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

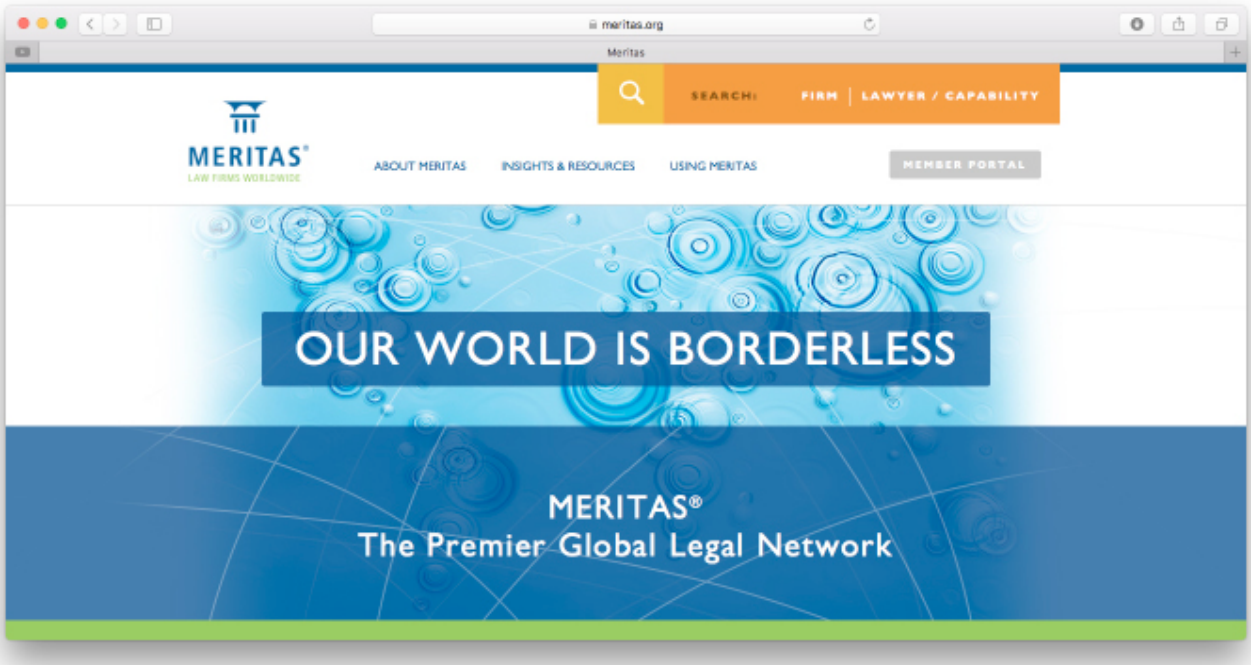
90+ COUNTRIES

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

NEW ZEALAND

FIRM PROFILE:

Martelli McKegg lawyers

Martelli McKegg is an Auckland based full service law firm specialising in Overseas Investment (into New Zealand), Corporate/Commercial, Mergers and Acquisitions, Intellectual Property and Technology, Real Estate, Building and Construction, Litigation/Dispute Resolution, Employment, Trusts, Estates and Relationship Property.

Established in 1921, we are very well regarded in the market with a number of partners nationally recognised for their expertise.

Our clients range from small family-owned businesses and private clients, through to some of the largest organisations in Australia and New Zealand across a variety of industries. We have particular experience acting for clients in the following sectors: manufacturing, import/export, wine and beverage, hospitality, tourism, entertainment, advertising, technology, telecommunications, property-development, forestry and industrial services.

We work hard to get to know our clients and to understand what our clients want to achieve. Our focus is to provide our clients with positive, practical legal advice, on time and within budget.

CONTACT:

MELISSA HIGHAM
mh@martellimckegg.co.nz

MIKE WORSNOP
mcw@martellimckegg.co.nz

+64 9 379 7333
www.martellimckegg.co.nz

Introduction

The protection of personal information is seen as important in New Zealand with robust privacy laws which are generally observed and enforced. New Zealand privacy laws were traditionally seen as "adequate" under the European Union's 1995 Data Protection Directive, however with the advent of the GDPR, New Zealand now lags behind the EU. Consequently, New Zealand's privacy laws are under review with changes designed to ensure that New Zealand is aligned with the EU and other major trading partners likely to come into force next year.

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

The principal personal information protection law in New Zealand is the Privacy Act 1993 (Act). A number of more specific privacy Codes of Practice have been issued pursuant to the Act for certain industries; namely:

(1) Civil Defence National Emergencies (Information Sharing) Code;

(2) Credit Reporting Privacy Code;

(3) Health Information Privacy Code;

(4) Justice Sector Unique identifier Code;

(5) Superannuation Schemes Unique Identifier Code; and

(6) Telecommunications Information Privacy Code.

There are also relevant provisions in the Unsolicited Electronic Messages Act 2007, which prohibit address harvesting software or harvested-address lists being used in connection with unsolicited commercial electronic messages (i.e. spam emails). Our answers below do not focus on this aspect.

2. How is personal information defined?

Under the Act, "personal information" means "information about an identifiable individual". An "individual" is defined to mean a "natural person, other than a deceased natural person", which excludes legal entities such as companies but would include the individual partners of a partnership or the trustees of a trust.

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

The Act centers around 12 information privacy principles. The wording of these principles contains a number of qualifications and exceptions, but they can be summarised as follows:

(1) Principle 1: An agency may only collect personal information necessary for a lawful purpose which is connected with a function of the agency.

(2) Principle 2: An agency must collect personal information directly from the individual, unless one of several exceptions applies.

(3) Principle 3: An agency must take reasonable steps to ensure an individual is aware of a number of matters, including the fact that the personal information is being collected, the purpose of the collection, the recipients of the information, the name of the agencies which will collect and hold the information, whether the supply of information is voluntary or mandatory (and under what laws), and the individual's rights under the Act.

(4) Principle 4: Personal information must not be collected in a way which is unlawful, unfair or unreasonably intrusive.

(5) Principle 5: An agency that holds personal information must ensure it is securely stored and protected from loss or misuse.

(6) Principle 6: If readily retrievable, an individual is entitled to confirmation from an agency of whether it holds their personal information and to be given access to it.

(7) Principle 7: Individuals have the right to request correction of personal information held, and if no correction is made may have a statement attached to the information noting that a correction was sought and not made.

(8) Principle 8: An agency must not use personal information without first taking reasonable steps to ensure it is up to date, complete, relevant and not misleading.

(9) Principle 9: An agency must only hold personal information as long as required for lawful purposes.

(10) Principle 10: An agency cannot use information for any purpose other than the one that it was obtained for, unless an exception applies.

(11) Principle 11: An agency must not disclose collected personal information unless pursuant to one of the purposes for which it was collected, or another exception applies.

(12) Principle 12: A unique identifier (such as tax identifiers and passport numbers) cannot be assigned to an individual unless it is necessary for the agency to carry out one of its functions efficiently, and the sharing of these identifiers is restricted.

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

As per the privacy principles, an agency collecting personal information must ensure it is doing so for a legitimate purpose connected to its functions, should seek to obtain the information directly from the individual if possible, and must take steps to inform the individual about the collection and their rights in accordance with principle 3.

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

As a general rule, the use and disclosure of personal information must be connected to the legitimate purpose for which it was collected. An agency should have processes in place to ensure information is up to date and complete before being used. Information must be securely processed and stored, kept only for so long as necessary, and the agency needs to have the ability to correct and modify stored personal information in case a correction request is received from an individual.

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

There is no general restriction on the transfer of personal information to other jurisdictions. However, the Privacy Commissioner has authority to prohibit a transfer of information from New Zealand to another State if satisfied the information would not be adequately protected or the transfer would lead to a breach of the relevant OECD Guidelines.

Where personal health information is to be stored in the cloud, the Ministry of Health requires that the agency undertake a cloud service risk assessment and for certain agencies there are enhanced requirements.

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?

As per privacy principles 6 and 7, individuals have the right to know whether an agency holds their information, to access the information, and to request that corrections be made. Agencies must notify individuals of these rights. There is no right to have information deleted or to withdraw consent to its retention.

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

Employees' personal information is not protected differently and is subject to the same privacy principles.

There are specific Codes of Practice issued by the Privacy

Commissioner in relation to certain industries, which override the privacy principles under the Act. These resemble the privacy principles but are tailored to the relevant area. These are specified above.

9. Which regulatory authorities are responsible for the implementation and enforcement of personal information protection laws in New Zealand?

The Act establishes the Office of the Privacy Commissioner, an independent Crown Entity which is responsible for implementing and enforcing the Act. In particular, the Privacy Commissioner has a role in receiving and determining privacy complaints, investigating breaches and authorising specific exemptions from the privacy principles. The Office of the Privacy Commissioner maintains a comprehensive website at https://www.privacy.org.nz with links to the relevant legislation and Codes of Practice.

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

Complaints regarding breaches of privacy are to be made in first instance to the Privacy Commissioner, which will review the complaint, investigate if necessary and if possible settle the complaint between the individual and the agency. The role of the Privacy Commissioner is to facilitate or mediate a settlement; the Privacy Commissioner cannot force the parties to settle. Most settlements take the form of an apology or release of information. Financial settlements are relatively uncommon.

If it is not possible to settle the complaint, or the agency contravenes an earlier assurance not to repeat a breach of the privacy principles, the Privacy Commissioner may refer the matter to the Director of Human Rights Proceedings for a civil action in the Human Rights Review Tribunal (essentially a specialist court). If the Privacy Commissioner or Director of Human Rights Proceedings decline to take action, the individual may bring the claim themselves.

The Human Rights Review Tribunal has a broad discretion in the orders it can make, which include an order restraining the defendant, costs and damages. There is no stated limit to the maximum damages awardable on a claim, but the awards to date are modest. Perhaps the most high-profile case to date has involved the internet tycoon, Kim Dotcom. In this 2018 case the Human Rights Review Tribunal made an award of NZ$90,000 plus costs in favour of Mr Dotcom.

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?

In March 2018, a new Privacy Bill was introduced to replace the existing Act and is currently working its way through Parliament. Much of the new Bill is remaining the same, with updates and clarification to the wording. The key amendments are:

(1) Mandatory reporting of privacy breaches that pose a risk of harm.

(2) A new requirement for New Zealand agencies to take reasonable steps to ensure personal information disclosed overseas will be subject to acceptable privacy standards.

(3) New powers for the Privacy Commissioner, including strengthened information gathering powers, an ability to issue enforceable compliance notices to agencies, and the ability to make binding decisions on access to information complaints.

(4) New criminal offences of misleading an agency in a way that affects a third party's information, and knowingly destroying documents containing personal information where a request has been made for it.

As the Bill is still at an early stage it is possible there will be further amendments before it is enacted. The Bill is currently with the Select Committee (the main opportunity for submissions

to be made and amendments recommended), with the Report of the Select Committee due in October 2018.

Conclusion

Agencies handling the personal information of New Zealand residents must ensure that they are properly acquainted with New Zealand privacy laws, implement appropriate policies around the collection, storage, use and dissemination of such information and have relevant contract documentation vetted for compliance. They must also ensure that they keep abreast of developments in what is currently an evolving area of the law.

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