Workplace Tips on Personal Data Protection

Know where personal data is stored, make sure it is adequately protected, and grant access only to authorised personnel – these are some of the important aspects of personal data protection in the workplace, say data protection officers (DPOs).

Protecting Personal Data Collected by the Organisation

Since the Personal Data Protection Act (PDPA) came into full effect on 2 July 2014, organisations in Singapore have been reviewing their data protection policies and practices to comply with this new law. Ensuring the protection of all personal data collected is an important step in good personal data management.

At Quality Hotel Marlow, all personal data provided by guests is confidential and treated with care. "All physical copies are locked in a secure manner and soft copies are software protected," said Ms Mayvin Loo, marketing communications executive and DPO for the hotel.

Controls also have to be put in place to make sure that only authorised personnel have access to personal data. Mr J. Lee, the DPO for a country club in Singapore, oversees the club's human resource function and is responsible for the storage of resumes and personal files of senior-level personnel. He thus holds the key, quite literally, to the respective cabinets. "We have to ensure that there is accountability," he said.

In his organisation, access to personal data is granted strictly on a need-to-know basis even within the same department. For example, within finance, personal data tied to the accounts payable, accounts receivable, purchasing or costing is not divulged unless there is a reason to do so. Mr Lee shared, "If the information is requested, whether by other departments or by colleagues within the same department, the request will have to be justified."

> TIP!
>
> *Install software like anti-virus, anti-spyware and personal firewall to secure electronic personal data. Keep the software updated and perform scans regularly.*

Keeping records about who had accessed the personal data, as well as how and when they used it, ensure that a trail exists if files go missing or are compromised.

With respect to electronic files, the use of passwords is often the primary form of protection and access control. In general, passwords should be at least eight alphanumeric characters long, with a mixture of upper and lower case letters, numbers and special characters. Other important password safeguards include making sure that it is not stored in the computer or written down where it can be easily accessed by another party.

TIP!

Protect user passwords by:

1. *Requiring that passwords be changed regularly.*
2. *Limiting the number of failed login attempts and locking the user out of the account when the limit has been reached.*
3. *Hiding the password characters when the user is keying them in.*

Properly Dispose the Personal Data You No Longer Need

To minimise the amount of personal data that an organisation has to protect, one way is to regularly review if the personal data is still required and to stipulate the retention period. Personal data that is no longer required should be properly disposed.

In a Sunday Times article earlier this year, it was reported that documents containing personal information were being thrown out as trash in the vicinity of Raffles Place. These included photocopies of passports, resumes of professionals and details of commissions paid to property agents.

The careless disposal of documents leaves personal data vulnerable to dumpster diving, which is a common method of stealing personal information by going through the trash. The information may be used by malicious third parties to gain access to an organisation's network.

To prevent this, organisations should have a proper method of disposing confidential documents that are no longer needed. "At our hotel, all hard copies are shredded prior to disposal, and electronic storage devices are sent for proper destruction and disposal," said Ms Loo of Quality Hotel Marlow.

TIP!

Properly dispose of personal data by:

1. *Using specific software to overwrite files or entire storage drives.*
2. *Using specialised hardware like degausser machines to destroy magnetically recorded data.*
3. *Promptly destroying any uncollected printouts and faxes that contain personal data.*

Communicate Policies and Practices Across Organisation

The Personal Data Protection Commission (PDPC) advocates for weaving the awareness of personal data protection into the fabric of organisational culture. This means an organisation should inform all employees of its data protection policies and their role in safeguarding personal data, and ensure that employees know what the internal processes are with regard to protecting personal data.

As Ms Ho Shin Tien, assistant manager with Crowe Horwath First Trust Technology Risk Advisory, pointed out, "After processes are developed to comply with the Act, it is important to train the employees and create awareness so that everyone is on the same page."

Mr J. Lee finds that this can be done most effectively through briefings and employees orientation on their first day of work, instead of relying on communications through emails or memos. This provides employees a chance to clarify doubts and increase their understanding of the responsibilities involved.

Personal data protection policies and practices have to be communicated to other levels of the organisation as well. At Quality Hotel Marlow, besides conducting in-house trainings for staff on a regular basis to update them on PDPA policies and compliance measures, Ms Loo also highlighted the need to familiarise top management with personal data protection obligations to get their buy-in.

Personal data protection is an ongoing journey. Everyone needs to be aware, to be involved and to be vigilant to ensure that the organisation is heading in the right direction.

More information on how to safeguard an organisation's electronic personal data can be found in the Personal Data Protection Commission's IT security guide for Small and Medium Enterprises.

TIP!

Establish policies to ensure personal data is taken care of, such as:

1. *Reviewing what personal data is collected and why, and where it is stored.*
2. *Enforcing ICT security policies, standards and procedures.*
3. *Conducting internal audits.*