Advertorial
presented by

PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

www.pdpc.gov.sg
www.linkedin.com/company/pdpc
www.facebook.com/PDPC.Singapore

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

PERSONAL DATA PROTECTION EVOLVES WITH TECHNOLOGY

Understanding its role as a data intermediary under the Personal Data Protection Act (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, helps 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 employee.

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." ♦

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