A GLOBAL ROADMAP TO PERSONAL DATA PROTECTION

Asia Pacific, Europe & USA

First Edition

MERITAS®
LAW FIRMS WORLDWIDE

A GLOBAL ROADMAP TO PERSONAL DATA PROTECTION

Asia Pacific, Europe & USA

Dennis Unkovic, Editor

du@muslaw.com
Tel: +1-412-456-2833

Meyer, Unkovic & Scott LLP
www.muslaw.com

Not so long ago, "data protection" meant a locked filing cabinet and a good shredder. No longer. In a single generation, protecting data went from safeguarding documents to securing information of almost every kind, both tangible and in electronic form. Although everyone understands what it means to protect a hard copy document, it is much harder to conceptualize protecting intangible information. To make matters worse, a data breach today can cause far more serious consequences than in years past. To cite just one example, the improper disclosure of one's personal data can easily result in identity theft, with the victim often left unaware of the crime until it is far too late to stop it.

With the endless march of technology and an increasingly connected world, protecting personal data is clearly more important than ever. In response, governments around the world have focused on enacting legislation to keep up with the fast pace of change. The EU's recent implementation of the General Data Protection Regulation (GDPR) is just the latest development in this crucial area of law. Outside the EU, however, there is little uniformity in how different regions and countries protect personal data. To help make sense of this, Meritas® has produced this guide by leveraging its top quality member firms from around the world, specifically our firms in Asia Pacific, Europe and the USA. The guide employs a straightforward question-and-answer format to be as simple and as easy to use as possible. The authors hope that this guide will provide readers with a convenient and practical starting point to understand a complicated yet vitally important subject to businesses everywhere.

Special thanks go out to Meritas® Board Member Yao Rao (China), who was the inspiration behind this publication, as well as to Meritas® Board Member Darcy Kishida (Japan) and Eliza Tan (Meritas® Asia Regional Representative), who provided crucial support. Without their hard work and dedication, this global look at the critical issue of Data Privacy would not have been published.

ABOUT MERITAS®

Founded in 1990, Meritas® is the premier global alliance of independent law firms working collaboratively to provide businesses with qualified legal expertise. Our market-leading member firms offer a full range of high-quality, specialized legal services, allowing you to confidently conduct business anywhere in the world.

As an invitation-only alliance, Meritas® firms must adhere to our uncompromising service standards to retain membership status. Unlike any other network or law firm, Meritas® collects peer-driven reviews for each referral, and has for more than 25 years.

7,500+ EXPERIENCED LAWYERS

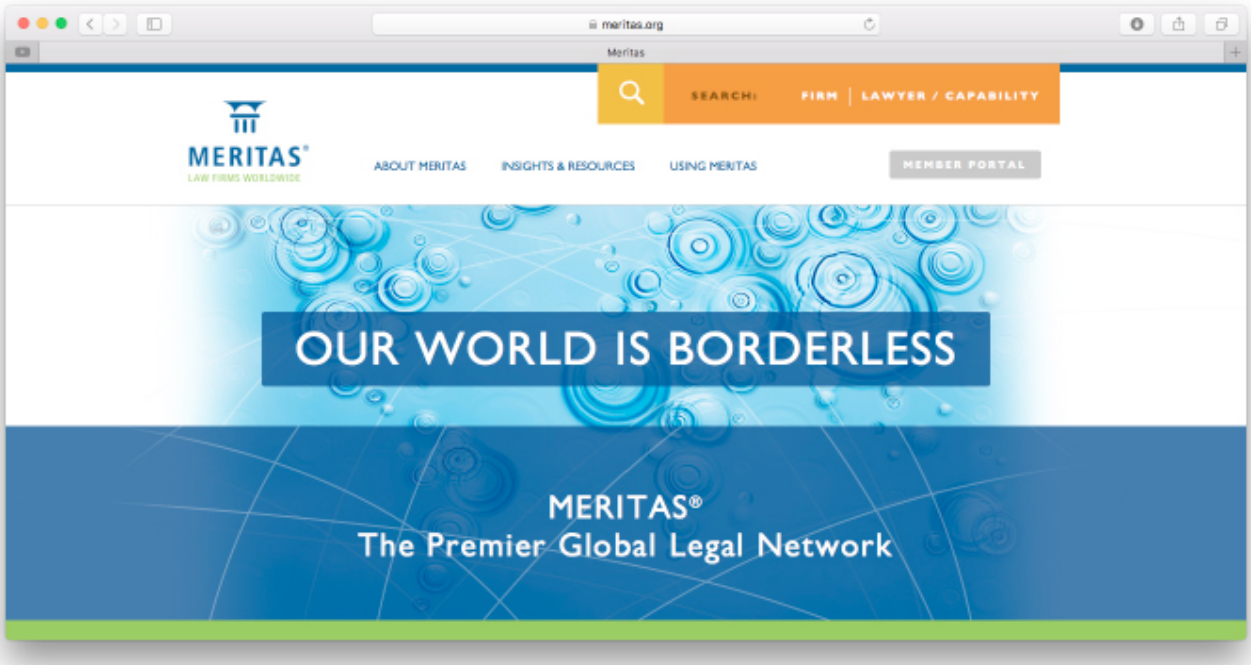
90+ COUNTRIES

180+ LAW FIRMS

240+ GLOBAL MARKETS

Using this exclusive ongoing review process, Meritas® ensures quality, consistency and client satisfaction.

With 180+ top-ranking law firms spanning more than 90 countries, Meritas® delivers exceptional legal knowledge, personal attention and proven value to clients worldwide.



For more information visit:

MERITAS®
LAW FIRMS WORLDWIDE

www.meritas.org

MERITAS®
LAW FIRMS WORLDWIDE

AUSTRALIA

FIRM PROFILE:

SWAAB

Swaab Attorneys is a Sydney based full service law firm. Established for well over 30 years, we pride ourselves on our ability to get on with business by providing great results, value for money and trusted advice, which is void of complexities, unnecessary delays and legal jargon, with a focus on building long-lasting and enduring relationships.

We do this because we're a passionate team of legal professionals who are committed to achieving exceptional results in everything we do and we believe that, with the spirit of generosity at our core, we can harness our strengths to overcome challenges together.

Our aim is to ensure the best possible and most rewarding experience for our clients. That is why we value our Swaab Brand of Service.

Our primary areas of law include: Corporate, Commercial, Property, planning & projects, Employment, Intellectual property & technology, Litigation and insolvency, Estate planning and Family law.

CONTACT:

MARY DIGIGLIO
med@swaab.com.au

JOHN HOVELMANN
jbh@swaab.com.au

+61 2 9233 5544
www.swaab.com.au

Introduction

Australian privacy law has national significance.

The main privacy law contains 13 principles, which have the force of law by virtue of the *Privacy Act* 1988 (Cth). The federal privacy regulator is the Australian Information Commissioner.

The 13 Australian Privacy Principles are:

(1) Open and transparent management of personal information

(2) Anonymity and pseudonymity

(3) Collection of solicited personal information

(4) Dealing with unsolicited personal information

(5) Notification of the collection of personal information

(6) Use or disclosure of personal information

(7) Direct marketing

(8) Cross-border disclosure of personal information

(9) Adoption, use or disclosure of government-related identifiers

(10) Quality of personal information

(11) Security of personal information

(12) Access to personal information

(13) Correction of personal information.

Some types of information and selected organisations are exempt. These include personal information about employees and the personal information dealings of most small businesses (those with an annual turnover of less than AU$3 million).

In addition some state laws regulate the personal information collection practices of certain sectors. For example, state laws may govern the personal information management practices of state government entities in the healthcare sector.

Major changes to Australian national privacy laws occurred in March 2014 (with the introduction of the Australian Privacy Principles) and in February 2018 (concerning the mandatory notification of certain types of data breaches, which are likely to cause serious harm to an individual).

Australia's statutory privacy law provisions do not generally provide for civil actions by affected individuals. However, some causes of action for breach of confidence exist.

There are some parallels between the concepts underlying Australia's notifiable data breach scheme and the personal data breach provisions under the GDPR (Articles 33, 34, 58 and 83). However, there are important differences. For example, the mandated "assessment phase" where one is not sure whether serious harm is likely, and the penalties attaching to failure to notify. The penalties are significantly higher in the EU.

Unlike the European GDPR, Australian privacy principles are not strictly based on statements of individuals' human rights and freedoms.

Australian privacy law does not include an express distinction between controllers and processors and does not mandate any particular terms for written contracts between controllers and processors.

Australia privacy law does not have an express equivalent of those provisions of the GDPR, which require at least one of six lawful bases for collection.

As to the territorial reach of the *Privacy Act* 1988 (Cth), it covers:

(1) Those who have some recognition under Australian law (for example are incorporated in Australia); and

(2) Those who do not have such recognition but who both carry on business in Australia and collect the relevant personal information in Australia.

As to cross-border disclosure of personal information, Australian law does not prohibit cross-border disclosures in circumstances where adequate protection of individuals' rights is not guaranteed. Instead, Australian law imposes, in effect, vicarious liability on the entity governed by the *Privacy Act* 1988 (Cth) for the data breaches of those to whom cross-border disclosures occur and who are not governed by that Act.

I. What are the major personal information protection laws or regulations in your jurisdiction?

(1) Australian Privacy Principles

under Australian federal statutory law, the *Privacy Act* 1988 (Cth). Note: Some Australian states have enacted state-based privacy legislation and there is the law of confidential information, which is non-statutory law applying throughout Australia.

(2) A federal statutory law regulating commercial electronic messages (the *Spam Act* 2003 (Cth). While the Spam Act does not regulate personal information protection, there are overlaps with the Privacy Act because the Privacy Act regulates use of personal information for direct (including electronic) marketing.

The answers below are limited to the *Privacy Act* 1988 (Cth) position.

2. How is personal information defined?

The definition of "personal information" under the *Privacy Act* 1988 (Cth) is *information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) Whether the information or opinion is true or not; and (b) Whether the information or opinion is recorded in a material form or not.*

This definition is limited to the personal information of individuals. Information identifying legal entities such as corporations and companies is not within the definition. Information identifying members of an unincorporated partnership may be within the definition.

3. What are the key principles relating to personal information protection?

There are 5 key principles:

(1) Managing personal information in an open and transparent way;

(2) Giving notices to individuals regarding the collection of solicited and unsolicited personal information including unsolicited personal information;

(3) Limiting uses and disclosures of personal information to primary and related secondary purposes of collection;

(4) Maintaining the quality and security of personal information; and

(5) Responding to requests for access to, and the correction of, personal information.

4. What are the compliance requirements for the collection of personal information?

Compliance requires:

(1) Creating the individual's awareness of the purposes of collection, holding, use and disclosure;

(2) Requiring consents where the collection, holding, use or disclosure is for marketing purposes and

(3) Taking reasonable security measures to guard against unauthorized access.

Australian law mandates the following:

Sensitive information: Obtaining consents to the collection of an individual's sensitive information. This is in addition to the requirement that the collection be reasonably necessary for one or more of the entity's functions or activities.

Contact information: Giving details of the entity's identity and contact details.

3rd party sources: Creating an awareness of this. This is particularly important as regards cookies and customer profiling.

Limited awareness circumstances: Taking such steps as are reasonable in the circumstances to ensure that individuals about whom the entity collects personal information are aware of it (in circumstances where they may not be otherwise – again important as regards cookies and customer profiling).

Purposes of collection: Taking such steps as are reasonable in the circumstances to ensure that there is an awareness of the purposes for which the entity collects personal information. This should be done in a way which enables the primary purpose of collection to be identified, a matter relevant to consents and secondary use. The manner of making individuals aware should be done in a way which is consistent with the entity's privacy policy. Where a purpose is direct marketing, a privacy policy/notice may not be sufficient. Opt ins may be needed. This might be done in separate legal terms or in specific opt in text to which the individual's attention is drawn in the relevant

communication channel. All direct marketing must be accompanied by a simple mechanism by which the individual may request not to receive direct marketing. An opt in is not required where the personal information is collected directly from the relevant individual in circumstances where the individual would reasonably expect the entity to use or disclose their personal information for that purpose. An opt in is always required for direct marketing use of sensitive information

Consequences: Disclosing the main consequences for individuals if some of their personal information is not collected by the entity.

Usual disclosures: Taking reasonable steps to make the individual aware of those entities to whom disclosures are usually made of the kind collected.

Access, correction and complaints: Giving the individual information about how they may access, correct and make complaints about the handling of their personal information.

Overseas disclosures: Outlining the likelihood of ex-Australian disclosures. Where practicable, the entity should specify the countries in which the overseas recipients are likely to be located.

5. What are the compliance requirements for the processing, use and disclosure of personal information?

See answer to Question 4.

6. Are there any restrictions on personal information being transferred to other jurisdictions?

Australian national privacy law does not prohibit overseas disclosures. However, the likelihood of overseas disclosures should be addressed in collection notices and there is transferor liability for transferee breaches where the transferee is not directly bound by the Australian *Privacy Act.*

7. What are the rights of an individual whose personal information is collected? Can he/she withdraw the consent to the retention of his/her personal information by a third party, and if so, how?

Individuals who complain to an entity about its personal information management practices have the right to be made aware of the entity's complaints procedures as part of the entity's privacy policy. In the absence of a contractual commitment to the contrary, individuals can withdraw their consent to the retention of their personal information by third party by communicating with the relevant data controller – contact details need to be disclosed as part of the entity's privacy policy. Consents to direct marketing may always be withdrawn. Complaints may be made by an individual directly to the Australian Information Commissioner, the contact details of which are at Question 9.

8. Is an employee's personal information protected differently? If so, what's the difference? Apart from the personal information of employees, are there any other types of personal information that receive special protection?

Employee personal information is not regulated by the *Privacy Act* 1988 (Cth).

The privacy rules for credit information and sensitive information are more stringent than for other types of personal information.

9. Which regulatory authorities are responsible for implementation and enforcement of personal information protection laws in your jurisdiction?

The Australian Information Commissioner. Contact details for the Australian Information Commissioner are:

Email: enquiries@oaic.gov.au

Tel: 1300 363 992

Postal address: GPO Box 5218, Sydney NSW 2001, Australia.

10. Are there any penalties, liabilities or remedies if any of the personal information protection laws is violated?

The Australian Information Commissioner may seek to impose civil penalty provisions for interferences with privacy. These

can include financial penalties in the order of AU$0.5million.

The Australian Information Commissioner has broad supporting powers. These are to investigate and conciliate and to make ancillary orders, for example obtaining documents and carrying out "own motion" assessments.

The Commissioner's authorised actions are also:

(1) Examining proposed legislation, which would allow interference with privacy or may have any adverse effects on people's privacy;

(2) Researching and monitoring developments in data processing and computer technology to ensure that adverse effects on people's privacy are minimised, as well as promoting an understanding and acceptance of the Australian Privacy Principles and their objects;

(3) Preparing and publicising guidelines for agencies and organisations to follow to avoid breaches of privacy; and

(4) Encouraging industries to develop programs to handle personal information consistent with the Australian Privacy Principles.

11. Is your jurisdiction planning to pass any new legislation to protect personal information? How is the area of personal information protection expected to develop in your jurisdiction?

None has been published by the regulator. Australia introduced mandatory notifiable data breach laws in February 2018, which have close parallels with those under GDPR.

Conclusion

For those who are likely to be subject to Australian privacy law, advice should be taken on whether they have an Australian-law compliant privacy policy and whether their communications with relevant individuals provide the necessary forms of awareness and, if necessary, consent.

When seeking local counsel, key issues for instructions are:

(1) How personal information is collected, stored, used and disclosed, and from whom;

(2) The types of personal information in question;

(3) How the information may be used and disclosed (and by and to whom);

(4) The mechanisms available to the collector to provide opt-ins and opt-outs;

(5) The range of contracts entered into by the collector, which have personal information management implications; and

(6) The extent to which Australian collections involve ex-Australian dealings or customers or data flows.

As with the the GDPR no amount of legal text will render an organisation's personal information management practices compliant with Australian law in the absence of other appropriate management practices, important amongst which are:

(1) Informed awareness;

(2) Measures which protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure;

(3) The giving of access to and rights to correct personal information; and

(4) Complaints management.

Prepared by Meritas Law Firms

Meritas is an established alliance of 180+ full-service law firms serving over 240 markets – all rigorously qualified, independent and collaborative. Connect with a Meritas law firm and benefit from local insight, local rates and world-class service.

www.meritas.org enables direct access to Meritas law firms through a searchable database of lawyer skills and experience.

MERITAS®
LAW FIRMS WORLDWIDE

www.meritas.org

800 Hennepin Avenue, Suite 600
Minneapolis, Minnesota 55403 USA
+1.612.339.8680