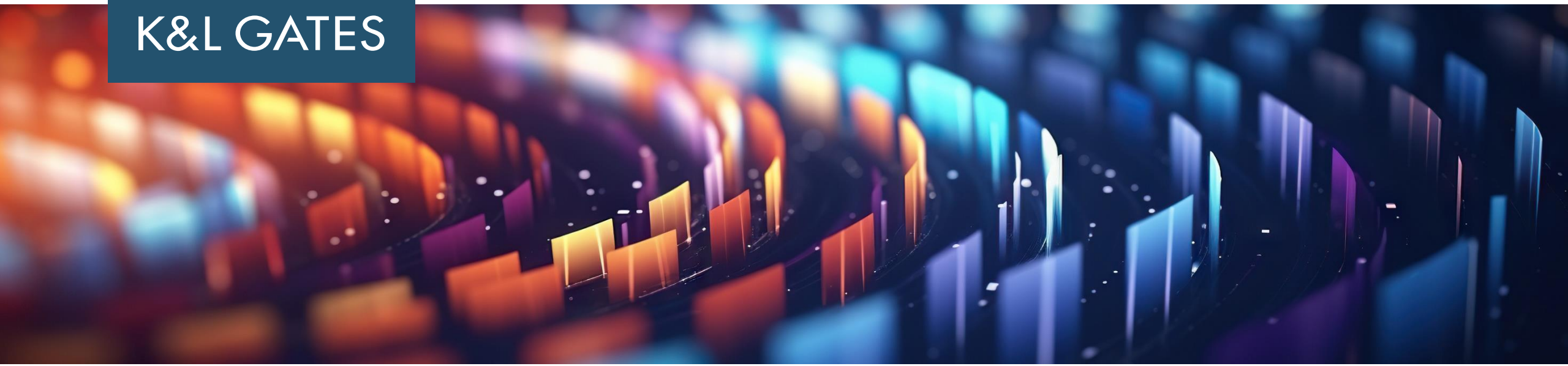
K&L GATES



Wednesday 12 February 2025

# Privacy Update – What you Need to Know

Presented by Cameron Abbott, Partner and Stephanie Mayhew, Lawyer

K&L GATES

# Contents

# Privacy Reforms – Tranche 1

# What is in Tranche 1?

| | |
|---|---|
| **Statutory Tort – Serious Invasion of Privacy** | A statutory tort for serious invasions of privacy to be introduced, based on the model recommended by the Australian Law Reform Commission in its Report 123. This will commence on a date to be proclaimed or within 6 months after commencement of the Act (10 June 2025) |
| **Additional Privacy Policy Content – Automated Decision Making** | Additional notice requirements in entities' privacy policies regarding use of automated decision-making. Some provisions relating to automated decisions have a two-year grace period, ending 10 December 2026 |
| **Making Overseas Disclosures Easier** | Introduction of an 'adequacy' recognition mechanism into APP 8, to make it easier for organisations to disclose personal information to third parties outside Australia – specific permitted countries or binding schemes will be specified for these purposes in the regulations, and disclosures to third parties in those countries or subject to those binding schemes will be permitted without the disclosing organisation being required to take additional steps to ensure the recipient complies with the APPs in relation to that information |
| **Anti-'doxxing'** | A new criminal offence for malicious release of personal data online, known as 'doxxing', with jail terms for publishing private details with the intent of causing harm, including up to seven years' imprisonment if the person or group is targeted on the basis of their race, religion, sex, sexual orientation, gender identity, intersex status, disability, nationality or national or ethnic origin |

| | |
|---|---|
| **Children's Online Privacy Code** | A definition of "child", and additional protections for minors, by paving the way for the introduction of Children's Online Privacy Code, which must be developed and registered by the Commissioner within 24 months of the law coming into force |
| **APP 11 – Security of Personal Information** | Currently, APP 11.1 requires an APP entity to take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure. The Act adds a new APP 11.3, which provides that 'reasonable steps' in APP 11.1 includes 'technical and organisational measures' – mirroring language used in the European General Data Protection Regulation |
| **New Penalty Tiers and Infringement Notice Powers** | New 'tiered' penalty provisions which will apply as soon as the law comes into force, allowing the Commissioner to issue infringement notices for specific breaches of the Australian Privacy Principles (APPs), including:<br>• Not having a privacy policy, or not having a fully compliant privacy policy<br>• Not allowing individuals to remain anonymous or use a pseudonym (unless it is impracticable to do so)<br>• Not keeping written records of certain disclosures<br>• Not complying with the direct marketing provisions in APP 7<br>• Not dealing with correction requests<br>• Not providing compliant notifications about data breaches |
| **Additional Regulatory Powers** | Additional entry, search and seizure powers to the Commissioner |
| **New Federal Court Powers** | Additional orders which may be made by the Federal Court for contraventions of the Privacy Act, including a new 'direct right' |

# What Missed the Cut?

## *Not* in This Tranche of the Reforms

- Removal of employee records exemption
- Removal of small business exemption
- Direct right of action
- 72-hour breach notification
- Specific breach preparation and response obligations
- Senior privacy role requirement
- Additional rights for individuals (DSARs)
- Overarching ‘fair and reasonable’ test
- Changes to ‘personal information’ definition
- Further Privacy Policy and Collection Notice content
- Privacy Impact Assessments for high privacy risk activities
- Requirement to keep records of all processing activities
- Changes to direct marketing requirements


AI and Privacy

# Privacy and Creating / Using AI Databases

- AI tools collect personal information in the initial creation of their databases:
  - APPs 1, 3, 5, 10, 11, 12, 13
- Organisations may use that personal information when they use the AI tools:
  - APPs 6, 7
- AI tools may collect personal information about users from sessions where the individuals interact directly with the tool:
  - APPs 1, 3, 5, 11, 12, 13

# Clearview AI

- Findings
  - Failed to take reasonable steps to implement practices, procedures and systems to ensure compliance with APPs (APP 1.2)
  - Collected sensitive information without consent (APP 3)
  - Collected personal information by unfair means (APP 3.5)
  - Failed to notify individuals of collection (APP 5)
  - Failed to take reasonable steps to ensure information was accurate (APP 10)
- Remedies
  - Cease to collect images and vectors
  - Destroy all images and vectors from individuals in Australia within 90 days
  - Confirm in writing to OAIC

# DSARs (Data Subject Access Rights)

| Current | Proposed |
| --- | --- |
| Access | Right to erasure |
| Correction | Right to object |
| Complaints | Right to explanation |
| | Right to identify source |

Creators and operators of AI tools and LLMs are not exempt from having to comply with DSARs, currently or in respect of proposed new rights.

# Tracking Pixels

# Tracking pixels

**User visits website with pixel installed**

Pixel loads and collects data (form inputs, IP address, geolocation, items viewed, cart additions, URL information) about user's activity.

Pixel transmits data to social media platform.

Social media platform matches pixel data with data about existing users of the platform.

**User leaves website and visits social media**


**User receives targeted ads and content from website on social media platform**

# Tracking Pixels: Risks and Pitfalls

### Third-party Pixel Providers

- Many third-party pixel providers offer non-negotiable terms and conditions that place the responsibility for compliance with relevant laws on the customer of the pixel service.
- Before entering into a contract with a third-party pixel provider, an organisation should carefully review the terms of the agreement to understand its obligations and ensure that the third party has appropriate processes in place to protect personal information and meet their compliance obligations.
- Organisations should also make sure they stay informed about any changes to the terms of the agreement, as these may alter the steps required to ensure compliance with privacy obligations.
- Failing to conduct thorough due diligence can lead to various privacy compliance issues and other legal risks (e.g., breach of contract if an organisation acts in a manner inconsistent with the terms and conditions of use).

### Not Going Back to 'Privacy Basics'

- Failing to address privacy compliance can lead to significant fines and reputational damage
- Common risks include:
  - Inadvertently collecting sensitive personal information through improperly configured pixels;
  - Failing to inform users about data collection practices
  - Relying on outdated or incomplete privacy policies
- Ad hoc or fragmented approaches to compliance invite regulatory actions, fines, and legal claims

# How to Comply

**Due Diligence & Data Minimisation:**

- Conduct thorough due diligence before deploying tracking pixels
- Limit data collection to the minimum necessary
- Regularly review tracking technologies—avoid "set and forget" approaches

**Consent & Sensitive Information:**

- Obtain express opt-in consent for sensitive information (e.g., health data)
- Provide clear opt-out mechanisms for direct marketing
- Implied consent through opt-out is acceptable only in limited cases

**Transparency Requirements:**

- Disclose the use of tracking pixels in privacy policies
- Explain how data will be used and shared
- Ensure third-party disclosures comply with the Australian Privacy Principles (APPs)
- Notify website visitors about tracking pixels through banners or pop-ups

**International Data Transfers:**

- Ensure compliance when sending personal information overseas
- Take steps to ensure overseas recipients comply with the APPs.
- Maintain clear documentation of international data flows

# Data Breaches and the Regulators' Enforcement Stance

# Setting the Scene

14 million customers affected by Latitude data breach

OAIC opens investigation into Optus over data breach

OAIC takes civil penalty action against Medibank

Qantas confirms technology issue caused data breach


26b records exposed in largest data leak of all time: Linkedin, Adobe, Twitter and more affected

Hackers target Binge, Dan Murphys, Guzman y Gomez, The Iconic

ASIC to target boards, execs for cyber failures

Ticketek Australia hit by data breach

Ticketmaster data breach affecting 560 million users

# There's a Breach! Who do we Notify?

| Regulator / Entity | Obligation |
|---|---|
| **OAIC** | Notify the OAIC of "eligible data breaches". Notice can be provided using OAIC online form: https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=OAIC-NDB<br>Note also: affected individuals must be notified |
| **ASIC** | Australian financial services (AFS) licensees and Australian credit licensees (credit licensees) are required to report reportable situations to ASIC via the prescribed form available in the ASIC Regulatory Portal. ASIC has recently issued new guidance on this |
| **ASX / stock exchange authorities** | Notify ASX immediately on becoming aware of any information that a reasonable person would expect to have a material effect on the price or value of an entity's securities |
| **Australian Cyber Security Centre (ACSC)** | Option to report cybercrime to ACSC online: https://www.cyber.gov.au/acsc/report |
| **Insurer** | Consider notifying your insurer of data breach even if you are not intending to make a claim or unsure if you will make a claim |

# Lessons Learned

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.

Very high chance an organisation will experience a data breach at some point in time (whether notifiable or not). The regulators know that data breaches occur – no well prepared 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. ASIC will also come after boards who are not cyber resilient and become subject to a breach.

Privacy practices / procedures that are not robust – or documentation being used is not specific to an organisation's personal information collection and handling practices, will become more of a problem if the organisation suffers a data breach incident.

# What’s Next?

# What's Next?

Current Bill (Tranche 1)

- Passed by both Houses of Parliament on 29 November 2024
- The Bill received Royal Assent on 10 December 2024 and is now in effect

Further Tranches?

- Federal election closing in
- More contentious changes left out
- The Government had largely agreed or agreed in-principle to the 116 proposals in the Privacy Act Review Report
- Likely transition period for more significant reforms seems to be around 24 months

# How to Prepare

# Lessons Learned

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

# How to Prepare: Artefacts to Consider

| | |
|---|---|
| **PIA Process** | Will enable:<br>• 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)<br>• More effective consideration and mitigation of privacy risks<br>• Compliance with requirement to undertake PIAs for high privacy risk activities |
| **Cybersecurity Framework (eg Nist)** | Will enable:<br>• Compliance with APP 11 - reasonable steps to secure personal information<br>• Reduce likelihood or frequency of data breaches and reduce severity of loss from incidents |
| **Employee Privacy Policy and Collection Notices** | Will enable:<br>• Compliance with existing privacy obligations in Fair Work Commission's view in circumstances similar to *Lee v Superior Wood*<br>• 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)<br>• Compliance with new privacy obligations with respect to employee records, when the employee records exemption is narrowed |
| **Privacy Policy and Collection Notices** | Will enable:<br>• Current compliance with APP 1 and APP 5<br>• Compliance with new legislation when enacted<br>• Reduced risk of standing out for regulatory scrutiny and potential to be the target of 'low tier' civil penalties |

# Contacts


## Cameron Abbott

Partner
Melbourne
+61 3 9640 4261
Cameron.Abbott@klgates.com



## Stephanie Mayhew

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

K&L GATES