The Privacy Act 2020: Considerations for Employers

In December 2020, New Zealand's updated Privacy Act came into force, marking a significant milestone for privacy protection in the digital age. It’s crucial for both employers and employees to understand this legislation and especially how it relates to the collection, use, and disclosure of personal information within the employment relationship. This blog post delves into the relevance of the Privacy Act 2020 in various employment scenarios, explaining the Privacy Principles and some of their implications for human resources and employment relations in businesses and organisations.

Understanding the Privacy Principles

The Privacy Act 2020 is underpinned by 13 Privacy Principles which govern how personal information should be handled, and they are particularly relevant to the HR functions of a business or organisation. Here's how:

1. **Purpose of collection of personal information**: Employers must have a clear and legitimate reason for collecting personal information from employees or job applicants.
2. **Source of personal information**: Generally, it’s best if personal information is collected directly from the individual concerned. This has implications for reference checks, which must be conducted with the individual's consent.
3. **Collection of information from subject**: Employers must inform employees and applicants why their information is being collected, how it will be used, who it will be shared with, how it will be stored and for how long.

4. **Manner of collection of personal information**: Information must be collected in a way that is lawful, fair, and not unreasonably intrusive.
5. **Storage and security of personal information**: Employers are required to keep personal information secure from unauthorised access or disclosure. This includes ensuring personal information such as terms and conditions of employment is not accessible to anyone not authorised, either in electronic files or hard copy. It also includes not discussing personal information with relatives or others without the employee's permission.
6. **Access to personal information**: Employees have the right to access their personal information and request corrections.
7. **Correction of personal information**: Employers must allow individuals to correct their information if it is wrong. Sometimes this can include retaining the earlier version as well as new information provided e.g. information gathered during an employment investigation.
8. **Accuracy of personal information to be checked before use**: Employers must ensure the information they use is accurate, up-to-date, and relevant.
9. **Agency not to keep personal information for longer than necessary**: Personal information should not be kept longer than needed for the purposes for which it was collected. Evaluative material must be destroyed once a decision is made e.g. during recruitment, unless the person has given permission for it to be held after such time.
10. **Limits on use of personal information**: Personal information collected for one purpose should not be used for another without the individual's consent.
11. **Limits on disclosure of personal information**: Disclosure of personal information is restricted and generally requires the individual's consent or must be legally justified.

12. **Cross-border disclosure protections**: Employers must ensure that any personal information sent overseas is protected by acceptable privacy standards.
13. **Unique Identifiers**: There are restrictions on assigning identifying numbers (such as employee numbers in HRIS) and other unique identifiers to individuals. Employers can only assign unique identifiers to employees when it is necessary for its functions.

Employment Scenarios and Obligations

Employer-Employee Relationship

Employers must ensure the privacy of employee information throughout the lifecycle of the employment relationship and beyond. This includes securing sensitive information such as medical records, financial details, and employment history. A breach could occur if an employee's personal information is inappropriately accessed or leaked, highlighting the necessity of robust information security practices and trained staff. Recorded phone calls, emails and hand-written notes could contain personal information as defined by the Act.

Employee's Use of Personal Information

Employees often have access to personal information in their roles, particularly in HR, payroll, finance, health and safety, and customer service positions. It's essential that they understand their obligations to protect this information and use it only for its intended purposes. Misuse of personal information, including for their own gain, may lead to a breach of the Act, and this could have disciplinary consequences for the employee (following due process), as well as potential legal consequences for both the employee and the employer.

Relationships Between Employees and Customers

In roles involving customer interaction, employees must also ensure no breach of the Act occurs in regards to a customer’s personal information. This includes not disclosing personal information without consent and ensuring that any information collected is used solely for

the purpose for which it was gathered, such as providing a service or support.

Employer Requirements

A notable requirement under the Privacy Act 2020 is the appointment of a Privacy Officer in each business and organisation. This individual works to ensure that the business or organisation complies with the Act, including managing personal information, responding to information requests, and leading the response to any privacy breaches.

Notifying the Office of the Privacy Commissioner

The Act also introduced mandatory reporting of privacy breaches that pose a risk of serious harm to individuals. Employers must promptly notify the Office of the Privacy Commissioner and affected individuals of any such breach. This requirement underscores the importance of having effective measures in place to mitigate, detect, report, and respond to privacy breaches.

Conclusion

The Privacy Act 2020 brings a comprehensive approach to personal information management within the workplace, highlighting the mutual responsibilities of employers and employees in protecting privacy. Understanding and adhering to the Privacy Principles is essential for maintaining trust, respecting individual rights, and mitigating risks associated with the handling of personal information. Employers should ensure that their policies, procedures, and training are up to date to comply with the Act.

If you would like to discuss this topic further, please do not hesitate to contact me.

021 932 332 marie@tovioconsulting.co.nz www.tovioconsulting.co.nz