A-Z Guide

PRIVACY

Contents

Overview

- The Privacy Act 2020 applies to many aspects of employment.
- The information privacy principles specify how personal information about an individual must be collected, protected, used and disclosed.
- The Privacy Act 2020 introduces a regime whereby the Privacy Commissioner must be notified of serious privacy breaches. Liability for privacy breach notifications sits with a business or organisation (an 'agency'), rather than individual employees.
- Employees may raise an employment relationship problem with their employer if they have had their privacy breached.

Introduction

In New Zealand three statutes, one of which is specialist, govern privacy issues. These are the Privacy Act 2020, the Official Information Act 1982 and the Health and Disability Commissioner Act 1994. This A-Z guide deals with only the Privacy Act 2020 and concentrates on employers' obligations to their employees and any other issues that arise out of employment.

Refer to the A-Z Guides on the Official Information Act 1982 and the Health and Disability Commissioner Act 1994 for information on those statutes.

There are other A-Z Guides that deal with the provisions of the Privacy Act 2020. The Act is discussed as it relates to the topic in:

- Application for Employment
- Disability
- Discipline
- Drug Testing
- Human Rights
- Medical Certificates
- Medical Examinations
- Records
- Recruitment and Selection
- Restructuring and Redundancy
- Serious Privacy Breaches
- Tape Recording
- Surveillance

Privacy Act

Purpose

The origins of New Zealand's privacy legislation can be found in Article 17 of the 1966 United Nations Covenant on Civil and Political Rights in 1978. This provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy" and that "everyone has the right to the protection of the law against such interference."

The Act brings us into line with, and gives effect to, internationally recognised privacy obligations and standards in relation to the privacy of personal information, including the OECD Guidelines and comparative jurisdictions.

- It was designed to meet the objective of this international obligation by providing a framework for protecting an individual's right to privacy of personal information, including the right of an individual to access their personal information.
- It establishes information privacy principles and codes of practice that relate to:
    - The collection, use, and disclosure, by public and private sector agencies, of information relating to individuals; and
    - Access by each individual to, and correction of, information relating to that individual held by public and private sector agencies.
- It provides for a Privacy Commissioner to investigate complaints about interferences with individual privacy and take appropriate action as necessary.

Part 3 of the Privacy Act 2020 sets out 13 information privacy principles which govern:

- Purpose of collection of personal information
- Source of personal information
- Collection of information from subject
- Manner of collection of personal information
- Storage and security of personal information
- Access to personal information
- Correction of personal information
- Accuracy of personal information to be checked before use or disclosure
- Agency not to keep personal information for longer than necessary
- Limits on use of personal information
- Limits on disclosure of personal information
- Disclosure of personal information outside New Zealand
- Unique identifiers

The Privacy Commissioner will be able to issue compliance notices to businesses or organisations requiring them to remedy any breach. This may identify particular steps that the Commissioner considers need to be taken, including a date by which the business or organisation must make the necessary changes.

Furthermore, the Commissioner may publish information about the business or organisation that breached the Act following the issuing of a compliance notice if it believes it is desirable to do so in the public interest. A fine not exceeding $10,000 may be imposed for noncompliance.

Definitions

The definitions provided here are extracted from the Act itself.

Agency
Means a person to whom this Act applies. This includes:

- A New Zealand agency, in relation to any action taken by that agency whether or not while the agency is, or was, present in New Zealand in respect of personal information collected or held by the agency;
- An overseas agency, in relation to any action taken by that agency in the course of carrying on business in New Zealand in respect of personal information collected or held by the agency;
- An individual who is not ordinarily resident in New Zealand, in relation to any action taken by that individual in respect of:
    - Personal information collected by that individual while present in New Zealand, regardless of where the information is subsequently held by the individual or where the individual to whom the information relates is, or was, located;
    - Personal information held by that individual while present in New Zealand (but not collected by the individual while present in New Zealand), regardless of where the individual to whom the information relates is, or was, located.

Collect
Any step to seek or obtain the personal information. Does not include the receipt of unsolicited information.

Correct
Altering personal information by way of correction, deletion or addition.

Document
Means a document in any form, and includes:

- Any writing on any material;
- Any information recorded or stored by means of any computer or other device, and any material subsequently derived from information so recorded or stored;
- Any label, marking, or other writing that identifies or describes any thing of which it forms part, or to which it is attached by any means;
- Any book, map, plan, graph, or drawing;
- Any photograph, film, negative, tape, or any other device in which one or more visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced.

Personal information
Information about an identifiable individual; and includes information relating to a death that is maintained by the Registrar-General under the Births, Deaths, Marriages and Relationships Registration Act 1995, or any former Act.

Unique identifier
In relation to an individual, means an identifier other than the individual's name that uniquely identifies the individual.

Information Privacy Principles

Collection

Principles 1 to 4 prescribe why and how personal information may be collected by employers.

The important points to note are:

- Personal information should only be collected by an employer for a lawful purpose connected with a function or activity of that employer. The collection of the personal information must be necessary for that purpose.
- If the lawful purpose for which personal information about an individual is collected does not require the collection of an individual's identifying information, the employer may not require the individual's identifying information.
- Personal information must be collected directly from the individual concerned.
- If an employer collects personal information from the individual concerned, the employer must take reasonable steps to ensure that the individual concerned is aware of:
    - The fact that the information is being collected; and
    - The purpose for which the information is being collected; and
    - The intended recipients of the information; and
    - The name and address of the business or organisation that is collecting and holding the information; and
    - Whether the collection is authorised or required by law and, if so, what law, and whether the supply of the information is voluntary or mandatory; and
    - The consequences of not providing the requested information; and
    - That they have the right to access the personal information and to correct it.

A business or organisation may collect personal information only by a lawful means that is fair and does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

The collection principles mean that you should not randomly collect personal information about an individual; any collection of personal information should be related to the individual's employment or prospective employment. If you seek information that has little, or nothing, to do with the individual's employment or prospective employment you risk a claim by that individual that you have interfered with their privacy.

An example of breach of privacy is where the employer contacts an employee's referees where the purpose is not related to the application for employment (for example, contacting the referee several months after employment has commenced, to discuss any misconduct or performance issues from the previous employment): *Wilson v Taupo Therapy Centre Incorporated* [AA 411/08; 04/12/2008; P Cheyne]

Protection

Principles 5 to 9 prescribe how personal information should be protected by employers.

The important points to note are:

- An employer that holds personal information must ensure that the information is protected by reasonable security safeguards against loss, unauthorised access, use, modification, disclosure, and other misuse.
- An individual is entitled to receive from an employer confirmation of whether the employer holds any personal information about them, and access to that information.
- An individual whose personal information is held by an employer is entitled to request the employer to correct the information. The employer holding the personal information must take reasonable steps to ensure the information is accurate, up to date, complete, and not misleading.
- If an employer that holds personal information is not willing to correct the information as requested and has been provided with a statement of correction, the employer must take reasonable steps to ensure that the statement of correction is attached to the information in a manner that ensures that it will always be read with the information.
- An employer that holds personal information must not use or disclose that information without taking reasonable steps to ensure that the information is accurate, up to date, complete, relevant, and not misleading.
- An employer that holds personal information must not keep that information for longer than is required for the purposes for which the information may lawfully be used.

The protection principles mean that if you collect personal information about an individual then you are obliged to ensure that it is fit for the purpose for which you collected it, before you use it. If you retain personal information about an individual then you are obliged to protect the integrity of that information. The principles also reinforce the idea that, while you may collect personal information about an individual related to the individual's employment, the individual concerned continues to have rights in respect of the personal information collected.

Use and disclosure

Principles 10 to 12 prescribe how personal information which has been collected may be used or disclosed by employers.

The important points to note are:

- An employer who holds personal information that was obtained in connection with one purpose may not use the information for any other purpose or disclose that information to another agency unless:
    - The use or 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; or
    - The information will be used in a form in which the individual concerned is not identified; or
    - The use or disclosure is authorised by the individual concerned; or
    - The disclosure is to the individual concerned; or
    - The information is publicly available; or
    - The use or disclosure is necessary to prevent a miscarriage of justice; or
    - The use or disclosure is necessary to prevent or lessen a serious threat to public health and safety or the life or health of an individual; or
    - The information 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
    - The disclosure is necessary to facilitate the disposal of a business as a going concern.

Disclosure of personal information outside New Zealand

An employer may disclose personal information to a foreign person or entity if:

- The individual concerned authorises the disclosure to a foreign person or entity after being expressly informed by the employer that the foreign person or entity may not be required to protect the information in a way that provides comparable safeguards to those in this Act; or
- The foreign person or entity is carrying on business in New Zealand and the employer reasonably believes that the foreign person or entity is subject to this Act; or
- The employer reasonably believes that the foreign person or entity is subject to privacy laws that provide comparable safeguards to those in this Act; or
- The employer otherwise reasonably believes that the foreign person or entity is required to protect the information in a way that provides comparable safeguards to those in this Act.

The use and disclosure principles mean that employers must use or disclose personal information in a way that is consistent with the purpose(s) it was collected for in the first place. There is scope to use or disclose the information if it is to, or authorised by, the individual concerned, or if the information is publicly available.

There are also certain other exceptions where information may be used or disclosed. The obligation to limit use or disclosure of personal information is expressly extended in the Act to foreign persons or entities outside New Zealand unless disclosure is authorised by the employee, or if the information is protected by the foreign entity to a similar standard.

Unique identifiers

Principle 13 prescribes how unique identifiers may be assigned.

The important points to note are:

- An employer may assign a unique identifier to an individual for use in its operations only if that identifier is necessary to enable the employer to carry out one or more of its functions efficiently.
- An employer may not assign to an individual a unique identifier that, to the employer's knowledge, is the same unique identifier as has been assigned to that individual by another agency unless the unique identifier is to be used by the employer solely for statistical or research purposes.
- An employer must take any reasonable steps to ensure that:
    - A unique identifier is assigned only to an individual whose identity is clearly established; and
    - The risk of misuse of a unique identifier is minimised
- An employer may not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned or is for a purpose that is directly related to one of those purposes.

The unique identifier principle ensures employers assign unique identifiers to individuals only when really necessary. Employers must clearly establish the identity of an individual assigned a unique identifier, and take care that it is not misused. Unique identifiers must be used for the purpose for which they are assigned.

Employee Access and Correction

Part 4 of the Act deals with an employee's access to, and correction of, personal information about them held by their employer. An employee is entitled to confirmation of whether the employer holds any personal information about them, and to access that information. They are also entitled to request the employer to correct the personal information about them, which must be accurate, complete and up to date.

These requests are referred to as an **IPP6 request**. Employees may make **correction (IPP7)** requests on a similar basis. An employer must, as soon as is reasonably practicable, and not later than 20 working days after the day on which the request is received, respond to a request.

If the employer that receives a request does not hold the information but believes that the information is held by, or more closely connected with, another employer then they must transfer the request within 10 working days and inform the requestor.

Charges may be imposed for providing assistance but only if the employer makes part or all the requested information available. Employers must provide reasonable assistance to an employee wishing to make, or making, an IPP6 or correction request. An employer may refuse access to any personal information requested, on grounds detailed in the Act.

Responding to requests

If an employer does not transfer an IPP6 or IPP7 (correction) request the employer must respond to the request no later than 20 working days after the request is received, and as soon as is reasonably practicable.

A response to an IPP6 request must notify the requestor that the employer:

- does not hold personal information in a way that enables the information to be readily retrieved; or
- does not hold any personal information about the individual to whom the request relates; or
- neither confirms nor denies that it holds any personal information about the individual to whom the request relates.

If an employer grants access to personal information, they must state:

- the way the information is to be made available; and
- the charge or cost for doing this (if any), and whether all or part of that charge is required to be paid in advance; and
- the requestor's right to make a complaint to the Commissioner about the charge that is payable (if any).

After giving notice and receiving any charge required to be paid in advance, the employer must make the information available to the requestor.

A response to an IPP7 request must notify the requestor that the employer:

- corrected, or will correct, the personal information; or
- will not correct the personal information; or
- the reason for the agency's refusal to correct the information; and
- the requestor's entitlement to provide a statement of the correction sought and to request that it be attached to the information; and
- the requestor's right to make a complaint to the Commissioner if the agency refuses to correct the information.

Time limits may be extended for IPP6 or IPP7 requests if a response cannot reasonably be given within the original time limit. Notice of the extension must be given to the requestor within 20 working days after the request is received. It must specify the reasons, length and that requestors have the right to make a complaint to the Commissioner about it.

Information in documents

If the personal information requested is contained in a document, and there is good reason under the Act for withholding some of that information, the employer may decide to make deletions or alterations of information that could be withheld that it considers necessary, when it provides its copy of the document.

If information is withheld the employer must inform the requestor of the reason for the information being withheld and the requestor's right to make a complaint to the Commissioner in respect of that decision.

Unless there is good reason for withholding it, information contained in a document may be made available to the requestor by:

- Giving the requestor a reasonable opportunity to inspect the document; or
- Providing the requestor with a copy of the document; or
- Giving the requestor an opportunity to hear or see the recording; or
- Providing a written transcript; or
- Giving an excerpt or summary of the contents; or
- Giving oral information about the contents.

The information must be made available in the way preferred by the requestor unless it would impair efficient administration or be contrary to a legal duty of the employer. If the information is not provided in the preferred way the employer must give the reason why it is not.

Reasons for refusing access

An employer may refuse access to requested personal information in these situations.

Section 49: Protection, etc, of an individual

- It would be likely to pose a serious threat to the life, health, or safety of any individual, or to the public; or
- It would create a significant likelihood of serious harassment of an individual; or
- It would include disclosure of information about the victim of an offence; or
- It would be likely to prejudice the health of the individual concerned; or
- It would be contrary to the interests of an individual under the age of 16; or
- It would be likely to prejudice the safe custody/rehabilitation of an individual who has been convicted of an offence or detained.

Section 50: Evaluative material - see page 10

Sections 51 to 52: Security, defence, international relations or trade secrets

- It would prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand; or
- It would disclose a trade secret or unreasonably prejudice the commercial position of the employer or individual concerned.

Section 53: Other reasons

- It cannot be found; or
- It would involve the unwarranted disclosure of the affairs of another individual or a deceased person; or
- It would be likely to prejudice the maintenance of the law; or
- It would breach professional privilege; or
- It would breach a condition of material placed in any library, museum or archive; or
- It would constitute contempt of court or of the House of Representatives; or
- The request is made by a defendant; or
- The request is frivolous or vexatious, or the information requested is trivial.

If an employer refuses access under these grounds, the employer usually must give the reason for the refusal and inform the requestor of their right to make a complaint to the Commissioner in respect of the refusal. The exception is if disclosure of the grounds would prejudice the interests being protected by non-disclosure.

If personal information is provided, the employer must be satisfied of the identity of the requestor. They must not provide information if they have reasonable grounds to believe that the request is made under the threat of physical or mental harm. They must ensure that any personal information provided is received only by the person making the request, or for whom the request is being made.

If an information privacy request would prejudice any interest otherwise protected by sections 49 to 53 then the employer may neither confirm nor deny that it holds the information, or some of it. The employer must inform the requestor of their right to make a complaint to the Commissioner in respect of their response.

Evaluative material

Section 50 prescribes circumstances when an employer may refuse access to personal information because it is evaluative material.

Access to personal information may be refused where:

- The disclosure of the information or of information identifying the person who supplied it would breach an express or implied promise:
  - That was made to the person who supplied the information; and
  - That was to the effect that the information or the identity of the person who supplied it, or both, would be held in confidence.
- For the purpose of determining the suitability, eligibility, or qualifications of the individual to whom the material relates:
  - For employment or appointment to office; or
  - For promotion in employment or office or for continuance in employment or office; or
  - For removal from employment or office; or
  - For the awarding of contracts, awards, scholarships, honours, or other benefits; or
- For the purpose of determining whether any contract, award, scholarship, honour, or benefit should be continued, modified, or cancelled; or
- For the purpose of deciding whether to insure any individual or property or to continue or renew the insurance of any individual or property.

It does not include any evaluative or opinion material that is compiled by a person employed or engaged by an employer in the ordinary course of that person's employment or duties.

Restructuring and redundancy

Employees have the right to information about themselves. Employers are not required to provide an affected employee with confidential information about *another* identifiable individual, if doing so would involve an unwarranted disclosure of the affairs of that individual.

Privacy Officers

Section 201 of the Act requires every employer to have at least one privacy officer.

They may be from within or outside the organisation and are responsible for:

- Encouraging your organisation's compliance with the information privacy principles;
- Dealing with requests made under the Act;
- Working with the Privacy Commissioner on investigations in relation to the organisation;
- Ensuring your organisation's compliance with the provisions of the Act generally.

Your organisation's privacy policy should describe the role of the privacy officer within your organisation. They are the person to whom all requests and complaints in relation to personal information are made. A reform of the Act is completed. For a summary of the new Act, please contact AdviceLine.

Remember

- Always call AdviceLine on 0800 300 32 to check you have the latest guide.
- Never hesitate to ask AdviceLine for help in interpreting and applying this guide to your fact situation.
- Use our AdviceLine employment advisors as a sounding board to test your views.
- Get one of our consultants to draft an agreement template that's tailor-made for your business.

This guide is not comprehensive and should not be used as a substitute for professional advice.

Published: **June 2024**

ema.co.nz | 0800 300 362