DATA PROTECTION & PRIVACY

New Zealand

LEXOLOGY
Getting The Deal Through

Consulting editor
Hunton Andrews Kurth LLP

Data Protection & Privacy

Consulting editors

Aaron P Simpson, Lisa J Sotto

Hunton Andrews Kurth LLP

Quick reference guide enabling side-by-side comparison of local insights into the legislative framework; relevant authorities; treatment of breaches; legitimate processing; data handling responsibilities of PII owners; security obligations; internal controls, including the data protection officer; registration formalities transfer and disclosure of PII; rights of individuals; judicial supervision; specific data processing use cases such as cookies, electronic communications marketing, and cloud services; and recent trends.

Generated 17 July 2023

Table of contents

Contributors

New Zealand

Derek Roth-Biester
derek.roth-biester@al.nz
Anderson Lloyd

Megan Pearce
megan.pearce@al.nz
Anderson Lloyd

Emily Peart
emily.peart@al.nz
Anderson Lloyd

LAW AND THE REGULATORY AUTHORITY

Legislative framework

Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The protection of personal information (PI) is primarily governed by the Privacy Act 2020 (the Act). The Act regulates the collection, storage, security, access and correction and other dealings with PI by both public and private sector organisations (referred to in the Act as 'agencies'). The Act adopts a principle-based framework centralised around 13 information privacy principles (IPPs). These IPPs originate from the Organisation for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which was adopted in 1980.

The government is also currently considering new primary legislation to provide for the overarching framework for a new consumer data right (CDR). Work is underway on the design and cost of the CDR, which will dictate the form and content of the draft CDR Bill. It is anticipated that the draft CDR Bill will be released for consultation by the end of 2023.

Law stated - 22 May 2023

Data protection authority

Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The Privacy Commissioner (the Commissioner) appointed under the Act is responsible for monitoring the operation of the Act in New Zealand as well as examining any proposed legislation or policy that the Commissioner considers may affect the privacy of individuals.

The Commissioner can instigate an investigation into an agency's dealings with PI on the Commissioner's initiative. The Commissioner may also (but is not always obliged to) instigate an investigation of an agency's dealings with PI as a result of a submitted complaint.

When investigating an agency's dealings with PI, the Commissioner can largely regulate their own procedure as they see fit (subject to the Act and its regulations).

When requested to do so by any agency, the Commissioner can conduct an audit of PI maintained by that agency to ascertain whether the information is maintained according to the IPPs.

The Commissioner can issue compliance notices requiring agencies to either do or stop doing something should the Commissioner consider that the agency has breached the Act or any code of practice issued under the Act. The penalty for failing to comply with a compliance notice can be up to NZ$10,000.

In respect of the obligations to be imposed by the CDR Bill, at this stage it is proposed that CDR enforcement be carried out by the Commerce Commission. The Commissioner will, however, have enforcement powers over any obligations in the CDR Bill that relate to privacy.

Law stated - 22 May 2023

Cooperation with other data protection authorities

Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

There is no express legal obligation under the Act for the Commissioner to cooperate with international data protection authorities. New Zealand is not currently a party to any binding cross-border privacy schemes, such as the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules System.

Under the Act, the Commissioner may refer matters to an overseas privacy enforcement authority where the complaint relates to a matter that is more properly within its jurisdiction.

The Commissioner, as a matter of good practice, continues to engage with the premier global network of privacy commissioners as a founding member of the Global Privacy Enforcement Network and a participant in the APEC Cooperation Arrangement for Cross-Border Privacy Enforcement. The Commissioner of New Zealand and Australia signed a memorandum of understanding (MOU) in 2008 to facilitate cooperation between their offices on privacy-related issues (including information sharing). However, the MOU is not intended to be legally binding but rather to provide a practical means of meeting the cooperation targets set out in the APEC Privacy Framework.

Law stated - 22 May 2023

Breaches of data protection law

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Under the Act, the Human Rights Review Tribunal (the Tribunal) can award damages for interference with an individual's privacy.

The Commissioner has the authority to make binding decisions on complaints about information access requests, not the Tribunal (although such decisions will be subject to a right of appeal to the Tribunal).

Following an investigation of any privacy complaint by the Commissioner, proceedings can be brought in the Tribunal in respect of the complaint in certain circumstances (including where the Commissioner has decided not to investigate the complaint). The Tribunal may award damages in respect of the interference with the privacy of an individual as compensation for the humiliation, loss of dignity and injury to feelings caused by serious breaches, as well as the loss of any benefit (monetary or other) that the individual might reasonably have expected to obtain if the interference had not occurred.

The penalties under the Act are modest when compared to other jurisdictions. The Act has a maximum fine of NZ $10,000 for certain breaches including: (1) misleading an entity to obtain access to someone else's PI and (2) destroying a document containing personal information with knowledge of a request related to it. The Commissioner has indicated that he wants to lessen the penalty gap when compared to a number of OECD jurisdictions, including by introducing civil penalties.

In contrast, the government has proposed significant penalties for breaches of the CDR regime. The fines currently being proposed for the most egregious breaches (involving knowingly misleading or deceiving behaviour) would be up to the greater of NZ$5 million and three times the value of any commercial gain (or if commercial gain cannot be determined, 10 per cent of the turnover in the relevant period). Such breaches may also constitute criminal offences.

Law stated - 22 May 2023

Judicial review of data protection authority orders

Can PI owners appeal to the courts against orders of the data protection authority?

If an agency disagrees with an access direction made by the Commissioner, an agency can appeal to the Tribunal against the direction. The agency has 20 working days from receiving the notice to lodge its appeal unless exceptional circumstances apply. The Commissioner has a right to be heard in any appeal.

The Tribunal may determine an appeal by confirming the direction appealed against, modifying the direction or reversing the direction order.

If the agency then fails to follow the Tribunal's orders or directions, the decision can be enforced in the District Court.

Law stated - 22 May 2023

SCOPE

Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Privacy Act 2020 (the Act) generally applies to:

- New Zealand residents and businesses;
- overseas businesses in the course of carrying on business in New Zealand; and
- individuals not resident in New Zealand in relation to personal information (PI) collected or held while in New Zealand.

Given the flexibility and nature of the information privacy principles (IPPs), New Zealand data protection law generally covers all sectors and organisations; however, certain agencies are excluded from application of the Act including:

- members of Parliament;
- courts and tribunals in relation to their judicial functions; and
- the news media when it relates to the collection and reporting of news and current affairs.

While New Zealand's intelligence and security agencies are not excluded wholesale from the application of the Act, non-compliance with certain IPPs is permitted under the Act to the extent the non-compliance is necessary to enable an intelligence and security agency to perform any of its functions.

Additionally, individuals who collect or hold PI for their own personal, family or household affairs are exempt from the IPPs (although this does not apply where the collection, disclosure or use would be highly offensive to an ordinary reasonable person).

Law stated - 22 May 2023

Interception of communications and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The Act does not expressly cover interception of communications, electronic marketing or monitoring and surveillance of individuals; although, the IPPs will apply in respect of the collection and processing of any PI collected through monitoring and surveillance activities. The relevant law in this regard is as follows:

- Under the Crimes Act 1961 (Crimes Act), a person faces up to two years' imprisonment if they intentionally intercept any private communications through an interception device (eg, recording device), other than when they are authorised to do so under other legislation (eg, the Search and Surveillance Act 2012). Any intentional disclosure of private communication, the substance and meaning of that communication or intentional disclosure of the existence of private communication could result in up to two years' imprisonment.
- Further, under the Crimes Act, there are criminal penalties for restricted monitoring and surveillance activities, including intimate visual recordings. Any individual that intentionally or recklessly makes, possesses (in certain circumstances) and publishes, imports or sells intimate visual recordings of another person is liable to imprisonment.
- The Search and Surveillance Act 2012 regulates police powers and their ability to monitor compliance with the law and their power to carry out investigations and the prosecution of offences.
- The Unsolicited Electronic Messages Act (2007) governs the sending of commercial electronic messages and prohibits the sending of unsolicited commercial electronic messages, in particular the use of address-harvesting software. It applies to any electronic message sent for a commercial purpose. 'Electronic message' is defined broadly to cover any form of message sent using a telecommunications service (but excluding voice calls) or to an electronic address, and therefore covers email, fax, text messages and other forms of electronic messages.

Law stated - 22 May 2023

Other laws

Are there any further laws or regulations that provide specific data protection rules for related areas?

The Privacy Commissioner (the Commissioner) may, from time to time, issue codes of practices under the Act to supplement the IPPs in respect of certain classes of information or certain classes of agency.

There are currently six codes of practice in operation: the Civil Defence National Emergencies (Information Sharing) Code, the Credit Reporting Privacy Code, the Health Information Privacy Code, the Justice Sector Unique Identifier Code, the Superannuation Schemes Unique Identifier Code and the Telecommunications Information Privacy Code. A further code of practice regulating the processing of biometric PI is set to be released in 2023.

The government is also considering new primary legislation to provide for the overarching framework for a new consumer data right (CDR). Work is underway on the design and cost of the CDR, which will dictate the form and content of the draft CDR Bill. It is anticipated that the draft CDR Bill will be released for consultation before the end of 2023.

Law stated - 22 May 2023

PI formats

What categories and types of PI are covered by the law?

All categories and types of PI are covered by the Act. Any information that falls within the definition of PI under the Act (ie, information about an identifiable individual) is protected.

Law stated - 22 May 2023

Extraterritoriality

Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The Act has extraterritorial effect in that it applies to overseas persons, organisations and businesses to the extent they are carrying on business in New Zealand, regardless of where the person, organisation or business is physically based or operating from.

The Act aligns its application to extraterritorial agencies with the position under the EU General Data Protection Regulation (GDPR). Some overseas entities may be deemed agencies carrying on business in New Zealand regardless of whether or not they:

- do so as a commercial operation or with an intent to make a profit;
- have a physical presence in New Zealand; or
- receive any payment for the supply of goods or services.

Law stated - 22 May 2023

Covered uses of PI

Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

The Act covers all uses of PI by an agency (with specific codes of practice modifying the Act for particular sectors).

The Act does not expressly distinguish between data controllers and data owners; however, the Act provides that where an agent (A) holds PI as an agent for another agency (B) (eg, for safe custody or processing), then PI is treated as being held by B and not A (unless A also uses or discloses the PI for its own purposes). Agencies that provide processing services to the original owner of the PI as its agent (ie, cloud providers and other service providers that process information on behalf of others) will still be held accountable for the PI that they hold, store and process to the extent that they use or disclose the information for their own purposes.

Law stated - 22 May 2023

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Under the Privacy Act 2020 (the Act), personal information (PI) must not be collected unless the collection is for a lawful purpose connected with a function or activity of the agency and the collection is necessary for that purpose. If the lawful purpose for which the agency intends to collect PI does not require the collection of an individual's information, then that agency may not require the individual's information.

There are also limits on how PI can be used once it has been collected. PI that was obtained in connection with one purpose can generally not be used for any other purpose unless:

- consent is obtained;
- the information is already in the public domain; or
- non-compliance is required in the circumstances (ie, to enforce the law, to protect public revenue, for the conduct of proceedings before a court or tribunal or to prevent or lessen a serious threat).

Law stated - 22 May 2023

Legitimate processing – types of PI

Does the law impose more stringent rules for processing specific categories and types of PI?

The Act does not expressly impose more stringent rules for processing specific categories and types of PI; however, codes of practice issued under the Act may modify the application of the information privacy principles under the Act to specific categories and types of PI. For example, codes of practice specifically regulating PI held for credit reporting purposes, health information and telecoms information have been issued in New Zealand.

The Privacy Commissioner has acknowledged that the processing of minors' PI is an area of growing concern and future reforms of the Act will likely include further specific protections over this category of PI.

Law stated - 22 May 2023

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

The Privacy Act 2020 (the Act) requires agencies collecting personal information (PI) directly from an individual to take steps that are reasonable in the circumstances to ensure that the individual is aware of certain information, including:

- the fact that the information is being collected;
- the purpose for which the information is being collected;
- the intended recipients of the information;
- the consequences for them if they do not provide all or part of the requested information; and
- how they may request access to and correction of PI.

Where the collection of PI is authorised or required by law, the individual must be also informed of the particular law by

which the collection of the information is authorised or required, as well as whether the supply of the information is voluntary or mandatory.

In August 2022, the government initiated a public feedback process in respect of the proposed expansion to the above notification regime to also apply to agencies when collecting PI indirectly via third parties. The government is presently considering the feedback received to determine the scope of any required amendments to the Act.

Law stated - 22 May 2023

Exemptions from transparency obligations

When is notice not required?

Notice is currently not required where either the collecting agency has taken the necessary steps concerning the collection of the same or similar information from the individual on a recent previous occasion or if the agency believes, on reasonable grounds, that:

- non-compliance would not prejudice the interests of the individual concerned;
- the non-compliance is necessary to avoid prejudice to the maintenance or enforcement of the law (including the conduct of proceedings before any court or tribunal);
- the non-compliance is necessary for the protection of public revenue;
- compliance is not reasonably practicable in the circumstances of the particular case; or
- where the PI collected will not be used in a form in which the individual concerned can be identified.

The notice requirements presently only apply where the agency is collecting PI from the individual concerned (whether directly or indirectly (ie, via automated collection technologies); however, the government is presently considering a proposed expansion to the Act's notice obligations to also apply to agencies when collecting PI indirectly via third parties, rather than from the individual concerned.

Law stated - 22 May 2023

Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PI?

Yes. Under the Act, no agency may use or disclose PI without taking reasonable steps to ensure that, having regard to the purpose for which the PI is proposed to be used, the PI is accurate, up to date, complete, relevant and not misleading.

Law stated - 22 May 2023

Data minimisation

Does the law restrict the types or volume of PI that may be collected?

While there are no express restrictions on the types or volume of PI collected, the Act requires that PI must not be collected by an agency unless it is collected for lawful purposes connected with the function or activity of the agency and the collection is necessary for that purpose.

Law stated - 22 May 2023

Data retention

Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

While there are no prescribed time frames for retention of PI under the Act, agencies must not keep PI for any longer than is required for the purposes for which the PI may lawfully be used.

New Zealand's Deputy Privacy Commissioner has recently commented that unwarranted data retention is emerging as a key area of non-compliance as evidenced in several recent domestic and global cyber-attacks. The Deputy Commissioner has called on businesses to ensure they have robust data retention policies in place.

Law stated - 22 May 2023

Purpose limitation

Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

Yes. As a general principle, any agency that holds PI must use that PI only for the purposes in respect of which the PI was obtained.

An agency may, however, use PI for a purpose other than the purposes in respect of which that PI was originally obtained where the agency reasonably believes:

- that the individual concerned has authorised the new use;
- that the source of the information is publicly available and it would not be unfair or unreasonable to use the information;
- the non-compliance is necessary to avoid prejudice to the maintenance or enforcement of law (including the conduct of proceedings before any court or tribunal);
- the non-compliance is necessary to prevent or lessen a serious public threat or the safety of the individual concerned;
- the PI will not be used in a form in which the individual concerned can be identified;
- the use is necessary to enable a New Zealand intelligence or security agency to perform its functions; or
- the disclosure is necessary to facilitate the sale of a business as a going concern.

Law stated - 22 May 2023

Automated decision-making

Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

The Act does not expressly cover automated decision-making; however, the Act's information privacy principles will continue to apply, meaning, for example, that agencies must have regard to the original purpose of collection and notice obligations when using PI for profiling.

The Privacy Commissioner (Commissioner), in carrying out automated decision-making, recommended that the government's use of algorithms retains an element of human oversight on the grounds that analytical processes should never entirely replace human oversight. However, it has been acknowledged that as technology continues to

evolve, the government will need to keep an eye on the balance between the importance of human oversight and possible efficiencies and improvements in service delivery. A code to regulate the use of biometric technologies, which includes profiling, is currently being explored by the Commissioner. With no legislation in place regulating automated decision-making technologies specifically, the Commissioner has encouraged agencies in the interim to make use of internal policies which ensure that artificial intelligence (AI) is being used ethically, and in compliance with the objectives of the Act.

Law stated - 22 May 2023

SECURITY

Security obligations

What security obligations are imposed on PI owners and service providers that process PI on their behalf?

The Privacy Act 2020 (the Act) requires that agencies protect personal information (PI) with such security safeguards as it is reasonable in the circumstances to take against loss, access, use, modification, disclosure and other misuse.

If it is necessary for the PI to be processed by a third-party service provider, the agency must do everything reasonably within its power to prevent unauthorised use or unauthorised disclosure of the PI by that service provider.

Law stated - 22 May 2023

Notification of data breach

Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The Act sets out a process for the management of a 'notifiable privacy breach' – that is, a privacy breach that causes, or is likely to cause, serious harm to an affected individual.

The Act mandates that agencies must notify the Privacy Commissioner (Commissioner) as soon as is practicable after becoming aware that a notifiable privacy breach has occurred. An agency is also required to notify affected individuals as soon as practicable after becoming aware that a notifiable privacy breach has occurred, unless it is not reasonably practicable, in which case a public notice is required unless an exception or delay applies.

While not an express requirement of the Act, the Commissioner has provided that, as a guide, it is expected that a breach notification should be made to the Office of the Privacy Commissioner no later than 72 hours after the agency is made aware of the breach.

Law stated - 22 May 2023

INTERNAL CONTROLS

Accountability

Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

There is no express requirement for agencies to implement self-auditing internal controls to demonstrate compliance with the Privacy Act 2020 (the Act); however, such internal controls are strongly encouraged as best practice and are intrinsically linked with compliance with many of the Act's information privacy principles.

Law stated - 22 May 2023

Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

The Act requires agencies to have at least one privacy officer (either from within or outside the agency).

The legal responsibilities of the data protection officer are, namely: encouraging the agency to comply with the information privacy principles (IPPs); dealing with requests made to the agency under the Act (eg, access requests); working with the Office of the Privacy Commissioner (OPC) in relation to investigations conducted pursuant to complaints made under the Act in relation to the agency; and otherwise ensuring compliance by the agency with the Act.

While there are no specific criteria for who qualifies for appointment as a privacy officer, the OPC recommends that the privacy officer should be familiar with the Act, IPPs and any other relevant regulations. Furthermore, they should be able to deal with complaints from individuals of alleged interferences with PI and train staff in agencies on best privacy management practices.

Law stated - 22 May 2023

Record-keeping

Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

The Act does not expressly require agencies holding or processing personal information (PI) to maintain specific internal records relating to the PI they hold; however, such internal records are strongly encouraged as best practice and are intrinsically linked with compliance with many of the Act's IPPs. For example, the Act requires agencies to:

- only hold PI for as long as is required for the purpose it may lawfully be used for;
- ensure that any PI held by that agency is protected; and
- take reasonable security safeguards to protect the PI against:
  - loss;
  - access;
  - use;
  - modification;
  - disclosure; or
  - another misuse.

Law stated - 22 May 2023

Risk assessment

Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

There are no express requirements to carry out risk assessments under the Act. However, a privacy impact assessment (PIA) is a tool voluntarily utilised by agencies to identify the potential risks arising from their collection, use or handling of PI under the Act and help ensure compliance with the IPPs. The Privacy Commissioner views a PIA as an increasingly useful tool that agencies of all sizes can fit within their existing internal policies to help them manage privacy more successfully.

Law stated - 22 May 2023

Design of PI processing systems

Are there any obligations in relation to how PI processing systems must be designed?

The Act contains no specific legal obligations on new processing operations to, for example, integrate data protection measures into an agency's processing activities and operations at the design stage.

To comply with many of the IPPs set out in the Act (including the restrictions on using and disclosing any PI other than for the purpose in connection with which the PI was obtained), most new PI processing operations will integrate data protection measures to ensure compliance with the Act into their business practices from launch and throughout the operation's lifecycle.

Law stated - 22 May 2023

REGISTRATION AND NOTIFICATION

Registration

Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

No.

Law stated - 22 May 2023

Other transparency duties

Are there any other public transparency duties?

No.

Law stated - 22 May 2023

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

How does the law regulate the sharing of PI with entities that provide outsourced processing services?

The Privacy Act 2020 (the Act) does not specifically regulate the transfer of personal information (PI) with third-party processors. However, where an agency (1) holds PI as an agent for, or for the sole purpose of processing the information on behalf of, another agency and (2) does not use or disclose the PI for its own purposes, the Act treats this as information held by the agency on whose behalf it is held or processed. Furthermore, the agency will then be liable for the acts or omissions of its agent regarding the processing of PI, unless done or omitted without the agency's express or implied authority. The Privacy Commissioner has produced an array of simple contractual clauses that agencies can adopt to help ensure that PI will be subject to appropriate contractual controls.

Law stated - 22 May 2023

Restrictions on third-party disclosure

Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

Under the Act there is a general restriction against disclosure for any purpose that is not one of the purposes in connection with which the information was obtained.

An agency must not disclose PI to any other agency unless it believes on reasonable grounds:

- that the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained;
- that the disclosure is to the individual concerned;
- that the disclosure is authorised by the individual concerned;
- that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to disclose the information;
- that the disclosure of the information is necessary:
  - to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution and punishment of offences;
  - for the enforcement of a law that imposes a pecuniary penalty;
  - for the protection of public revenue; or
  - for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation);
- that the disclosure of the information is necessary to prevent or lessen a serious threat to:
  - public health or public safety; or
  - the life or health of the individual concerned or another individual;
- that the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions;
- that the information:
  - is to be used in a form in which the individual concerned is not identified; or
  - is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
- that the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern.

Law stated - 22 May 2023

Cross-border transfer

Is the transfer of PI outside the jurisdiction restricted?

Under the Act, agencies are only able to disclose PI to foreign persons or entities if:

- the individual authorised the disclosure (after having been expressly informed by the agency that the overseas person may not be required to protect the information in a way that, overall, provides comparable safeguards to those in the Act);
- the overseas person is otherwise 'carrying on business in New Zealand', such that the agency reasonably believes that the overseas person is subject to the Act;
- the overseas person is subject to the laws of a 'prescribed country' or a participant in a 'prescribed scheme'. Noting that as of May 2023 there are no prescribed countries or prescribed schemes that have been approved as such by regulations to the Act; or
- the agency believes on reasonable grounds that the overseas person is required to protect the PI in a manner comparable to that required by the agency under New Zealand law.

Law stated - 22 May 2023

Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The restriction against the disclosure of PI to overseas persons under the Act will usually not apply to transfers to cloud storage providers or other overseas processors (to the extent that entity is engaged on behalf of another agent under a services or agency arrangement and is not otherwise using the PI for its own purposes). Responsibility of the storage and security of PI will remain with the PI owner.

Law stated - 22 May 2023

Localisation

Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

No.

Law stated - 22 May 2023

RIGHTS OF INDIVIDUALS

Access

Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Yes. The individual to whom the particular personal information (PI) relates has a right to receive, upon request,

confirmation from the agency of whether or not it holds such PI and a right to access the PI.

If an agency receives a request for access to an individual's PI, it has 20 working days to respond to the request (including stipulating what charge may be applied in respect of the management of the request). This time limit may be extended if the request is for a large quantity of information or consultation with other third parties is required in respect of the request.

The Privacy Commissioner (the Commissioner) will make binding decisions on complaints about information access requests, rather than the Human Rights Review Tribunal (the Tribunal); although, such decisions are subject to a right of appeal to the Tribunal.

Law stated - 22 May 2023

Other rights

Do individuals have other substantive rights?

Where an agency holds PI about an individual, that individual can request the correction of their PI.

Where an agency that holds PI is not willing to correct that information following a request by the individual concerned, the agency will, if so requested by the individual, take reasonable steps to attach a statement that a correction of the relevant PI has been sought.

In New Zealand, there is currently no express right that entitles individuals to request that an agency delete their PI; however, the Commissioner has indicated that a right to erasure is being considered.

The government is considering new primary legislation to provide for the overarching framework for a new consumer data right (CDR) giving consumers a mechanism to securely share data that is held about them with trusted third parties. Work is underway on the design and cost of the CDR, which will dictate the form and content of the draft CDR Bill. It is anticipated that the draft CDR Bill will be released for consultation before the end of 2023.

Law stated - 22 May 2023

Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Following an investigation of any privacy complaint by the Commissioner, if the alleged interference cannot be settled between the relevant parties, proceedings can be brought in the Tribunal and remedies sought can include damages. The tribunal may award damages in respect of the interference with the privacy of an individual to appropriately compensate them for the humiliation, loss of dignity and injury to feelings caused by serious breaches, as well as the loss of any benefit (monetary or other) that the individual might reasonably have expected to obtain if the interference had not occurred.

Law stated - 22 May 2023

Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

The enforcement of the Privacy Act 2020 (the Act) (including an agency's compliance with any access request) is

primarily the responsibility of the Commissioner or the authorities to which the Commissioner delegates its investigations. If following the relevant investigation by the Commissioner the complaint cannot be settled between the relevant parties, proceedings can be brought in the Tribunal. If the aggrieved individual disagrees with the Tribunal's decision, it can be appealed to the High Court. In which case, the judiciary can play a role in enforcing the Act.

Law stated - 22 May 2023

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described?

Information privacy principles are not intended to apply to the collection of personal information (PI) by an agency that is an individual where that PI is collected or held by that individual solely or principally for the purposes of, or in connection with, that individual's personal, family or household affairs. However, this exclusion will not apply once the relevant PI is collected, disclosed or used, if such collection, disclosure or use would reasonably be considered highly offensive.

Law stated - 22 May 2023

SPECIFIC DATA PROCESSING

Cookies and similar technology

Are there any rules on the use of 'cookies' or equivalent technology?

Currently, the Privacy Act 2020 (the Act) does not contain any express provisions regarding cookies or equivalent technology. Information privacy principles (IPPs) will apply in respect of personal information (PI) collected via cookies or similar technologies.

Law stated - 22 May 2023

Electronic communications marketing

Are there any rules on marketing by email, fax, telephone or other electronic channels?

The Unsolicited Electronic Messages Act 2007 (UEMA) regulates the conditions for direct marketing by email, instant messages, texts and fax. The UEMA requires that all commercial electronic messages: may only be sent with the consent of the recipient; must include accurate information about the individual who authorised the sending of the message; and must include a functional unsubscribe facility. Certain commercial emails (ie, messages that provide factual information about the goods acquired, a subscription, a membership, an account, a loan or a similar ongoing relationship) are not deemed as commercial electronic messages and, therefore, will not be subject to the restrictions under the UEMA.

There is no specific legislative scheme limiting direct marketing by telephone to individual subscribers, and voice calls made using a standard telephone service are specifically excluded from the scope of the UEMA. However, telemarketing activities that collect and store personal data must comply with the Act, IPPs and other enactments.

Law stated - 22 May 2023

Targeted advertising

Are there any rules on targeted online advertising?

Currently, the Act does not contain any express provisions regarding targeted online advertising or behavioural advertising. The IPPs will apply in respect of PI used for such advertising.

Law stated - 22 May 2023

Sensitive personal information

Are there any rules on the processing of 'sensitive' categories of personal information?

There are no specific restrictions relevant to the processing of 'sensitive' categories of PI under the Act.

However, if PI is sensitive, this may influence the application of certain processes under the Act. For example, in assessing whether a privacy breach has caused 'serious harm', the nature of the PI (whether sensitive or not) will be considered among other factors. The Privacy Commissioner (the Commissioner) has emphasised that agencies who handle sensitive PI need to ensure this type of PI is handled with caution and appropriately in the circumstances (notably those involved with artificial intelligence (AI) technologies or processing of biometric PI).

Law stated - 22 May 2023

Profiling

Are there any rules regarding individual profiling?

There are no express requirements or regulations related to the various uses of data profiling. However, the IPPs will apply to agencies use of PI for individual profiling.

Law stated - 22 May 2023

Cloud services

Are there any rules or regulator guidance on the use of cloud computing services?

Cloud computing services are not specifically regulated under the Act. The Commissioner released a guide titled 'Cloud Computing: A guide to making the right choices' in February 2013 outlining some high-level guidance for businesses looking to move into cloud computing. This guidance includes a 10-step checklist for small businesses that asks small businesses to, among other things:

- ensure adequate research is carried out on the relevant provider;
- understand what business information and personally identifiable information will be stored by the provider; and
- understand how the provider will see the business' information and how the information can be accessed, managed and deleted as necessary once it has been stored on the cloud.

Law stated - 22 May 2023

UPDATE AND TRENDS

Key developments of the past year

Are there any emerging trends or hot topics in international data protection in your jurisdiction?

There continues to be ongoing debate as to whether the Privacy Act 2020 (the Act) went far enough and whether the enhanced privacy protections are sufficient to warrant the retention of New Zealand's adequacy status with the EU, currently under review.

A close watching brief will be kept on the European Commission's review of New Zealand's adequacy status (and the proposed reform to the Act's transparency obligations triggered by such review). If New Zealand's status is revoked, then the administrative requirements are more onerous for transfers of personal data between New Zealand and the EU (and now also the UK).

Further, widespread adoption of artificial intelligence (AI) technology has seen regulators across the globe deliberating appropriate regulation of such technologies and how best to fill the gaps present in existing data protection and privacy laws. In New Zealand, the Privacy Commissioner has acknowledged that while the Act is technology-neutral, it will need further reform to ensure it is fit for purpose going forward noting that the conversion (regarding regulation of AI technologies) is becoming more urgent as private developers release more advanced and competing AIs, and it will require a collective response from public sector and private businesses.

Law stated - 22 May 2023

Jurisdictions

Australia	Piper Alderman
Austria	Knyrim Trieb Rechtsanwälte
Belgium	Hunton Andrews Kurth LLP
Brazil	Mattos Filho Veiga Filho Marrey Jr e Quiroga Advogados
Canada	.
Chile	Magliona Abogados
China	Mayer Brown
France	Aramis Law Firm
Germany	Hoffmann Liebs Fritsch & Partner
Greece	GKP Law Firm
Hong Kong	Mayer Brown
Hungary	VJT & Partners
India	AP & Partners
Indonesia	SSEK Law Firm
Ireland	Walkers
Italy	ICT Legal Consulting
Japan	Nagashima Ohno & Tsunematsu
Jordan	Nsair & Partners - Lawyers
Malaysia	SKRINE
Malta	Fenech & Fenech Advocates
New Zealand	Anderson Lloyd
Pakistan	S.U.Khan Associates Corporate & Legal Consultants
Poland	Kobylanska Lewoszewski Mednis
Portugal	Morais Leitao Galvao Teles Soares da Silva and Associados
Serbia	BDK Advokati

South Africa	Covington & Burling LLP
South Korea	Bae, Kim & Lee LLC
Switzerland	Lenz & Staehelin
Taiwan	Formosa Transnational Attorneys at Law
Thailand	Formichella & Sritawat Attorneys at Law
Turkey	Turunç
United Arab Emirates	Bizilance Legal Consultants
United Kingdom	Hunton Andrews Kurth LLP
USA	Hunton Andrews Kurth LLP