
# Lessons from PDPA Enforcement Decisions:Protection Obligation

***Lax IT security has been a common cause of the breach of the Protection Obligation among organisations here. Of the 24 enforcement decisions published by the Personal Data Protection Commission (PDPC) thus far, 18 of them were due to either inadequate IT measures to secure personal data, or organisations not placing sufficient emphasis on the importance of security measures at the onset.***

In 2014, one entertainment group made headlines when personal details belonging to some 317,000 of its members were leaked online. Findings by the PDPC revealed that the organisation had not appointed a Data Protection Officer (DPO) and the implementation of the personal data protection policies and security measures were lax within the organisation. The absence of a DPO contributed to the organisation's lack of proper handling of personal data.

Among the findings by the PDPC, emails containing large amount of personal data were sent via Gmail without password protection, and an unused administrator account with the same user name and password "admin" remained in the system for nearly one year after the employee had left the organisation. This placed the personal data of its members at risk as an employee could have siphoned information through unauthorised access into the system using the unused administrator account.

Another major flaw of the organisation was its assumption that the responsibility of securing its customer database fell solely on its web and IT developer. This was despite not having a contract with the vendor nor making it clear that the security of the customer database was part of their scope of work. These and other lapses resulted in a serious breach of the PDPA, leading to a financial penalty of $50,000 being imposed on the organisation.


In the same year, the PDPC received complaints on two food caterers after customers discovered that they could easily view the personal particulars of other customers by manipulating the URL of the order preview page.

Akin to the case of the entertainment group, both caterers had poor access controls to personal data, failed to enforce the password policy and one of them did not have a DPO during the time of the complaint. They too did not instruct their respective web vendors to implement reasonable security measures on their websites. For their part, a financial penalty of $3,000 was imposed on each caterer for breaching the PDPA.

While there is no "one size fits all" solution for complying with the Protection Obligation of the PDPA, these and other cases highlight some of the security arrangements that organisations should take into consideration, in order to protect the personal data in their possession or under their control.

## Adopting appropriate security arrangements

It is also increasingly apparent from the slew of enforcement cases that the presence of a DPO is integral to the protection and care of personal data. A DPO will enable an organisation to better manage its personal data inventory, design personal data policies and processes according to the organisation's needs, and continually ensure that these policies and processes are adhered to.

"The clear designation of a DPO would ensure there is always someone keeping an eye on the movement and handling of personal data. The DPO would also be able to preempt potential breaches of the personal data and take preventive measures to mitigate such risks," said Mr Desmond Chow, Director and DPO of P2D Solutions.

To this end, organisations must adopt reasonable security arrangements to protect personal data in their possession or under their control. This means putting in place safeguards that fit the nature of the personal data, the form in which it has been collected (physical and/or electronic), and the possible impact on the individual concerned if the personal data was leaked or misused.

At StarHub, customers and employees' personal

data are stored and managed separately in a central system. All requests for access to the personal data goes through an approval workflow where the DPO, or other trained colleagues, would evaluate if the requests and intended activities are in line with the organisation's personal data protection policy, before access is granted. "It is important to know how each business unit collects, uses and discloses personal data. With this knowledge, we are able to assess, govern and rationalise how information is to flow in compliance with the PDPA," said StarHub's DPO, Ms Amelin Lim.

## Administrative, physical and technical data protection measures

Security arrangements for personal data protection may be grouped into three broad areas – administrative, physical and technical.

Administrative measures at Mediacorp include consolidating customers' personal data into databases that are encrypted and can only be accessed by authorised personnel with login credentials. Employees who need to access the databases containing personal data are required to sign a confidentiality obligation document. "This serves a dual purpose," said Mr Lee Choon Fatt, DPO of Mediacorp. "First, it acts as a form of access control, limiting access only to staff who have a valid need or purpose. Secondly, it helps us clearly identify which employees require advance training on data protection and what their areas of concern might be."

Regular communications and training sessions are also conducted for staff and partners at StarHub. For example, the DPO briefs new hires during their orientation programme, conducts awareness sessions for external partners, and comes up with refresher programmes for employees to reinforce their knowledge of the PDPA.

Physical measures for personal data protection could include among other things, locking of documents or devices containing personal data when not in use, marking confidential documents clearly and prominently, and properly disposing of devices and documents that contain personal data through shredding, pulping or similar means.

Sharing P2D Solutions' experience from advising clients, Mr Chow imparted that "common mistakes which can compromise the protection of personal data include using a document containing personal data as rough paper and not maintaining shredding machines regularly. When the shredder stops

working, employees tend to turn to the waste bin and this is how personal data gets leaked at times" said Mr Chow.

At StarHub, employees are required to protect documents that contain sensitive information with password, especially when sharing them over emails. The respective passwords are then sent separately to authorised recipients to enable them to access the data, said Ms Lim.

Other technical measures that organisations should have in place include installing antivirus, anti-spyware and other relevant IT security measures, as well as ensuring that these are kept updated, said Mr Chow. The appropriate level of security should also be applied to public-facing websites or applications that collect and store personal data, in order to prevent data from being inadvertently exposed. An example would be to disable the auto-fill function in online forms so that the personal data is not exposed to subsequent users of the website.

## Managing data intermediaries

As seen in the earlier cases, both the food caterers and the entertainment group are data controllers. Data controllers (or primary data owners) are required to fulfil all nine obligations of the PDPA, including taking steps to ensure that their data intermediaries (DI) are well equipped to fulfil the Protection and Retention Obligations.

Furthermore, as cited in the PDPC Advisory Guidelines on Key Concepts in the PDPA, organisations are advised to set out clearly in their written contracts with DIs, their respective rights and obligations, and their responsibilities and liabilities in relation to the personal data in their possession or under their control.

## Conclusion

Prevention is always better than cure. As data is increasingly being collected, stored and used in the digital space, the imperative for IT security can no longer be ignored. Organisations which take the protection of their customers' personal data seriously and keep that their employees and DIs on the same page will undoubtedly enjoy a higher level of trust and good reputation among their stakeholders.

- **Guide on data protection clauses for agreements relating to the processing of personal data**
- **Guide on building websites for SMEs**
- **Guide on disposal of personal data on physical medium**
- **Guide to securing personal data in electronic medium**
- **Guide to preventing accidental disclosure when processing and sending personal data**

**[1] The PDPA defines a data intermediary (DI) as an organisation that processes personal data on behalf of another organisation but does not include an employee of that other organisation.**