

# New Zealand Privacy and Data Protection Checklist



## About the New Zealand Privacy & Data Protection Compliance Register

The New Zealand Privacy & Data Security Compliance Register is essential for organisations navigating privacy laws, especially the Privacy Act 2020. It provides guidance on 13 privacy principles, including personal information handling, data security, breach management, workplace privacy, and cross-border transfers. The module also covers industry-specific codes for sectors like health and telecommunications, equipping organisations with the knowledge to develop effective privacy policies and ensure compliance.

## About the Expert

### Tania Goatley

Partner, Bell Gully



Tania has assisted with cyber security breaches across multiple jurisdictions and has advised on the first mandatory reportable privacy breach under the Privacy Act. Regularly advises clients on privacy and cyber security issues, including advising:

- » a client operating in the telecommunications sector as to how to deal with a breach that involved the public disclosure of phone numbers that were designated as 'unlisted'.
- » the receivers of a New Zealand retailer that went into liquidation on how to deal with, use, and protect databases containing customer information across multiple jurisdictions.
- » a multinational media company about its privacy and cyber security practices, including assisting to manage data security incidents and corresponding with official agencies to mitigate any fallout.

She has a strong media law background, advising on defamation claims, appearing in Court on name suppression issues, and providing media law training to journalists. She advises on all aspects of intellectual property law, including copyright, passing off, and trademark infringement disputes and litigation.

In addition to her particular areas of expertise, Tania provides general advice on commercial and contractual disputes and litigation with successful outcomes for her clients.

Chambers Asia Pacific 2023 ranks Tania as a leading lawyer for intellectual property and technology, media and telecommunications. The Legal 500 Asia Pacific 2023 recommends Tania for data protection, intellectual property and technology, media, and telecommunications.

Tania is recognised as a media and entertainment lawyer of the year and trademark lawyer of the year in the Women in Business Law Awards APAC 2023 shortlists.

Tania is an active member of the International Association for the Protection of Intellectual Property (AIPPI) and the Intellectual Property Society of Australia and New Zealand (IPSANZ).

### **Expertise**

Media and communications, Consumer law, Intellectual property, Litigation and dispute resolution, Privacy and data protection, Information, Communications and technology, Cyber security

# PRIVACY & DATA PROTECTION CHECKLIST

This checklist has been designed to help you identify your requirements.

## Overview

Requirement	Needs work	Don't know	Meets requirement
-------------	------------	------------	-------------------

Does an agency comply with all laws that govern the regulation of privacy and confidentiality in New Zealand?

## Collecting Personal Information

Requirement	Needs work	Don't know	Meets requirement
-------------	------------	------------	-------------------

Does the agency apply the relevant information privacy principles (IPPs) when collecting personal information, to ensure that collection is fair, transparent and respectful of personal privacy?

Does the agency collect personal information only in circumstances where it is necessary and lawful, using methods that are fair, transparent and respectful of individuals' privacy?

Does the agency have policies and procedures in place for handling unsolicited personal information, including whether and/or how to retain, return or destroy it, in accordance with the information privacy principles (IPPs)?

When collecting personal information about a person, does the agency, unless exempted from complying, notify the person of their rights with respect to collection as well as why, how and by whom the information will be collected, used and disclosed?

When collecting personal information, does the agency use methods that are lawful, fair and respectful of individuals' privacy in personal affairs?

# PRIVACY & DATA PROTECTION CHECKLIST

This checklist has been designed to help you identify your requirements.

## Using and Disclosing Personal Information and Identifiers

Requirement	Needs work	Don't know	Meets requirement
-------------	------------	------------	-------------------

Does the agency restrict its use and disclosure of personal information to the purpose(s) for which it was originally collected unless a relevant exemption applies?

Does the agency only use or disclosure of personal information for the purpose(s) for which it was obtained, unless otherwise authorised under the information privacy principles (IPPs)?

Does the agency obtain prior consent to send commercial electronic messages to persons, and ensure that all messages contain accurate sender details and an unsubscribe facility?

Does the agency avoid assigning unique identifiers to individuals unless it is necessary to carry out its functions?

## Ensuring the Security of Personal Information

Requirement	Needs work	Don't know	Meets requirement
-------------	------------	------------	-------------------

Does the agency have systems and processes in place to protect personal information from unauthorised access, use or disclosure at all times, from collection to disposal or destruction?

Has the agency put in place appropriate safeguards and security mechanisms to ensure that the personal information it holds is kept safe from loss, damage, misuse and unauthorised access or use?

Does the agency have policies and procedures in place for responding to privacy breaches including notifiable privacy breaches?

Does the agency securely dispose of personal information once it has been used for its intended purposes?

# PRIVACY & DATA PROTECTION CHECKLIST

This checklist has been designed to help you identify your requirements.

## Enabling Access and Correction of Personal Data

Requirement	Needs work	Don't know	Meets requirement
Does the agency have policies and procedures in place to facilitate individuals accessing and correcting personal information that the agency holds about them?			
Does the agency have systems and processes in place to allow individuals to access personal information that the agency holds about them?			
Does the agency have systems and processes in place to allow individuals to correct personal information that the agency holds about them?			
Does the agency have policies and procedures in place for assisting individuals who wish to make an IPP 6 request or correction request?			
Does the agency have policies and procedures in place for cooperating with the Privacy Commissioner during complaint and review investigations?			

## Workplace Privacy

Requirement	Needs work	Don't know	Meets requirement
Does the agency have policies and procedures to ensure that workplace privacy is maintained and records about employees are collected and retained in accordance with the law?			
Does the organisation only require disclosure of criminal convictions that are not concealed under the Clean Slate Scheme?			
Has the agency informed employees of any internet and email monitoring it will undertake on workplace devices and established clear rules for appropriate work and personal use?			
Does the agency keep adequate records of employees' terms of employment and entitlements, and provide access to, or copies of, those records upon request?			
Does the agency that monitors its employees at the workplace do so in accordance with applicable legislative requirements and a workplace surveillance policy?			
Does the person carrying on a business or undertaking in New Zealand have appropriate policies and procedures in place for managing information about workplace injuries and incidents, including notification procedures, and policies and processes for assisting inspectors and health and safety medical practitioners?			
Does the organisation ensure it has policies and processes in place that support employees to make protected disclosures and maintain the confidentiality of any disclosures made?			

# PRIVACY & DATA PROTECTION CHECKLIST

This checklist has been designed to help you identify your requirements.

## Applicability of Privacy Laws

Requirement	Needs work	Don't know	Meets requirement
Does the agency have policies and procedures in place that enable it to comply with the information privacy principles (IPPs) and/or any codes of practice issued under the Privacy Act 2020 (NZ), if any such code applies to the agency's industry, type of information held or functions and activities?			
Does the agency that collects, stores, uses and discloses personal information have policies and procedures in place which enable it to comply with the information privacy principles (IPPs)?			
Do credit reporters adhere to the supplements and modifications to privacy law contained in the Credit Reporting Privacy Code 2020 (NZ)?			
Does the health agency adhere to the supplements and modifications to privacy law contained in the Health Information Privacy Code 2020 (NZ)?			
If the agency is a specified justice sector agency, does it adhere to the Justice Sector Unique Identifier Code 2020 (NZ) in lieu of Information Privacy Principle 13?			
Does the superannuation scheme entity have policies and procedures in place for assigning unique identifiers, which comply with the Superannuation Schemes Unique Identifier Code 2020 (NZ)?			
Does the telecommunications agency adhere to the supplements and modifications to privacy law contained in the Telecommunications Information Privacy Code 2020 (NZ)?			
Does the agency adhere to the supplements and modifications to privacy law contained in the Civil Defence National Emergencies (Information Sharing) Code 2020 (NZ)?			
Does the tenancy database operator ensure its collection, storage and disclosure of tenant information is done in accordance with the information privacy principles (IPPs)?			

## Cross-border Transfers of Information

Requirement	Needs work	Don't know	Meets requirement
Does the agency ensure that transfers of personal information into and out of New Zealand maintain appropriate privacy safeguards in line with the Privacy Act 2020 (NZ) and international and foreign privacy laws?			
Does the agency ensure it continues to fulfil its privacy obligations with respect to any information that is transferred overseas, and does it consider the risks to information privacy involved in any such transfer, such as whether or not the overseas jurisdiction adheres to international privacy guidelines?			
If an overseas entity operates in and brings personal information into New Zealand, does it ensure it complies with the Privacy Act 2020 (NZ) as well as any local privacy laws in the originating jurisdiction?			

# PRIVACY & DATA PROTECTION CHECKLIST

This checklist has been designed to help you identify your requirements.

## Organisational Governance and Privacy Programme

Requirement	Needs work	Don't know	Meets requirement
Does the agency instituted a governance and management framework that facilitates its compliance with privacy laws?			
Does the agency appoint a privacy officer who is responsible for promoting privacy and managing the agency's compliance with the Privacy Act 2020 (NZ)?			
Does the agency put in place systems, processes and management practices to cultivate a culture in the agency that encourages and enables compliance with privacy laws?			
Does the broadcaster maintain its programmes to standards that respect the privacy of the individual, and does it have in place systems for individuals to complain about a breach of privacy in a broadcast?			
Does the agency put in place systems, processes and management practices to ensure that it complies with its obligations relating to information sharing agreements?			

## Managing Complaints and Investigations

Requirement	Needs work	Don't know	Meets requirement
Does the agency have procedures in place to receive, respond to and manage complaints received both internally and by the Privacy Commissioner?			
Does the agency appointed a privacy officer who is responsible for managing the agency's compliance with privacy laws?			
Does the agency have procedures in place to assist and cooperate with the Office of the Privacy Commissioner in responding to complaints and related investigations?			

# PRIVACY & DATA PROTECTION CHECKLIST

This checklist has been designed to help you identify your requirements.

## Information Matching Programmes

Requirement	Needs work	Don't know	Meets requirement
Does the agency operate an information matching programme with the appropriate legal authority, using systems, processes and safeguards in accordance with the information matching rules?			
If the agency is operating a programme under an information matching provision, has it first entered into an approved information matching agreement?			
Does the agency comply with relevant limitations and restrictions associated with taking adverse action against an individual, based on information derived from an information matching discrepancy?			
If the agency has entered into an information matching agreement, has it given notice to individuals who will be affected by the information matching program and/or related adverse action?			
If the agency is in an information matching programme, has it established systems and procedures for transferring personal information between parties to the agreement in accordance with documented technical standards?			
If the agency is in an information matching programme, has it established appropriate safeguards to protect personal information used in the programme and controlled the instigation of adverse action?			
Does the agency have systems and processes in place which enable it to report on the efficiency of the information matching programme, when requested to do so by the Privacy Commissioner?			

## Ensuring the Accuracy of Personal Information

Requirement	Needs work	Don't know	Meets requirement
Does the agency take reasonable steps to ensure the accuracy of personal information it handles?			
Does the agency take reasonable steps to ensure that the personal information held by the agency is accurate, up to date, complete and relevant, and that the personal information is not misleading?			
Does the agency take reasonable steps to ensure that before using or disclosing personal information, it verifies that the information is accurate, up to date, complete, relevant and not misleading?			

# PRIVACY & DATA PROTECTION CHECKLIST

This checklist has been designed to help you identify your requirements.

## Protecting Confidential Information from Disclosure

Requirement	Needs work	Don't know	Meets requirement
-------------	------------	------------	-------------------

Does the agency have policies and procedures in place to ensure that confidential information is not disclosed in a way that is not authorised by law?

Does the agency have policies and procedures in place to ensure it does not disclose confidential information when there is no lawful reason to do so?

Does the agency comply with the communications principles governing digital communications and implement policies and procedures to ensure that digital communications are not made in a way that disclose personal information or cause harm or intend to cause harm?

## Investigations and Enforcement

Requirement	Needs work	Don't know	Meets requirement
-------------	------------	------------	-------------------

Does the agency participate appropriately in Privacy Commissioner and Human Rights Review Tribunal proceedings and comply with any related directions or orders?

Does the agency ensure that internal decision-making about privacy and personal information is done so consistently with the rights contained in the Bill of Rights Act 1990 (NZ) and the Human Rights Act 1993 (NZ)?

Does the agency assist the Privacy Commissioner in the conduct of any investigation by complying with the Privacy Commissioner's directions and/or requirements?

Does the agency comply with the directions and summonses from the Human Rights Review Tribunal, if the agency is a party to proceedings or required to give evidence or produce documents or material relevant to proceedings?

Does the agency have policies, procedures and systems in place which enable it to comply with orders or directions issued to it in relation to upholding or enforcing the Privacy Act 2020 (NZ)?

# PRIVACY & DATA PROTECTION CHECKLIST

This checklist has been designed to help you identify your requirements.

## Complying with the Payment Card Industry Data Security Standard

Requirement	Needs work	Don't know	Meets requirement
If the organisation stores, processes or transmits payment cardholder data, does it comply with the Payment Card Industry Data Security Standard?			
Does the organisation install and maintain network security controls to protect cardholder data that it stores, processes or transmits?			
Does the organisation ensure that it does not use vendor-supplied defaults for system passwords and other security parameters?			
Does the organisation establish and implement procedures for the protection of stored cardholder data, including procedures to keep cardholder data storage to a minimum and to protect keys used to secure stored data, and does it ensure the use of the procedures on an ongoing basis?			
Does the organisation ensure that it uses strong cryptography and security protocols to safeguard cardholder data during transmission over open, public networks?			
Does the organisation ensure that it deploys and maintains anti-virus mechanisms to protect its systems against malware, and that it conducts periodic reviews to identify emerging malware threats that may require addressing?			
Does the organisation implement required measures for the secure development and maintenance of its systems and applications?			
Does the organisation ensure it restricts access to cardholder data by operational need?			
Does the organisation ensure that users are properly identified and authenticated before they can access system components?			
Does the organisation establish, document and implement procedures for the restriction of physical access to cardholder data?			
Does the organisation track and monitor all access to network resources and cardholder data, including through the use of audit trails to link access to system components to each individual user?			
Does the organisation perform regular testing of its security systems and processes, including testing for wireless access points, running internal and external network vulnerability scans, performing penetration testing and utilising mechanisms to detect changes and prevent intrusions?			
Does the organisation have an information security policy in place that it publishes, maintains and disseminates, as well as related procedures including an incident response plan and procedures for managing relationships with third-party service providers?			

## Your No-Obligations Demonstration

If you would like a demonstration of the Privacy & Data Protection compliance register, click or scan the QR code. →



## About LexisNexis Regulatory Compliance

LexisNexis Regulatory Compliance helps you forge a clear path to compliance.

With LexisNexis content know-how at the core, our compliance registers, alerts, and information-driven solutions make compliance uncomplicated for GRC professionals across the globe.

- Find relevant obligations faster with jargon-free registers that are aligned with your business processes.
- Stay up to date with near real-time alerts delivered straight to your inbox when you may be impacted by regulatory change.
- Explore your compliance obligations under a particular regulator, or a particular compliance source, with SourceData.
- Engage with the wider compliance community and LexisNexis experts through the Community Portal, our self-support platform.
- Access comprehensive, current LexisNexis content that meets your unique needs, with key core modules relevant to all businesses, and a rapid accelerating roadmap of industry-specific modules that guide your path to compliance.

Authored by leading legal, attorney and industry experts, and supported by flexible technology that works the way you do, LexisNexis Regulatory Compliance gives you peace of mind while saving time and money.

**Call** 0800 800 986

**Email** [compliance@lexisnexis.co.nz](mailto:compliance@lexisnexis.co.nz)

**Visit** [www.lexisnexis.co.nz/compliance](http://www.lexisnexis.co.nz/compliance)

## About LexisNexis

LexisNexis is part of RELX Group, a world-leading provider of information and analytics for professional and business customers across industries. LexisNexis helps customers to achieve their goals in more than 175 countries, across six continents, with over 10,000 employees.