ADVICEWISE PEOPLE

PEOPLE

BUSINESS

EMPLOYMENT LAW

Year-end closedowns

In the June 2020 newsletter we reported on an Employment Court case on the correct way to calculate holiday pay during a customary closedown, for employees who are not entitled to annual holidays at that point. With the year-end looming, you might want to refresh your memory.

The essence of the case was that it is compulsory to pay the employee 8% of gross earnings since commencement of employment or since the employee last became entitled to annual holidays. It's important to note that the whole 8% is paid out.

Of course, any amount paid for annual holidays in advance or with the employee's pay under section 28 of the Holidays Act 2000 (casuals and fixed term appointments) is to be deducted.

The first day of the closedown then becomes the employee's anniversary date.

In addition, employer and employee can mutually agree that paid leave in advance be taken for the period of the closedown.

Christmas and New Year public holidays 2020/2021

Where any of the four year-end public holidays fall on a Saturday or Sunday, the following Monday or Tuesday becomes the public holiday. This year-end's public holidays are -

- Christmas Day Friday 25 December 2020
- Boxing Day Saturday 26 December 2020 or Monday 28 December 2020
- New Year's Day Friday 1 January 2021
- Saturday 2 January 2021 or Monday 4 January.

Persons who would otherwise work on Friday 25 December 2020, Saturday 26 December 2020, Friday 1 January 2021 or Saturday 2 January 2021, get the day off on full pay. If they perform work on any of these days, they are paid time-and-a-half for the hours actually worked plus an alternative holiday.

Persons who would not otherwise work on Saturday 26 December 2020 get Monday 28 December 2020 off as a public holiday, on full pay. The same applies to Saturday 2 January, which is transferred to Monday 4 January 2021. If they perform work on either of these Mondays, they are paid time-and-a-half for the hours actually worked plus an alternative holiday.

Note that Christmas day 2020 is not Mondayised, so if it is not otherwise a working day for an employee, they are not paid for it. The same for New Year's Day 2021.

Privacy Act 2020

The updated Privacy Act 2020 comes into effect on 1 December 2020. The following is a summary of important changes made.

Class actions

A major change will allow the Human Rights Review Tribunal to award up to $350,000 to each member of a class action.

Children and young people
Privacy Principle 4 has been clarified, requiring agencies to ensure the way they collect information from children and young people is fair.

Mandatory reporting of privacy breaches
Reminiscent of the Health and Safety at Work Act 2015, the Privacy Act makes it compulsory to notify the Commissioner of privacy breaches.

If a business or organisation has a privacy breach that it believes has caused (or is likely to cause) serious harm, it must notify the Office of the Privacy Commissioner and affected individuals as soon as possible. Under the Act, it is an offence to fail to inform the Privacy Commissioner when there has been a notifiable privacy breach.

The Act clarifies that liability for breach notifications sits with the business or organisation, and not the individual employees.

Not all privacy breaches need to be reported. The threshold for a notifiable breach is 'serious harm'. This can be assessed by considering, for example, the sensitivity of the information lost, actions taken to reduce the risk of harm, the nature of the harm that could arise, and any other relevant matters.

The Office of the Privacy Commissioner has a new online privacy breach notification tool called NotifyUs and updated guidance ahead of the new Act to help businesses and organisations with this new requirement. Current guidance on handling privacy breaches can be found here.

Compliance notices
The Privacy Commissioner will be able to issue compliance notices to businesses or organisations to require them to do something, or stop doing something, in order to comply with the Privacy Act. Compliance notices will describe the steps that the Commissioner considers are required to remedy non-compliance with the Act and will specify a date by which the organisation or business must make the necessary changes.

Enforceable access directions
The Privacy Commissioner will be able to direct agencies to provide individuals access to their personal information. This will allow faster resolution of complaints relating to information access under principle 6. Access directions will be enforceable in the Human Rights Review Tribunal.

Disclosing information overseas
A new privacy principle 12 has been added to the Privacy Act to regulate the way personal information can be sent overseas. Under principle 12, an organisation or business may only disclose personal information to an agency outside of New Zealand if the receiving agency is subject to similar safeguards to those in the Privacy Act.

If a jurisdiction does not offer similar protections, the individual concerned must be fully informed that their information may not be adequately protected and they must expressly authorise the disclosure.

Extraterritorial effect
The new Privacy Act now clearly states that it has extraterritorial effect. This means that an overseas business or organisation that is 'carrying on business' in New Zealand will be subject to the Act's privacy obligations, even if it does not have a physical presence here. This will affect businesses located offshore, such as Google and Facebook.

New criminal offences
The Privacy Act 2020 introduces new criminal offences. It will now be an offence to mislead an agency in order to access someone else's personal information – for example, impersonating someone in order to access information that you are not entitled to see.

It will also be an offence for an organisation or business to destroy personal information, knowing that a request has been made to access it. The penalty for these offences is a fine of up to $10,000.

Privacy Officers
At least one privacy officer must be appointed. They will be responsible for among others—

- encouraging the agency to comply with the Information Privacy Principles
- dealing with requests made to the agency
- working with the Commissioner in relation to investigations conducted under Part 5 in relation to the agency
- ensuring that the agency complies with the provisions of the Act.

Further changes
The new Act retains the privacy principles of the current legislation, with some changes. Principle 1 has been clarified to ensure that businesses and organisations do not collect identifying information from people if it is not necessary.

There are new withholding grounds for access requests under principle 6. These grounds for refusal include evaluative material, protection of the individual, trade secrets, and others.

The Codes of Practice, such as the Health Information Privacy Code, will be updated in accordance with the provisions in the new Act. The Commissioner's Office will be releasing further guidance on all the key changes later this month.

Privacy, Covid-19 and the 'Serious Threat to Public Health' exception

The Privacy Commissioner, John Edwards, has just published timely and practical advice on this subject on their website. The following is an edited extract.

While New Zealand has experienced pandemics in the past, the epidemiological characteristics of this virus, global nature and the connected nature of our lives means controlling COVID-19 will require both ongoing vigilance and speed of response.

Knowing who is potentially at risk and being able to rapidly and effectively locate and isolate positive cases has been critically important in NZ's science-based approach to fighting the virus. This brings personal information and privacy into play.

Serious threat to public health or safety exception
The 1993 and 2020 Privacy Acts envisaged a scenario where the collection, use and disclosure of personal information would be needed to combat a serious threat to public health or safety. The serious threat to public health or safety ('public health exception') was designed specifically for this purpose. It permits the collection, use and disclosure of personal information where it is necessary to prevent or lessen a serious threat to public health or public safety[1].

While the public health exception has existed since 1993, it has been very rarely used. People are more familiar with the parallel exception for a serious threat to the health and safety of an individual. Agencies

therefore appear uncertain about how to use the public health exception where the threat affects a community or wider section of the population.

How can agencies determine whether a public health exception is applicable?
To make use of the Privacy Act's public health exception decision-makers within an agency need to believe, on reasonable grounds, that:

- a serious threat to public health and safety exists;
- that the collection, use or disclosure of personal information is necessary to prevent or lessen the serious threat; and
- in the case of health agencies, that it is either not desirable or not practicable to obtain authorisation from the individual concerned**[2]**.

The key point is that public health is at stake. A decision-maker's "reasonable belief" regarding both the existence of a serious threat and the extent to which the use or disclosure of personal information is necessary to prevent or limit this serious threat should therefore be on made on health grounds and based on current best practice epidemiological or clinical advice.

This makes the serious threat to public health exception an ideal regulatory tool for dealing with a dynamic, evolving public health threat like Covid-19 where the "rules" need to keep adapting to meet live challenges.

The Ministry of Health has the lead role in advising the Government and New Zealand on whether a situation represents a serious threat to public health. The Ministry of Health is also responsible for coordinating and disseminating best practice scientific advice on what is necessary to prevent or lessen the threat of COVID-19.

This by extension includes the information necessary in order to monitor and control the risk to New Zealand from the movement of people across our border, and track, trace, isolate and quarantine infection risk within New Zealand.

Agencies are entitled to rely on this advice in making decisions regarding whether the collection, use and sharing of personal information is necessary to prevent or lessen the threat posed by the transmission of Covid-19.

Is information sharing about groups of individuals permitted?
Public health is, by definition, focussed on keeping the community well and on groups of people rather than individuals. This provides a basis for the collection, use and disclosure of personal information about a **class** of individuals that is reasonably considered to be necessary based on relevant criteria, rather than on an individualised basis.

The reasons for sharing aggregated data about a class of individuals (for example people seeking to enter New Zealand or people testing positive and their close contacts, or people working in at-risk situations) should be based on best-practice health advice.

Given the ongoing nature of the threat it is likely that agencies involved in pandemic management will need to continue to share information and will need to make regular assessments of the extent to which the "serious threat to public health and safety" exception still applies as they do so.

Good privacy practice still applies – maintaining trust and confidence is critical

Even where the public health exception is being relied on, good basic privacy practice remains important in order to maintain trust and confidence of the community. The public health exception applies to the source of personal information (2), use (10) and disclosure (11) information privacy principles.

The other principles, including those covering collecting only what is necessary, safe storage and security, access by individuals to their own data, and ensuring accuracy before disclosure still apply.

Maintaining trust and confidence also involves agencies being transparent about what data they're collecting and what it will be used for. If specific data needs to be collected and then shared for the Covid-19 response, best practice would see an agency advising individuals of this at the time of collection or when an individual was signing up for or receiving a service (for example, when making a booking to come to New Zealand).

This could also mean that agencies do not need to rely on the public health exception, as onward use or disclosure for Covid-19 purposes was one of the purposes of collecting the information in the first place.

[1] See Information Privacy Principles 10 (use) and 11 (disclosure). For the avoidance of doubt, from 1 December 2020 the exceptions for principle 2 (source of personal information) are being expanded to include collection necessary to prevent or lessen a serious threat to the life or health of the individual concerned or any other individual.
[2] Health Information Privacy Code Rule 11(2)

Bullying and harassment at work

MBIE has released an Issues Paper on bullying and harassment (including sexual harassment) at work in New Zealand and is inviting submissions by 31 March 2021. The agency is keen to hear from persons or groups familiar with or who have experience or knowledge of systems that prevent or respond to bullying and harassment at work.

The Issues Paper is accompanied by Summary and there are templates for making submissions on either of these. In addition, there is an online survey.

Small business cash flow loan scheme extended

The Government has announced a three-year extension of the Small Business Cashflow Loan Scheme, and a provision of up to two years interest free. The scheme, which was due to expire at the end of the year, will now end on 31 December 2023. The interest free period has been extended from one year to two years.

This article is brought to you by the Window and Glass Association's free employment helpline 0800 692 384. If you have any questions or would like to discuss the article above, please call Philip or Anthony on the helpline.