Technology, Media & Telecommunications

PDPC Handbook on How to Guard Against Common Types of Data Breaches

Introduction

In this digital age, organisations often find themselves grappling with issues of personal data, including how to protect personal data in the organisations' possession, and how to defend their systems against data breaches.

As Singapore's main authority in matters relating to personal data protection, the Personal Data Protection Commission ("**PDPC**") has published a new handbook that highlights the five most common gaps in Information and Communication Technology ("**ICT**") system management and processes ("**Handbook**"). The Handbook also identifies the corresponding ICT good practices that organisations should put in place to prevent data breaches.

The Handbook is distilled from past data breach cases handled by the PDPC, and provides a helpful guide for organisations to assess the adequacy of their data protection systems and processes and to implement any of the relevant recommendations. In this regard, our Technology, Media and Telecommunications team from Rajah & Tann Singapore LLP, as well as our team from Rajah & Tann Cybersecurity, are well placed to assist in assessment and remedial efforts.

This Update provides a summary of the key issues raised in the Handbook and the corresponding recommendations from the PDPC.

Common Gaps in ICT System Management

The Handbook identifies the following as the most common issues:

(a) Coding;
(b) Configuration;
(c) Malware and Phishing;
(d) Security and Responsibility; and
(e) Accounts and Passwords.

Coding

Mistakes made during the programming phase of software development can lead to application errors that result in disclosure of personal data.

Such errors can be avoided through clear business requirements translated into clear technical implementation and adequate planning of testing scenarios, as well as through careful code reviews. Organisations should also be aware that poor documentation may lead to errors due to lack of clear knowledge of how the components or modules of the ICT system work.

The Handbook makes the following recommendations:

(a) **Design before coding** – Practise designing before coding and perform thorough impact analysis of any software or code changes to identify their potential effects.
(b) **Proper documentation** – Document all software functional and technical specifications (e.g. program specifications, system specifications and database specifications).
(c) **Thorough testing** – Ensure that the application is thoroughly tested with comprehensive testing such as unit testing, regression testing, security testing, and User Acceptance Testing.
(d) **Perform code reviews** – In addition to reviewing their own code, code authors can also conduct peer code reviews.

Configuration

An ICT system consists of various components that often have configurable settings and parameters. Unsecured settings, including leaving settings in their default, can result in unintended disclosure of personal data. This includes not using HTTPS protocol, improperly configured firewall rules, not scanning certain file types or specifying sufficient follow-up action in antivirus software, and not setting restrictions/access control for access to folders with personal data. Code management/deployment issues such as configuration issues in code management/deployment systems can also result in wrongly deploying test code to production environment.

The Handbook makes the following recommendations:

(a) **"Harden" system configuration** – This may be achieved by making appropriate changes to settings instead of relying on default settings, such as firewall configuration or web server configuration.
(b) **Automate build and deployment processes** – This can minimise manual steps and reduce the likelihood of human error, such as by executing predefined scripts.
(c) **Systematic management of configuration settings** – This includes: (i) documenting, updating and reviewing baseline configuration settings; (ii) establishing procedures for configuration management, code management and code deployment; (iii) noting down any configuration changes made when troubleshooting; and (iv) conducting regular security review and testing.

Technology, Media & Telecommunications

Malware and phishing

Phishing email attacks are often used to trick employees into revealing their login credentials or other sensitive information, or downloading attachments containing malware.

The Handbook makes the following recommendations:

(a) **Conduct regular phishing simulation exercises** – This is to train employees to be alert to phishing attacks.
(b) **Educate employees** – Employees should be educated and regularly reminded to be alert to phishing and other forms of social engineering.
(c) **Consider restricting Internet access** – This is especially relevant where there is direct access from endpoints to large amounts of personal or sensitive data.
(d) **Install endpoint security solutions** – This serves as defence against malware, and should be kept updated. Organisations should keep proper records of the endpoint security solutions and versions installed on all their systems and their employees' computers.
(e) **Back up information** – Ensuring personal data in an organisation's possession is automatically and regularly backed up will provide an effective recovery plan against ransomware.

Security and responsibility

The security of an ICT system needs to be taken into consideration during the design and development phases, and thereafter as part of system maintenance as well. Many organisations use production data for system testing in their test environment. However, as test environments tend to be much less secured, there is a high risk of data breach.

The Handbook makes the following recommendations:

(a) **Synthetic data** – Create synthetic data for development and testing purposes in non-production environments instead of using real data.
(b) **Protect personal data through access control** – Without proper access control mechanisms, any webpage or document in a publicly accessible website can be indexed by search engines and appear in search results.
(c) **Establish clear responsibility for ICT security** – This includes system patching, security scans, and checking of log files for anomalies.

Accounts and passwords

Accounts and passwords need to be managed securely as they can enable unauthorised access to ICT systems if they fall into the wrong hands, particularly for administrative or privileged accounts. Some of

the common mistakes observed include having default or weak passwords, or keeping passwords in clear text in publicly accessible web folders.

The Handbook makes the following recommendations:

(a) **Review user accounts periodically** – Remove accounts that are no longer needed.
(b) **Ensure that passwords are not exposed in code or configuration files** – This should be stated clearly in ICT policies and made known to the employees or vendors.
(c) **Minimise risk of brute force attacks** – This may include locking the user account upon a pre-defined number of failed login attempts, implementing a delay after a failed login attempt, or using CAPTCHAs.
(d) **Implement a strong password policy** – This may include: (i) enforcing a password history policy to ensure that employees do not reuse their previous passwords; (ii) encouraging users to use passphrases, which may be long and complex, yet easy to remember; and (iii) discouraging users from using the same passwords across different systems.[1]
(e) **Stronger requirements for administrative accounts** – This may include a complex password or 2-Factor Authentication ("**2FA**") / Multi-Factor Authentication. This is important for administrative accounts to systems that hold large volumes of personal data, or personal data of a confidential or sensitive nature (e.g. financial or health records).

Concluding Words

As the Handbook contains examples of common errors in ICT system management and processes compiled from the PDPC's own experience of past cases, and practical guidance how they may be remedied, organisations would be well-minded to assess their own systems to determine whether there are any similar weaknesses. Organisations should also consider the recommendations in the Handbook to determine if they are relevant and whether efforts should be made to implement them within the organisation.

In this regard, the team from Rajah & Tann Cybersecurity can assist in the assessment of your data protection controls and processes, as well as any efforts at ensuring compliance with existing obligations and standards. The Rajah & Tann Cybersecurity team can advise on the following:

(a) Assessing whether the system configurations are indeed hardened;
(b) Conducting regular phishing simulation exercises;
(c) Educating employees on cybersecurity and data protection;
(d) Reviewing access control to ensure that it is properly and effectively maintained;

[1] See the case of *Re Chizzle Pte Ltd* [2020] SGPDPCR 1, where the organisation, Chizzle Pte Ltd, was found to have failed to make reasonable security arrangements to protect personal data in its possession. Notably, the PDPC highlighted that the password "Chi!zzle@2018", while meeting complexity rules, was in fact a weak password. Passwords thus should not contain the name of the organisation, and digits included in the password should not be easily guessable (such as dates).

(e) Reviewing clients' policies for clear responsibilities; and
(f) Assessing whether strong authentication (e.g. 2FA, strong password policies) is enforced.

The full Handbook is available here.

For further queries, please feel free to contact our team below.

Technology, Media & Telecommunications

Contacts

Rajah & Tann Singapore LLP

Rajesh Sreenivasan
Head, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

T +65 6232 0751

rajesh@rajahtann.com

Steve Tan
Deputy Head, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

T +65 6232 0786

steve.tan@rajahtann.com

Lionel Tan
Partner, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

T +65 6232 0752

lionel.tan@rajahtann.com

Benjamin Cheong
Partner, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

T +65 6232 0738

benjamin.cheong@rajahtann.com

Rajah & Tann Cybersecurity

Tanya Tang
Partner (Chief Economic and Policy Advisor), Competition & Antitrust and Trade;
Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

T +65 6232 0298

tanya.tang@rajahtann.com

Wong Onn Chee
Chief Executive Officer, Rajah & Tann Cybersecurity

T +65 6932 2606

onnchee@rtcybersec.com

Please feel free to also contact Knowledge and Risk Management at eOASIS@rajahtann.com

Our Regional Contacts

RAJAH & TANN | *Singapore*
Rajah & Tann Singapore LLP
T +65 6535 3600
sg.rajahtannasia.com

R&T SOK & HENG | *Cambodia*
R&T Sok & Heng Law Office
T +855 23 963 112 / 113
F +855 23 963 116
kh.rajahtannasia.com

RAJAH & TANN 立杰上海
SHANGHAI REPRESENTATIVE OFFICE | *China*
Rajah & Tann Singapore LLP
Shanghai Representative Office
T +86 21 6120 8818
F +86 21 6120 8820
cn.rajahtannasia.com

ASSEGAF HAMZAH & PARTNERS | *Indonesia*
Assegaf Hamzah & Partners

Jakarta Office
T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office
T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.co.id

RAJAH & TANN | *Lao PDR*
Rajah & Tann (Laos) Co., Ltd.
T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

CHRISTOPHER & LEE ONG | *Malaysia*
Christopher & Lee Ong
T +60 3 2273 1919
F +60 3 2273 8310
www.christopherleeong.com

RAJAH & TANN | *Myanmar*
Rajah & Tann Myanmar Company Limited
T +95 1 9345 343 / +95 1 9345 346
F +95 1 9345 348
mm.rajahtannasia.com

GATMAYTAN YAP PATACSIL GUTIERREZ & PROTACIO (C&G LAW) | *Philippines*
Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)
T +632 8894 0377 to 79 / +632 8894 4931 to 32
F +632 8552 1977 to 78
www.cagatlaw.com

RAJAH & TANN | *Thailand*
R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

RAJAH & TANN LCT LAWYERS | *Vietnam*
Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 28 3821 2382 / +84 28 3821 2673
F +84 28 3520 8206

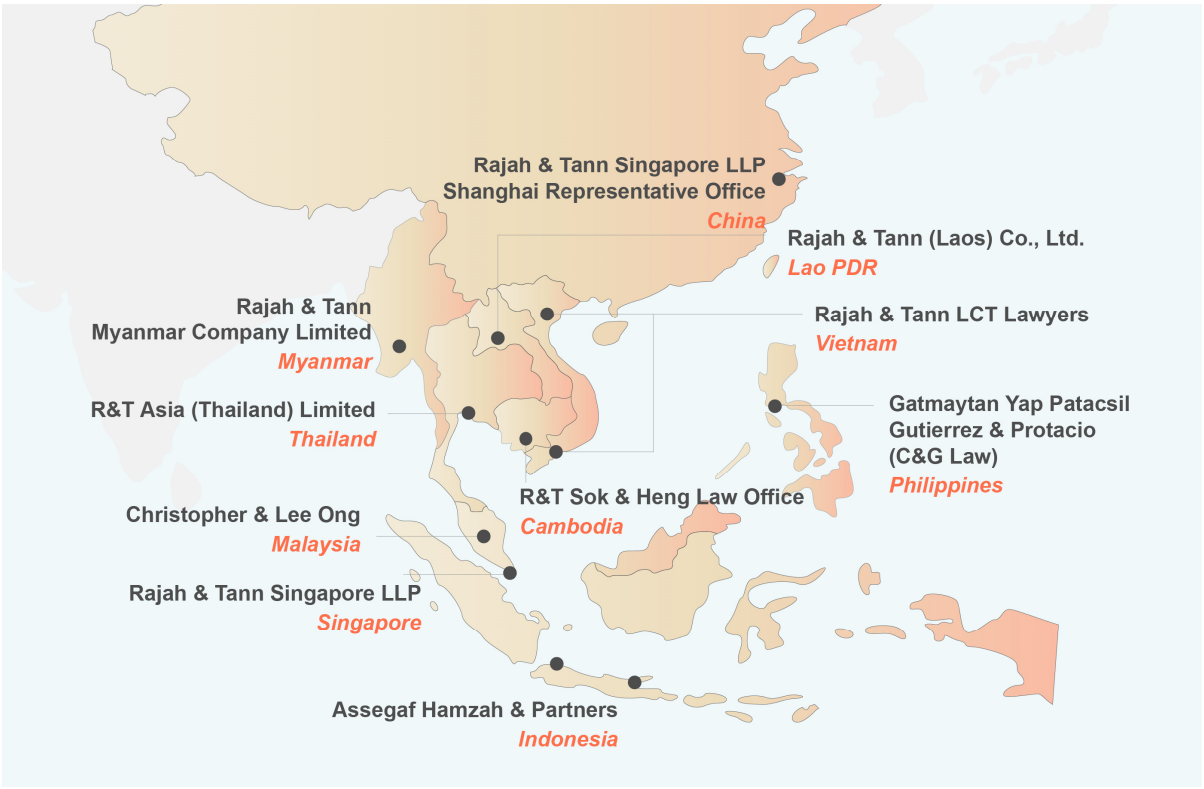
Hanoi Office
T +84 24 3267 6127
F +84 24 3267 6128
www.rajahtannlct.com

Rajah & Tann Asia is a network of legal practices based in Asia.

Member firms are independently constituted and regulated in accordance with relevant local legal requirements. Services provided by a member firm are governed by the terms of engagement between the member firm and the client.

This update is solely intended to provide general information and does not provide any advice or create any relationship, whether legally binding or otherwise. Rajah & Tann Asia and its member firms do not accept, and fully disclaim, responsibility for any loss or damage which may result from accessing or relying on this update.

Our Regional Presence



Rajah & Tann Singapore LLP is one of the largest full-service law firms in Singapore, providing high quality advice to an impressive list of clients. We place strong emphasis on promptness, accessibility and reliability in dealing with clients. At the same time, the firm strives towards a practical yet creative approach in dealing with business and commercial problems. As the Singapore member firm of the Lex Mundi Network, we are able to offer access to excellent legal expertise in more than 100 countries.

Rajah & Tann Singapore LLP is part of Rajah & Tann Asia, a network of local law firms in Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam. Our Asian network also includes regional desks focused on Brunei, Japan and South Asia.

The contents of this Update are owned by Rajah & Tann Singapore LLP and subject to copyright protection under the laws of Singapore and, through international treaties, other countries. No part of this Update may be reproduced, licensed, sold, published, transmitted, modified, adapted, publicly displayed, broadcast (including storage in any medium by electronic means whether or not transiently for any purpose save as permitted herein) without the prior written permission of Rajah & Tann Singapore LLP.

Please note also that whilst the information in this Update is correct to the best of our knowledge and belief at the time of writing, it is only intended to provide a general guide to the subject matter and should not be treated as a substitute for specific professional advice for any particular course of action as such information may not suit your specific business and operational requirements. It is to your advantage to seek legal advice for your specific situation. In this regard, you may call the lawyer you normally deal with in Rajah & Tann Singapore LLP or email Knowledge & Risk Management at eOASIS@rajahtann.com.