Copeland Ashcroft
WORKPLACE LAWYERS
employment health & safety immigration

PRIVACY 101

Introduction

1. The Privacy Act 2020 (**Act**) applies to "agencies" which is any person or body of people which collects and holds personal information about other people.

2. Personal information might include names and contact details of customers, personal details including health information about employees, financial information and the like. It is important that this information is protected, and likely that every business is an "agency", collecting personal information in some form.

3. The Act is based on 13 Privacy Principles that, in summary, provide that agencies must:

   3.1 Only collect information they need;

   3.2 Collect information directly from the individual where possible;

   3.3 Be open about what information will be used for;

   3.4 Be fair about how information is collected;

   3.5 Keep information secure;

   3.6 Let people access their own information;

   3.7 Correct information if the person it relates to thinks it is wrong;

   3.8 Make sure information is accurate before use;

   3.9 Dispose of information if it is no longer needed;

   3.10 Only use information for the reason it was collected;

   3.11 Only share information with good reason;

   3.12 Only send information overseas if it will be adequately protected; and

   3.13 Only use unique identifiers when it is clearly allowed.

What is a Privacy Officer?

4. Agencies are required to have a Privacy Officer.

5. A Privacy Officer does not need any formal training but should understand the Act and what to do if a breach occurs or if the agency receives a request for personal information.

6. The Privacy Officer will also assist the Privacy Commissioner if there is an investigation into a privacy breach.

What happens where someone requests information under the Act?

7. An agency has 20 working days to respond to the request for information but must do so as soon as reasonably practicable.

8. The agency should either give notice that the information will be made available, how it will be made available and whether there will be a charge payable in respect of the request. The notice should also include the requestor's right to make a complaint to the Commissioner about that charge that is payable (if any).

9. Alternatively, if the information is not able to be provided, respond to the requestor confirming:

   9.1 The agency does not hold the information in a way that it is readily accessible; or

   9.2 The agency does not hold any personal information about the individual;

9.3 The agency does hold personal information about the individual and that some of that information is granted or refused; or

9.4 The agency neither confirms nor denies that it holds any personal information about the individual.

What happens if there is a privacy breach?

10. If a breach of privacy occurs, an agency should:

10.1 Contain the breach;

10.2 Assess the risk;

10.3 Notify those affected by the breach; and

10.4 Prevent future breaches by putting necessary procedures in place.

11. Agencies are required to report any privacy breaches to the Privacy Commissioner where the breach has caused or is likely to cause serious harm.

12. It is not enough for an agency to "remedy" the breach themselves to avoid reporting the breach to the Privacy Commissioner.

Do special rules apply to sending information overseas?

13. Agencies are now required to undertake due diligence when sending information overseas to make sure that the information is protected by similar privacy laws as New Zealand.

14. This might be where agencies have offices in other countries or if information is electronically stored and able to be accessed from overseas.

What is a compliance notice and what are the penalties for a breach?

15. The Privacy Commissioner can issue compliance notices which requires an agency to comply with the direction within a certain period. This might be where the Privacy Commissioner requires an agency to disclose information or to stop the disclosure or use of information.

16. Failure to comply with a compliance notice could result in a fine of up to $10,000.

Are there different rules for the health sector?

17. The Health Information Privacy Code 2020 applies to all agencies providing personal or public health or disability services such as Primary Health Organisations, District Health Boards, Rest homes, supported accommodation, doctors and the like.

18. The Health Information Privacy Code 2020 sets out specific rules for agencies in the health sector.

Are there different rules for the public sector?

19. Additionally, the Official Information Act 1982 and Local Government Official Information and Meetings Act 1987 may apply.

Our team of specialist workplace lawyers throughout the country are always happy to answer your questions, contact us here