Employee Data Privacy – New Zealand

Breach Notification

Are there any data breach notification requirements?

A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. Local data protection regulations have required data controllers to report such breaches in certain circumstances.

Under the Privacy Act 2020 (Part 6), New Zealand employers and other agencies are required to notify the data protection Commissioner as soon as practical in the event that a data breach is reasonably believed to have caused or, is likely to cause serious harm to affected individuals. In determining whether a breach caused or is likely to cause serious harm, employers should consider:

- actions taken by the employer to reduce the risk of harm;
- whether the personal data is considered sensitive;
- the nature of the potential harm to individuals;
- if known, the person or body that may receive personal data as a result of the breach;
- whether the personal data is protected via security measures; and,
- other relevant factors.

Notification to the Privacy Commissioner should (Sec. 117):

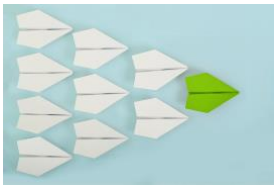
- include a description of the breach, including the number of impacted individuals and the identity of a person or body that the employer suspects may be in possession of personal information as a result of the breach (if known);
- explain steps that the employer has taken or plans to take relating to the privacy breach, including whether affected individual(s) have been or will be contacted;
- if public notice is given, explain the reasons for the public notice (instead of individual notice);
- if notice to impacted individuals is being delayed, include the allowed reason for exception; the reason why the delay is needed; and, the expected period of delay;
- include the names or description of other agencies that the employer has contacted in relation to the privacy breach and the reason for contacting them; and,
- include the appropriate contact information that the Commissioner can reach out to with any questions.

Notice to Individuals

Individuals who are impacted by a notifiable privacy breach must generally be notified as soon as practical. If it's not reasonable to notify individuals, then the employer must instead notify the public of the breach (no affected individuals should be identified in the public notification).

Notification to individuals or their representatives must include:

- a description of the privacy breach and whether the employer has identified a person or body who is suspected to be in possession of the affected personal data (the notice should not identify that person or body);
- an explanation of the steps taken or intended to be taken by the employer in relation to the privacy breach;
- when possible, the steps an individual can take to mitigate or avoid potential loss or harm as a result of the breach (if any);
- a confirmation that the privacy Commissioner has been notified;
- a statement that the individual has the right to make a complaint to the Commissioner; and,
- details of a contact at the employer who individuals can reach out to with questions.



HR Best Practices:

In the event of a notifiable breach, inform the data protection Commissioner and impacted individuals as soon as practicable. Employers should develop and implement a data breach action plan with notification, incident documentation and response procedures.

Last updated October 2022.