Employee Data Privacy – The Republic of the Philippines

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.

Employers in the Philippines (and other personal information controllers) should notify the National Privacy Commission (NPC) and affected data subjects (such as impacted employees) within 72 hours of "sensitive personal information or any other information that may…be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject (Implementing Rules and Regulations of the Data Privacy Act of 2012, Rule IX. Sec. 38)." A full report of the personal data breach must be submitted to the NPC within five days, unless the Commission grants additional time to comply.

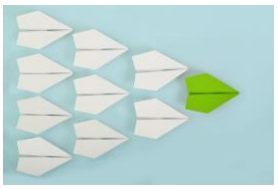
In some circumstances notification may be delayed "only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system (Implementing Rules and Regulations of the Data Privacy Act of 2012, Rule IX. Sec. 39)."

If it's not possible to notify impacted individuals within the required period, employers can request from the NPC permission to delay the notification or to exempt the notification requirement.

Notification should include the:

- nature of the breach;
- sensitive personal information that may have been involved;
- measures taken to address the breach and reduce the potential harm;
- assistance that will be provided to impacted individuals; and, the
- way(s) to contact representatives of the personal information controller (i.e., the employer) including contact details.

The National Privacy Commission should be notified through a written or electronic report with the above information. The report should also include the employer's designated representative and contact information. All security incidents should be documented via written reports, regardless of whether the obligation to notify is required. These should be sent to the National Privacy Commission on an annual basis.



HR Best Practices: Incidents in the employment context which might trigger a requirement to notify include a laptop left on a train, or an email containing HR information sent massively to incorrect addresses. However, the National Privacy Commission and impacted employees may not have to be notified of a breach if it is unlikely to risk the individual's sensitive personal information