what to include in your Data Breach Response Plan – understand and implement this
- You can place your organisation in the best position to effectively respond to an incident by knowing what data you collect and where it is stored (undertaking a data inventory/ROPA assists with this), how it is protected (security-wise), and being ready to respond with a clear and practised data breach response plan
- Know who is in your breach response team, ensure your staff know who to report/escalate to when they identify an incident, and practice, practice, practice

Cyber Updates: Lessons Learned from Data Breaches

- Very high chance an organisation will experience a data breach at some point in time (whether notifiable or not)
- The OAIC knows that data breaches occur – no matter how well prepared you may be – but focus their investigation on how well prepared organisations are / how they respond to incidents that do arise
- Organisations have to learn from other organisation's mistakes - the OAIC will scrutinise an organisation that has made the same reported mistakes as high profile data breaches e.g. holding 10 year old information about former customers
- If an organisation's privacy practices / procedures are not robust – or they are using documentation not specific to their personal information collection and handling practices, this will become more of a problem if the organisation suffers a data breach incident. The OAIC will use non-compliance in these 'smaller areas' to be critical of the organisation
- Similar to the above point – if an organisation has particular privacy policies and procedures in place but don't actually use or refer to these, particularly in circumstances when that organisation has been breached e.g. has a data breach plan but they have no training or understanding about how to action it – this will also give rise to potential breaches of the APPs / enforcement action / penalties
- The regulators talk to each other when there is a breach / an organisation is being scrutinised over a particular issue – you therefore need a team who understands all of the potential issues / likely regulatory action to enable the organisation to be proactive about what may be coming and how best to deal with it. This includes both at a state and federal level

Contacts

Rob Pulham

Special Counsel
Melbourne
+61 3 9640 4414
Rob.Pulham@klgates.com

Stephanie Mayhew

Lawyer
Sydney
+61 2 9513 2371
Stephanie.Mayhew@klgates.com

K&L GATES