PwC Thailand's approach to data protection and information management

May 2022

pwc

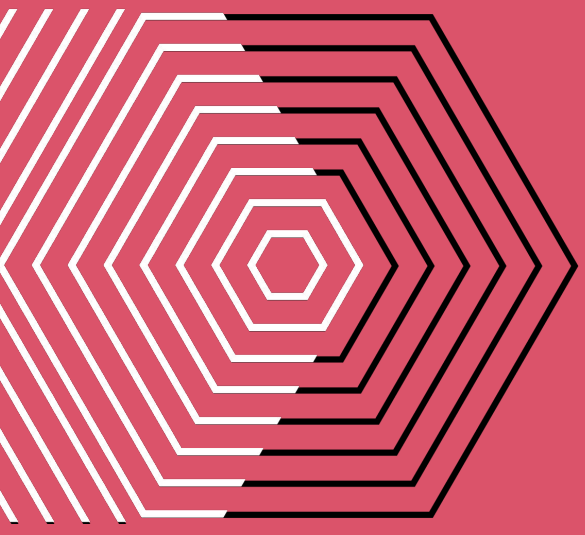
Table of contents

Document control

Version	Author	Date	Description
2022_v1.0	Pilumpa Katchawattana	January 2022	Initial draft

Document review

Version	Author	Date	Description
2022_v1.0	Svasvadi Anumanrajdhon	May 2022	Approved



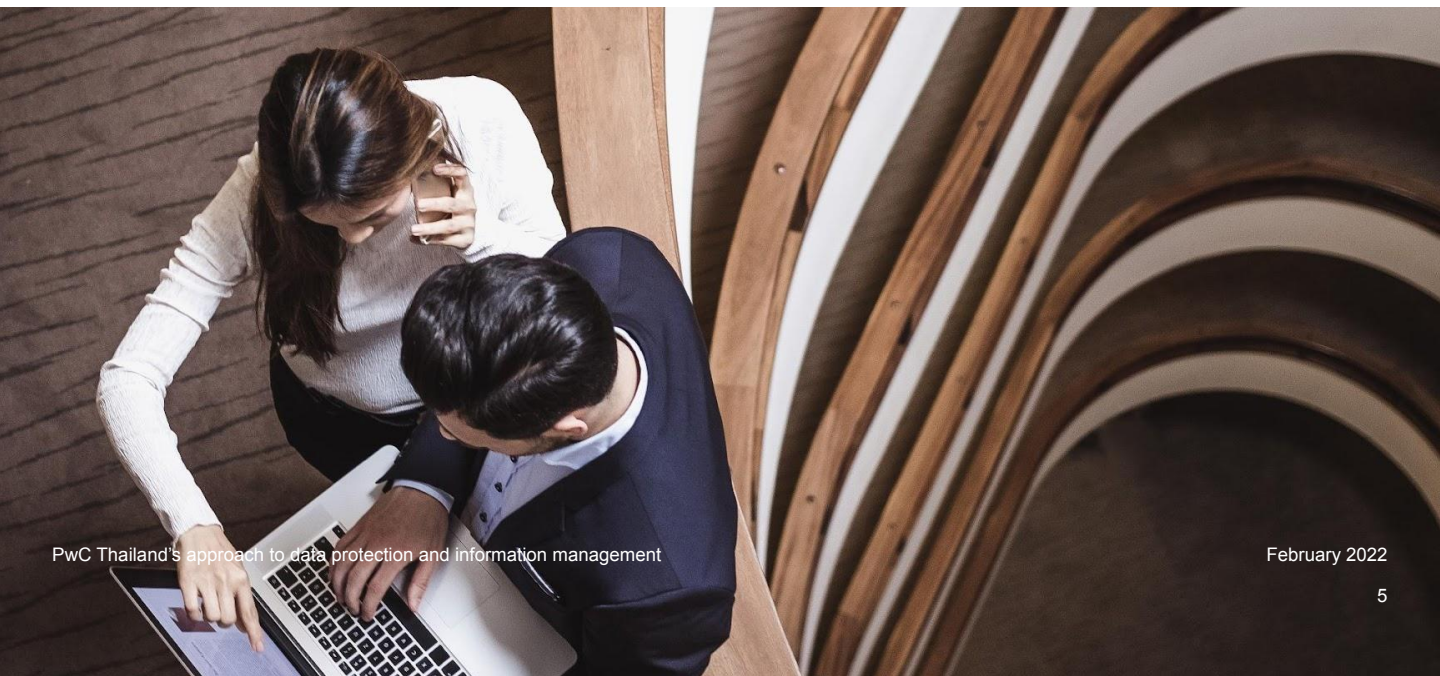
Introduction

Introduction

PwC Thailand takes management obligations very seriously. Protecting personal and client data is fundamental to the way we operate as a firm. The secure handling of data is an obligation that applies to all partners, staff and contractors of PwC Thailand.

PwC Thailand is part of a global network of PwC Member Firms who are committed to establishing robust data protection standards. The PwC global network's approach to data protection and information management is governed by the following principles:

- Accountability and credibility – we take responsibility for our obligations, are accountable to data subjects, clients and others, and abide by our contractual commitments regarding data protection.
- Trust and transparency – we only collect and use personal data in lawful ways that build trust amongst our people, our clients and others. We are clear and open with our people, clients, vendors and other stakeholders about how we handle, use and protect data.
- Fairness and respect – we use data in a fair and respectful manner. If the use of personal data may impact an individual directly, we assess the benefit against potential risks to preserve fairness and respect for the individuals concerned.
- Compliance – we implement systems and processes designed to achieve compliance with our legal obligations to protect personal data and to support and encourage the proper handling and use of all other data held by the PwC Thailand, including confidential information.



Introduction

- Consistency – we have a uniform and coordinated approach to data protection across the PwC Thailand.

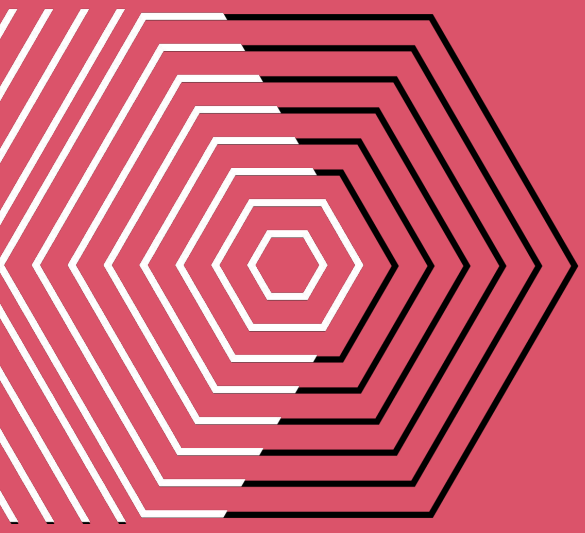
- Collaboration – we enable the secure transfer and sharing of data between member firms to serve our clients and support business objectives and operations, including the use of Network applications.

- Security – we invest in security so that confidential information is appropriately safeguarded. We leverage our Network Information Security (NIS) framework, services and technologies to protect data.

- Innovation and value – we enable the development of new business opportunities and client solutions recognise and support the use of data to realise business objectives and solve important problems, but to do so lawfully and responsibly.

- Minimisation – we collect and store only the data that is necessary for our purposes and we only hold data for as long as legally or operationally required. We ensure that any redundant data is destroyed in a timely manner according to our Data Retention Policy that we have in place.

Our Data Privacy Statement can be accessed via this link.



Frequently asked questions on data protection

Frequently asked questions on data protection

1. Has PwC Thailand appointed a Data Protection Officer (DPO)?

Yes, Khun Svasvadi Anumanrajdhon is the firm's DPO. Refer to DPO Charter for more information about the roles and responsibilities of the DPO.

2. Does PwC Thailand have a set of data protection policies?

We have a suite of internal policies covering topics such as Confidentiality, Privacy, Information Security, Data Classification & Handling and Clear Desk. These detailed internal policies are published within the firm but, with the exception of the firm's Data Privacy Statement, are confidential and cannot generally be shared with third parties.

3. How does PwC comply, and demonstrate its compliance, with its data protection obligations

PwC Thailand has complied with the requirements of Personal Data Protection Act, B.E. 2562 (2019) which is known as PDPA and the Network Data Protection Programme (NDPP). We have established a dedicated DPO office to help and support DPO on the implementation and oversight of relevant data protection policies and processes which cover the following key elements of data privacy:

1. Policy and governance
2. Notice and consent management
3. Data life cycle management (including record of data processing)
4. Data Subject Right (DSR) management
5. Privacy by design (including Data Processing Impact Assessment)
6. Information security
7. Privacy incident management
8. Third party management
9. Cross-border data transfer
10. Training and awareness

Frequently asked questions on data protection

4. What behaviours and culture do you promote in respect of data protection?

The correct handling of personal data processed by the firm is a responsibility for all partners, staff and contractors of PwC Thailand. In addition to privacy and data protection legislation, we have a professional obligation to our staff, clients and other third parties to keep information confidential and secure, to protect it from unauthorised access and to comply with relevant regulations and policies.

The awareness of the importance of personal data protection has been cascaded to our staff via our timely communication informing them of their roles and responsibilities to uphold these standards and policies. This helps ensure that our staff has the commitment to safeguard personal data while providing high quality services to clients.

5. Does your firm monitor or otherwise audit your adherence to your data protection policies?

The firm's data protection and information management policies and standards are supported by ongoing compliance checks and monitoring. These activities are carried out by PwC's Internal Audit and as part of the Information Protection Network Standard process.

6. Is PwC Thailand a data controller or a data processor?

When acting as an independent, professional advisor, the nature of the service will mean that PwC is acting as controller. An example of this is when we are carrying out audits where we have our own professional obligations.

In certain other circumstances, as necessitated by the nature of our work, PwC Thailand can and will act as a data processor where it is performing activities on behalf of our clients. Where PwC acts as a processor, we will only process personal data in accordance with the client's written instructions and comply with the obligations placed on us by law as a processor.

Frequently asked questions on data protection

7. What organisational and technical security measures does PwC Thailand have in place to protect personal data?

Security

Information security is a high priority for PwC. PwC member firms are accountable to their people, clients, suppliers and other stakeholders to protect information that is entrusted to them. It is our policy that our information assets and personal data of our employees and clients are protected from internal and external threats, whether deliberate or accidental, and that confidentiality, integrity and availability of information is maintained.

PwC's Network Information Security (NIS) team is responsible for designing, implementing and maintaining information security capabilities and services for the PwC global network of Member Firms. NIS leads PwC's Network Security Cyber Readiness Programme, which is a multi-year programme to enhance existing capabilities and build new capabilities to combat the ever more complex cyber threats.

The PwC Information Security Policy (ISP) has been developed to safeguard the confidentiality, integrity, and availability of the information and technology assets used by the PwC member firms and is aligned with ISO/IEC 27002:2013 Information Technology - Security techniques Code of Practice for Information Security Management industry standard. The Network Information Security organisation will coordinate an annual review of the PwC ISP Framework and publish amendments in accordance with the defined PwC ISP governance procedure. The PwC ISP directly supports the firm's strategic cyber-readiness to proactively safeguard its assets and client information.

PwC Thailand must comply with the PwC ISP, controls and supporting standards that are designed to establish the controls necessary to protect information assets. An annual review of alignment and these processes is conducted as part of the governance procedure.

Additionally, adequate controls have been implemented to properly detect and defend the firm against malicious software designed to disrupt computer operations. To keep up with the changing threats, encryption methods and up-to-date malware protection software are implemented to protect data on servers, workstations, laptops, mobile and removable devices.

Penetration and Vulnerability Testing

Continuous vulnerability scans are performed by our NIS team on a daily basis which covers both external and internal equipment. NIS and TH IT reviews vulnerabilities, patches and fixes in order to determine risk and the relative priority for patch deployment in accordance with the PwC security policy.

Frequently asked questions on data protection

8. Do your applications adhere to data protection by design and default requirements?

The PwC network and each of the individual PwC firms are strongly committed to protecting the privacy of personal data that they maintain about PwC clients, employees and other individuals. As part of this commitment to privacy, PwC regularly reviews its data protection practices to comply with applicable laws, industry standards and best practices. All member firms are required to have an extensive data protection programme which places accountability and transparency in how PwC collects, processes, protects and disposes of personal data. As part of ongoing efforts to maintain this programme, use of new or development of existing technologies are subject to extensive tech reviews by relevant subject matter experts including data privacy. Internal reviews ensure that all technologies are able to demonstrate adherence to data protection by design and default requirements.

9. Do you have an incident response procedure?

PwC recognises that security incidents are disruptive and may cause damage to individuals, clients or the business function. We must be prepared to combat these threats and quickly respond to prevent impacts that may result in financial, legal or reputational implications. In order to be properly prepared, an incident management programme has been implemented to identify, classify, escalate, respond and resolve security incidents in a timely manner and reduce impact to the individuals and the business.

Detection or suspicion of a security incident is critical for early identification and containment of the impacts. PwC personnel has been familiar with the process and points of contact to report and escalate any suspected violation or perceived security incident.

10. Do you encrypt electronic devices used to process personal data?

PwC Thailand's email system is set to run with Opportunistic Transport Layer Security (TLS) (encryption up to 256-bit AES). Emails will automatically benefit from encryption where the recipient party also runs Opportunistic TLS. PwC Thailand also has the capability to set up forced TLS between PwC and third parties to guarantee encryption.

All PwC Thailand laptops are protected using hard drive encryption software using a minimum 128-bit AES encryption algorithm. This software enforced password controls and uses a dynamic password time-out to prevent password attacks. The software is bound to the hard drive, protecting the underlying data and not just host systems. All PwC Thailand laptops are equipped with software that restricts the use of removable media (e.g. USB flash drives).

11. What backup and business continuity procedures do you have in place to mitigate against data losses?

Data back-up

All Personal Computers are backup on a weekly basis.

The Backup of data on all systems on the central server (except for the Client PC's data backup system) will be performed on a daily basis.

All backup sets will be replicated to the DR site to ensure that they will have backup sets in case of disaster at the Data Centre.

- The copy of Personal Computer's daily data backups are kept for seven (7) days.
- The daily data backups will be overwritten after seven (7) days.
- The weekly data backups will be overwritten after four (4) weeks.
- The monthly data backups will be overwritten after three (3) months.
- The year end backup data sets (annual backup) are kept for no less than ten (10) years, after which the backup data set will be erased.

Business Continuity Management

PwC Thailand has a Business Continuity strategy and plan in place. Our business continuity strategy ensures that critical business services and processes are supported by resilient solutions, and that the firm is able to manage major incidents and crises. Business continuity planning is done throughout the firm as a formal work programme to ensure systems supporting critical business services and processes can be recovered within a defined and acceptable timeframe and sensitive and critical information are protected.

To ensure that critical services and processes that rely on technology applications and infrastructure are available when needed, we specified the key applications requiring Disaster Recovery (DR) solutions and pre-arranged a DR site.

Business continuity strategy
Our business continuity strategy ensures that critical business services and processes are supported by resilient solutions, and that the firm is able to manage major incidents and crises. Business continuity planning is done throughout the firm as a formal work programme to ensure systems supporting critical business services and processes can be recovered within a defined and acceptable timeframe and sensitive and critical information are protected.

Disaster recovery and technology resilience
To ensure that critical services and processes that rely on technology applications and infrastructure are available when needed, we specified the key applications requiring Disaster Recovery (DR) solutions and pre-arranged a DR site.

Incident management
We have planned process outlines and the responsible person to identify, investigate, contain, and recover from any potential threats to data security and the integrity of the PwC brand.

Business continuity planning
Our BCP provides guidance to restore critical services in the event of a disaster. Our BCP is reviewed and updated annually or when there are significant changes to key factors i.e. organisation, threats and risks.

Business continuity activities
Our BCP includes a recovery plan matrix which enables critical business services and processes to resume to an acceptable level within an agreed timeframe following a disruption.

Business continuity plan testing
Our annual testing covers BCP, DR and call tree. The outcomes of BCP testing are reported to and approved by the firm's leadership.

Frequently asked questions on data protection

12. What processes do you have in place to ensure suppliers, subcontractors or other third parties comply with the law?

Prior to appointing any external service in progress includes a review of their ability to provide the proposed service, financial stability and information security arrangements.

Non disclosure agreement will be necessary if the 3rd party will have access to the firm's confidential information or PwC's environment.

As is common with most professional service providers, we use a number of third party processors to provide certain business critical elements of our IT systems and the support for them. Information about the third party processors we use is available in our privacy statement.

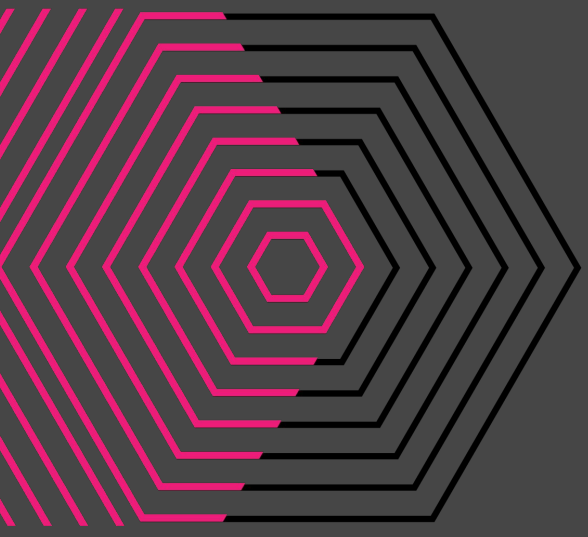
As part of third party risk assessment, we continuously review our contractual provisions with key suppliers and third parties to make sure that they adequately cover the standards required under PDPA. In addition, Data Protection Schedule (DPS) including Personal Data Security Controls are required to be completed and signed.

13. Do you transfer any personal data outside of Thailand?

The PwC global network has an agreement between all Member Firms to facilitate secure information transfers between Member Firms and to protect personal data that is transferred out of Thailand. The agreement also imposes obligations in connection with transfers of client confidential information between firms, regardless of where they are located. The agreement binds all PwC Network firms to confidentiality obligations whenever they hold information that is confidential to another party whether inside or outside the network.

Some of the suppliers we use in order to operate certain business elements of our IT systems are located outside Thailand.

For more information regarding the PwC Thailand, its organisation and legal structure, and the relationship between member firms please refer to PwC Thailand's Assurance Transparency Report located on our website.



Frequently asked questions on information management

Frequently asked questions on information management

1. Does PwC Thailand have policies in place regarding information management and security?

Yes, PwC Thailand has in place relevant information protection policies that sets out the requirements for managing information and security of the firm and an associated retention schedule that sets out retention periods for maintaining work papers that support professional services provided to our clients. We're in the process of streamlining our retention policy to cover internal firm documents. These policies are governed by PwC Thailand's Technology, Security and Information Protection Governance in conjunction with the Office of General Counsel and Risk and Quality organisations.

2. What information is covered by the PwC Thailand Information Management policy?

The PwC Thailand Information Management policy sets out the requirements for managing all information that is handled by PwC Thailand. Information processed by the firm but subject to the control of clients, individuals or other third parties is managed in accordance with the relevant third party's instructions.

3. What information is covered by PwC Thailand's Retention Schedule?

The firm's Retention Schedule applies across both hard copy and electronic records which are controlled by PwC Thailand and which are retained for evidentiary and administrative purposes. Relevant law and regulation as well as business and operational needs are considered in identifying the retention periods for records.

4. What information will PwC Thailand hold?

Due to the nature of the services the firm provides to clients, in most cases PwC Thailand will be acting as an independent professional adviser. As such, PwC Thailand will determine what information is collected during the provision of the services, how it is managed and for how long it is retained. Information retained will include work papers and other evidence of work performed in order for the firm to be able to demonstrate compliance with its professional standards and obligations under the terms of engagement with our clients.

Where PwC Thailand is processing information under the direct instruction of a third party, the decisions regarding what information the firm processes, how it is managed and for how long it is retained, will be made by that third party and not PwC Thailand.

Frequently asked questions on information management

5. How does PwC Thailand store electronic and hard copy records?

PwC Thailand stores its electronic records in dedicated systems of record. Each system of record has the necessary functionality to ensure records are properly structured, secured, managed and deleted when they reach the end of their respective retention period. After the work has been delivered, hard copy records are predominantly held off site at a third party secure storage facility that is also subject to robust processes and controls to ensure their alignment to the firm's retention requirements.

6. How long does PwC Thailand retain information for?

Records created, sent or received by the firm that are necessary or appropriate to record, support or otherwise form the basis of the firm's professional work product or administrative functions, are retained for the retention period specified in the firm's Retention Schedule (which is in line with local law and regulation, legislative and business requirements). PwC Thailand's default retention period for engagement records or work papers is 10 years from the date of report. Information which does not constitute a work paper should be destroyed at the end of its active business use.

7. Can I request that my data be removed as soon as our engagement ceases?

Where PwC Thailand is acting as an independent professional adviser, as is the case in most engagements, PwC Thailand is required to retain its work papers and evidence of work performed in order to be able to demonstrate compliance with professional standards and obligations. As such, PwC Thailand reserves the right to retain such information for the periods specified in its Retention Schedule.

In instances where PwC Thailand is processing data under the direct instruction of a client, we will on request, return or delete data in a timely manner. PwC Thailand. however, still reserves the right to retain any internally created working papers that evidence work performed for risk management purposes.

Frequently asked questions on information management

8. How will data be destroyed?

At the end of its life, all electronic storage media (hard drives, back-up tapes etc) are subject to audited, secure destruction, either using physical measures (such as drilling or crushing), or logical means using multiple random overwrites. All items marked for destruction are securely transported, tracked and certificated.
Secure locked confidential waste bins are available on every floor of our offices for hard copy documents. Contents of such bins are destroyed securely by a third party specialist waste manager.

9. Are there any exceptions that would prevent information from being destroyed?

Records that are the subject of a pending, threatened or reasonably anticipated lawsuit, government investigation or subpoena are retained and preserved unaltered until such time as the PwC Thailand Office of General Counsel instructs otherwise.

10. What behaviours and culture do you promote in respect of information management at PwC Thailand?

Whilst only appointed custodians can perform deletion of records from the firm's systems of record, all partners, staff and contractors have a responsibility to manage information in accordance with the firm's policies.

PwC Thailand personnel are required as part of their induction or onboarding programme (and annually thereafter) to complete an electronic awareness training package that informs them of the appropriate behaviours for protecting information. This training sets out their personal responsibilities and tests their understanding of these matters. Regular communications are also sent out in the form of emails or alerts from DPO Office to all partners and staff to build up their awareness and understanding.