K&L GATES

Tuesday 15 October 2024

Privacy Regulatory Reform – Ensuring Organisational Readiness

Presented by Rob Pulham, Special Counsel – K&L Gates, and Stephanie Mayhew, Lawyer – K&L Gates

K&L GATES

Contents

Introduction

Introduction

- Australia's privacy reforms in a global context
- Changing approach of our regulator
- Today's sessions:
  - Morning: Status of privacy reforms, key points for employers, and tips for marketing and gathering consents
  - After lunch: Cyber security and breach response, SOCI, and cyber risk management
  - Afternoon: New privacy rights, privacy litigation and class actions, and AI

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.
Additional Privacy Policy Content – Automated Decision Making	Additional notice requirements in entities' privacy policies regarding use of automated decision-making (the transitional provisions allow for a period of 24 months before this takes effect).
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.

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

What else is in tranche 1?

Children's Online Privacy Code	A definition of "child", and additional protections for minors, by paving the way for the introduction of a Children's Online Privacy Code, which must be developed and registered by the Commissioner within 24 months of the law coming into force.
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 of up to AU$66,000 for specific breaches of the Australian Privacy Principles (APPs), including: ▪ Not having a privacy policy, or not having a fully compliant privacy policy ▪ Not allowing individuals to remain anonymous or use a pseudonym (unless it is impracticable to do so) ▪ Not keeping written records of certain disclosures ▪ Not complying with the direct marketing provisions in APP 7 ▪ Not dealing with correction requests ▪ 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' (more on this later).

OAIC’s Enforcement Stance

A Changed Enforcement Approach?

Structural and Personnel Changes at OAIC

There are also signs of revived interest and renewed activity in this space:

- Increase in privacy job ad activity
- Potential interest from litigators and class action funders to test the new rights

- Moved back to the intended three Commissioners
- A new Privacy Commissioner, Carly Kind, who has talked up enforcement
- The Tranche 1 reforms reduce the barriers to the OAIC being able to litigate privacy breaches and enforce compliance with the Privacy Act

What’s Next?

What's Next?

Current Bill (Tranche 1)

- Remains before Parliament
- Second reading speech has been agreed to, and EM provided
- Referred to the Senate Legal and Constitutional Affairs Legislation Committee, with report due 14 November 2024
- Various crossbench amendments sought e.g. definition of 'consent', amendments to definition of 'personal information', recognition reform is 'urgent'

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

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
  - 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: • 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 (eg 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

Contacts

Cameron Abbott

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

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