



Data protection and privacy services

Going beyond compliance with the Personal Data Protection Act (PDPA) to navigate the data protection challenges ahead.



EY

Building a better
working world

When data and privacy is protected,
it creates growth, prosperity and
peace of mind for millions of people.

At EY, we train and nurture our data protection and privacy professionals from different backgrounds and walks of life to apply their skills and insights to ask better questions. It's these better questions that lead to better answers, benefiting our clients, their clients and the wider community.

EY teams aim to protect the digital economy, and in doing so, to help build a better working world.

www.ey.com/en_sg/advisory/data-protection-privacy



Introduction: a new data privacy era

Organizations around the world face a paradigm shift in privacy and data protection regulation. Stringent regulatory demands and rising customer expectations put sustained compliance firmly in the spotlight.

Regulators in many countries recognize the seriousness of data risks today, and are introducing and enforcing new data privacy and protection requirements. Since the European Union's (EU) new General Data Protection Regulation (GDPR) came into effect on 25 May 2018, it ushered in a welcomed harmonization of fragmented data protection laws across EU Member States and unprecedented levels of data protection for EU residents, backed by fines of up to €20 million or 4% of global revenue, whichever is higher.

In Southeast Asia, there is also a clear emphasis on data protection. Countries like Singapore, Malaysia, Philippines, Thailand, Indonesia and Myanmar have established laws on privacy and data protection, while Vietnam and Cambodia have laws that broadly cover some elements of data protection.

In Singapore, the country's Personal Data Protection Commission (PDPC) issued a public consultation in May 2019 proposing data portability and data innovation provisions. Singapore organizations are also moving with times by having discontinued the widespread practice of collecting, using or disclosing consumers' NRIC information since 1 September 2019.

The acceleration of global privacy regulation

The map highlights where key, new or redefined privacy regulations have been introduced across the globe and in addition to GDPR.



Personal data protection and privacy regulations across ASEAN countries:

■ Singapore

The Personal Data Protection Act 2012 (PDPA)

■ Indonesia

Electronic Information and Transactions (EIT Law)

■ Malaysia

The Personal Data Protection Act 2010 (PDPA)

■ Laos

Laos Electronic Data Protection Law (EDPL)

■ Philippines

Data Privacy Act of 2012 (the Act) or Republic Act No. 10173

■ Thailand

Personal Data Protection Act (PDPA) B.E. 2562

■ Vietnam

Decree on Personal Data Protection

■ Myanmar

Protecting the Privacy and Security of Citizens (Union Parliament Law 5/2017)

There are no laws or regulations that are specifically related to data protection in Brunei and Cambodia.



1

Changing gear for the new normal

Organizations are responding to the changes in the global regulatory landscape by shifting focus. Before GDPR came into force and the recent updates to PDPA, most were focused on assessing data privacy maturity, and implementing new policies and procedures. Now, attention has turned to operationalizing privacy processes and the challenges of sustained compliance.

New risks demand a new approach

Data protection laws in Singapore, the region and beyond bring wide-ranging impact and the stringent rules require a fundamental organizational shift, even for businesses that are compliant with existing legislations.

When the steep financial penalties for non-compliance and data losses are added to the cost of reputational damage, sanctions, remediation and the potential impact on digital transformation, the risk of inaction is clear.

Privacy regulations present organizations with new and ongoing challenges relating to the privacy and compliance journey. These impact the entire organization and requires ongoing management of the privacy risk faced by organizations.

1 Compliance complexities

Regulations like PDPA come with penalties for failing to comply with the requirements.

Navigating the complex patchwork of regulatory requirements is hardly straightforward. It starts with organizations building up their data protection competency.

The PDPC has rolled out a data protection competency roadmap that encompasses data protection management, risk management, breach management, stakeholder management, data protection audit and assurance, and data governance.

2 Reputational risk

Organizational reputation is increasingly linked to the organizations' ability to protect their customers' privacy. Privacy breaches can cause reputational damage to organizations.

Companies are starting to recognize that investing in the risk and compliance agenda, while accelerating technological transformation, builds stakeholder confidence and is a business imperative.

Building resilience and strengthening the ability to bounce back from incidents will require organizations to nurture a culture of proactive data compliance.

3 Organizational challenges

To comply with privacy regulations, organizations need to be accountable. While adherence to minimum compliance requirements may reduce the risk of facing fines or loss of trust, there are significant risks in having such a reactive compliance attitude.

Organizations must step up and develop a common framework for privacy terminology, technology and performance metrics to enable cross-functional collaboration and a risk-informed leadership. As organizations innovate and transform, they need to build privacy risk considerations into their processes and systems.

Organizational-wide transformation across technology, people and processes

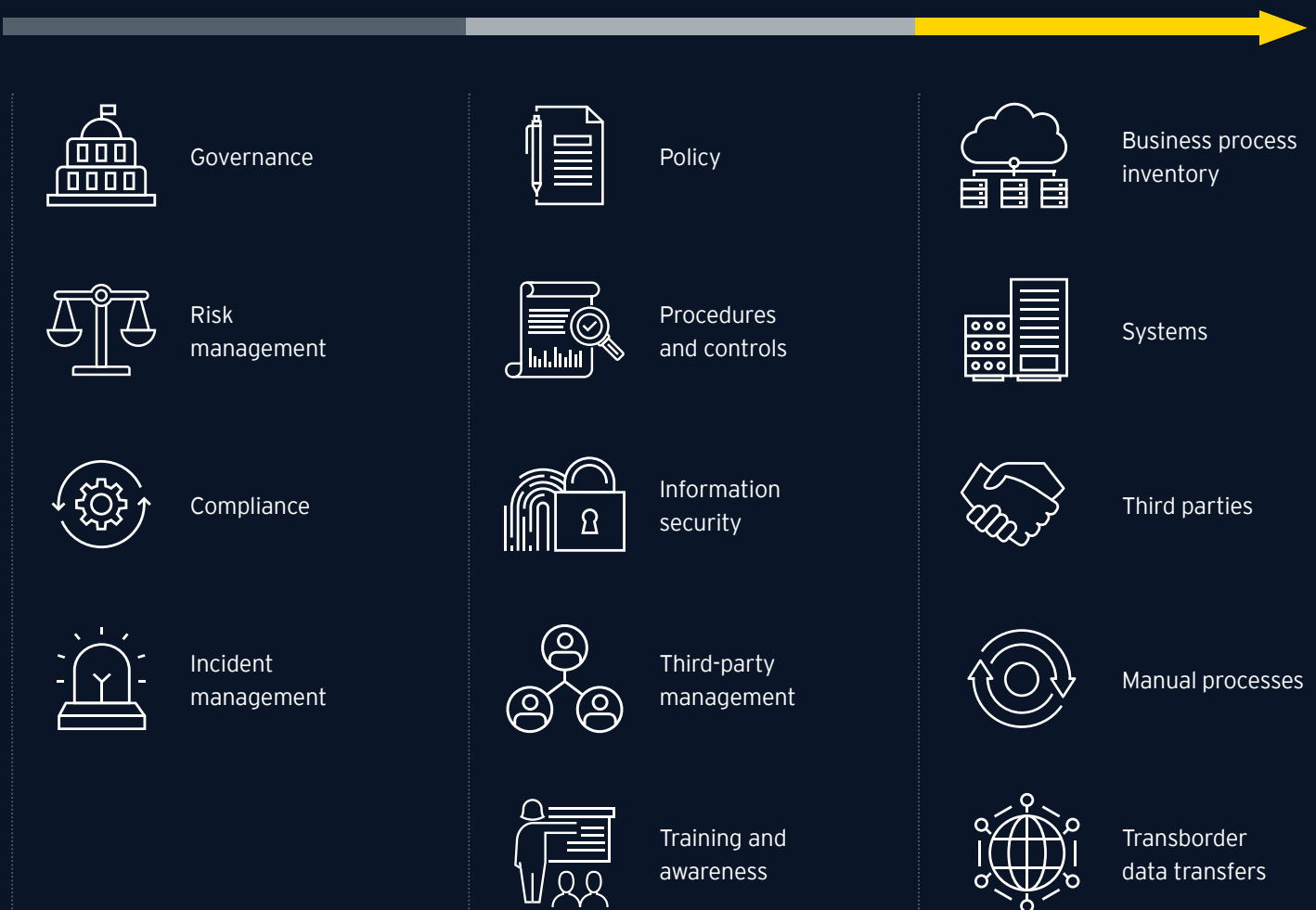
The illustration below provides the different elements to support compliance with data privacy and protection requirements. EY professionals use this framework as guidance to perform current state assessment, combining the overview of effective technology, people and processes, to provide sustained value.

Are you ready for PDPA and other data protection regulations? Ask yourself these questions:

How are you managing it?

How are you controlling it?

What are you doing with the data?





Helping you navigate data protection challenges

Apart from the urgency of working towards compliance, there is also the opportunity to take a strategic approach to data protection. EY risk-based and multidisciplinary approach targets investment where it matters most for regulatory compliance and competitive advantage.

EY data protection services

1

Micro-learning and quick digital guides

Design data protection awareness content provided to employees in small, very specific bursts. Powerful digital guide that provides tailored messaging and direction to learners as the organization progresses in its data protection maturity.

2

Crisis simulation

Organize simulations for the C-suite to practice making decisions in a simulated crisis involving data breach or leakage. These simulations are powerful in delivering successful and high impact trainings through these interactive and active learning experiences.

3

Maturity review

Benchmark of the organization's maturity against the EY data protection framework and market-leading standards as they continue their journey beyond compliance.

4

Seamless integration

Provide EY privacy program support as a managed service offering for organizations looking to outsource the function of Data Protection Officer (DPO), and receive ongoing support and guidance on data protection and processing operations such as maintaining data inventories and performing privacy impact assessments.

5

Internal audit and compliance with assessment

Conduct a detailed assessment and audit of the organization's compliance with the data protection regulation to identify and assess the controls that have been established to mitigate the risk of a data loss.

6

Breach management support

Support maturity of client's crisis management, incident management and cyber breach response through gap assessment on breach readiness, design and implementation, assess severity and breach impact, and validation of breach process.

7

Privacy transformation

Develop data protection framework, policies and procedures.

Drawing on our extensive privacy knowledge, proven tools and methodologies, EY teams help to identify clients' highest risks, and design and execute a tailored roadmap for compliance and beyond.

The pulse on data protection

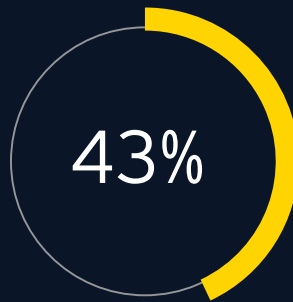
The charts below showcases Southeast Asia (SEA) findings from *EY Global Information Security Survey 2020*.

Rising cyber and privacy threat



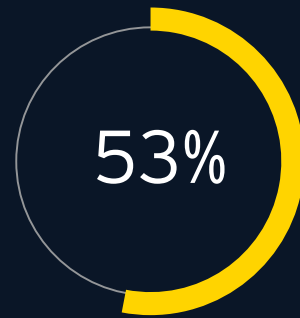
of SEA organizations experienced a significant or material breach in the last 12 months.

Risk planning still an afterthought



of SEA organizations say cybersecurity is involved right from the planning stage of a new business initiative.

Investment limited to business-as-usual

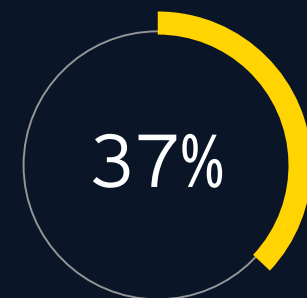


of SEA organizations spend less than 15% of their organization's cybersecurity budget on new initiatives.

Lack of confidence in current measures



of SEA organizations say that they cannot quantify the effectiveness of their cybersecurity spending to their boards.



of SEA organizations say that the relationship between cybersecurity and the lines of business is at best neutral, to mistrustful or non-existent.

Helping you to comply with PDPA requirements

Organizations that want to demonstrate their compliance with PDPA first need to ensure that they meet its requirements. In practice, many organizations are finding this a challenging goal and some have a significant distance to go. There are a range of services for organizations at varying stages of their data protection maturity journey to consider.

Solution	How do we do it?	What do you get?	Timescales
PDPA speed assessment	Talk through your current compliance with the PDPA, and identify overall significant gaps and remediation required.	Dashboard showing your organization's readiness to comply with each of the key PDPA requirements.	One day
PDPA "360 degree" assessment	Develop detailed questionnaires and workshops to do a deep dive of your PDPA compliance position.	<ul style="list-style-type: none"> ▶ Risk assessment and maturity evaluation report based on industry framework and PDPA ▶ Recommendations and roadmap for remediation ▶ Identification of product and process specific risks 	Two to four weeks depending on the size and complexity of the organization
Data Protection Impact Assessment (DPIA)	Design a tailored DPIA template, which will be used to interview systems and projects owners, and review of design and documentation to assess the risk of harm to individuals through the misuse of their personal information.	Assessment of your systems or projects identifying key data protection risks.	One to two weeks depending on the size and complexity of the project and systems
"Know your personal data" data inventory	Scan an agreed data sample from your network and interrogate the content of documents to understand which personal data you have in your organization and where it is.	<ul style="list-style-type: none"> ▶ Inventory map of your organization's personal information ▶ Process or system specific personal information flow diagrams and documentation 	2 to 12 weeks depending on the size and complexity of the organization
Data protection improvement program	Design and execution of data protection improvement programs, including the development and implementation of: <ul style="list-style-type: none"> ▶ Data protection framework ▶ Privacy governance and organizations designs ▶ Policy and procedures ▶ Training and awareness ▶ Incident management ▶ Third-party management ▶ Risk management ▶ Procedure and controls ▶ Information security controls ▶ Binding corporate rules program compliance ▶ Ongoing compliance and monitoring 	<ul style="list-style-type: none"> ▶ Up-to-date data protection framework based on leading practices that are in compliance with PDPA ▶ Improve the maturity of your data protection management across your people, processes and policies ▶ Prepare you for the journey towards Data Protection Trustmark (DPTM) 	3 to 24 months depending on the size and complexity of the organization

Why EY?

1

Extensive privacy knowledge and experience

EY member firms employ over 200 Certified Information Privacy Professionals (CIPPs) and privacy lawyers to help organizations to better understand data privacy risk and regulatory compliance. Close cooperation with EY technology professionals means EY teams can translate client requirements into a customized approach.

2

Highly experienced

For over a decade, EY teams have assisted multinational organizations in understanding privacy and data protection and regulations such as GDPR and PDPA. Using their deep industry and client knowledge, EY teams have helped clients across all sectors achieve both compliance and competitive advantage through effective GDPR programs, from gap analysis through to ongoing managed services.



3

Global framework

EY teams use a risk-based, multidisciplinary approach supported by robust tools and methodologies to help you to understand the impact of privacy on your organization, achieve timely and consistent privacy compliance and leverage privacy for wider strategic benefit.

4

Professional approach

EY teams work within common global structures, where they can easily draw on EY industry and functional professionals from the legislation, regulation and business practice across the globe to provide insights. EY teams have implemented successful rollouts across multiple countries.



Contacts

To find out how EY data protection and privacy service offerings can support your organization through your privacy compliance journey, please get in touch.



John Ho Chi

Partner, Advisory Services,
Ernst & Young Advisory Pte. Ltd.
+65 6309 6956
john.ho-chi@sg.ey.com
linkedin.com/in/johnhochi



Steve Lam

Partner, Advisory Services,
Ernst & Young Advisory Pte. Ltd.
+65 6309 8062
steve-yk.lam@sg.ey.com
linkedin.com/in/stevelyk



Ch'ng Choon Huat

Director, Advisory Services,
Ernst & Young Advisory Pte. Ltd.
+65 6309 8062
choon-huat.chng@sg.ey.com
linkedin.com/in/choon-huat-chng



Building a better
working world

In this data-driven
world, is trust the
hardest thing
to build?

ey.com #BetterQuestions



The better the question. The better the answer.
The better the world works.

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation is available via ey.com/privacy. For more information about our organization, please visit ey.com.

© 2020 Ernst & Young Advisory Pte. Ltd.
All Rights Reserved.

APAC no. 12002166
ED None.

UEN 198905395E

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com