Are you ready for the PDPA?

Fujitsu Security

FUJITSU

shaping tomorrow with you

Data is the heart of the fourth industrial revolution

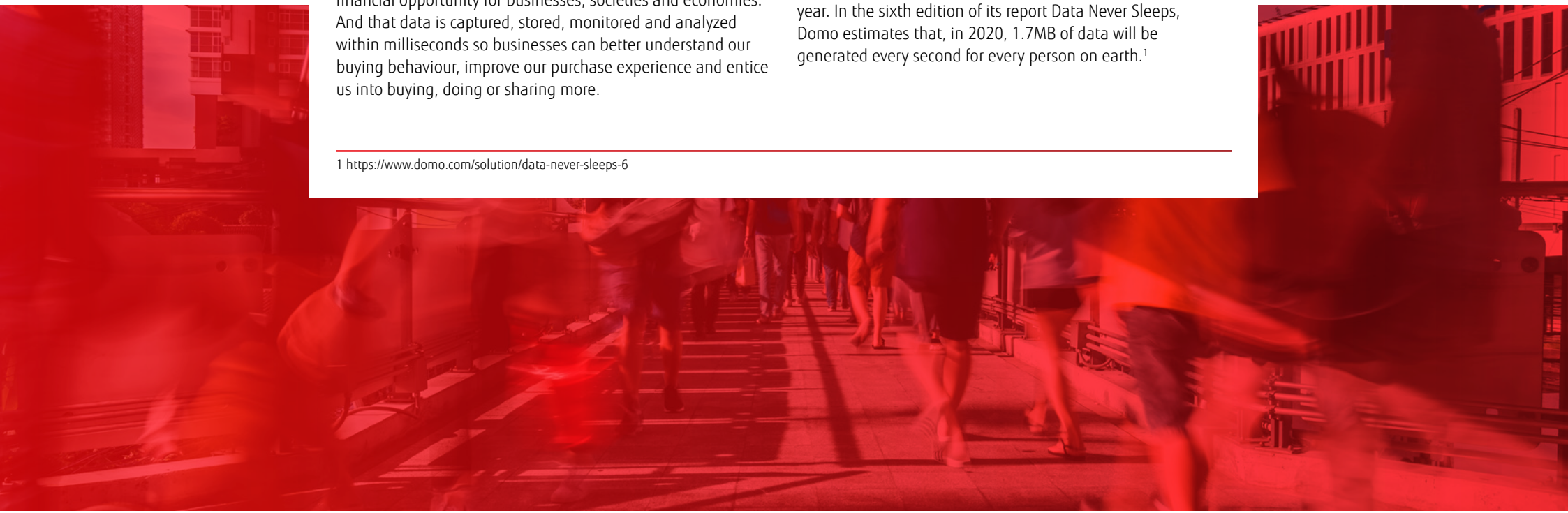
Data is the defining hallmark of the fourth industrial revolution, commonly referred to as Industry 4.0. Every second of every day, people all over the world share personal data about where they are, what they do, who they know and what they buy.

Individuals share that personal information to use a rich variety of data-driven conveniences. Real-time navigation, instant communication and purchasing items via mobile devices are just a few examples.

The data that swirls around the world as people exchange their information for access to services represents a lucrative financial opportunity for businesses, societies and economies. And that data is captured, stored, monitored and analyzed within milliseconds so businesses can better understand our buying behaviour, improve our purchase experience and entice us into buying, doing or sharing more.

As we embrace data-driven services to improve how we live and work, the appetite for even more services grows. This has given rise to a long list of new technologies and industries to meet our personal and commercial needs. Examples include Internet of Things (IoT) sensor data, blockchain, artificial intelligence and its subset, machine learning, robotics, 3D printing, and biotechnology. These new industries and technologies need vast amounts of data to fuel their application, performance and relevance to our lives.

The global growth of data is increasing exponentially every year. In the sixth edition of its report Data Never Sleeps, Domo estimates that, in 2020, 1.7MB of data will be generated every second for every person on earth.[1]



1 https://www.domo.com/solution/data-never-sleeps-6

Why privacy and personal data protection matters

Access to data-driven conveniences has revolutionized how we live and work, yet that access comes with a cost: the cost of sharing our Personal Information (PI) with a business. PI is any information that can be used to directly, or indirectly, identify, contact or locate a single, specific person.

Most people willingly share their PI to access the conveniences of the digital era. We share our name and address information so purchased items can be delivered to our homes. We share credit card and bank account details to transact online. And we share our email address to support ongoing communications with vendors.

Yet global headlines around data breaches, cybercrime and progressively more advanced security threats are making governments, businesses and individuals nervous about how PI is secured by organizations.

When data falls into the wrong hands through loss or theft, there are serious implications for intellectual property, profitability, reputation and security.

The protection, security and privacy of PI is critical to the success of the data-driven economy.

The protection, security and privacy of PI is critical to the success of the data-driven economy.

This is why countries all over the world are moving fast to introduce legislation to protect their citizens' PI. Europe, Australia, Canada, Greece, Japan, Korea, China, Brazil, Chile and South Africa all have laws in place to protect citizen PI. The United States has no single principle data protection act but certain states, including California and Texas, are drafting their own.

In 2019, Thailand demonstrated it is a country that understands both the value of data and the importance of data management and security, by passing into law two Acts specifically designed to protect data in the digital and physical domains:

1. The Personal Data Protection Act (PDPA).
2. The Cyber Security Act (CSA).

What are the Personal Data Protection Act (PDPA) and Cyber Security Act (CSA)?

The first Thailand Personal Data Protection Act (PDPA) came into effect in 2019. Businesses (as data controllers) have one year to comply with the new Act.

The PDPA aims to safeguard a data owner from the unauthorized or unlawful collection, use, or disclosure and processing of their PI.

Under the Act, Thai data owners have the right to data portability and the rights to request access to their PI and to delete, destroy, correct, restrict processing of or anonymize their PI.

The PDPA requires companies, regardless of location, who work with people in Thailand to:

- have a legal basis to collect and use personal information (sometimes requiring consent)
- respect heightened requirements for sensitive personal data
- implement appropriate security measures
- advise of data breaches. A data controller must notify the office of the Personal Data Protection Commissions of any data breach within 72 hours, unless the breach has no risk of affecting personal rights and liberties. The controller must also notify the data owner(s) of any data breach that has a high risk of affecting personal rights and liberties and provide them with remedial measures[1]
- facilitate the rights of people regarding access to their personal data.

The PDPA includes civil and criminal penalties for non-compliance. Civil penalties include administrative fines up to 5M THB and punitive damages up to twice the amount of actual damages. Criminal penalties include imprisonment of at least 6 months and fines up to 1M THB. Civil damages under the PDPA can multiply as Thailand allows data subjects to bring a class action lawsuit. The director of a company could also be subject to penalties under the PDPA.

In parallel to the PDPA, the new Cybersecurity Act (CSA) allows the Thai government to track, monitor and access digital data if it deems 'cyberthreats' are damaging to the critical digital infrastructure of the Kingdom. Private organizations that use, or provide, computer systems for work across national security, financial services and services targeted towards the public must:

- give the names and contact details of key stakeholders who own, use, or have computer systems
- conform to code of conduct and cybersecurity standards as prescribed by law
- conduct thorough risk assessments
- notify stakeholders of instances of cyberthreats.

As the first legislation of this kind in Thailand, the PDPA and CSA will fundamentally change the way data is managed, monitored and secured across the country.

1 https://www.multilaw.com/Multilaw/Multilaw_News/Jurisdiction_News/Tilleke_Gibbins_Thailands_Personal_Data_Protection_Act.aspx

Are you ready for the PDPA? : Three recommendations for PDPA compliance

The new legislation is highly detailed and requires new processes, policies and, in some cases, technology adoption by businesses. Complying with the PDPA may seem overwhelming yet the penalties for non-compliance are significant. Fujitsu recommends three actions to help ensure smooth PDPA compliance by the May 28, 2020 deadline:

1. Understand the PDPA requirements and deadline

With the compliance deadline coming soon in May 2020, make time to become familiar with the specific PDPA requirements that impact your organization. Download a copy of the PDPA or contact us to speak with our PDPA legal consultant for information about the specific requirements for your business.

2. Align people, policy, processes and technology

A common misunderstanding is that the PDPA requires organizations to add security technologies or IT skills to better protect data. In fact, the PDPA requires comprehensive improvement in data handling and management.

Robust PDPA compliance happens when a business combines organizational data management controls with technical controls. Organizational controls align people, policy and processes to data management and privacy. Technical controls ensure the right technologies are in place to reliably and effectively manage data handling.

The organizational and technical controls of most organizations aren't often naturally strong enough to manage PI as required by the PDPA. And, for many Thai businesses, data management practices and technologies are long out of date, requiring urgent updating to accommodate the new laws. Appropriate consulting advice is essential to rapidly find and plan the needed changes to align people, policy, processes and technology.

3. Seek advice

The fastest, most comprehensive path to compliance is through consulting advice. Although the Thai laws are new, many consulting firms have reacted quickly to help businesses achieve compliance. Look for a consulting partner who has already helped other businesses with compliance readiness, knows how to perform PDPA gap analysis and can rapidly develop a comprehensive roadmap tailored to meet your organization's specific needs. Contact us for more information.

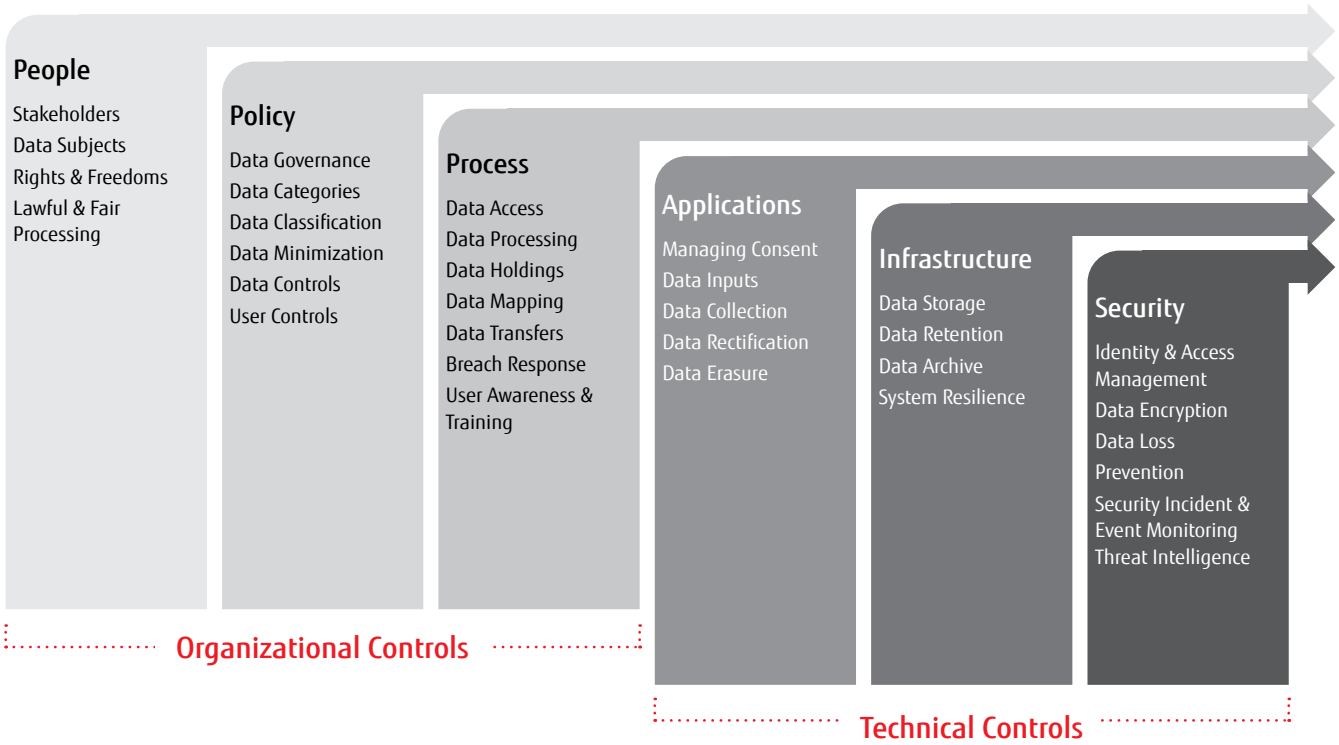


Figure 1: Combining organizational controls (people, policy and processes) with technical controls (technology) delivers 'privacy by nature' and ensures complete PDPA compliance

How Fujitsu supports roadmaps towards PDPA compliance

Fujitsu has the expertise and combination of technologies and services to quickly assess an organization's compliance readiness and build a roadmap towards PDPA compliance. We have long experience working with data management, protection and privacy processes and technologies, supporting our own operations and those of our customers.

We've already helped Thai businesses become PDPA compliant. Doing so requires beginning with a deep understanding of the unique profile of each organization. We do that through a consulting-led approach to understand each organization before tailoring recommendations for that organization's particular circumstances. Our consulting methods incorporate five core pillars, including: endpoint security; data center security; network security; cloud security; and security services.

Fujitsu's local and global Security Operations Centers (SOC) give 24 x 7 secure service tailored to meet each customer's requirements, drawing on more than 40 years of experience securing different environments. Our next SOC is due to open soon in Thailand, ideally positioned to help local organizations with ongoing PDPA compliance.

Our data management solutions are delivered through a range of professional and managed services based on best-of-breed technologies, and proven processes and policies. From supporting simple Q&A to sophisticated technological innovation, we offer multiple levels of consulting advice and support to match the needs and requirements of every organization seeking PDPA compliance.

Getting started

Contact us for more information about the next steps you can take to create a compliance roadmap to make sure your organization is ready to meet the PDPA deadline.