Recent Findings by the Privacy Commission - What Employers Need to Know

Introduction

The Privacy Act 2020 governs how personal information must be handled in New Zealand, placing strict obligations on employers to protect their employees' data. I provided an article about the Privacy Act and its Principles in March, which you can read here.

Recent findings from the Privacy Commission have highlighted several cases where employers have breached these obligations, which of course can lead to significant consequences.

This article provides an overview of these findings, common pitfalls, and practical steps employers can take to ensure compliance.

Understanding the Privacy Act 2020

The Privacy Act 2020 governs how organisations and businesses can collect, store, use and share a person's information. For employers, this means ensuring that any personal data collected, stored, and used is done so in a way that is lawful, fair, and transparent. There are 13 Principles in the Act, that detail how employers should collect, handle and use personal information. The principles (including links to the full wording for each) are as follows:

- **Principle 1 - Purpose for collection**

- **Principle 2 - Source of information - collection from the individual**
- **Principle 3 - What to tell the individual about collection**
- **Principle 4 - Manner of collection**
- **Principle 5 - Storage and security of information**
- **Principle 6 - Providing people access to their information**
- **Principle 7 - Correction of personal information**
- **Principle 8 - Ensure accuracy before using information**
- **Principle 9 - Limits on retention of personal information**
- **Principle 10 - Use of personal information**
- **Principle 11 - Disclosing personal information**
- **Principle 12 - Disclosure outside New Zealand**
- **Principle 13 - Unique identifiers**

Recent Findings by the Privacy Commission

In recent months, the Privacy Commission has investigated several cases where employers have breached the Privacy Act. These cases provide important lessons for all businesses:

Case 1: Failure to Check Templates Leading to a Privacy Breach

Summary: This case involved a company that failed to update its document templates after making significant changes to its privacy policies. As a result, an employee's personal information was incorrectly shared with another party. The error occurred

because the outdated template used did not reflect the current privacy practices of the organisation.

Privacy Commission Findings: The Privacy Commission found that the company had not sufficiently updated its internal guidelines or provided adequate training to staff on the new privacy policies. This oversight led to the unintentional disclosure of personal information, violating the Privacy Act's requirements for maintaining accurate and secure personal data.

Outcome: The company was required to update all document templates, conduct a thorough review of its privacy practices, and provide additional training to employees to prevent similar breaches in the future.

Case 2: Misuse of Personal Information in Employment Context

Summary: An employee raised concerns after discovering that information collected during an internal investigation was later used for purposes unrelated to the investigation. Specifically, the information was included in a separate report that was shared with external parties, without the employee's knowledge or consent.

Privacy Commission Findings: The Privacy Commission determined that the employer had breached the Privacy Act by using the employee's personal information for a different purpose than originally intended. The Commission emphasized the importance of purpose limitation, where personal information should only be used for the purpose for which it was collected unless consent is obtained.

Outcome: The company was ordered to cease using the information for any other purpose and to delete the records in question. The Privacy Commission also recommended that the company revise its internal protocols to ensure that personal data is only used in compliance with the stated purposes.

Case 3: Inadequate Handling of Employee Medical Records

Summary: This case involved a healthcare provider that failed to protect the medical records of its employees adequately. The breach occurred when sensitive medical information was stored on a shared drive accessible to all staff, leading to unauthorized access by individuals who had no legitimate reason to view the records.

Privacy Commission Findings: The Privacy Commission found that the healthcare provider had not implemented sufficient security measures to protect sensitive employee data, thus breaching the Privacy Act. The lack of proper access controls allowed unauthorized employees to view confidential medical information.

Outcome: The healthcare provider was required to implement stricter access controls and ensure that only authorised personnel could access sensitive information. Additionally, the organisation was instructed to provide privacy training to all employees to prevent future breaches.

Common Pitfalls for Employers

- **Lack of Clear Policies:** Without clear data handling and privacy policies, employees may mishandle personal information.

- **Inadequate Training:** Employees who handle personal data must be adequately trained on privacy laws and company policies.
- **Poor Security Measures:** Failing to implement strong security measures, such as encryption and access controls, can lead to data breaches.
- **Failure to Monitor Compliance:** Regular audits and reviews of data handling practices are crucial to ensure ongoing compliance.

Practical Steps to Ensure Compliance:

1. **Conduct Regular Privacy Audits:** Review your data handling practices regularly to identify and address potential weaknesses.
2. **Implement Strong Security Measures:** Ensure that all personal data is stored securely, with access limited to authorised personnel only.
3. **Provide Staff Training:** Regularly train and refresh your staff on privacy laws and company policies to ensure they understand their responsibilities.
4. **Create Transparent Policies:** Develop clear, transparent policies regarding data collection, use, and disposal, and communicate these to your employees.
5. **Engage with Employees:** Be open with your employees about how their data is being used and offer them ways to access and correct their personal information.

Conclusion

The recent findings by the Privacy Commission serve as a timely reminder of the importance of complying with the Privacy Act 2020. By understanding common pitfalls and implementing best practices, employers can safeguard their employees' personal information and avoid the serious consequences of a privacy breach.

Do not hesitate to contact me if you have any questions about this article or if you would like assistance to implement any of the suggested measures or practical steps that can help avoid potential pitfalls and ensure compliance.

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