2023 Australian Privacy Law Reform Proposals

In February 2023, the Commonwealth Government released its much-anticipated Australian privacy law reform proposals. Our privacy practitioners at CyberCX have distilled the 116 proposals down to key considerations for Australian businesses.

UPDATE: On 28 September 2023 the Government released its response to the proposals. We've updated this information sheet to indicate which reforms are already law ●, have been agreed to (A) and which have been agreed to in-principle (A)

Applicability

(A) The **Definition of Personal Information** may expand to include any information that *relates* to a person, which would increase the personal information holdings of a business. It may include personal device identifiers, certain IP addresses and certain metadata that are arguably not captured under current definition.

(A) **Employee Records** may be included in the definition of Personal Information where data relates to an employee, which will likely afford this data and the data subjects all the protections and rights available under the Act. Employee records are currently exempt.

(A) **Small business** (defined as having an annual turnover of $3M or less) personal information handling may be captured , either in full or for the handling of certain categories of information or for high-risk processing. Small businesses are currently exempt.

Penalties & Enforcement

(A) A **Strengthen Regulator** through an industry funded model, not unlike that of ASIC, will mean that the Privacy Commissioner will have greater funding and therefore capacity to enforce the Act.

● **Increased Penalties** which became law in December 2022 include the ability to fine up to $50m, three times the benefit obtained from a breach, or if that cannot be determined, 30% of an entity's turnover for the period of the breach (with a minimum of twelve months), per privacy breach.

● **Increased Commissioner Powers** which also became law in 2022, include a greater ability to fine and conduct investigations, including in a data breach scenario.

Individual Rights

(A) A **Right to Erasure** will be an express right to have your data destroyed in the absence of any other legal requirement for an organisation to hold an individual's personal information.

(A) A **Right to Sue for Privacy Breaches** will likely be made available when an entity is responsible for serious invasion of privacy. This would include the right to sue for data breaches, but also where a company has misused an individual's data.

(A) **Automated Decision Making** (such as an AI application processing an individual's information) will likely need to be disclosed and this will possibly work in tandem with an individual **Right to Object** to the data being used, and decisions being made, in that way. This right will likely also have broader application to data processing.

Lawful Handling

(A) A **Fair and Reasonable Test** will likely be introduced to ensure that all personal information processing by an entity is within a reasonable person's expectations and is not harmful to them.

(A) **Geo-location data** may require consent for its processing in most circumstances.

(A) **Consent** may be enhanced, with a clearer definition of what constitutes consent and new a requirement on entities to make it as easy to withdraw consent as it was to provide it. Further there will likely be enhanced protections in this domain for **Children** and other classes on individuals considered to be **Vulnerable Persons.**

(A) **Online privacy settings** may be required to follow the Privacy by Default principle

(A) Where **Collection** hasn't been directly from an individual, entities may be responsible for ensuring that it has occurred lawfully at the point of original collection or creation.

Accountability

(A) **Privacy Impact Assessments** will likely become mandatory for any personal information processing by an entity that is considered an inherently high risk to privacy, or likely to have a significant impact on the privacy of individuals e.g. the processing of biometric or other sensitive information.

(A) The **Controllers and Processers** concept as found in the GDPR, will likely be introduced to distinguish between entities that have the direct relationship with an individual and/or which are making decisions about how personal information will be processed, versus those that are processing on behalf of a controller.

(A) A **Record of Processing** will likely be required to be maintained for all personal information processing activities.

(A) A **Privacy Officer** will likely need to be appointed and will be required to be a senior position and can be someone who has other responsibilities.

Security

(A) **Mandatory Data Breach Notifications** will likely need to be made to the regulator within 72 hours of discovery of a notifiable data breach, where currently entities have 30 days to report.

(A) **Retention and Destruction** requirements will likely be enhanced to ensure entities aren't retaining data longer than is necessary.

(A) **Re-identification of De-identified Information** will likely become a criminal offence where the re-identification has been with the intention to cause harm or to obtain another illegitimate benefit.

CyberCX