PERSONAL DATA PROTECTION IS EVERYBODY'S BUSINESS.

All businesses, big and small, collect, use and disclose personal data about individuals for various reasons and through multiple avenues.

Practising good personal data management can increase business efficiency and effectiveness, boost customer confidence and enhance your organisation's public image.

How an organisation implements data protection policies and practices, however, depends very much on its nature of business, scale of operations and a host of other factors.

This publication shares the varying journeys that some organisations have gone through to better protect personal data, whether it is those of customers or employees.

These are their stories.

Carpe Diem's data protection measures have helped to streamline business processes and foster trust with parents, says Mr Tan Kiah Hui, its group data protection officer.

CHALLENGES

Carpe Diem needed to address areas in business processes and documents that could lead to unauthorised disclosure of personal data.

STEPS TAKEN

- Developed data flow diagrams to identify areas where personal data could be compromised
- Implemented new visitor forms to collect only necessary personal information
- Limited access to children's registration records
- Compliance manuals and training were also provided
- All personal data is classified as confidential

BENEFITS

- Streamlined business processes
- Built trust with parents
- Successfully turned data protection into a competitive advantage

SECURING PERSONAL DATA IS CHILD'S PLAY

Childcare service provider Carpe Diem took just three months to shore up its data protection measures while streamlining its business processes

Parents who visit Carpe Diem's 26 childcare centres can now be assured that their personal data is better protected, thanks to new data protection measures that kicked in last year to build consumer trust.

For one thing, they no longer need to fill in a visitor log book with personal data like they did before. "As the log book was viewed by all visitors, the personal information in it could be inadvertently disclosed," said Mr Tan Kiah Hui, the group data protection officer (DPO) at Carpe Diem who was tasked with beefing up the childcare service provider's data protection practices.

"So, at some centres, we did away with the log book and provided new individual forms for visitors to fill, while our staff will fill up visitors' details at centres that are still using log books," he added. This new process ensures that new visitors would not be able to view the personal data of previous visitors.

Also, the forms only require visiting parents to provide necessary information such as their names, contact numbers, and the age of their child.

"We no longer require potential customers to fill in their addresses as it is unnecessary at this early stage," Mr Tan said, adding that this has helped to streamline business processes by avoiding the collection of duplicate data such as addresses, which would otherwise be collected again if a parent decides to enrol a child.

Mr Tan said consent is also sought for the collection and use of data – and only for specified uses. This further ensures that no unnecessary personal data is collected, thus minimising the risk of data breaches.

Since July 2014, the Personal Data Protection Act (PDPA) requires all organisations in Singapore to seek consent and notify individuals on the collection, use and disclosure of personal data for specific purposes. They must also safeguard all personal data under their care.

Identifying potential data breaches

Complying with the new data protection rules is not as onerous as it seems, as Mr Tan has found. After he attended a Workforce Skills Qualifications (WSQ) accredited course in June 2014 that helped him to understand the broad concepts under the PDPA, he sprung into action and concluded his compliance efforts in just three months.

For a start, Mr Tan took up a certification course in information privacy management offered by a local PDPA training provider, which also guided him on what to include in a data protection policy.

Armed with his new knowledge from his previous job at a bank, he developed data flow diagrams, which showed where and how data was collected, used and disclosed for business processes such as child registration.

"The data flow diagrams were useful in identifying areas where personal data could be compromised," Mr Tan said.

For example, he found that letting all teachers access children's registration records could lead to potential data breaches. Such records typically include parents' personal data such as salary figures that may be required for childcare subsidy applications.

Limiting access to personal data

The PDPA requires organisations to make security arrangements to protect personal data, so measures were swiftly put in place to address potential problem areas. Access to children's registration records is now limited to authorised staff, while personal data has been excluded from "communications books" used by teachers to update parents on a child's progress and behaviour in school.

Additionally, all personal data is now classified as confidential and recorded in physical documents, which are kept safely in Carpe Diem's offices under lock and key, to minimise the risk of data falling into the wrong hands.

Mr Tan has also developed a "mission statement" that underpins the data protection practices of all Carpe Diem childcare centres, along with privacy notices, policies and an information security policy. These were consolidated into a compliance manual, which staff can refer to anytime.

Overcoming barriers

Not surprisingly, Mr Tan faced resistance from some employees while shoring up the company's data protection practices, as the new measures made it less convenient for staff to access personal data.

"The teachers are often not aware of why we're doing this, so I had to educate them about the importance of safeguarding personal data," he said.

Mr Tan also trained the childcare centres' appointed DPOs, who have in turn trained their colleagues. Each DPO is required to submit a PDPA compliance report to Mr Tan for review twice a year.

In all, Carpe Diem spent about S$10,000 for all its 26 centres on training four staff members, certification and legal fees.

Building trust with parents

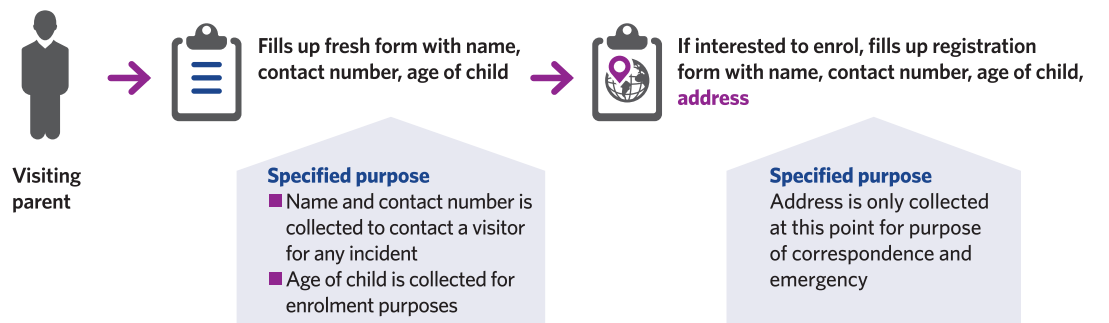
Mr Tan felt the effort was worthwhile as the company has managed to foster trust with parents who can be assured that their personal data, as well as that of their children, would remain secure.

Indeed, parental trust may well be Carpe Diem's competitive advantage. Mr Tan said the company is likely to be the only childcare service provider in Singapore with a certified information privacy manager as its DPO. "Parents trust that we know what we're doing with their personal data," he said.

Mr Tan's work does not end even though Carpe Diem's data protection policies are firmly in place. "Compliance is an ongoing process, as there may be gaps in processes that may crop up later on. We have to be ready to tweak things along the way," Mr Tan said.

REVISED WORKFLOW

Previously, parents were required to fill in a logbook with their addresses. In view of possible over collection of personal data, a new data collection workflow was introduced.



Adequately respecting and protecting personal data complete the user-experience and ensure great holidays for customers, says Ms Janet Chan of Chan Brothers Travel.

CHALLENGES

Juggling the data protection preferences of thousands of individuals and maintaining satisfactory user experience in the face of PDPA compliance proved challenging for Chan Brothers Travel.

STEPS TAKEN

- **Formation of data protection team to monitor PDPA obligations and to assist colleagues with compliance**
- **Enhanced IT security and frontline notifications to offer customers the option to opt out of marketing and publicity promotions**
- **Dedicated email account to handle access and correction requests**

BENEFITS

- **Increased customer confidence and trust in Chan Brothers**
- **Better online user experience resulting in higher number of online transactions**
- **More effective internal handling of customers' personal data**

TRAVEL AGENCY GOES THE EXTRA MILE TO PROTECT PERSONAL DATA

For Chan Brothers Travel, ensuring correct use of customers' personal data extends beyond the management of its 120,000 strong customer database

It is common for travel groups to take a picture together as keepsake, and this is one of the bigger selling points marketed by tour agencies to entice travelers to take up celebrity packages. Chan Brothers Travel (Chan Brothers) is one of those that offers such opportunities – travelers can take pictures with their favourite celebrity and even appear on television in "My Star Guide", a local reality travelogue where selected local artistes play the role of a tour guide and "lead" tour groups overseas.

In its 11th season this year, the successful programme is one area of concern for Chan Brothers when implementing data protection policies for the tours, as the entire trip is captured on camera and presented on television.

"Not everyone in the tour wants to be on television or in photos that we use for marketing communication purposes," says Ms Janet Chan, Chan Brothers' Senior Business Development Manager for E-Commerce Marketing and Data Protection Officer (DPO). "Even if they join the celebrity tour, it doesn't automatically mean that they want to be photographed or filmed."

To ensure compliance with the Personal Data Protection Act (PDPA) which allows individuals to decide how they want their personal data to be collected, used and disclosed, Chan Brothers makes it a point to notify customers of the nature of the tour. Customers may state their preference in relation to video or photo exposure when they purchase a tour package, especially for celebrity packages where the entire tour process is documented and presented on TV.

During pre-travel briefings, Chan Brothers' travel advisors will once again verbally remind travelers to inform their tour leaders of their preferences during the trip.

360° User-experience

Managing Chan Brothers' customer preferences extends beyond the duration of the tours; it starts from the day the customer contacts Chan Brothers and ends long after the fulfilment of the tour package.

The company's standard operating procedure (SOP) is to first notify customers of the purpose of the collection of their personal data once they express interest in signing up for a package. This is done by frontline staff. The information is generally mandatory for the company to see through the delivery of its services, such as to help customers with their hotel or airline reservations.

With regard to marketing, customers are given a choice to opt out. "One of the first changes we made to our processes was for our in-house information technology (IT) team to include an opt-out selection for customers. This seemingly small change made a huge difference to the overall customer experience," says Ms Chan.

The IT team is also in charge of regularly reviewing the agency's IT security polices and keeping up with the latest trends in cybersecurity, so that sufficient measures are in place to secure the company's online transactions. Existing measures such as secured login, automated logout mechanisms and systematic updates of firewalls, to name a few, are constantly updated with the latest patches to ensure there are no loopholes in safeguarding customers' data.

Ms Chan adds, "With enhanced IT security, customers are also more comfortable making online transactions, which has a positive impact on our revenue streams and user experience."

Since the company has an estimated 120,000 customers and followers in its SMS and eDM (electronic direct mail) databases, and providing access as well as keeping personal data accurate are requirements of the PDPA, Chan Brothers has created a dedicated email account to handle all access and correction requests.

Internal Processes Matter Too

Aside from ensuring compliance in customer-facing practices, the company also enhanced its internal data protection policies to help employees handle personal data better. For example, all hardcopy registration forms must now be shredded before disposal. Third party vendors, too, are required to adhere to Chan Brothers' data protection policies.

Ms Chan further shares that Chan Brothers' data protection policies are made available on the company's intranet for employees' easy reference. As the DPO, she conducts regular training to keep employees up-to-date on data protection policies and practices.

She is supported by a team comprising designated personnel from each major department, namely e-Commerce, Marketing Communications, Customer Service, IT, Human Resource and Finance. The team reviews existing procedures in their relevant departments every quarter to ensure that there are no loopholes in safeguarding customer's personal data.

Personal Data Protection a Worthwhile Effort

Although it took some getting used to, Ms Chan says that targeted marketing has proven to be both efficient and effective.

She explains, "We now only send marketing SMSes to customers who are willing to receive information by SMS, and this improves the effectiveness of our promotions. Checking our telemarketing list against the DNC Registry is also relatively quick. We usually set aside just one day for the checks to be completed."

Aside from the purchase of credits to check their telemarketing list against the DNC Registry, Ms Chan attributes the bulk of the cost of complying with the PDPA to time and resources spent in implementing the company's data protection policies and practices.

Ms Chan says, "Our efforts have been worthwhile because customers are now more aware of our personal data protection practices. Our policies have made our processes more transparent and increased customer trust in us."

The banking industry is driven by human interactions, which in turn are the focal point of DBS' personal data protection policies.

CHALLENGES

Personal data protection requirements under the PDPA were not new ideas to DBS, but the PDPA gave rise to broader implications that had to be managed.

STEPS TAKEN

- **Integrated personal data protection into an overall data governance approach that applies across all of the bank's operations**
- **Appointment of a data protection officer to provide guidance on best practices and to engage in regular discussions with authorities**
- **Used aggregated data to analyse customer service issues**

BENEFITS

- **More effective implementation of personal data protection policies that are integrated in existing work flows**
- **The DNC Registry has allowed for dedicated use and focus of resources, leading to better customer experiences**
- **Use of data analytics to enhance customer services**

PERSONAL DATA PROTECTION: AN INTRINSIC PRIORITY OF SINGAPORE'S LARGEST BANK

DBS sees personal data protection as integral to its business and encourages a wider acceptance and discussion of the issue

DBS has over four million customers in Singapore alone. With over 280 branches across 18 markets worldwide, DBS considers personal data protection an intrinsic priority of the bank.

"We deal with personal data all the time," says Mr Lam Chee Kin, DBS' Managing Director and Head of Group Legal, Compliance and Secretariat. "Handling it responsibly with confidentiality, privacy and security is an inherent part of providing trusted service to customers. We consider quality privacy and data governance practices a requisite to doing business."

Mr Lam is also a member of the Data Protection Advisory Committee, which comprises individuals from various sectors that advises the Personal Data Protection Commission (PDPC) on matters relating to the review and administration of Singapore's personal data protection framework.

Pre-Personal Data Protection Act (PDPA), DBS already understood what a data protection regime would look like because several of the territories it operates in – Hong Kong, for example – had introduced similar laws much earlier than Singapore. In compliance with these jurisdictions, DBS had integrated the processes into its framework for handling individuals' personal data, including that of customers and staff.

With customer relationships being key to banking business, Mr Lam emphasises that the way they deal with their customers is something they take very seriously. "People want to be treated with respect. Therefore we design our data protection practices to be sensitive to this."

"Often people want their financial product or service without fuss, and they can get irritated by poorly-designed consent forms or lengthy explanation of how personal data will be used. That's a potential issue arising from being pedantic and ignoring practical approaches while implementing data protection procedures. If you don't give the customer a good experience, you lose the customer."

Under One Roof

Like all banks in Singapore, DBS comes under the regulation of the Monetary Authority of Singapore (MAS) by virtue of the nature of its business. It is guided by established banking principles including client confidentiality, and now, the PDPA.

For DBS, adopting a single data governance approach that encompasses all elements of related compliance applicable to all of its business units across the globe is preferred, as opposed to having separate frameworks for individual elements.

In terms of differing jurisdictions, Mr Lam acknowledges that negotiating these differences is difficult and his advice to Small and Medium Enterprises (SMEs) with overseas operations is to consider applying the "80-20 rule". Broadly speaking, the 80-20 rule calls for an estimation of the countries that can be brought under a single framework. These would typically be countries that have reasonably harmonised or similar laws and regulations. One can expect there to be countries that cannot be integrated under an umbrella framework, and these are usually jurisdictions with very strict or localised definitions of concepts such as privacy.

Mr Lam adds, "The biggest challenge for us continues to be bringing everything together – including data protection rules – in a way that the whole organisation, complete with differing laws from other jurisdictions, can operate smoothly and without confusion."

One concern that relates to this is information sharing, particularly when it is at odds with cross-border or cross-entity banking regulations. Customers tend to expect the same service whether the branch is in Singapore or overseas, without being aware that it is not necessarily a straightforward process.

For instance, if a customer sends an enquiry to a branch overseas, he would expect the branch to be able to pull out all his records with the bank, regardless of where the information resides originally. DBS has to navigate both data protection and financial regulations, which govern cross-border exchange of customer data, to ensure that customer experience is as seamless as possible.

Another development which impacted overall customer experience was the introduction of the Do Not Call (DNC) Registry under the PDPA.

According to Mr Lam, operationalising this element in their processes was "a bit of a task" because DBS had to integrate its processes with that of the registry and build appropriate interception points for its marketing teams.

"However, the DNC provisions have helped us to better understand which of our customers want to be contacted for marketing purposes, which allows for dedicated use and focus of resources and thereby, a better customer experience," he adds.

The PDPA also requires the appointment of a data protection officer (DPO), and one has been duly appointed in Singapore.

Rather than appointing a DPO in every department, DBS finds that channeling data protection issues through a single contact point in the bank ensures that data protection rules are integrated into the way DBS works. Furthermore, having a single DPO streamlines engagement with regulatory bodies.

Personal Data Protection and Beyond

While DBS takes its data protection and accompanying privacy responsibilities seriously, a broader interest is how to turn responsible treatment of customers' personal data into a competitive advantage.

"We want to provide seamless banking services to customers," says Mr Lam. "And that requires the use of data analytics."

An example of how DBS has been using data analytics to serve customers better would be the roll-out of pop-up automated teller machines (ATMs) during the Lunar New Year festive season. This is the time of the year where there are more people visiting ATMs to withdraw new notes for distribution of red packets.

Through the use of aggregated data, DBS was able to discern where the highest traffic spots were and introduced "pop-up" ATMs at those locations in 2015. The 29 pop-up ATMs, specially designed to meet customers' need for greater ease and convenience, were set up at 10 community clubs island-wide.

The obstacle to the use of data analytics, however, may be the public's lack of awareness and understanding of how their personal data can be used for the greater good. Mr Lam highlights Singapore's aspirations to become a Smart Nation and points out that the success of this is largely dependent on a much more open sharing and utilisation of data, including personal data.

Mr Lam says, "Responsible use of data will give businesses a competitive advantage. If a company shows that it protects data well and uses data responsibly, chances are that it will be perceived favourably by customers."

CHALLENGES

As a healthcare service provider, Eu Yan Sang has been complying with patient confidentiality rules and is familiar with having to protecting the personal data of its customers and patients. But with the PDPA coming into effect, it had to review those measures to ensure compliance.

STEPS TAKEN

- **Engaged external legal advice on how to comply with PDPA obligations**
- **Audited its processes and workflows to ascertain potential gaps**
- **Conducted training for staff and compiled compliance manual**
- **Improved data accuracy through customer self-registration on tablets**
- **Limited telemarketing activities to existing customers**

BENEFITS

- **Provided opportunity to review business processes to ensure that personal data of customers / patients are protected**
- **Enhanced data protection measures has improved brand equity**

BUILDING ON A TRUSTED BRAND

Eu Yan Sang is living up to its reputation as a trusted brand through better personal data protection measures

Traditional Chinese Medicine (TCM) company Eu Yan Sang has been safeguarding personal data even before Singapore's data protection laws kicked in last July.

In 2001, it had already implemented measures to comply with patient confidentiality rules set by the Traditional Chinese Medicine Practitioners' Board, which requires healthcare providers to secure the medical information of their patients.

Ms Tang Yock Miin, general manager of Eu Yan Sang's legal and corporate secretarial department says these measures include keeping patient record cards under lock and key, which can only be accessed by clinic assistants and certain management staff on a "need-to-know" basis.

Eu Yan Sang was founded as a Chinese medical hall in 1879 and is a leading integrative health and wellness company that now operates nearly 30 TCM clinics in Singapore, and over 250 retail outlets offering health and wellness products across Asia.

To better understand the needs of its customers, Eu Yan Sang collects the personal data of patients as well as those who sign up for its Eu Rewards membership programme at its retail stores.

"The data would give us insights into their demographics and lifestyles so we can tailor programmes and activities for them," says Ms Tang.

Early mover

Since July 2014, the Personal Data Protection Act (PDPA) requires all organisations in Singapore to seek consent and notify individuals on the collection, use and disclosure of personal data for specific purposes and safeguard such data under their care, among other obligations.

For Eu Yan Sang, complying with the PDPA was simply a matter of beefing up its existing data protection measures.

And it did so as early as October 2012, when it engaged a law firm to do an organisation-wide review of its data protection policies and brief its top management team on the nine PDPA obligations.

The lawyers then proceeded to conduct an audit of the company's data protection processes through written questionnaires and face-to-face interviews with staff and business heads from the retail and clinic businesses, which were flagged out as the two business units affected by the new law.

"We were asked if we had obtained consent, whether we had notified customers about the purpose of collecting personal data, and what we did to ensure the security of personal data," says Ms Tang, who is one of the three appointed data protection officers at Eu Yan Sang. The other two data protection officers are the directors of the company.

The audit revealed potential gaps that needed to be plugged. For example, the auditors found that the Eu Rewards membership forms that were sent from retail outlets to Eu Yan Sang's head office were sometimes not kept under lock and key.

"We addressed that gap by ensuring that employees lock up the forms to prevent personal data from being compromised," Ms Tang says, noting that these are simple yet overlooked practices. "The computer systems that employees use to key in personal data in the forms are also password-protected to prevent unauthorised access."

Ensuring data accuracy

Transferring information from patient registration forms may lead to data errors due to misinterpretation of customers' handwriting, Ms Tang says.

To ensure its customers' data is accurate, Eu Yan Sang has deployed tablet computers as self-registration tools at busier clinics, so that patients can enter their personal information on their own.

The tablets will also be rolled out to retail outlets at a later date, for customers who wish to sign up for the Eu Rewards programme. "That will minimise errors in deciphering what a customer has written," Ms Tang says.

Telemarketing to members

Under the Do Not Call (DNC) Registry rules, telemarketers are not allowed to send telemarketing messages or make telemarketing calls to Singapore telephone numbers listed in the DNC Registry – unless they have clear and unambiguous consent from customers.

As Eu Yan Sang only sends telemarketing messages to Eu Rewards members who have consented to receiving such messages, it does not need to check the DNC Registry. That has helped to lower compliance costs.

Compliance training

Eu Yan Sang compiled its data protection measures into a staff compliance manual, which provides general information on the PDPA obligations and work processes to guide staff on what they should do when dealing with personal data.

"For instance, they have to notify customers on the purpose of collecting personal data," says Ms Tang.

Eu Yan Sang and its law firm also conducted training sessions in English and Chinese languages to familiarise all employees, including retail and clinic staff, with the company's data protections measures.

Some customers, however, have questioned the need to fill in additional fields in membership forms that require them to indicate if they would like to receive telemarketing messages from Eu Yan Sang.

"We just had to explain to customers that we need their consent to send them telemarketing messages," Ms Tang says. "But with the increase in consumer education, consumers are now used to such processes and have become kinder to us."

Eu Yan Sang viewed personal data protection as critical to its core business strategy and hence had made a deliberate decision to invest heavily on staff training and legal advice. Ms Tang says the data protection measures have also given the company an opportunity to review its business processes and strengthen its brand equity.

"Eu Yan Sang is a trusted brand," she says. "The assurance that the personal data of our customers is well-protected adds value to our brand."

IPTECH treats all data collected as personal data and takes efforts to fulfil its role as a data intermediary.

CHALLENGES

IPTECH processes more than half a million records a year on behalf of its clients, which means that it plays a crucial role in ensuring that both the company and its clients are compliant with the PDPA. Maintaining continued compliance is its biggest challenge since technology is always evolving.

STEPS TAKEN

- **Regular testing of servers and systems**
- **Data disposal policies that encompass destroying paper documents properly, automatic purging of digital data and manual purging of back-up files**
- **Tighter server settings including the locking of redundant ports**
- **Timely update of security patches**

BENEFITS

- **Increased client confidence in IPTECH's services**
- **Reduced risks of accidental exposure of personal data**
- **Employees understand their obligations over the data collected and how to protect it**

PERSONAL DATA PROTECTION EVOLVES WITH TECHNOLOGY

Understanding its role as a data intermediary under the PDPA, IPTECH describes itself only as strong as its weakest link

Local information technology (IT) service provider IP Technology Solutions (IPTECH) describes itself as "the last mile" in the communications chain between its clients – the majority of which are from the MICE (meetings, incentives, conferences and exhibitions) industry – and their target audiences. An SME with 10 employees, IPTECH provides technology solutions for event registration and such, helping clients to process over half a million records a year.

Due to the sheer volume of data collected, it is often difficult for IPTECH to differentiate between business contact information and personal data.

"We need to treat all data collected as personal data. As our role is that of a data intermediary, under the PDPA, we are bound by the Protection and Retention Limitation obligations," explains Mr Rocky Chia, IPTECH's director and data protection officer.

IPTECH makes it a point to advise clients on security features to bolster collection of personal data on their websites, such as using Secure Socket Layer (SSL) certificates which allow secure connections between a web server and a browser and including Captcha codes in online forms.

Before the PDPA came into full effect in 2014, IPTECH focused on server and application security, and only had basic password policies in place. However, Mr Chia says the company's data protection policies have since improved.

For example, clients used to be able to access their event data and documents using a single identity input and password. Now, systems have been enhanced to a two-factor authentication (2FA) process with audit logging by IPTECH. This means that in order to access the data, clients have to provide two different types of credentials or identification.

Where previously there was no retention limitation policy, now IPTECH has also made it mandatory to retain personal data only for specific periods.

Strengthening The Weak Links

IPTECH manages its online infrastructure and development work from its main office and is only as strong as its weakest link, according to Mr Chia. To ensure that its servers are not compromised as a result of work done at its office, IPTECH implemented changes across multiple aspects, including tighter physical security with closed-circuit cameras, replacing access cards for employees every quarter, and documenting security policies relating to refreshing personal identification numbers (PINs) as well as restricting employees to handle personal data for clients only within IPTECH's premises.

Another enhancement that IPTECH made to its processes was to tighten server settings and strengthen its online infrastructure. This includes server hardening and locking down redundant ports, periodic Penetration Testing (PT) and Vulnerability Assessments (VA), and security patch management. Mr Chia explains that the latter is not always as straightforward as it appears to be.

Patch management involves more than scheduled updating of the latest security release. He elaborates that it is also necessary to conduct tests to ensure that the server continues to function after a new security patch is installed. This is one important service that IPTECH provides as part of its maintenance of clients' IT systems.

Another adjustment that IPTECH made to its processes was in relation to file retention. Prior to the implementation of the PDPA, IPTECH retained information generated by its clients, whether for an event or as part of a campaign, in some instances indefinitely or for as long as clients requested. It has since limited the retention period. In the case of an event, for example, IPTECH's systems will automatically purge all related files two weeks after the end of each event, and back-up files are manually purged by its employees.

This saved one of IPTECH's clients from considerable embarrassment when an employee from the client's side mistakenly triggered an email to be sent to some 20,000 attendees long after the event had ended. The email blast was prevented because there were no email addresses to send it to.

"We also have a 'use it and delete it' policy in place," Mr Chia adds. "Clients often send us hardcopy Excel spreadsheets of customer information. That is a paper trail right there, so we input the relevant information to our system and destroy the paper documents."

"Our clients depend on us to help them comply with the PDPA… any breach on our side would be detrimental to both ourselves and our clients," says Mr Chia.

Investing In Compliance

To date, IPTECH has invested about $30,000 in business and man-hour costs to ensure its servers and applications are PDPA-compliant. Costs attributed to external vendors include tests such as PT and VA, and in-house outlay includes internal audits, research and development.

Mr Chia regards such expenditure as investment because the data protection processes ultimately help IPTECH to preserve the integrity of its core business. Benefits include clients having more confidence in IPTECH's services, and employees having a better understanding of the data they collect and protect, leading to heightened vigilance.

In addition, Mr Chia sees PDPA compliance as an ongoing effort and insists on reminding and updating employees regularly on the company's data protection policies. Such discussions usually take place during their fortnightly project meetings.

He explains, "We have to be in the know in order to handle new threats so as to ensure continued compliance. We do this by keeping up to date with new technologies and new technological threats. At the end of the day, the PDPA is a good wake-up call to always be vigilant."

Joshua Research Consultants designs its call centre and processes with a focus on personal data protection.

CHALLENGES

Being a people-oriented business, the key challenges for Joshua Research Consultants have been to manage internal stakeholders' mindsets and behaviours, and the public's perception towards market research.

STEPS TAKEN

- **Call centre designed with data protection in mind**
- **Ground-up approach to understanding and strengthening data protection measures for office and call centre processes**
- **Stricter policies for call centre agents, improved physical security measures and an internal do-not-call list**
- **Upgrading of IT systems and hardware to support enhanced SOPs**

BENEFITS

- **Internal stakeholder buy-in for new policies**
- **Strengthened client confidence in its service offerings**
- **Increased business opportunities**

DATA PROTECTION BY DESIGN CORNERSTONE OF MARKET RESEARCH FIRM'S PDPA COMPLIANCE

Joshua Research Consultants faces added challenges posed by the public's perception of market research surveys

For the longest time, market research firms have found it a challenge to solicit responses through telephone surveys. While technology has aided telephone research through advances such as computer-assisted telephone interviewing, answering machines and caller identification have contributed to declines in response rates. This was not helped by the launch of the Do Not Call (DNC) Registry in Singapore in January 2014.

The intent of the DNC Registry is to minimise unsolicited telemarketing messages for individuals who opt in. It does not cover messages that do not contain any element of marketing, such as market research and opinion polling, among other exclusions in the Personal Data Protection Act (PDPA). These exclusions were formulated to help organisations carry out their non-marketing operations smoothly.

However, the difference between these exclusions and telemarketing messages is not always clear-cut. While the Personal Data Protection Commission (PDPC) had set out to educate members of the public on the exceptions to the DNC provisions through advertising and outreach, some continued to have a negative impression of telephone surveys.

Mr Alan Tay, Managing Director and data protection officer for Joshua Research Consultants (JRC), observes that the instinctive reaction from the public has been to reject such calls altogether, resulting in lower response rates to surveys and research programmes, hence affecting overall statistical data.

To alleviate this problem, the JRC call centre team is put through rigorous training to equip them with the skills set to deal with public perceptions.

"Being able to assure the public that we are conducting market research surveys and that we are not selling anything has helped us with our survey response rates," says Mr Tay.

JRC provides market research services and data collection to clients in the Asia Pacific region and has offices in Singapore, Malaysia and China. Its Singapore headquarters employs 15 full-time staff and approximately 150 part-time staff in its call centre and for street surveys.

Data Protection by Design

In the burgeoning era of the Internet, information security has become all the more important. This is why JRC had embarked on data protection for its call centre even before the PDPA came into full force in July 2014.

According to Mr Tay, JRC had designed its call centre with data protection in mind – the facility is located in a unit separate from the main office and is only accessible to management and call centre agents. Furthermore, entry into the call centre is constantly logged through the use of access cards.

The space is also segregated into multiple soundproof rooms so that personal data is not inadvertently disclosed.

Technology-wise, JRC segregates its local area network (LAN) and WIFI systems to reduce the possibility of an unauthorised external party tapping into the WIFI to access the corporate network.

Another security precaution is the use of tablets for street surveys. Surveys in paper forms may easily be misplaced, leading to the loss of personal data. By using information technology (IT) as a solution, it has brought about better productivity and introduced a more secure way of handling personal data that JRC collects. "Should a tablet be lost or misplaced, we are also able to erase the contents remotely to minimise any leak of personal data," Mr Tay adds.

JRC also enhanced its standard operating procedures (SOPs) relating to its IT processes and systems, which among others entail stronger password policies for all devices, regular asset management, and tighter access control.

Mr Tay acknowledges that the SOPs relating to the call centres might have been fluid in the early days. He recalls an incident in another country where a call centre agent had retained an interviewee's telephone number for his own use.

To ensure that a similar situation does not arise, JRC now makes it mandatory for call centre agents to leave their belongings in a locker. This applies to all items, including mobile phones. All materials necessary for them to carry out their tasks, including writing paper, will be issued by JRC.

At the end of their shifts, the agents must surrender their writing paper – complete with notes that they might have taken down – for shredding. The paper is collected, shredded and disposed of regularly by a professional shredding contractor.

"The PDPA has given us ground to implement even stricter measures because the implications of non-compliance are too severe to ignore," Mr Tay says.

The stricter measures imposed on call centre agents, especially the prohibition of mobile phones in the call centre rooms, met with initial resistance, but dedicated training and information sharing on PDPA requirements have enabled Mr Tay to change their mindsets and behaviours.

Mr Tay says the time and effort invested to engage staff in discussions about the PDPA, its implications and the new processes that had to be implemented within the organisation were well-spent. "Previously, they complained a lot about the restrictions imposed on them, but now they express understanding."

Weighing the Costs

JRC undertook the development and implementation of data protection policies in-house, adopting a ground-up approach. "When we embarked on this exercise, we felt that it should not be a top-down approach as that is usually met with high resistance. Internal stakeholders, such as staff members, should take some ownership."

He reckons that he and his team spent a total of eight months researching, discussing and developing improved data protection policies and practices for the company. There were also open discussions with full-time staff members.

Other costs of compliance relate to the IT enhancements and staff training, as well as man-hours put into issues management.

"We take issues management very seriously," Mr Tay says. "There was a gentleman whose name and contact details happened to be on two of our projects' databases, each belonging to a different client. He had told the first call centre agent to remove his name from the call list, but we didn't know then that he was on the other database as well. So, when he received another call from us, he was annoyed! It took us three weeks to investigate and settle the matter, but it was important that we did."

To prevent the same issue from arising, JRC created its own do-not-call list which identifies recipients who have opted out of participating in market research surveys. The list will be run through before every new project to ensure that the recipients' numbers are omitted from the project.

Weighing in on the time and effort spent, Mr Tay says, "It is all worthwhile. Many of our clients are MNCs and large corporations so they demand very high standards. We are delivering to those standards, which has opened up greater business opportunities for us. Our clients and stakeholders have more confidence in us now."

Mr Suhaimi Salleh, President of LBKM says complying with the PDPA has given donors and beneficiaries greater confidence that their personal data is protected.

CHALLENGES

For decades, LBKM had no official policy on how to handle personal data. With the enactment of the PDPA, it had to shore up its data protection measures by developing a formal data protection policy.

STEPS TAKEN

- **Appointed data protection officer**
- **Engaged consultancy firm to conduct PDPA readiness and security audit**
- **Provided option on donation forms for donors to consent (or indicate that they no longer consent) to receiving fundraising letters**
- **Improved physical and electronic security of bursary/scholarship applications and donation forms**

BENEFITS

- **Instilled confidence among donors and beneficiaries that their personal data is protected**
- **Beneficiaries are more likely to contribute to LBKM knowing that their personal data is secure**

DATA PROTECTION IS 'COMMON SENSE'

Non-profit organisation LBKM has rolled out a slew of measures to safeguard the personal data of donors and beneficiaries

As a bursary and scholarship-disbursing organisation, Lembaga Biasiswa Kenangan Maulud (LBKM) plays a key role in helping needy students achieve academic success.

Since its inception in 1965, LBKM, a non-profit organisation funded almost entirely by donations from the public and corporate sponsors, has awarded more than 24,000 bursaries and scholarships to students – from primary to postgraduate level.

Each year, it receives about 1,800 bursary and scholarship applications, along with their personal data such as contact information, academic records, identity card numbers and family incomes. LBKM uses the data to process, assess and disburse bursaries and scholarships to qualifying students.

Prior to the enactment of the Personal Data Protection Act (PDPA), LBKM had no official policy on how to handle personal data. That said, its employees have always been practising good data management habits when handling the personal data of its donors and scholarship and bursary applicants.

"Those who handle the applications know that all personal data should be kept confidential," says Mr Suhaimi Salleh, President of LBKM. "We also keep the application forms and supporting documents like school results under lock and key. Not even the President gets access to the data, unless there are specific queries related to an applicant."

With the PDPA, LBKM recognises the importance of developing a formal data protection policy. This will also go a long way to give employees clarity on good data management practices and build the trust of donors and bursary applicants.

LBKM thus took steps to understand the law and to beef up its data protection measures.

'COMMON SENSE' RULES

LBKM started its compliance journey by first appointing its data protection officer, Mr Muhd Hassim Ahmad. He attended three data protection workshops organised by the National Council of Social Service and the Personal Data Protection Commission (PDPC) to familiarise himself with the new law.

At around the same time, LBKM engaged a local consultancy firm for $4,000 to conduct a PDPA readiness and security audit, and to identify gaps in its data management practices.

With help from the firm, LBKM also developed a data inventory map detailing how personal data is collected and used, as well as trained its staff on the basics of personal data protection.

"Many of the data protection rules are common sense," Mr Suhaimi says. For example, the PDPA requires organisations to avoid retaining documents containing personal data, if doing so is no longer necessary. LBKM now shreds all application forms and academic certificates of applicants a year after they are received.

However, it still retains the contact details of scholarship and bursary recipients in a password-protected computer system. The purpose: to get in touch with recipients down the road to ascertain the impact of LBKM's financial assistance on their lives as a measurement to assess their schemes.

In addition, LBKM keeps the personal data of some 1,300 donors and sponsors to support accounting and reporting functions. It also sends them letters on sponsorship and fundraising opportunities.

"For the regular donors and sponsors whose personal data we collected prior to the enforcement of the PDPA, we have continued to send them our fundraising appeals," Mr Suhaimi says.

"But if they find these letters intrusive and don't wish to continue receiving them, they can indicate that they do not consent by not ticking the consent checkbox on our new donation form that is included with each letter."

To aid business continuity, PDPA allows organisations with existing personal data collected and used before 2 July 2014 to continue using it for the same purposes for which the data was collected without obtaining fresh consent – unless an individual has indicated that he does not consent to the use.

To ensure bursary application and donation forms are secure, LBKM has taken several measures. It has relocated a key staff member who processes applications and donations near its office entrance to a deeper location in the office, plus secured computers with passwords to prevent unauthorised access. Signs were also put up to remind staff about best practices in data protection.

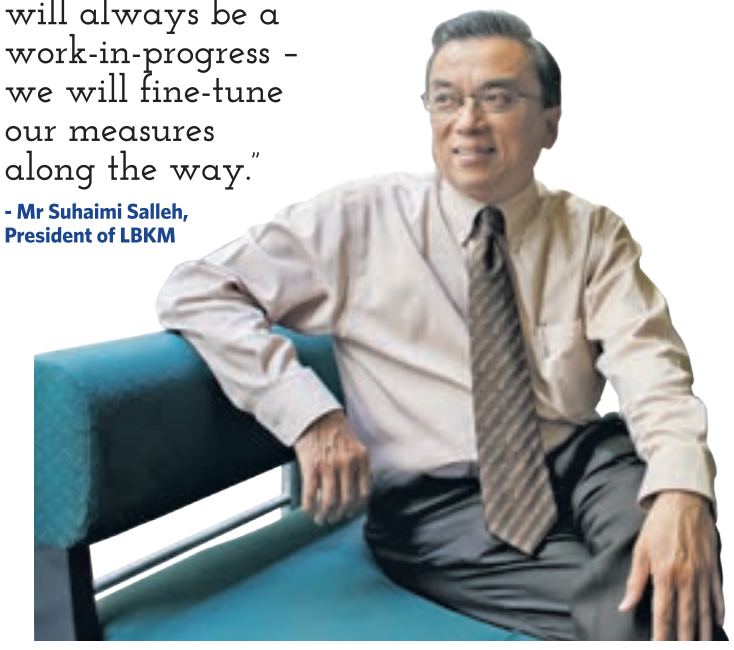
As an added measure, LBKM board members and external panels who review and assess bursary and scholarship application documents can only do so at LKBM's office. Previously, they had received the documents via snail mail, which meant there was always a risk of losing the documents through the postal system.

In addition, Mr Suhaimi says LBKM has also put in a process to track all feedback on their data management practices and investigations accordingly, so that the organisation can continue to review and refine its processes.

"Data protection will always be a work-in-progress; we will fine-tune our measures along the way," he says. "More importantly, complying with the PDPA has given our donors and beneficiaries greater confidence that their personal data is protected."

"And with that confidence, we hope our donors will continue to donate to LBKM, and our bursary and scholarship recipients who have benefited will also give back to LBKM's future fundraising efforts."

> "Data protection will always be a work-in-progress – we will fine-tune our measures along the way."
>
> **- Mr Suhaimi Salleh, President of LBKM**



Complying with the PDPA is in line with MasterCard's corporate mission to make payments safe, simple and smart, says Mr Derek Ho (left), senior counsel for privacy and data protection at MasterCard Asia-Pacific, Middle East and Africa.

CHALLENGES

MasterCard's data protection and privacy policy was in place before the PDPA came into full effect, but it had to review its processes and ensure employees understand their data protection obligations

STEPS TAKEN

- **Took part in PDPC's public consultations to understand policy principles**
- **Reviewed data protection and privacy policies**
- **Organised staff training**

BENEFITS

- **Builds consumer trust**
- **Contributed to successful marketing campaign**
- **Built smaller databases and avoided risks and costs associated with over-retention of data**

PRIVACY BY DESIGN

Building a culture of privacy has been the cornerstone of MasterCard's data protection efforts

> "The cornerstone of our brand is trust, and that's critical because consumers now expect us to handle their personal information properly. We can't break that trust."
>
> **Mr Sam Ahmed, group head of marketing at MasterCard Asia Pacific**

When MasterCard was conceptualising its Priceless Singapore programme, its marketing teams were well aware that they should not collect personal data beyond the needs of the programme.

"We knew that we should only collect personal data for the purpose of allowing cardholders to redeem offers and experiences, and nothing else," says Mr Derek Ho, senior counsel for privacy and data protection at MasterCard Asia-Pacific, Middle East and Africa.

Such guiding principles have been internalised by employees at MasterCard, where a culture of protecting personal data is prevalent across the organisation.

"We embed data protection principles throughout our product lifecycles, whether we are planning a marketing campaign or building a mobile app," Mr Ho says.

He adds that this 'privacy by design' approach - a key feature of MasterCard's global Privacy and Data Protection Program – makes it easier to identify data protection issues early on, rather than after a product or campaign is launched.

"The success of the Privacy and Data Protection Program is due to the close collaboration that we have with product and marketing teams in the organisation," he says. "They help us better understand proposed uses of personal data so that we can apply our data protection principles to those uses."

How MasterCard uses data

As a payment technology company that processes electronic payment transactions, MasterCard collects data such as credit card account numbers, merchant names and locations, as well as the date, time and the total amount of transactions.

The primary use of the information captured in MasterCard's transaction payment system is to process and complete electronic payment transactions.

Transaction data is also used for processes related to those transactions, such as resolving cardholder disputes, detecting and preventing fraud, and addressing account data compromise events, including data breaches at merchants.

"Importantly, we do not receive the cardholder's name or other contact information. Nor do we receive information about the type of merchandise or service that is purchased," Mr Ho says, adding that all data, including personal data, is protected and secured according to MasterCard's data protection policies and controls.

Meeting PDPA obligations

More than a year before the Personal Data Protection Act (PDPA) kicked in, MasterCard reviewed its existing data practices to determine if they complied with the new data protection law.

These included the introduction of product and campaign specific privacy notices instead of relying on its global privacy policy to inform individuals of MasterCard's data processing practices for programmes like Priceless Singapore.

That was because MasterCard had noted that PDPC's Advisory Guidelines had recommended that organisations might need to provide more specific and clear descriptions of how an individual's personal data is used.

After reviewing its contractual arrangements, MasterCard also modified its agreement templates and introduced requirements for its service providers to comply with data protection rules, Mr Ho says.

Meanwhile, it conducted training sessions before and after the PDPA came into effect to raise awareness of the new law. These included online training, videos and providing staff with easy reference documents which MasterCard calls "Privacy at a Glance", plus desktop reminders of key privacy principles.

"In the lead-up to the implementation of the PDPA, we also conducted a series of events during the international Privacy Awareness Week for our employees in Singapore to raise their awareness of data protection," Mr Ho says.

'Data protection incredibly contextual'

While MasterCard did not face major hurdles in complying with the PDPA, Mr Ho says one of the common challenges that any organisation may face is that data protection is "incredibly contextual".

Mr Ho says: "What may be an appropriate use of data in one context may not be appropriate for another, and what may be an acceptable collection of data to one person may not be acceptable to another.

"The way we generally approach and overcome the challenge is to make an effort to understand the context in which data is being collected and used, and to apply the legal rules and principles appropriate for the situation, be it in marketing, human resources, sales, information security, technology, or government relations. All this requires collaboration and partnership with the business."

Mr Ho adds that understanding the PDPC's position on what it believes to be an acceptable practice as described in its advisory guidelines will also enable organisations to craft solutions appropriate for their businesses.

Looking beyond compliance cost

While Mr Ho could not reveal the cost of MasterCard's PDPA compliance efforts, he notes that the Privacy and Data Protection Program has delivered value way beyond the cost of the program.

For example, by only collecting data that is required for the business activity, MasterCard is able to ensure that smaller databases are built, hence reducing the associated costs of maintaining large databases. Data that is no longer required for legal or business purposes is deleted to avoid the risks and costs associated with over-retention of data.

Complying with the PDPA also dovetails with MasterCard's corporate mission to make payments safe, simple and smart, and in earning and maintaining the trust of its employees, cardholders and customers.

Indeed, that trust was instrumental to the success of MasterCard's New Year's Eve marketing campaign, where its marketing and privacy teams came together to develop an effective and transparent way of ensuring individuals understood how their information would be collected and used.

Mr Sam Ahmed, group head of marketing at MasterCard Asia Pacific, says: "The cornerstone of our brand is trust, and that's critical because consumers now expect us to handle their personal information properly. We can't break that trust."

Implementing its personal data protection policy has been a relatively smooth journey for MMI, which made staff and customer acceptance of the new policy a priority.

EARLY CHILDHOOD EDUCATOR SIMPLIFIES PERSONAL DATA PROTECTION REQUIREMENTS

CHALLENGES

The PDPA presented MMI with the opportunity to develop and implement a more wide-ranging and comprehensive personal data protection policy, but not without initial resistance from internal stakeholders.

STEPS TAKEN

- **Chief DPO attended a training course and drafted an enhanced personal data protection policy with the help of a lawyer**
- **Mapped out areas where personal data are collected and used and set out policies to deal with these areas**
- **Entrusted responsibility of data protection to all staff members, particularly heads of departments, centre managers and principals**
- **Broke the PDPA into relatable, bite-sized information for staff members to understand their role in protecting personal data**

BENEFITS

- **A more comprehensive and systematic policy, which plugged gaps in the operations**
- **Processes are more systematic, resulting in greater efficiency**
- **Armed staff with a better understanding of the processes to protect personal data**
- **Greater confidence in the use and protection of parents and students' personal data**

Modern Montessori International spares no effort to ensure all stakeholders understand the requirements of the Personal Data Protection Act

Having helped early childhood educator Modern Montessori International Group (MMI) meet a series of international and industry standards, such as those developed by the International Organisation for Standardisation (ISO), MMI's Manager (Chairman's Office), Mr Steven Kho, is no stranger to implementing processes.

So when tasked to ensure that MMI was Personal Data Protection Act (PDPA) compliant, he was clear about what he needed to do.

"We identified all the personal data we have, followed by the situations where our staff needed to use these data," says Mr Kho. "This allowed everyone to be clear about how to handle and process personal data. We identified areas that could go wrong and focused on developing solutions for those areas."

Raising Standards

A Small and Medium Enterprise (SME), MMI provides pre-school education for children through 30 centres in Singapore, as well as in other parts of the world such as India, Kenya, Malaysia, Nigeria, Thailand and Vietnam. It also conducts teacher-training courses for adults, offering diplomas in the Montessori method of education and early childhood care.

"Before the introduction of PDPA, we were more concerned about copyrights relating to the use of a child's image in our marketing and publicity materials. As a result of the PDPA and its mandatory requirements, our data protection policies now cover more processes and are more comprehensive," says Mr Kho.

Enrolment, for example, is one key process that has been enhanced.

During registration, parents are required to fill up a form containing personal data such as contact details, birth certification numbers and other relevant personal data.

As a personal data protection measure, MMI explicitly seeks the parent's consent for the use and disclosure of the data to support the provision of service. This includes sharing the personal data with pre-school education industry regulator Early Childhood Development Agency (ECDA), providing vendors with the student's data for the organisation of extra co-curricular activities, and using pictures or videos taken of students during activities for MMI's online and offline publications.

To ensure that there is no misunderstanding, MMI also consolidates what parents have consented to in a list that is distributed to parents along with its standard enrolment handbook.

In its dealings with third-party vendors and contractors, MMI places personal data protection-related conditions in the contract agreements.

"There are times when we have to share personal data with third-parties such as bus operators, field trip organisers and event managers. Through the conditions, we can hold them to agreements not to misuse the information we provide them and not to share that data for unsolicited marketing calls or other unauthorised purposes," Mr Kho says.

Entrusting Compliance to the Whole Organisation

It is no mean feat managing the personal data of more than 3,000 students and some 300 staff members across 30 education centres in Singapore. As such, PDPA compliance is a shared responsibility at MMI.

"We believe that everyone in the organisation has a responsibility to protect personal data," says Mr Kho. "All department heads at MMI headquarters play a crucial role in enforcing our personal data protection policies. In our pre-school centres, the centre managers and principals take on the role of data protection officer."

Mr Kho is the chief data protection officer for the organisation. To familiarise himself with the relatively new law at the onset, he enrolled for a course that provided an introduction to the fundamentals of the PDPA which was designed for non-legally trained persons, offered under the Workforce Development Agency's (WDA) Business Management Workforce Skills Qualifications framework.

He found the curriculum straightforward and useful in his development of MMI's enhanced data protection policy. He then consulted a lawyer to firm up the overarching policy.

Implementation of the new processes took three to four months, and the transition was fairly smooth apart from some internal resistance.

Mr Kho recalls that the most often asked question was, "We haven't had problems before, so are these changes really necessary?"

To help staff members internalise the requirements, he explains the obligations of the PDPA in parts and how each applies to MMI's operations during the training sessions. He feels that showing how the new data protection procedures are relevant to each staff member's area of work helps increase acceptance of these measures.

"When you do it this way, staff members will be keen to learn as they are familiar with the operational situation," he shares. "They may even be able to provide feedback or suggestions to improve the data protection policy."

He believes that MMI is now more systematic in its handling of personal data, which increases efficiency. He also feels more confident when speaking to parents and students about the security of their personal data with the organisation.

Overall, MMI spent an estimated $20,000 in the development and implementation of an enhanced personal data protection policy in line with the PDPA. The bulk of this cost was expended on man-hours used to draft and implement the new procedures, staff training, and the upgrading of MMI's information technology (IT) systems to include access control and boosted password protection.

When asked what advice he might have for other SMEs, Mr Kho says, "They should not feel that the PDPA is difficult to comply with. What they need to do is to understand how the PDPA relates to aspects of their company's operations. Once they are able to identify the processes that have to be improved or put in place, they will not find it difficult to develop the policies."

NTUC roped in its service excellence team and set up its own Do-Not-Call registry to manage voice calls and text messages to over 800,000 members.

CHALLENGES

NTUC had to review its policies, systems and processes to fully comply with the PDPA.
In doing so, it faced difficulties in interpreting the new law and had to ensure that any new measures would not affect customer experience.

STEPS TAKEN

- **Formed its Data Protection Office comprising representatives from IT, legal and service excellence teams**
- **Developed enterprise-wide data inventory map**
- **Prepared specific advisories and guidelines for NTUC and its affiliated unions and association.**
- **Developed new SOPs and service guides, e.g. member retention upon receiving consent withdrawal requests**
- **Set up its own Do-Not-Call registry**
- **Trained all employees, union leaders and management staff**

BENEFITS

- **PDPA provided good data protection framework**
- **Strengthened data protection measures**
- **Building trust with union members**

LABOUR MOVEMENT LEADS THE WAY IN DATA PROTECTION

Managing the personal data of over 800,000 members is no small feat for the National Trades Union Congress (NTUC), a national confederation of trade unions in the industrial, service and public sectors in Singapore.

It currently manages the personal data – such as contact details and employment information –on behalf of 57 unions and one affiliated taxi association.

With the massive amount of personal data under its care, it is even more critical for NTUC to embrace best practices in data protection.

That includes obtaining consent from members to use their personal data to provide services as well as to inform them about membership matters, as required under the data protection provisions under the Personal Data Protection Act (PDPA).

NTUC also obtains consent to share personal data with its supermarket chain NTUC Fairprice so that members can enjoy shopping rebates, or with the Employment and Employability Institute (e2i) to facilitate job training for members.

Besides obtaining consent from members for such purposes, the NTUC has implemented strict IT policies and other standard operating procedures (SOPs) and data protection policies.

Despite having such practices in place before the PDPA kicked in, NTUC reviewed its data protection measures in early 2013 to ensure compliance with the new law.

Cross-functional team

Under the leadership of NTUC's chief information officer Dr Kwong Yuk Wah, a high-level data protection office comprising representatives from NTUC's information technology, legal and service excellence teams, was formed.

Dr Kwong, who doubles as the labour movement's chief data protection officer, says the service excellence team, in particular, plays an important role to ensure NTUC's data protection measures do not affect customer experience.

"For instance, one of the obligations of the PDPA is to allow the withdrawal of consent," she says. "But if a member withdraws his consent for the use of his personal data for purposes such as facilitating job training, we may not be able to provide such services to him."

That's where the service excellence team steps in to establish SOPs or service guides that require staff to explain to individuals about what a withdrawal of consent means for their membership.

Building data inventory maps

Led by its data protection office, NTUC created an enterprise-wide data inventory map, which details the types of personal data collected such as those of union members, members of its various communities, union leaders, employees and individuals who enquire about NTUC's services.

The data inventory map also includes details of where data is stored, along with a list of organisations to which personal data could be disclosed, as indicated in NTUC's consent forms.

"We don't pass personal data to organisations that are not included in the data inventory map," Dr Kwong says, adding that all personal data is secured through security and access control systems.

So far, NTUC has not had to disclose personal data to organisations that are not found in the data inventory map, Dr Kwong says. "But should the need arise, the names of additional organisations will be added to our map and consent forms."

In drafting the data inventory map, NTUC also referred to the Personal Data Protection Checklist for Organisations provided by the Personal Data Protection Commission (PDPC) to ensure that all data protection measures are met.

Cost Savings through NTUC's Do-Not-Call Registry and Exemption Order

Most of NTUC's calls and text messages to members are often related to membership services.

For the existing base of members prior to 2 July 2014, NTUC has avoided incurring hefty costs to obtain consent by relying on an exemption order for telemarketing messages that lets organisations send text and fax messages on related products and services to individuals with whom they have an ongoing relationship, unless the individual chooses to opt out.

The unions too may send text messages to invite members for events such as dinner and dance, and other union-related activities. "We've set up an NTUC Do-Not-Call Registry specifically for this purpose so that unions can check before sending out such messages. Our registry has records of which union member has withdrawn consent for the sending of specified messages," Dr Kwong says.

Staff training

To get employees and union leaders up to speed on NTUC's data protection measures, Dr Kwong's team developed a comprehensive training programme for 1,800 union leaders, NTUC's top management and 650 employees, including appointed compliance managers in over 20 departments and 57 affiliated unions and one association.

They were trained not just on PDPA obligations, but also on NTUC-specific guidelines and scenarios, such as whether handing over an identity card during membership registration could be considered as deemed consent. All trainees had to pass a multiple-choice quiz.

"We also created an information portal to help staff and union leaders better understand NTUC's data protection policies, advisories and guidelines," Dr Kwong says.

Dr Kwong says there have been no major challenges in complying with the PDPA, except with interpreting various aspects of the law before the PDPC released its advisory guidelines.

"For example, we weren't sure of how we should seek clear and unambiguous consent, a process which we have refined after going through the guidelines," she says. "The best practices in the guidelines also came in handy while we were reviewing our data protection procedures."

By providing a data protection framework, the PDPA has given NTUC the opportunity to ensure its data protection measures are comprehensive, Dr Kwong says.

As compliance is an ongoing exercise, NTUC plans to introduce a new mobile app by the end of this year to help unions register new members without relying on paper forms.

Dr Kwong says: "We want to use more technology to protect the data, to avoid situations when personal data could be exposed when membership forms are misplaced".

Be it recruitment candidate or employee data, PrimeStaff Management Services treats both with extreme care.

GOOD DATA PROTECTION POLICIES ENHANCE TRUST IN HR CONSULTANCY

Careful handling of personal data helps PrimeStaff Management Services maintain a high level of trust and confidence with its clients

CHALLENGES

PrimeStaff's employees handle personal data on a daily basis. Their biggest challenge is to ensure employees comply with its personal data protection policies to fulfil their functions and operations.

STEPS TAKEN

- **Regular employee training on PDPA requirements and on the importance of protecting personal data protection**
- **Enhanced security measures in IT systems such as restricting access to and transfer of personal data**
- **Development of new forms to notify and obtain consent from potential candidates**

BENEFITS

- **Increased trust and confidence among clients, candidates and employees that their personal data is protected**
- **Reduced risk of personal data leaks and misuse**
- **Enhances professionalism and instills pride in PrimeStaff employees who know they are entrusted with sensitive personal data**

In the recruitment industry, information on people is the biggest asset. Yet this could become a double-edged sword if not managed well.

"People looking for jobs always want assurance that their data is safe with us; good personal data protection practices is one of the basic expectations of us as recruitment consultants," says Mr Ronald Lee, managing director of human resource (HR) firm, PrimeStaff Management Services.

Established in 1994, the home-grown SME places people not only in Singapore, but also around Southeast Asia and Australia. PrimeStaff was named "Best Recruitment Firm – Overall (Singapore)" and "Best Recruitment Firm for HR Positions" at the HRM Asia Awards in 2015.

"Because of the trans-boundary nature of our business, we recognised the need to develop a privacy policy that is of international standards," Mr Lee says.

PrimeStaff had a personal data privacy policy in place before the Personal Data Protection Act (PDPA) came into full effect in July 2014. The policy then was focused largely on putting in place measures to restrict access to files containing personal data, and the blocking of file sharing sites and non-corporate email access to prevent unauthorised transfer of data to any third parties.

"Things are different now with the mandatory requirements of the PDPA," Mr Lee adds. "The new requirements imposed by the Act means we need to obtain consent to use personal data, and the resultant shift in customer expectations is a motivating factor that keeps us on our toes."

Period Of Transition

PrimeStaff took several months to align its personal data protection policies to meet the PDPA's obligations. The process started with a team of five, including Mr Lee. They attended introductory talks, seminars and other related courses to familiarise themselves with the requirements of the PDPA.

Given the company's specialised function, the bulk of personal data handled by PrimeStaff is for the purpose of recruitment for client organisations, and they handle the personal data of about 40,000 individuals. So it was clear to the team that ensuring the personal data remained safe and secure was of utmost importance.

"Our biggest challenge is ensuring that no personal data is leaked by our employees, whether unwittingly or deliberately, because our consultants handle so much personal data on a daily basis," Mr Lee shares.

To prevent softcopies of personal data being downloaded and transferred, the team enhanced the security of the company's information technology (IT) systems, including blocking access to free email service providers such as Google mail, Yahoo mail, Hotmail and other media-sharing sites such as Dropbox, iCloud, Google Drive. Third-party storage devices such as thumb drives and CD readers are also fully or partially disabled so that information cannot be readily copied or transferred.

Other steps taken by PrimeStaff included the development of new forms to document consent from potential candidates to use their data for recruitment, and the introduction of a retention limitation policy.

The company's retention policy limits its consultants from keeping a candidate's data unnecessarily. Some personal data is typically kept for a period of time in order to recommend suitable job openings. However, the data would be deleted when it is no longer needed for legal and business purposes.

Candidate Data Vs Employee Data

Apart from candidate data, PrimeStaff is mindful that it has to protect its own employee data too. As an HR consultancy, PrimeStaff believes all personal data is important and does not treat employee data any differently. Therefore file access control measures are put in place to ensure only the relevant employee has access to employee data.

Mr Lee explains, "Access and processing of employee data are restricted. Only HR or the Payroll department and recruiters are allowed access to such data based on whether they have been tasked to use or process the data to fulfil the purpose it was collected for."

"For IT systems, once properly put in place, they are less likely to pose compliance problems," says Mr Lee. For example, once a file access control measure is set, employees who do not have permission to handle the information will not be able to access the file.

"However, there is less certainty with people," he adds. To help reduce human errors, PrimeStaff makes it a point to conduct regular training for its employees. These sessions reinforce the importance of protecting personal data and update employees on new developments and regulations in the HR industry.

Compliance A Worthwhile Effort

Mr Lee estimates that the company spent about $45,000 to hone and implement its personal data protection policy to comply with the PDPA. He attributes 93 per cent of the cost to man-hours spent understanding the application of the PDPA to PrimeStaff's operations as well as in developing and implementing policies to comply with the PDPA. Training fees accounted for the rest of the cost.

However, Mr Lee considers these to be necessary compliance costs. "Knowing how careful we are with personal data increases the trust and confidence our clients and candidates have in us. We allocated more time and effort on compliance with the PDPA so as to get this right, which in turn enhances our position as a preferred HR consultant."

With a strong focus on customer service and keeping personal data secure, RedMart aims to encourage more shoppers to buy online – Mr Christopher Y. Chan, Director, Legal and Government Affairs

CHALLENGES

Being a start-up and fairly new to the Singapore market, RedMart has to manage the growth of a thriving e-commerce business alongside personal data protection in a short span of time.

STEPS TAKEN

- **Introduced apps designed for warehouse and delivery staff that provide minimal customer information to facilitate the execution of a successful order**
- **Tightened security of customer databases with access controls and data flow mapping**
- **Included confidentiality clauses in employment contracts**

BENEFITS

- **Birth of innovative apps that secure personal data**
- **Processes are streamlined due to elimination of excess information shared**
- **Changing customer attitude towards e-commerce through an environment of trust**

ONLINE GROCER GROWS PERSONAL DATA PROTECTION ALONG WITH BUSINESS

Burgeoning growth drives RedMart to design its processes around personal data protection

Since its founding in 2011, the primary focus of RedMart, an online grocery service provider, has been to grow the business by providing its customers with the best possible experience. And that starts with ensuring customers feel assured their personal data is secured when shopping with RedMart. This was what prompted the company to design its processes around personal data protection.

"Personal data protection is important; however, for many start-ups, it can be secondary to achieving growth and profitability. At RedMart, we believe that data protection is directly related to customers trusting our company, which is a necessary part of ensuring growth," explains Mr Christopher Y. Chan, Director of Legal and Government Affairs at RedMart.

Mr Chan joined the company in 2015 as its first attorney and is also RedMart's designated data protection officer.

With the enactment of the Personal Data Protection Act (PDPA) in November 2012, RedMart revised its data protection policy to ensure that their customers' personal data is well accounted for. That was first in the tweaks that RedMart undertook to ensure compliance with the PDPA.

Designing Operations Around Personal Data Protection

At its core, RedMart is a logistics company powered by technology. It has the in-house expertise to develop systems to meet the demands of the market and regulations such as the PDPA.

"A lot of our business processes are designed to maximise customer experience whilst ensuring data protection," Mr Chan says. "Previously, delivery personnel were given invoices with customers' name, address, email address and contact number. Now, our delivery representatives only see what they need to."

All delivery representatives of RedMart are provided with its Delivery Buddy mobile application (app) to assist them in carrying out their tasks. The app shows only the customer's name and delivery address, and helps map out the most efficient route around Singapore to ensure on-time deliveries.

To notify customers of the arrival of their deliveries, the app triggers a SMS notification to the customer via a RedMart secured server. This eliminates the need for the delivery representative to know the customer's contact number, and vice-versa.

On the rare occasions where a delivery representative needs to contact a customer during delivery, they will use the app to directly place the phone call to the customer. The call is then logged in RedMart's system so that it knows when and who called a customer for tracking purposes.

Mr Chan explains that the need to make an actual phone call is rare, typically arising in situations when the delivery representative is unable to find the entrance to the property or cannot enter a secured area. Using the SMS service to inform a customer of an impending delivery is generally sufficient.

"We give our delivery representatives enough information to do their job, and not more; to respect and protect our customers," Mr Chan adds.

RedMart also uses a Picking app that was designed for warehouse staff who have to navigate through more than 30,000 products in a 100,000 square-foot warehouse at Jurong Fishery Port. The only information that these staff members have access to are the customers' name and general locations of delivery.

In addition to fine-tuning of customer and delivery-centric processes, some adjustments were made to internal processes.

Mr Chan says, "We investigate all data protection-related complaints and issues that are brought to our attention. Relevant personnel are given briefings on the importance of protecting personal data and all employment letters include a confidentiality clause that staff must agree to."

Driving Secure Online Grocery Shopping

While online shopping is a growing global trend, Mr Chan reckons that many buyers in Singapore are still conservative when it comes to online shopping because of the personal data that is required to effect transactions.

Online shoppers have to minimally provide RedMart with their names, delivery addresses, email addresses, contact numbers and payment details to place an order.

Each shopper is then assigned a customer identification number through which they can track their orders, look up order histories, as well as opt out of the various notification channels offered.

Just how secure is RedMart's customer data?

"We have taken some steps to secure customer databases, such as mapping the flow of data and restricting access via login permissions to only authorised personnel who need to know the information, such as customer service officers or programmers working on a specific issue," Mr Chan says. "Even I cannot access the customer database because I don't qualify as an authorised personnel!"

Other information technology (IT) enhancements adopted by RedMart include, among others, the installation of firewalls, internal risk audits and regular breach checks. Yet another layer of protection is provided by its cloud-based servers in Singapore where RedMart stores its customer information.

With a strong customer-first focus, RedMart is doing what it takes to earn and keep their customers' trust. Mr Chan says, "If online shopping is made easy and we have a good data protection policy to ensure safe transactions, we can change behaviours."

Personal Data Protection a Continued Focus

Acknowledging that implementing data protection safeguards requires time, technology, and financial resources, Mr Chan points out that allocating human resources has been the company's key challenge to date.

He highlights that it is difficult to measure or quantify the resources and man-hours expended on tackling data protection issues, as it is an ongoing process. Personal data protection will continue to be a focus for the company as it grows and expands.

RedMart employs over 700 people, and it is the IT team and data protection officer that RedMart looks to for support in complying with the PDPA.

"We take PDPA compliance very seriously and recommend that other SMEs do so too," Mr Chan advises. "Take a common sense approach to data protection and start with identifying the types of personal data you hold. Appointing a data protection officer is also essential because he or she would be able to cast an eye over data protection matters on a daily basis."

DISCLOSURE OF PERSONAL DATA FOR ORDER PROCESSING

RedMart has developed multiple applications to ensure only relevant personal data is disclosed at each stage of order processing.

Customer puts in an order online, providing personal data such as name, email, phone number, address and payment details. An email confirmation is received.

Customer name and general location of delivery made known to warehouse staff. Only the customer's name and address are revealed for the purpose of delivery.

Customer is notified of the arrival by an SMS triggered by the app. Where necessary, the app can be used to place a call directly to the customer. Call is logged for tracking purposes.

The sensitive and discreet treatment of beneficiary, donor and volunteer data is a priority for Tan Tock Seng Hospital's Development Fund and Volunteer Management Office – Mrs Eunice Toh, Executive Director of TTSH Community Fund and Director of TTSH Development Fund & Volunteer Management

PERSONAL DATA PROTECTION A PRIMARY PRIORITY FOR HOSPITAL COMMUNITY FUND

The concept of protecting personal data is nothing new to Tan Tock Seng Hospital's Development Fund and Volunteer Management Office, which has managed scores of personal data belonging to beneficiaries, donors and volunteers for more than a decade

Among the programmes that Tan Tock Seng Hospital's (TTSH) Development Fund and Volunteer Management Office help administer is the TTSH Community Fund, the hospital's charity arm that was first set up in 1995 to help needy patients. Today, the TTSH Community Fund supports more than 2,500 patient cases each year, particularly the elderly and those who have exhausted all avenues of financial help. The TTSH Community Fund also seeks to promote better patient care through medical research and training.

Due to its raison d'etre, it is no surprise that the TTSH Community Fund holds troves of personal data. In addition to patient beneficiaries, it has in its possession the data of a few thousand donors–both individuals and corporations.

Separately, the Development Fund and Volunteer Management Office also manages the records of some 700 volunteers across 27 programmes, about half of whom are actively serving the TTSH Community Fund.

In view of the nature of work that this team undertakes, sensitivity and discretion are of the utmost importance when handling beneficiary and donor data, regardless of the Personal Data Protection Act (PDPA).

Mrs Eunice Toh, Executive Director of TTSH Community Fund and Director of Development Fund and Volunteer Management, says, "We don't take it for granted that we can use personal data provided to us, either by a donor or a beneficiary, for our publicity purposes. A donor may want to keep a low profile, or a beneficiary may be self-conscious. It is thus necessary to seek their approval if such personal information is going to be used."

"To us, the PDPA is an excellent reminder of the importance of personal data protection policies," she adds. "As the PDPA places a mandatory obligation on organisations to comply with its requirements, it reminds us to check for gaps in our existing policies."

Chasing Paper

As TTSH Community Fund's data protection officer, Mrs Toh works closely with a staff member each from Finance and Volunteer Management / Fundraising support to assess and develop suitable data protection policies. Notably, the mountain of paperwork that comes through creates the biggest challenge for the team, which has to tackle the issue of data protection across multiple facets of the division's operations.

Fundraising, a critical aspect of TTSH Community Fund's work, requires donors to submit their personal particulars through hardcopy forms. In Finance, receipts and payment vouchers would also contain donor and beneficiary information. While volunteers are encouraged to complete their applications online, dealing with hardcopies is inevitable.

Mrs Toh acknowledges that the sheer volume of physical paperwork that the team manages could give rise to the risk of data protection breaches, which is why she lauds the PDPA for bringing these issues to the fore.

Among the data protection measures that the TTSH Community Fund has implemented is ensuring that hardcopies containing personal data are always locked in cabinets and accessible only to authorised personnel. Similarly with its computerised accounting system, access to donor and beneficiary information is granted only to authorised personnel.

Aside from collecting personal data, the TTSH Community Fund also proactively obtains consent to use the said data. A visible use of donors' personal data, for example, is the acknowledgement of their contributions in the Roll of Honour, which occupies a conspicuous position at TTSH's ground floor main lobby.

Mrs Toh explains, "It is important for us to obtain donors' consent before we place their names on the Roll of Honour because there will always be donors who prefer to remain anonymous. We also try to promote the Fund so written consent of beneficiaries, be these needy patients or grantees who are awarded grants, is another important point to note for media and publicity purposes. Confidentiality of their personal data cannot be compromised or taken for granted simply because we are assisting them with funding support."

To ensure that donor and beneficiary data is not inadvertently disclosed, the TTSH Community Fund shares its personal data protection policies on the hospital intranet so that all other departments are also aware of the correct procedures for handling such data.

A Continual Journey

Mrs Toh opines that the data protection policies and practices that the team has in place are simple and well-suited for their purposes. The financial cost of compliance was negligible because development and implementation of data protection policies were all done in-house, and the Fund's database was relatively small. However, Mrs Toh felt the real cost was the time and effort spent to read about the PDPA and brainstorm for the data protection policies.

"When the PDPA came into force, we studied the requirements, reviewed our existing policies and made the necessary enhancements. All that was done within a month because we already had a comprehensive structure in place and were clear as to what our obligations to stakeholders were," Mrs Toh says.

Of course, the work does not stop there. Staff members are continually reminded to handle personal data responsibly and Mrs Toh notes that they are more mindful now when preparing reports and handling forms. Volunteers, too, are briefed on data protection policies before they are deployed and are required to sign a non-disclosure agreement which prohibits the exposure of any confidential information that they acquire in the course of their volunteer service.

Additionally, Mrs Toh insists on reviewing and updating TTSH Community Fund's compliance policies and standard operating procedures (SOPs) every one to two years.

Evidencing the effectiveness of the team's data protection policies, Mrs Toh was invited to share the template she had developed at a conference hosted by Charity Council in 2012, shortly after the PDPA was announced. She also gave a talk on the same subject to voluntary welfare organisations in 2014.

She says, "We don't protect personal data just because of the law. Protecting personal data is a matter of integrity. It is every individual's prerogative to decide how the personal data they provide can be used, so it is important for us to ask for consent."

CHALLENGES

Although sensitive and discreet treatment of personal data had always been a priority for the TTSH Development Fund and Volunteer Management Office and TTSH Community Fund, the introduction of the PDPA was a timely reminder to review its policies.

STEPS TAKEN

- Studied the requirements of the PDPA, reviewed existing policies and made enhancements accordingly, along with corresponding staff and volunteer training
- Personal data protection policies are shared on the hospital's intranet so other departments are aware
- Obtain written consent from beneficiaries and grantees before personal data is used for media and publicity
- Have volunteers sign non-disclosure agreements before deployment
- Ensured that physical access to personal data is effectively managed through SOPs
- Data protection policies and SOPs are reviewed and/or updated every one to two years

BENEFITS

- Reviewing policies periodically helped sieve out gaps in personal data protection
- Staff members are more mindful when preparing reports and handling forms, thereby increasing protection of personal data
- Donors have more confidence in the TTSH Community Fund

Complying with the Personal Data Protection Act has helped York Hotel to build trust and credibility with customers.

CHALLENGES

Personal data protection is not new to York Hotel. However, further measures were needed to comply with the PDPA as practices were inconsistent between the various departments of the hotel.

STEPS TAKEN

- **Attended training and workshops at PDPC**
- **Hired law firm to review data protection related terms used across customer touch points**
- **Reviewed business processes**
- **Developed SOP document, which includes complaints-handling processes**

BENEFITS

- **Builds trust and credibility with customers**
- **Customers more receptive to sharing personal data**
- **Reduces risk of sensitive personal information falling into the wrong hands**

CUSTOMERS REST EASY WITH DATA PROTECTION

York Hotel has been obtaining consent from customers for its marketing efforts for the past three years

York Hotel is no stranger to safeguarding the personal data of its customers.

Since 2012, hotel customers who would like to receive information on marketing promotions and events are required to provide clear consent.

Take the hotel's annual Penang Hawkers' Fare lucky draw, for instance.

Each lucky draw form includes fields for customers to indicate if they would like to receive the hotel's marketing promotions via e-mail or telemarketing calls. Those who choose to do so have to sign on the forms, and provide their consent by ticking a checkbox.

Ms Audrey Liau, York Hotel's marketing communications manager, says: "The forms represent explicit consent and is a safeguard for us. We only contact customers who have provided such consent. We don't even contact those that indicated interest but did not sign off."

As an added measure, the forms filled by these customers would be shredded once the lucky draw is concluded to prevent unauthorised access to personal data.

Meanwhile, the signed forms of customers who have provided consent would be scanned and saved onto a password-protected PC, before being kept under lock and key.

The hotel had also implemented similar measures for guest comment cards, through which consent is sought for the purpose of contacting guests to learn more about their stay.

While personal data protection is not new to York Hotel, Ms Liau says further measures were needed in order to fully comply with the Personal Data Protection Act (PDPA).

The PDPA requires all organisations in Singapore to seek consent and notify individuals on the collection, use and disclosure of personal data for specific purposes. They must also safeguard all personal data under their care.

Acquiring data protection knowhow

Ms Liau knows that training is key to getting buy-in from her co-workers in any compliance effort, but first, she needed to beef up her knowledge of the PDPA.

In early 2014, Ms Liau and the hotel's financial controller attended training workshops and briefings conducted by the Personal Data Protection Commission (PDPC) which were useful in providing an overview of the new data protection law.

They also took up a workshop on the fundamentals of the PDPA for non-legal personnel, a certified and subsidised course brought about by PDPC and the Workforce Development Agency (WDA).

The two-day course aims to help organisations deepen their understanding of the PDPA by going through key concepts under the PDPA, so that they are able to develop data protection policies and processes to meet their organisation's need.

Participants such as Ms Liau who have successfully completed the course and assessment will also be awarded with a Business Management Workforce Skills Qualifications (BM WSQ) Statement of Attainment.

Ensuring compliance

With the newly acquired knowhow, Ms Liau worked with a team of eight managers, including top executives, across the hotel to put together a SOP (standard operating procedures) document.

"Besides detailing the obligations of the PDPA – such as obtaining consent from customers – that we need to comply with, the SOP also includes business processes such as our internal processes for handling complaints," Ms Liau says.

"For example, if a guest says he has not given consent to be contacted but has received e-mails from us, we'll check the forms to see if that's indeed the case. We'll remove his personal information from our database if we find that consent was not given and apologise to the guest," she explains.

York Hotel also hired a law firm to review data protection related terms it had been using across customer touch points such as its website and lucky draw forms. "For example, they helped us to fine-tune the language that we should use to seek consent from customers," Ms Liau says.

A review of business processes by Ms Liau and her team also revealed that consent was not sought for contact information collected by the corporate sales department through lucky draw contests.

While the contact information could be business contact information, Ms Liau says some business customers provide their personal e-mail addresses in lucky draw forms. "We'd rather be safe and protect ourselves by seeking their consent upfront," she says.

With the SOP in place, Ms Liau and her team conducted training sessions to brief about 200 hotel employees on the new measures, and the need to comply with the law.

But the new rules took some getting used to by some employees. "We faced some resistance at first, as there was extra work for some staff," Ms Liau explains.

For one thing, the hotel's restaurant staff are now required to check the Do Not Call (DNC) Registry, before calling regular customers to market annual promotions such as Chinese New Year reunion dinners.

That said, the hotel's staff became more receptive to the new rules after they learned more about the PDPA through their training sessions and the benefits of compliance.

Building trust and credibility

By taking on most of the training and policy development in-house, York Hotel spent just $5,000 on training and legal fees to comply with the PDPA.

Ms Liau says the money was well-spent, as it has helped York Hotel to build trust and credibility with its customers.

"We are able to assure customers that their personal data will be sufficiently protected. Our customers are now more receptive to sharing their personal data," she says, adding that "compliance also reduces the risk of sensitive personal information falling into the wrong hands".

LEARNING POINTS

Obligations under PDPA

- Know that both the organisation and its Data Intermediary (DI) have obligations under the PDPA. DIs who are processing personal data for their clients have to take note of their protection and retention limitation obligations.
- Engage in close discussion with DIs to ensure that the appropriate level of security is provided for the protection of personal data.
- Include clauses on personal data protection in contracts with third-parties.

Policies and Processes

- Appoint a Data Protection Officer (DPO) to help the organisation with personal data management and to handle personal data-related queries or complaints.
- Design your operations around data protection policies, which may lead to innovations that streamline processes.
- Make information about your data protection policies, practices and complaints process available on request.

Collection, Use and Disclosure

- Notify individuals on the purpose of the collection, use and/or disclosure of their personal data.
- Use or disclose personal data only for the purpose it was collected, and obtain consent from the individuals.
- Ensure that personal data, in particular those collected using publicly-shared devices, will not be inadvertently disclosed to other individuals.

Care for Personal Data

- **Administrative Measures**

- ✓ Put in place measures for the sending of mass emails, letters or any other communications to prevent sending to the wrong recipients.
- ✓ Ensure that only the appropriate amount of personal data is held, as holding excessive data will also increase the efforts required to protect personal data.
- ✓ Stop keeping personal data if there is no longer any business or legal purpose. Consider anonymisation if the data may be further used.
- ✓ Educate employees on their role in protecting personal data that is under your organisation's control or in the organisation's possession.
- ✓ Review your personal data protection policies and practices regularly.

- **Physical Measures**

- ✓ Store confidential documents containing personal data in locked file cabinet systems.
- ✓ Restrict employee access to such confidential documents on a need-to-know basis.
- ✓ Properly dispose of such confidential documents that are no longer needed, through shredding or pulping.

- **Technical Measures**

- ✓ Protect personal data stored in an organisation's IT system, such as:
  - using strong passwords that are difficult to deduce;
  - conducting security audits and tests;
  - regularly updating security patches;
  - disabling accounts that are no longer necessary or in use; and
  - using an appropriate level of security in a public-facing website or application that collects and stores personal data.
- ✓ Ensure that IT service providers are able to provide the requisite standard of IT security.

Do Not Call

- Obtain clear and unambiguous consent from individuals for telemarketing purposes or check the Do Not Call (DNC) Registry.
- Keep an internal record of the individuals who have opted out of your organisation's telemarketing activities.

PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

www.pdpc.gov.sg www.linkedin.com/company/pdpc