Understanding the Role of Data Intermediaries in Data Protection and Retention

At PurpleForest Events Pte Ltd, strict USB policies help ensure that only non-personal data is stored on external thumb drives. Compulsory password changes are enforced to minimise the risk of hacking, and employees' laptop accounts are locked to prevent the inadvertent download of data exfiltration malware.

"As an events management company, PurpleForest receives personal data from and on behalf of its clients," said Mr Soh Junhao, Director of PurpleForest. The company processes the personal data on behalf of other organisations and may act as their data intermediary when it provides its various event management services and solutions to them. For example, PurpleForest operates as a data intermediary when providing event RSVP and registration services such as recording and organising the personal data of attendees on behalf of its clients.

Another organisation that may act as a data intermediary for a client is Mobile Credit Payment Pte Ltd (MC Payment), an omni-channel electronic processing technology enabler and payment solutions service provider. The company provides various payment solutions to businesses ranging from large corporations to small and medium enterprises.

"We ensure that our clients comply with the Personal Data Protection Act (PDPA) and that they have provided information on their data protection policies and the terms and conditions on their website before they go "live" or process with us," said Mr Anthony Koh, Group Chief Executive Officer of MC Payment.

"We ensure that our clients comply with the Personal Data Protection Act (PDPA) and that they have provided information on their data protection policies and the terms and conditions on their website before they go "live" or process with us,"

- Mr Anthony Koh Soh
Group Chief Executive Officer of MC Payment

Under the PDPA, an organisation that engages a data intermediary to process personal data on its behalf will have to ensure that such processing is in compliance with the PDPA.

The data intermediary will also have to ensure compliance with the PDPA. However, the PDPA does not directly impose most of the data protection obligations on a data intermediary which is processing personal data on behalf of another organisation under a written contract[1], except for the obligations relating to the security and retention of the personal data[2].

Meeting the Protection Obligation with Reasonable Security Arrangements

A data intermediary must make "reasonable security arrangements" to protect personal data from unauthorised access, collection, use, disclosure or any similar risks, even though it is processing the personal data on behalf of another organisation.

PurpleForest, for example, ensures that all its employees' laptop accounts are locked such that only the IT administrator can access the system and install any software and programmes. "This ensures that Trojans or potential data stealing malware occurrences are kept to a minimum," said Mr Soh. It also stores its data with a corporate cloud service provider that adheres to the ISO/IEC 27001 standard for information security management.

As an additional measure, scheduled security scans are set up by the cloud service provider and within the employee's own computer system to automatically detect malware. These security scans are conducted every two days. A compulsory password change is also enforced by the cloud service provider every three months, reducing the likelihood of external hacking. The passwords are required to include alphanumeric characters and symbols, and have to be eight characters long.

PurpleForest also enforces a strict blanket policy on the use of USB removable storage as well as optical discs media. Only PowerPoint slides, videos and production artwork may be stored on these devices. Employees can only access and work on personal data using their corporate cloud server account.

If an employee misplaces a company laptop or mobile smartphone with access to the cloud server account, the IT administrator will immediately disable the cloud server access on the mobile device and enforce a compulsory password change. "This will ensure that even if the equipment is picked up by a third party, he or she will not be able to access the contents on the company's cloud server," said Mr Soh.

MC Payment, which is certified to Level 1 of the Payment Council Industry Data Security Standards, the highest level for the industry, ensures that all sensitive data is handled and stored according to the industry security standards. This means putting in place policies which cover various aspects of data protection such as IT security, data storage and handling, as well as procedures and processes for managing sensitive data. An incident management procedure is also in place, so in the event that any data is compromised, MC Payment is prepared and able to respond to information security breaches promptly and effectively.

Ensuring All Employees Are On Board

One common challenge that organisations face is the need to ensure that all their employees are aware of the importance of personal data protection and the policies and processes that they have to adhere to.

---

[1]*The contract must be evidenced or made in writing.*

[2]*These refer to the obligations in sections 24 and 25 of the PDPA. For ease of reference, these obligations are commonly called the Protection Obligation and the Retention Limitation Obligation.*

At MC Payment, besides having in place a User Management Policy, which governs data protection and access control processes, employees are briefed on any newly implemented data protection policies and processes, and their acknowledgement of these policies are tracked and recorded. In addition, MC Payment also makes it compulsory for employees to attend in-house and external trainings on data protection.

Some organisations also enforce personal data protection through employment terms and conditions. "Rules and regulations governing the use of personal data in the course of work are drawn up as part of our employment contract," said Mr Soh. All employees at PurpleForest are not allowed to hold on to offline copies of documents relating to personal data. "Failure to comply with these rules and regulations may result in the termination of their employment – this is to reflect the company's serious stand in protecting personal data under our care."

No "One Size Fits All" Solution

There is no "one size fits all" solution for the protection of personal data by data intermediaries – each organisation is urged to consider adopting security arrangements that are "reasonable and appropriate" in their own circumstance. The measures taken will depend on various factors such as the nature of the data, the form in which it has been collected, and the possible impact on individuals should the personal data fall into the wrong hands.

For example, data such as financial or medical information may require more stringent security arrangements as compared to information about a person's job experience or educational background. And generally speaking, it would be reasonable to expect a greater level of security for highly confidential employee appraisals as compared to more general information about the projects an employee has worked on.

In its advisory guidelines on key concepts in the PDPA, the Personal Data Protection Commission (PDPC) states that organisations should design and organise their security arrangements to fit the nature of the personal data that they hold and the possible harm that might result from a security breach. They should also have an incident response plan in place, as well as implement robust policies and procedures to ensure appropriate levels of security for personal data of varying levels of sensitivity.

Meeting the Retention Obligation

Besides putting in place security arrangements to protect personal data, all data intermediaries are also required to meet the Retention Limitation Obligation under the PDPA. This means that they have to cease retention of documents containing personal data, or remove the means by which the personal data can be associated to specific individuals, as soon as the retention no longer serves the purpose the personal data was collected for, and is no longer necessary for legal or business purposes.

Holding personal data for an indeterminate period of time increases its exposure to security risks. However, as each organisation has its own specific business needs, the Retention Limitation Obligation does not specify a fixed duration for which an organisation can retain personal data.

For PurpleForest, personal data is retained only up to the completion of an event, after which it is handed back to the client together with any other event-related materials it may have developed for the client such as artworks and marketing collaterals. The information is transferred to offline media such as DVDs and/or portable hard disks and handed over to the client for their archival. Mr Soh estimates that this typically happens within two to six weeks after the event, depending on the scale of the project.

When this is done, all related information is removed from PurpleForest's systems. The person in charge of each event is tasked with the collection and safe-keeping of hardcopies that contain personal data, for example, the event registration lists. After the event, these are handed over to the company's data protection officer for accountability and shredding, usually within one working day. At the same time, all

personal data in digital form is deleted from the company's cloud servers.

As a general practice, a data intermediary should review the personal data it holds on a regular basis to determine if that personal data is still needed. Personal data must not be kept "just in case" it may be needed for purposes other than what has been communicated to the individual at the point of data collection. A data intermediary holding a large quantity of different types of personal data may also have to implement varying retention periods for each type of personal data where appropriate.

Setting Out the Responsibilities and Obligations

Under the PDPA, organisations are ultimately accountable for personal data that is being processed on their behalf by their data intermediaries. As they hand over the data to a third party for processing, therefore, it is important that they include provisions in their written contract to clearly set out the data intermediaries' responsibilities and obligations to ensure compliance with the PDPA.

Data intermediaries that process personal data on behalf of another organisation under a written contract, on their part, have to ensure that they meet the security and retention obligations with respect to the data that they handle on behalf of their clients, as well as any data protection requirements set out in the contracts with their clients. They have to develop an organisational culture where reasonable measures are taken to protect third-party personal data and to remove or anonymise them after they are no longer needed.

A data intermediary is fully responsible under the PDPA for other activities which do not constitute processing personal data on behalf of another organisation under the written contract, e.g. collecting any personal data on its own accord or using personal data for its own purposes, or any processing of personal data on behalf of another organisation that is not pursuant to a contract made or evidenced in writing. Please see Chapter 6 of PDPC's Advisory Guidelines on Key Concepts for more information relating to data intermediaries, including the meaning of "processing" under the PDPA.