Protecting the Personal Data of Job Applicants and Employees

Most employers are aware of the PDPA and have implemented some measures to comply with the PDPA. This is according to a 2015 survey conducted by the Personal Data Protection Commission.

The survey found 92 percent of employers to be aware of the PDPA, and 86 percent had implemented some compliance measures.

Pretty encouraging figures to ponder over since the PDPA came into force in 2014[1]. Nonetheless, Executive Director of the Singapore National Employers Federation (SNEF), Mr. Koh Juan Kiat, believes that more can be done to close certain gaps, by "developing comprehensive policies and procedures to ensure that all the legal obligations of the PDPA are observed." Mr. Koh highlighted that "employers, especially their human resource representatives, must know the organisations' legal obligations under the Personal Data Protection Act (PDPA) and have in place policies and procedures to comply with them".

SNEF has observed that some employers might not have fully grasped the concept of personal data, and that personal data in written form is only one of many forms of personal data that they are collecting. Personal data may also be captured in photographs or CCTVs (in the form of an individual's image). Irrespective of the type of personal data, organisations should treat the personal data of their employees and job applicants with equal care as they would treat the personal data of any other individuals. Organisations have to comply with the PDPA when they collect, use or disclose personal data, such as notifying the individual of the purposes and obtaining their consent. They must also protect the personal data in their possession or under their control, unless an exception applies for certain obligations.

Obtaining Consent

The PDPA does not prescribe the manner in which organisations should obtain consent from an individual for the collection, use and disclosure of his personal data, although written consent is encouraged to prevent potential disputes.

The PDPA also provides for "deemed consent" to apply in certain situations. For example, a job applicant who voluntarily provides his personal data when applying for a job with the organisation may be deemed to have consented to the organisation's collection and use of his personal data for the purpose of processing his job application.

There may also be certain situations where consent is not required to collect, use or disclose personal data, such as when it is necessary for certain evaluative purposes, for instance, obtaining references from a potential job applicant's former employer to determine his suitability for employment, or obtaining performance records to determine an employee's suitability for promotion.

Organisations also do not have to obtain the consent of the employee when their collection of the employee's personal data is reasonable for the purposes of managing or terminating the employment relationship with him, for example, collecting his bank account details for payment of salaries etc. However, organisations do need to notify employees of the collection, use or disclosure of their personal data for such purposes. Organisations may wish to consider if it would be appropriate to notify their employees through avenues like employment contracts, employee handbooks, or notices in the company intranet.

Securing Personal Data

Making reasonable security arrangements to protect personal data in its possession or under its control is another obligation under the PDPA. There is no "one size fits all" solution in protecting personal data and organisations should consider the nature of personal data, the form in which personal data has been collected and potential impact on the individual concerned if there was unauthorised access to the personal data when determining the security arrangements to adopt.

Recruitment company, PrimeStaff acknowledges the protection of personal data it collects in the course of its business as a business imperative. Its managing consultant and head of HR functions, Mr. George Gaspar, shared that the company has been protecting personal data even before the PDPA was enacted and explains the business philosophy as "an important part of protecting our reputation."

Amongst the slew of measures adopted by PrimeStaff include authorised personnel such as its recruiters and consultants having controlled access to PrimeStaff's Applicant Tracking System which stores job applicants' data. In addition, when an applicant is assessed to be suitable for a particular role, his profile is sent to the client, but not before personal data such as NRIC number or contact information are removed.

A second measure involves the banning of external email services such as Gmail and Hotmail in the workplace to prevent data leakage. "When it comes to work-related matters, employees have to use the corporate email system," said systems administrator Mr. Wong Chew Foong, who is also PrimeStaff's Data Protection Officer. "We block all third-party email service providers and also media-sharing web sites such as Dropbox, iCloud and Google Drive to prevent soft copies of personal data from being transferred. Corporate email is the only way for our consultants to communicate with our applicants and clients."

Efforts have also been made to partially disable third-party storage devices such as thumb drives in a way that information can only be copied from the device to the computer, but not the other way round. And a strict hand phone policy ensures that employees conduct business communications using only company issued mobile devices.

---

[1]Provisions relating to the DNC Registry came into effect on 2 January 2014 and the main data protection rules on 2 July 2014.

The People Challenge

"One of the bigger challenges in ensuring compliance with the PDPA has to do with people", Mr. Wong noted. "A lot of information is transmitted daily. Employees can present a challenge because they may, unknowingly, accidentally or even deliberately do something that contravenes the PDPA."

To address this, whenever new employees join PrimeStaff, the dos and don'ts of personal data protection are clearly explained to them. The PDPA obligations are also reiterated during their monthly town hall meetings.

Internal training and sanctions are an important part of the equation. "If an employee breaches our policies, he has to face the consequences," said Mr. Gaspar. Training and constant reminders on personal data protection have proven to be effective too, as Mr. Gaspar was happy to note that "in all these years, there has not been a single case where we needed to penalise anyone".

Dealing with Data Intermediaries

Besides ensuring that their own policies, practices and systems are aligned with the requirements of the PDPA, organisations are also accountable for personal data that is being processed on their behalf by data intermediaries; another common PDPA compliance gap identified by SNEF. "Some organisations do not have a strict process to ensure that their data intermediary (third party) takes proper security measures to protect personal data. This is crucial when businesses outsource functions such as payroll and employee benefits," said Mr. Koh.

Before organisations hand over their employees' personal data to a third party for processing, it is important that organisations talk to their vendor about the standards of personal data protection and include provisions in their written contract to clearly set out the data intermediary's responsibilities and obligations in handling the personal data.

Meeting the Retention Limitation Obligation

As part of the overall framework for personal data protection, the PDPA also requires employers and recruitment agencies to comply with the Retention Limitation Obligation. For example, after an employer has decided which job applicant to hire, the personal data that it has collected from other job applicants should only be retained for as long as it is necessary for business or legal purposes.

At PrimeStaff, when consent for the retention of personal data of a job applicant is given, the personal data of the job applicant is typically retained for three years unless the applicant opts out before that. "We keep the data in view that there would be another opportunity for the job applicant", said Mr. Gaspar. "Our observation shows that after three years, the data often has no more value. The applicant may have found another job or the information on the resume goes out of date."

Job applicants may also withdraw their consent for the retention, use and disclosure of their personal data by giving reasonable notice to effect the changes. To facilitate such withdrawal, organisations are to make available their consent withdrawal policy and advise job applicants on the manner to submit the withdrawal and the consequences of such withdrawal.

Conclusion

Organisations need to be equally mindful of their obligations under the PDPA when it comes to the personal data of their employees. It is essential for employers and recruitment agencies to have in place policies and processes to comply with the PDPA, obtain consent from their employees for the collection, use and disclosure of their personal data when required to do so, and ensure that their personal data is properly protected, accurate and stored only for the period that it is needed.