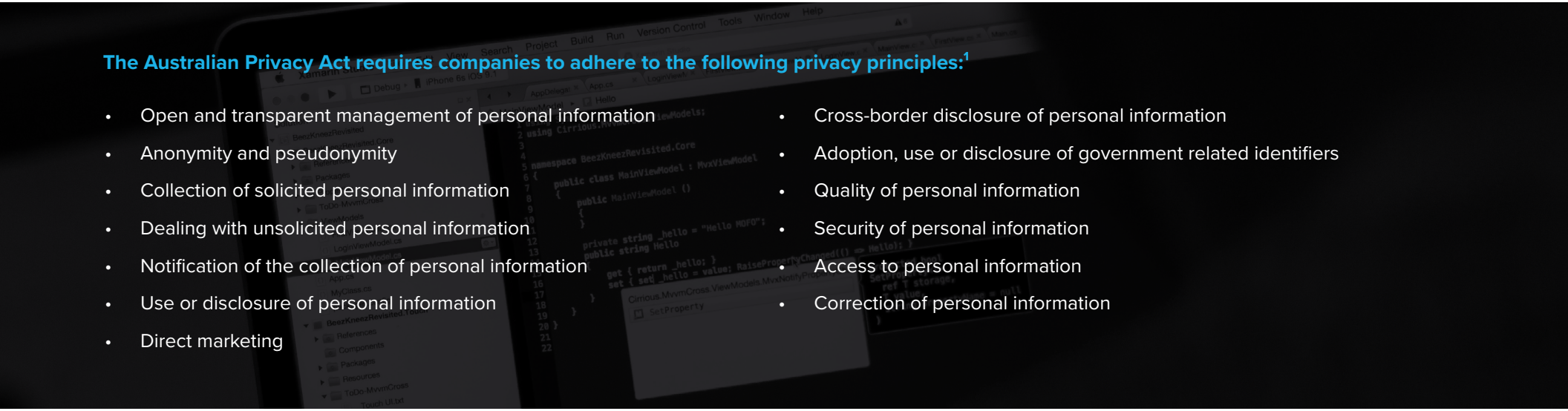
How Data Discovery Helps Businesses Stay Compliant With The Australian Privacy Act

GROUND LABS

Table of Contents

What is the Australian Privacy Act?

Australia's privacy law is sometimes referred to as the "Australian GDPR," but is formally called The Privacy Act 1988. Since its introduction in 1988, the law has undergone over 80 revisions that incorporate various updates and amendments. The Privacy Act is intended to provide a basis for how Australia regulates privacy. It also ensures individual privacy is respected.



The Australian Privacy Act requires companies to adhere to the following privacy principles:[1]

- Open and transparent management of personal information
- Anonymity and pseudonymity
- Collection of solicited personal information
- Dealing with unsolicited personal information
- Notification of the collection of personal information
- Use or disclosure of personal information
- Direct marketing
- Cross-border disclosure of personal information
- Adoption, use or disclosure of government related identifiers
- Quality of personal information
- Security of personal information
- Access to personal information
- Correction of personal information

Under the Privacy Act, Australian organizations and their coinciding privacy policies must address:

- The type of personal information being gathered and stored
- How it is found and stored
- Why the information is kept and used
- How individuals can exercise their rights with their personal information
- How to file a complaint about a company's handling of an individual's PII
- Information about overseas relocation of personal information

Australian Privacy Principles apply to any "APP entity." APP entities include government agencies in Australia, Australia Capital Territory, and Norfolk Island, organizations, and private businesses that have an annual turnover of more than $3 million.[2] Most Australian states and territories also have their own data protection legislation applicable to their residents, businesses, and other types of organizations.

SECTION 2

Consequences of Noncompliance

Direct Financial Consequences

Companies that violate the Australian Privacy Act can incur high fines. **To determine the maximum potential fine for a violation of the law, the Australian court looks at the following three numbers, and chooses whichever is the highest:**[3]

AUD $10,000,000

3 times the value of any benefit obtained from the breach

10% of the total turnover of the organization during the 12 months leading up to the end of the month when the breach occurred

No company is immune to these fines; there have been many high-profile cases of businesses that failed to comply with the Australian Privacy Act. For example, a judge recently ruled that Uber violated the Privacy Act when it failed to protect personal data from over 1 million Australian customers and drivers during a data breach in 2016.[4]

Customer Trust

The consequences of a data breach extend beyond the direct fines as well — loss of customer trust and lost business are also significant repercussions. A Privacy Act fine in itself might seem small and be manageable for an organization, but losing your customers' trust can have a devastating impact on your brand and shareholder value. In 2020, the average cost due to business loss from a data breach was $1.52 million — an amount that can have a significant impact on a company's bottom line.[5]

Common Compliance Challenges

Although Australian Privacy Act regulations have been in place for years, many companies are still facing challenges when trying to maintain compliance.

Misunderstanding Where Data is Stored and Processed

Many organizations misunderstand the amount of personal data they store and collect. They assume that all of their customers' PII data is stored in one or two databases, but this assumption is typically incorrect. In fact, companies often unknowingly store data in a myriad of locations. As a result, these companies draw conclusions and establish policies based on inaccurate assumptions around what they think their data storage should be rather than how it actually is processed and stored.

Companies often unknowingly store PII in many locations, including:


Cloud Storage Providers


Databases and Servers


Email


Workstations

COVID-19 Challenges

Due to COVID-19, throughout 2020 and 2021, more employees have been working from home. The sudden shift to remote work has left businesses vulnerable to increased risk of data breaches and loss, making it harder to stay compliant with the Australian Privacy Act.

Some circumstances that can put businesses at risk of breaking their compliance include when employees:[6]

- Process, store, or send information through inadequately secured personal devices (e.g. personal mobile phones) or on unsecured Wi-Fi networks
- Transfer documents and data carriers from the office to their homes
- Use tools that do not provide adequate data protection (e.g. unsecured messaging apps)

SECTION 4

Data Discovery: The First Step in Achieving Compliance

Organizations should never take a “wait-and-see” approach when it comes to compliance: they need to be proactive. The first step in achieving proactive compliance is to develop a baseline understanding of what data your organization has and where it resides: this is a process known as data discovery.

With data discovery from Ground Labs, you can start identifying and guarding the PII of your Australian consumers and ensure compliance with Australian data protection laws.

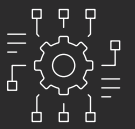
SECTION 5

Data Discovery: The First Step in Achieving Compliance

Scan for over 300 different types of structured and unstructured data including pre-configured, Australian-specific PII patterns.

Demonstrate Australian Privacy Act compliance with custom reporting and analytics available in Enterprise Recon.

Accurately map data across networks, servers, and platforms to keep tabs on PII and more easily respond to consumer requests.



Easily build custom data types and search platforms to locate and remediate unique data types to address your organization’s unique Australian Data Privacy needs.

Search within both structured and unstructured data sources including files, databases, emails, cloud, big data and more.

Reduce the overall time and investment required to reach and uphold PII compliance, even as regulations change over time.

Search across the entire organization with support for Windows, macOS, Linux, FreeBSD, Solaris, IBM AIX and much more.

Execute a proactive approach to data security - as opposed to a reactive approach that relies on damage control post-breach - to build a stronger foundation of trust within your organization.

SECTION 6

Establishing Ongoing Widespread Compliance

Compliance regulations are constantly changing, which means that compliance is not a one-time checkmark, but an ongoing obligation. The Australian Privacy Act has been updated countless times since it was established in 1988. And organizations have many other regional and industry-specific privacy laws to contend with. In fact, Gartner predicts that by 2023, 65% of the world population's personal data will be protected by various privacy regulations.[7]

With Enterprise Recon, organizations can keep up with these ongoing compliance requirements. Enterprise Recon helps companies create an inventory of sensitive data, providing ongoing data surveillance around the clock via the Enterprise Recon dashboard.

SECTION 7

Conclusion

Ongoing compliance with the Australian Privacy Act is critical for organizations today because failing to comply with the law can lead to hefty fines and significant customer loss. Privacy laws are constantly evolving, highlighting the importance of keeping up with all relevant regulations around the globe. Adapting to regulations in real-time will not cut it; your team needs to build a system that can handle these changes as they happen. The first step to preparing for ongoing compliance is data discovery.

Are you ready to get your organization better prepared to achieve Privacy Act compliance? Book a demo with a member of the Ground Labs team by visiting: https://calendly.com/ground-labs-global-sales-team.

CITATION

[1] "Australian Privacy Principles quick reference," Office of the Australian Information Commissioner, https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-quick-reference/.

[2] "Chapter B: Key concepts," Office of the Australian Information Commissioner, https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts/.

[3] "Chapter 6: Civil penalties — serious or repeated interference with privacy and other penalty provisions," Office of the Australian Information Commissioner, June 2020, https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-6-civil-penalties/.

[4] Asha Barbaschow, "Uber found to have interfered with privacy of over 1 million Australians," ZDNet, July 23, 2021, https://www.zdnet.com/article/uber-found-to-have-interfered-with-privacy-of-over-1-million-australians/.

[5] "Cost of a Data Breach Report," IBM, 2020, https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf.

[6] Ewelina Witek, "GDPR: How to make your business more resilient against data protection breaches in light of the COVID-19 crisis?" Deloitte, March 2020, https://www2.deloitte.com/ce/en/pages/about-deloitte/articles/how-to-make-your-business-more-resilient-against-data-protection-breaches-during-COVID-19.html.

[7] "Gartner Says By 2023, 65% of the World's Population Will Have Its Personal Data Covered Under Modern Privacy Regulations," Gartner, September 14, 2020, https://www.gartner.com/en/newsroom/press-releases/2020-09-14-gartner-says-by-2023--65--of-the-world-s-population-w.