EXPANDED PRIMER & BACKGROUNDER!

Introduction

Data has become a new currency as well as an asset of many companies, large and small. The value of trade in data may one day surpass trade in goods and services. The rapidly evolving global norm is for personal data (data from which a person can be identified) to be regulated and protected.

Many business leaders recognise the importance of data privacy. Many have noted data privacy as a basic human right. Trust is an essential ingredient in managing data, including facilitating its exchange. Good data privacy practices make for competitive advantage. Businesses and individuals need to trust the internet as a means of transmitting and providing access to confidential and often sensitive information and they also need to trust that the systems which protect that data are safe, secure and reliable. Civil society has similar objectives. Government plays a key role in this process, both as a regulator and as a user of data itself.

How is data regulated and how can I manage to advantage? What is the EU GDPR and why is it relevant in Thailand? If it is Personal Data which is protected, what about commercially-derived data which is based on analysis of aggregated consumer behaviour? Can I view my own records (and correct them, or even take them down)? Do I have a 'right to be forgotten'? If I need to send data overseas, what are the cross-border rules? What is extra-territoriality? How can I best manage data?

This SEMINAR BOOKLET contains the programme, speaker bios, a background paper covering a Primer and data, data privacy / data protection issues, and recognizes the Sponsor and Supporters without whom the Seminar would be much less interesting.

Agenda

Time	Item
0815 – 0845	**Registration**
0845 – 0900	**Opening** **Welcome**: MC **Opening Remarks**: **Mr Philipp Dupuis, Head of Economic & Trade Section, EUD Thailand** **MC** explains the Forum
0900 – 0910	**Primer on Data –** concepts, terms and expressions**.** See THIS BOOKLET for more details **Professor Dan Svantesson** Editor, Oxford Journal of Online Data Privacy; Co- Director, Centre for Commercial Law, Bond University, Australia.
0915 – 1030	**Moderated Topic Session: Data Privacy and Data Protection in the '4.0' world** **Professor Dan Svantesson** GDPR –and the proposed Thai law. Key issues; how is the world grappling with regulation, extra-territoriality and governance? **Ms Siranya Rhuvattana, Senior Associate, Baker McKenzie -** major local and regional issues in managing data; the proposed Thai law. **Mrs Kari Laumann, VP Privacy Asia, Telenor ASA**. Operational and strategic issues in managing data; Privacy. Moderator: **Mr Bob Fox Chair, Digital Economy/ICT group JFCCT and EABC.** Questions of participants and Role Play. Questions from floor using Pigeonhole. Please use your own handheld device to access the Pigeonhole platform, via your own 4G cellular or the hotel's WiFi.
1035 - 1040	**Closing**

Speaker Biographies

Mr Philipp Dupuis Head of Economic & Trade Section, EUD Thailand	Philipp Dupuis is since August 2015 Head of the Economic and Trade Section of the Delegation of the European Union in Thailand. He also covers Cambodia, Laos and Myanmar. Between August 2009 and July 2015, Philipp Dupuis has been Deputy Head of the Unit in charge of the trade relations with North America in the Directorate General for Trade of the European Commission in Brussels. In parallel, he was EU deputy chief negotiator for the EU-Canada Comprehensive Economic and Trade Agreement (CETA). Prior to that he was involved in trade relations and negotiations with the Americas and the Middle East, and in the management of the Generalised System of Preferences (GSP). Between 2001 and 2005 he served as Head of the Economic and Trade Section of the EU Delegation to Mexico and Cuba. Before joining the European Commission in 1995, Philipp Dupuis was a consultant for Andersen Consulting in Frankfurt/Germany carrying out projects in the financial sector. He studied Business Administration and, as subsidiary major, Political Sciences at the University of Mannheim in Germany and made a Banking Apprenticeship at the Deutsche Bank in Darmstadt/Germany. Born 1965 in Darmstadt / Germany, of German nationality.
Professor Dan Svantesson Editor, Oxford Journal titled 'International Data Privacy Law', Co-Director, Centre for Commercial Law, Bond University Australia, Expert Internet & Jurisdiction Policy Network	Professor Dan Jerker B. Svantesson is a Co-Director of the Centre for Commercial Law at the Faculty of Law, Bond University (Australia) www.bond.edu.au , a Researcher at the Swedish Law & Informatics Research Institute, Stockholm University (Sweden), and a Visiting Professor at the Faculty of Law, Masaryk University (Czech Republic). He specialises in international aspects of the IT society, a field within which he has published leading books and articles, and given presentations in Australia, Asia, North America and Europe. Professor Svantesson held an Australian Research Council Future Fellowship (2012-2016) and was recently identified as the Field Leader for "Technology Law" in a study published by *League of Scholars* together with *The Australian*. He is an Editor for International Data Privacy Law, published by Oxford University Press https://academic.oup.com/idpl and a Member of the Editorial Boards for International Journal of Law and Information Technology, Commonwealth Law Bulletin, International Review of

Law Computers and Technology, Masaryk University Journal of Law and Technology and Computer Law and Security Review.

Professor Svantesson is a member of the Internet & Jurisdiction Policy Network's Contact Group on Data & Jurisdiction www.internetjurisdiction.net and is currently working as the lead author on the Internet & Jurisdiction Policy Network's first Global Status Report.

Professor Svantesson studied law in both Sweden (Master of Arts Jurisprudence & Bachelor of Arts Jurisprudence at Luleå Tekniska Universitet) and Australia (PhD & Master of Laws International Law at University of New South Wales)

Ms. Siranya Rhuvattana

Senior Associate, Baker McKenzie

Siranya Rhuvattana is a senior associate at Baker & McKenzie, Bangkok office and is currently active in the intellectual property and technology practice group. Her main areas of practice include data privacy, information technology and intellectual property. Siranya has extensive experience in the areas of data privacy, data analytics, electronic transactions, and cloud computing, as well as blockchain-based transactions, computer crime and cybersecurity.

Siranya regularly advises on data privacy compliance, having helped many Thai companies implement data protection strategies and privacy compliance programs both domestically and for their overseas operations.

As Thai and foreign companies have increasingly begun to focus on compliance with a more complex regulatory environment around their use of data, Siranya's practice has expanded to include significant work related to implementation of the European Union General Data Protection Regulation and the impending passage of the revised Thai Personal Data Protection Bill.

Siranya earned her LL.B. from the Chulalongkorn University with first class honors in 2008. In 2009-2010, she was a legal consultant at PricewaterhouseCoopers Legal and Tax Consultants when she won the Endeavour Postgraduate Award 2011, Full Scholarship from the Australian Government to pursue her LL.M. at Melbourne Law School. In 2013 Siranya earned her second LL.M. in Competition, Innovation and Information Law from New York University School of Law. Following law school, she was a trial lawyer representing and counseling companies in commercial disputes at a New York based law firm.

Siranya is a member of the Bars of New York and Thailand

Mrs. Kari Laumann

Vice President, Privacy, Asia, Telenor Group

Mrs. Kari Laumann is Vice President with responsibility for privacy in Asia for the Telenor Group. Telenor started more than 160 years ago as a national telecoms operator in Norway. Today Telenor has 172 million mobile customers across eight markets, almost 35 times the population of Norway.

Mrs. Laumann is a sociologist with a bachelors degree from Simon Fraser University in Canada, and a masters degree from the University of Oslo, Norway. Laumann has extensive experience through public service in Norway ranging from the Ministry of Foreign Affairs, to the Norwegian Board of Technology and the Norwegian Data Protection Authority.

Her professional career has focused on topics in the interface between technology and society, with an emphasis on privacy in the last ten years. Privacy and ethical implications of artificial intelligence has been one of her key areas of professional interest in recent years. Mrs. Laumann is a Norwegian national based in Bangkok, working with Telenor's Asian business units on privacy issues

Mr. Bob Fox (Moderator)

Chairman, JFCCT & EABC Digital Economy/ICT Group

Mr. Robert Fox ("Bob") is Chairman Digital Economy / ICT group JFCCT and EABC and holds regional roles in trade and investment policy in the services sector. He has a regional consulting business on trade and investment and is Regional Director Asia Pacific for a technology and services company.

He was group CEO of one of Malaysia's largest listed companies (a multi- service telecoms operator), regional director Asia Pac for business strategy and development for BT (British Telecom), regional director Asia Pac for a NASDAQ listed broadband services company and later a similar role for a US/Israeli consumer analytics company. He was one of the founders of Starhub Singapore, a member of the senior executive team to launch the UAE's second telecoms operator from Dubai, project director and main board (University Council) member for Bond University, Australia's first and only full scale private university (now in its 29th year) and CEO of Australia's first high end mail order company. He was with Baker & McKenzie (foreign investment, joint ventures, competition) for some years.

He has been involved with data protection policy and legislative developments in Malaysia, Singapore and Thailand. In Thailand he has devised and developed policy recommendations on a number of areas including Rule of Law, arbitration, fast track licence reform, SOE and telecoms reform, Cybersecurity, Work Permit & Visa and foreign investment (FBA).

Academic qualifications include BA LLB (UNSW), Master's - Stanford University Graduate School of Business (where he was a Sloan Felllow), and various ICT, stock exchange and director certifications. He is a mediator certified by THAC. Earlier he was an AFS Scholar.

Dr Pojanath Bhatanacharoen (MC)
Executive Director, Thai-Swedish Chamber of Commerce

Pojanath is the Executive Director of the Thai-Swedish Chamber of Commerce (TSCC). She is Bangkokian by birth but grew up in Gothenburg, Sweden. She moved to England to pursue her studies and received a PhD in Politics at Newcastle University in 2009. Her thesis focused on how small EU states could influence the negotiations on agricultural policy in WTO negotiations at both EU and WTO levels.

In 2010, she joined a multi-disciplinary team at Durham University to conduct postdoctoral research on tipping points with particular focus on diffusion of innovation. She has co-authored papers on management fashion and management gurus which explore how management ideas become popular and how celebrity consultants apply different techniques to communicate their ideas to the audience.

She is passionate about sustainability, which is a big concern for Swedish companies, and--in her capacity as the TSCC Executive Director--is engaging in projects which address some burning issues such as waste management and plastic reduction.

Primer

This Primer has a short description of concepts and a comparison table. More details below.

1. Concepts about Data

See Backgrounder.

2. Legal Concepts

Personal Data – data relating to an individual (natural person) who can be identified from that data.

Data Subject – the person whose personal data is at issue. 'Personal Data Owner' in the PDPA

Data Controller – primary custodian and manager of data, makes decisions about collection, use, disclosure.

Data Processor – carries out processing on behalf of Data Controller

Open Data: data which is shared for public and private research and analytical and other purposes. Typically this is de-personalised or was not originally personal data

Consent – from Data Subject about collection, use, disclosure.

Typical three stages of management of data: Collection, Use, Disclosure, collectively 'processing' in GDPR.

Disclosure: to third parties for processing to produce marketing information (including derived data), or for product definition or other purposes. May be domestic or cross border.

Cross Border Rules: The legal rules of country A about transferring data from country A to another country or to an international organisation. There are model rules such as APEC's Cross Border Rules (CBR) and by practice, emerging global standards.

Extraterritoriality: The application of a one economy's law outside that economy (eg GDPR outside the EU; the PDPA outside Thailand)

Conflict of Laws rules: The system of legal rules which determines matters such as jurisdiction and relevant law applicable to a data transaction or parts of a data transaction. This situation often occurs due to extra-territorial application. The leading non-government policy body dealing this these complex issues is probably the Internet & Jurisdiction Policy Network www.internetjurisdiction.net (HQ Paris).

Data Localisation: The idea that data about a country's citizens should not be transferred across borders.

Data Nationalisation: Similar to Data Localisation: the idea that data about a country's citizens is somehow the property of the state or at least subject to state control.

Big Data: the concept of large amounts of data due to records about a large number of data subjects, each with a number of fields or data points. Big Data also describes the phenomenon whereby these are managed.

Data Portability: A concept to get around incompatible silos or walled gardens. Requires common technical standards to allow transfer from one data controller to another; supports interoperability.

Data Adequacy: Recognition that the jurisdiction (country or international organisation) to which data is to be transferred has data protection regulation which is adequate and sufficient to allow for cross border data flows.[1]

Privacy Shield: a means for self-certification or outside verification for US-EU data transfers. Replaces Safe Habor which was legally challenged[2]

Derived Data: Personal data or non-personal data which is generated from raw personal data records. Examples are customer profiles, or customer segment profiles. Who owns, and whether access is provided to derived data records can be an issue.

Sensitive Data: A sub category of Personal Data eg medical records, beliefs, ethnicity. It may also include financial records. Special treatment is usually prescribed.

Binding Corporate Rules concept is one of the basis upon which data may be transferred across borders. Applies in an enterprise or group of enterprises.

APEC Privacy Framework: Principles and implementation guidelines; sets up APEC Cross-Border Privacy Rules (CBPR) system, similar to Privacy Shield. CBPR is not a set of laws but rules which can be invoked (see more in the Backgrounder).

3. Primer: Comparison Table

Some key similarities and differences between the EU GDPR and the Thai PDPA.

Topic:	EU GDPR:	Thai PDPA:
Extraterritoriality	Article 3 provides broad extraterritorial scope of application.	Section 5 provides broad extraterritorial scope of application; largely copied from GDPR
Data Protection Officer (DPO)	Articles 37-39 provide detailed regulation on the designation, role and tasks of a data protection officer.	Sections 40-41 provide detailed regulation on the designation and duties of a data protection officer.
Cross-border data transfers	Articles 44-50 provide detailed regulation of cross-border data transfers. See also note above about Data Adequacy.	Section 28 provides detailed regulation of cross-border data transfers; not very different to GDPR
Consent	The reliance on consent is a central feature of the GDPR. ('Unambiguous'). Must be express but can be oral.	The reliance on consent is a central feature of the PDPA. Treatment differs a little from GDPR

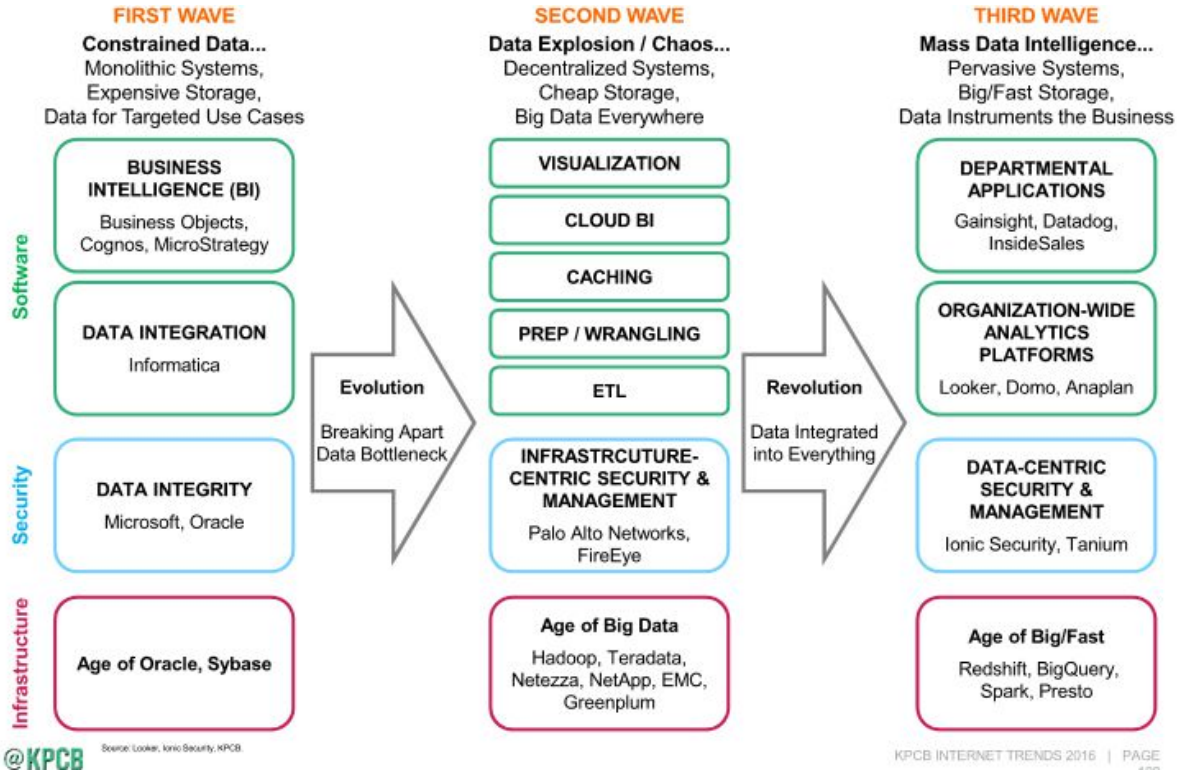
[1] EU and Japan Data Privacy Deal 2018 is the first such EU deal. http://europa.eu/rapid/press-release_IP-18-5433_en.htm

[2] https://www.twobirds.com/en/news/articles/2016/global/safe-harbor-replacement-approved-by-european-commission

Topic:	EU GDPR:	Thai PDPA:
'Right to be forgotten'	Article 17 provides a specific right to erasure ('right to be forgotten').	No exact equivalent provision but a right to erasure if Data Controller is non compliant (s. 33)
Data portability	Article 20 provides a specific right to data portability.	PDPA s. 31 is similar
Automated decision-making	GDPR Article 22 contains detailed rules regarding automated individual decision-making, including profiling.	The Thai PDPA contains no equivalent provision.
Data protection by design, and by default	Article 25 provides an articulated obligation of data protection by design, and by default	The Thai PDPA contains no equivalent provision.
Security	Article 32 prescribes encryption, confidentiality and testing of systems.	PDPA s. 36 places onus on Data Controller and on Processor to implement security measures (less prescriptive than in GDPR)
Notification	Data Controller must advise Supervisor authority 'without undue delay' and within 72 hours of breach(?)	Must advise Owner 'without delay' s. 36 and for high volume, to the PDP Committee.
Binding Corporate Rules	Article 47 applies in an enterprise context.	PDPA s. 29 is similar.
Level of fines	Infringements may be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. (Article 83)	The highest fines possible under the Thai PDPA are up to THB 5 m (Section 82). PDPA also has potential imprisonment for a term not exceeding one year (Section 77).

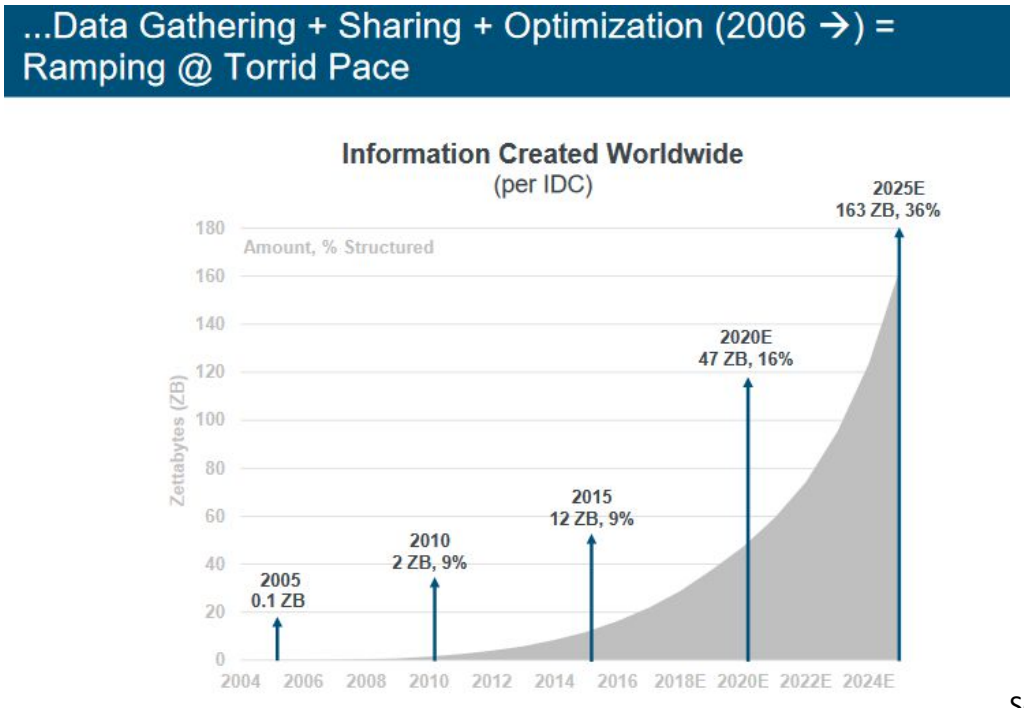
1. About Data

This chart shows how data is now pervasive, fast and big. It needs a systematised approach to management and respect for privacy and accuracy.



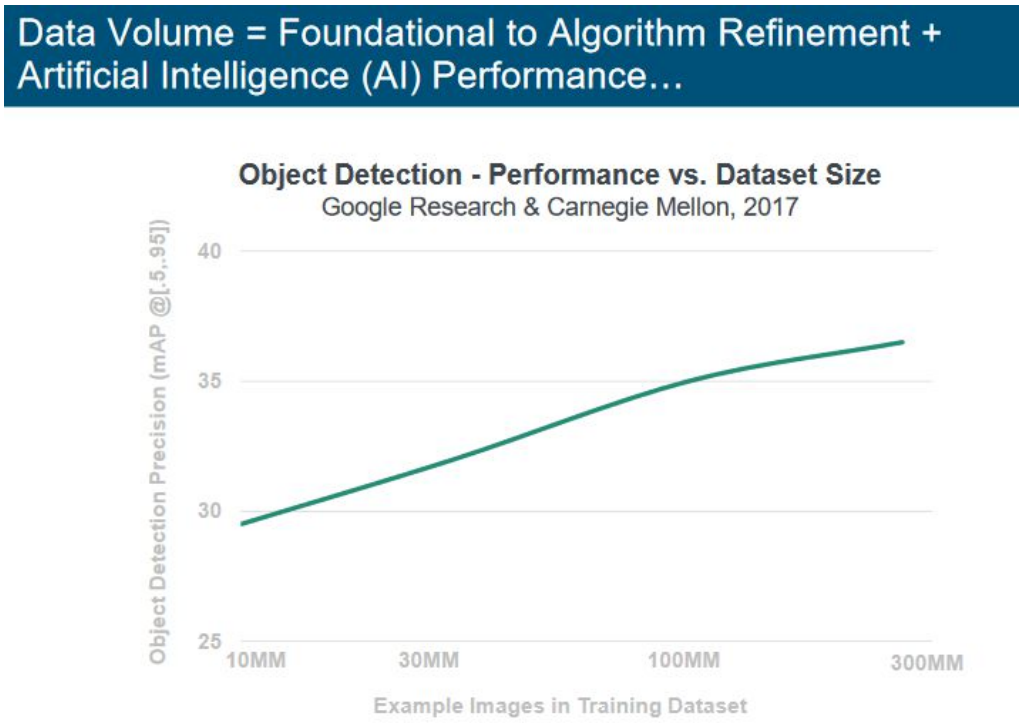
Source above: Mary Meeker, Internet Trends 2016.

Chart below shows ZetaBytes (ZB) of data used.

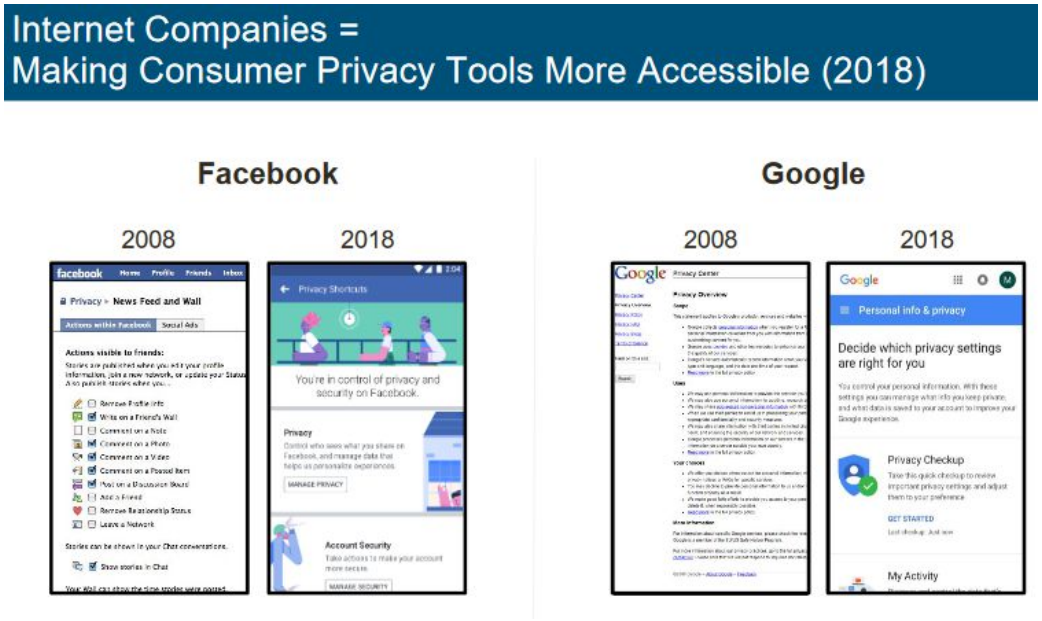


Source above: IDC used in Kleiner Perkins' Mary Meeker INTERNET TRENDS 2018 (May 2018) slide 189.

The chart below shows the value of big data sets:

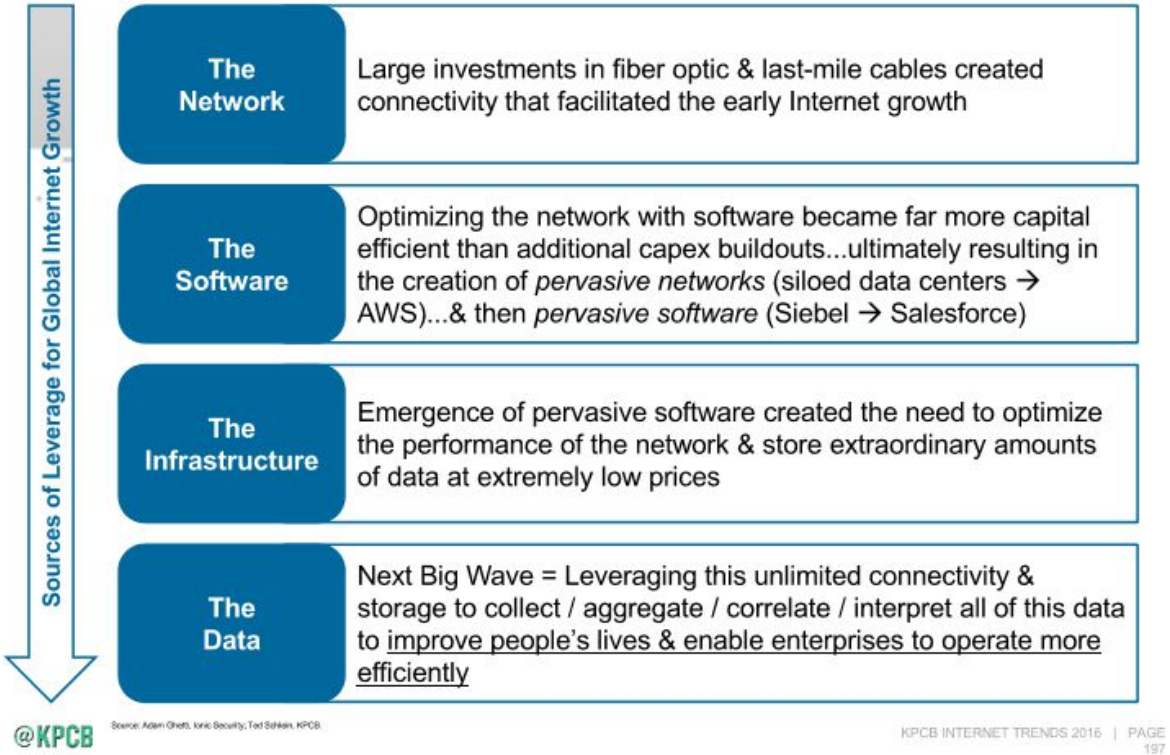


Source above: Kleiner Perkins' Mary Meeker INTERNET TRENDS 2018 (May 2018), slide 196



Source above: Kleiner Perkins' Mary Meeker INTERNET TRENDS 2018 (May 2018) slide 207

This chart below shows that to gain competitive advantage, data has to recognised as an asset and a tool.



Source: Mary Meeker, Internet Trends 2016

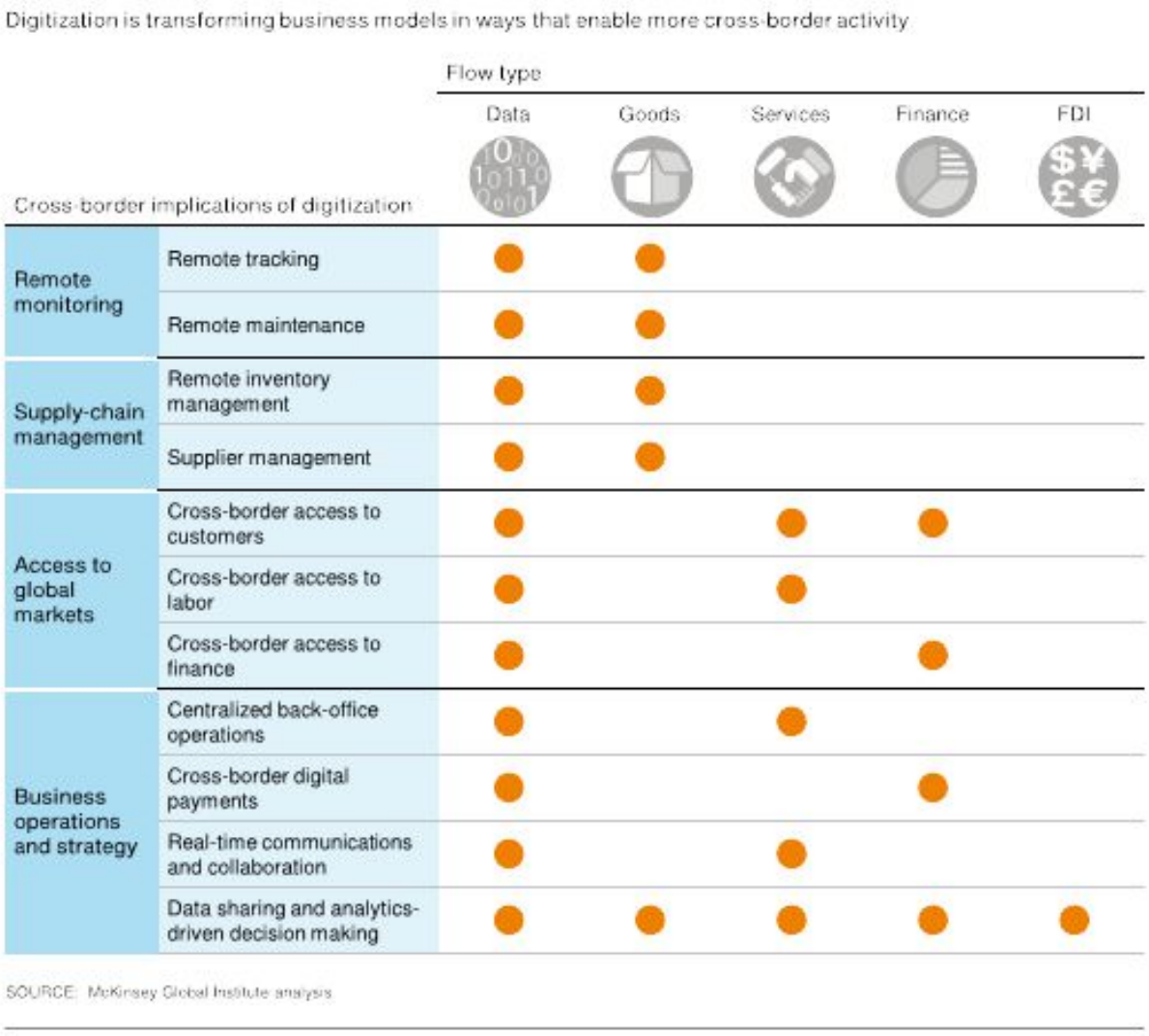
A McKinsey Global Institute (MGI) study "Digital globalization: The new era of global flows" showed that although the global goods trade has flattened and cross-border capital flows have declined sharply since 2008, globalization is not heading into reverse. Rather, it is entering a new phase defined by soaring flows of data and information. Extracts:

> "Remarkably, digital flows—which were practically nonexistent just 15 years ago—now exert a larger impact on GDP growth than the centuries-old trade in goods…
>
> "The amount of cross-border bandwidth that is used has grown 45 times larger since 2005. It is projected to increase by an additional nine times over the next five years as flows of information, searches, communication, video, transactions, and intracompany traffic continue to surge. In addition to transmitting valuable streams of information and ideas in their own right, data flows enable the movement of goods, services, finance, and people. Virtually every type of cross-border transaction now has a digital component.
>
> "Approximately 12 percent of the global goods trade is conducted via international e-commerce. Even the smallest enterprises can be born global: 86 percent of tech-based start-ups surveyed by MGI report some type of cross-border activity.
>
> "Individuals are using global digital platforms to learn, find work, showcase their talent, and build personal networks. Some 900 million people have international connections on social media, and 360 million take part in cross-border e-commerce. Digital platforms for both traditional employment and freelance assignments are beginning to create a more global labor market.
>
> "Although there is substantial value at stake, not all countries are making the most of this potential. The latest MGI Connectedness Index—which ranks 139 countries on inflows and outflows of goods, services, finance, people, and data—finds large gaps between a

handful of leading countries and the rest of the world. Singapore tops the latest rankings, followed by the Netherlands, the United States, and Germany. China has grown more connected, reaching number seven, but advanced economies in general remain more connected than developing countries. In fact, each type of flow is concentrated among a small set of highly connected countries.

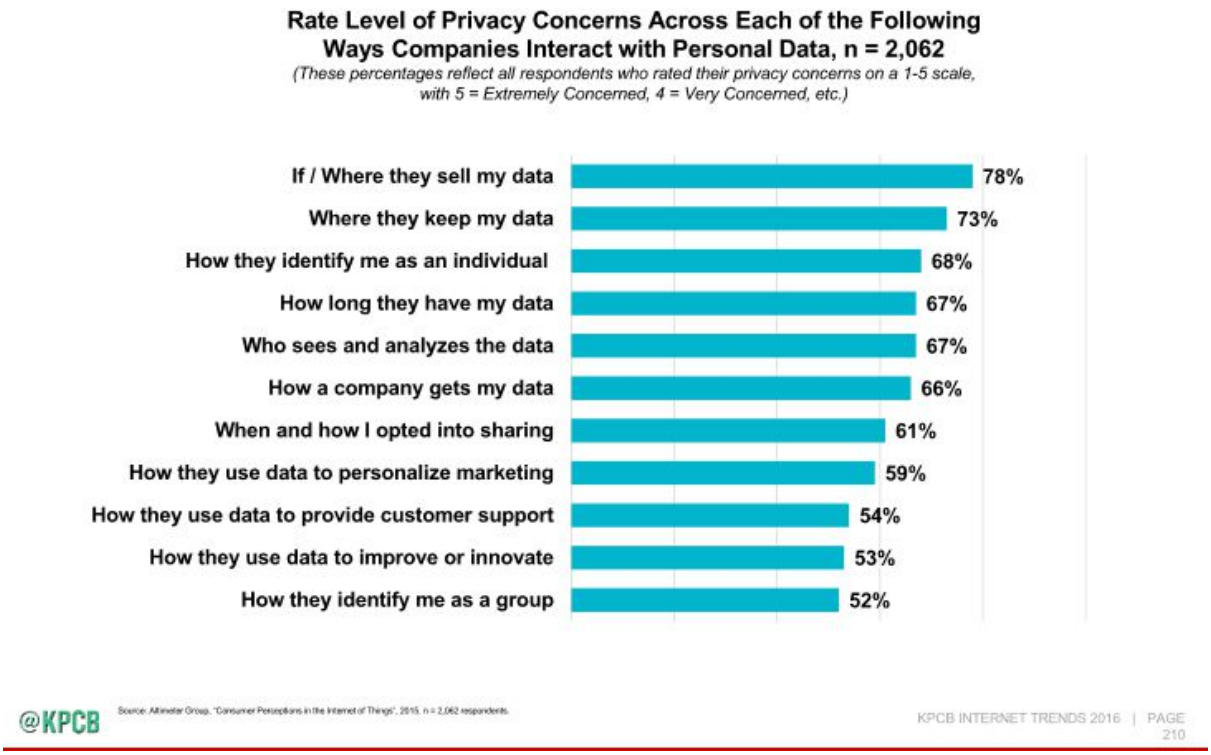
"Lagging countries are closing the gaps with the leaders at a very slow pace, ... For countries that have been slow to participate, the opportunities for catch-up growth are too substantial to ignore."

The chart below from MGI illustrates the enormous dependence on cross border trade, in goods and services, supported by data. Thus getting the cross border data regulation regime right in ways which is predictable, supports privacy and security is essential if Thailand is to be an attractive location where cross border data plays a significant role.



Source above: MGI.

Turning to Privacy, concerns (circa 2016) are noted:



Source above: Mary Meeker, Internet Trends 2016

2. Data Protection law fundamentals

a) Objective to create an attractive, efficient and respected data services hub
b) Clear duties of data controller / data processor
c) Integrity about personal data. Data owner effective ability to correct data. There are consumer protection objectives as well as an economic objectives; the two are related.
d) Privacy of commercial and commercial data and communications. (In the 'Trusted Internet' concept, security and privacy should not be opposites).
e) Security so that privacy harmonises with data security.
f) Workable and not burdensome cross border Rule-of-Law based regime, and not so lax as to make Thailand a port of convenience ('The Liberia of data services'). Cross border should not be a back door method to unauthorized disclosure but should enable ease of use for analytics, customer and product management and foreign end-use purposes.
g) Some kind of anti-data nationalization and anti-localisation regulation and practice, but with specific, limited exemptions where the onus is on the Data Controller seeking not to disclose. (There is often sector specific legislation governing certain data sets; see more below).
h) Promotion of the system via industry education with a mindset that privacy is economically and socially valuable.
i) Clear understanding of what is personal data and what is not. Public data / open data are important for various applications including smart cities, improved transport management,
j) Easy dispute resolution via a government endorsed Centre (or reputable private centre) and by supporting Arbitration.
k) Harmonisation as far as possible with accepted international standards and practices. The GDPR for example applies to many companies in Thailand not just on cross border issues but also on how certain data must be managed.

3. Data Subject's ability to see and correct.

Consistent with building a reputable data services hub, a Data Subject's ability to view and correct his or her personal data is important. As a matter of practice, some Data Controllers holding Derived Data (eg an analysis of a Data Subject's spending profile or behaviour) consider this to be intellectual property of the Data Controller and many would not want to allow the Data Subject to view it. At the very minimum, the Data Subject should be able to view and correct (and consistent with withdrawing consent prospectively), even delete his or her basic personal data which was collected.

4. State actors exemptions

There are a number of user groups: business, individuals, government, civil society. Is it wise to exempt state actors (government as user) as broadly as s.4 PDPA proposes? A new subsection (2) appears in s. 4(2) - is exempting the legislature, now in s. 4(4) appropriate? Disclosure of personal data could be a back door way of misuse for wrong purposes. Thus rather than a full exemption from all provisions of the law, some safeguard could be considered to ensure that the data is managed properly.

The EU's General Data Protection Regulation – why it matters also outside the EU

In 2016, the EU's Data Protection Directive which came into force in 1995, was replaced by the General Data Protection Regulation (GDPR) which came into force in May 2018.

The move from a Directive (that must be implemented within the law of each Member State) to a Regulation (with direct application in the Member States) aims to ensure greater harmonisation within the EU.

The degree of international reaction to the GDPR is such that some have suggested that no other law making initiative in world history has attracted greater global attention.

There are at least six different reasons why the world has paid so much attention to the GDPR. First, the GDPR, like many data privacy laws before it, makes the claim of applying also to parties outside the jurisdiction that implemented it; in this case the EU.

The GDPR claims a broad scope of application going well beyond the EU. Article 3 of the GDPR outlines the type of connecting factors (EU links as it were) that will trigger the application of the GDPR. This is Extra-territoriality. Put simply, the GDPR applies to any data controller or processor with an establishment in the EU, regardless of whether the processing takes place in the EU or not. It also applies to a controller or processor not established in the EU where it engages in the processing of personal data of data subjects who are in the EU, either by offering goods or services to such data subjects in the EU (a form of 'targeting test'), or by monitoring their behaviour within the EU. Finally, Article 3 contains the somewhat vague rule that the GDPR applies to the processing of personal data by a controller not established in the EU, but in a place where Member State law applies by virtue of public international law.

By the time the GDPR took effect, there was little guidance as to the exact reach of the GDPR's application. This resulted in an unhelpful degree of uncertainty amongst controllers and processors not established in the EU that potentially, but not clearly, are caught by the GDPR's scope of application. However, the EU's Article 29 Working Party's general factsheet aimed at helping Asia Pacific Privacy Authorities understand the basic requirements included in the GDPR states that:

> "The GDPR applies to data controllers and data processors with an establishment in the EU, **or** with an establishment outside the EU that target individuals in the EU by offering goods and services (irrespective of whether a payment is required) or that monitor the behavior of individuals in the EU (where that behavior takes place in the EU). Factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.
> Data controllers and/or data processors not established in the EU, but whose activities fall within the scope of the GDPR, will generally (some exceptions apply) have to appoint a representative established in an EU member state. The representative is the point of contact for all Data Protection Authorities (DPAs) and individuals in the EU on all issues related to data processing (Article 27)."[3]

The second reason why the world has paid so much attention to the GDPR is that it imposes significant limitations on cross-border data flows. Many aspects of modern society, such as international financial transactions, travel and communication, depend upon cross-border data transfers. At the same time, data being transferred across borders commonly involve a degree of loss of control over that data, and even more so of the scope of direct influence of the body tasked with upholding data protection in the country from which the data originates. This conundrum has been a central issue in international data privacy initiatives since the start of the 1980s.

The long-standing debate regarding the circumstances under which data may be transferred across borders has continued in recent years, most notably in the context of transatlantic data transfers, but also beyond that.

Third, the GDPR indirectly influences data privacy laws around the world. It has already sparked reform discussions in some countries outside the EU. Given the experiences gained from the influence of the EU's Data Protection Directive it may safely be assumed that many countries around the world will be inclined to draw upon the Regulation when creating, or reforming, their own data privacy laws. The Thai Personal Data Protection Law is an example of this, not least Section 5 which largely mirrors GDPR Article 3. In this sense, the GDPR may be seen to spark the start of increasingly broad claims of jurisdiction in data privacy laws around the world.

As the GDPR continues to influence data privacy laws around the world, a degree of harmonisation can be expected. At the same time, the actual application of the data privacy laws is impacted by underlying values. The EU's application of the GDPR will be guided by the fact that the Charter of Fundamental Rights of the European Union specifically enshrines the protection of personal data (Article 8). Where other states adopt laws based on the GDPR, their application of those laws will be guided by those states' underlying values. This may result in differing application of seemingly identical, or near identical, legal norms.

Fourth, as part of the mechanisms adopted to increase the effectiveness of the enforcement of the GDPR, Article 27 of the GDPR requires a controller or processor not established in the Union, but falling within the GDPR's scope of application, to designate in writing a representative in the Union.

A fifth reason why the GDPR has gained so much international attention is found in the heavy fines that may be imposed as a result of breaches of the GDPR. Article 83(5) makes possible fines up to

[3] Article 29 Working Party, EU General Data Protection Regulation: General Information Document, p. 2 http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49751&lipi=urn%3Ali%3Apage%3Ad_flagship3_pulse_read%3BaEuuvVHcSFSSShxXB0Rnjg%3D%3D.

€20 million, or 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Sixth, the GDPR has gained international attention due to the fact that some multinationals have opted to adopt the GDPR as their standard of operation globally. In this 'standard setting' manner, the GDPR expands the data privacy rights enjoyed by users in states not bound by the GDPR.

Despite the significance of these six reasons why the the world has paid so much attention to the GDPR, perhaps the greatest achievement of the GDPR is the extent to which it has manged to put data privacy on the corporate agenda, and the degree to which it has managed to affect consumer attitudes and mind-sets. Strong data privacy protection is now not merely a matter of ensuring minimal legal compliance. Rather, strong data privacy protection a clear competitive advantage in the increasingly data-driven economy.

The draft Thailand Personal Data Protection Act (PDPA)

A very early draft personal data protection law was made several years also. During 2015 a then newly-proposed Personal Data Protection law was one of a number of new 'digital economy' laws and was publicly reviewed. It lay in the background until early 2018 when a revitalised office of Permanent Secretary of Ministry of Digital Economy & Society (MDES) issued a well-received discussion draft. This draft law was revised in May 2018 and then in September 2018 where public hearings were held, in late September. This September draft law ('PDPA') adopts and introduces various concepts from the EU General Data Protection Regulation ("GDPR"). Key amendments to the PDPA includes, *among others*, a shorter transition period from 1 year to 180 days, more explicit extraterritorial applicability, more stringent consent requirements, explicit consent requirements for sensitive data and new relevant exemptions, and the prescribed criminal and administrative fines and imprisonment.

Various new obligations and concepts are introduced into the PDPA. Compliance with the PDPA, when it enters into force, is now a board level accountability matter, as organizations are required to ensure that they put in place data governance. Governance will also involve both appropriate policies together with responsibility. Data controllers and data processors will need to put in place appropriate security measure for personal data, to guard against loss, unauthorized access, use, modification and disclosure. Unlike the previous draft, the September draft PDPA requires a controller or processors to appoint a Data Protection Officer ("DPO"). Offshore data controllers and data processors will be required to appoint a representative in Thailand. When the law enters into force, organizations will need to carry out an analysis of their footprint and local business activities in Thailand to determine whether they are required to appoint a DPO and a representative in Thailand. There will need to be a review of internal policies and procedures, including policies relating to accountability (e.g. information security, retention, breach, and data subject rights).

Among other legal requirements, the PDPA will significantly strengthen the rights of individuals by clarifying and extending existing rights and introducing new rights for individuals. These include the right to data portability and the right to object. These new rights have generated significant concern because of the need to assess whether businesses should put in place new or updated processes and procedures to deal with the practical implications of the extended rights. Businesses should establish procedures to respond to data subject requests corresponding to the individual data protection rights under the PDPA which cover internal roles and responsibilities, timelines and methods for responding and organizational and technical measures to ensure that any request is addressed consistently across the systems where the relevant personal data is stored.

Although the PDPA reflects various GDPR rules, and has tended towards importing GDPR rules,, the language of certain relevant provisions differ. Some of the requirements under the PDPA go beyond the GDPR. These include the notification obligations which require more detailed information to be notified to data subject, broader liabilities of the representative in Thailand for offshore data controllers and data processors, imprisonment penalty, etc. Compliance with the PDPA could be challenging for any type and size of business.

A compliance map, requirement-by-requirement of the two would be a healthy step, given that compliance with both will be needed in many cases.

Some key concepts based on both GDPR and PDPA

1. Personal data

Data privacy laws seek to protect the individual's privacy by protecting her 'personal data' (or 'personal information'). Consequently, the most effective way to avoid having to comply with data privacy laws is to avoid contact with others' personal data. At the same time, the value of personal data is indisputable and indeed the core of several businesses models, particularly online.

The GDPR (Article 4(1)) defines personal data as:

> *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*

The Thai PDPA (Section 6) defines personal data as:

> *"Personal Data" means any data pertaining to a person, which enables the identification of such person, whether directly or indirectly, but not including data of the deceased specifically*

2. Consent

Data privacy laws have for a long time relied upon the concept of consent. The thinking is that – in the spirit of freedom of contracts – individuals can agree to virtually any form of collection, processing, use and disclosure of their data. In many ways, consent works like a 'miracle cure' for what otherwise would be seen as abuse of personal data.

Consent is typically required for a variety of purposes including for the collection of personal data, use of personal data and disclosure of personal data, and may also be a valid ground for other activities such as the cross-border transfer of personal data.

The GDPR (Article 4(11)) defines consent as:

> *'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*

In Article 7, the GDRP includes detailed rules regarding conditions for consent:

> *1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.*
> *2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.*

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

The Thai PDPA does not define consent as such. However, the central role of consent is emphasised in numerous sections. For example, section 19 reads as follows:

The Personal Data Controller shall not collect, use or disclose personal data if no consent of the Personal Data Owner is, or has been, given in advance, unless permitted to do so by the provisions of this Act or any other law.
Application for consent shall be made in writing, or via electronic means, unless it cannot be done by its nature.
In applying to obtain consent from the Personal Data Owner, the Personal Data Controller must also indicate the purpose of collection, use or disclosure of Personal Data, and such application for consent must be clear and shall not be made to cause deception or misunderstanding to the Personal Data Owner in respect to such purpose. The Committee may require the Personal Data Controller to apply for consent from the Personal Data Owner in accordance with to the form and statements as prescribed by the Committee.
The Personal Data Owner may withdraw his/her consent at any time, unless there is a limitation of right for the withdrawal of consent by law, or in the contract, which gives benefits to the Personal Data Owner.
In the event that the withdrawal of consent will affect the Personal Data Owner in any matter, the Personal Data Controller shall inform the Personal Data Owner of such effects relating to the withdrawal of consent.
The application for the Personal Data Owner's consent which is not in accordance with those prescribed in this Chapter shall have no binding effect to the Personal Data Owner and shall not enable the Personal Data Controller to collect, use or disclose the Personal Data.

Section 24 (3) allows collection if there is public disclosure relying on direct or implied consent.

3. Data controller

A common feature of many data privacy frameworks is that they focus on regulating the conduct of 'controllers', 'data controllers' or 'personal data controllers' (all having roughly the same meaning). It is such controllers that bear the primary responsibility for compliance.
The GDPR (Article 4(7)) defines controller as:

'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law

The Thai PDPA (Section 6) defines controller as:

"Personal Data Controller" means a person or juristic person having the power and duties to make decisions regarding the collection, use, or disclosure of the Personal Data

4. Data processor

While the data controller bears the primary responsibility for compliance, also other parties – namely those classed as data processors – involved in the data processing must take account of data privacy laws.

The GDPR (Article 4(8)) defines processor as:

> *'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*

The Thai PDPA (Section 6) defines processor as:

> *"Personal Data Processor" means a person or juristic person who operates in relation to the collection, use or disclosure of the Personal Data pursuant to the orders given by or on behalf of a Personal Data Controller, whereby such person or juristic person is/are not the Personal Data Controller*

5. Sensitive data

Many data privacy frameworks include a special sub-category of personal data; that is, 'sensitive data'. Personal data types classed as sensitive data include categories of personal data such as data on an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, health, genetic and biometric data. Such data is commonly provided with extra safeguards. S. 26 PDPA requires express consent to disclosure but with exceptions.

6. Derived data

Derived data (or 'inferred data') – data generated from other data – may still be caught by data privacy laws as also such data may be personal data, or indeed, sensitive data. An analysis or profile made by a Data Controller about a customer (which could include value judgements about the customer's expected value to a service provider) is a kind of derived data. . Some service providers have been reluctant to share such derived data with data subjects. This is a matter of particular relevance in the context of big data.

7. Inspection, Deletion, Take Down

While Article 17 GDPR supports these concepts and allows this with conditions, PDPA s. 33 allows data to be taken down where a Data Controller is non compliant with the PDPA.

Jurisdiction reputation relies on accuracy and confidence in the system. Consistent with these principles is the right to correct, take down etc. The system is not perfect.

8. Cross-border data transfers

National data privacy laws are easily circumvented if the personal information they are meant to protect can be transferred to third countries without appropriate controls and limitations. On the other hand, the societies we have built are now interacting to such a degree that crucial aspects of our societies would grind to a halt if personal information was not allowed to be transferred between countries. Against this background, it is not surprising that that cross-border issues have been a longstanding driving force behind international work on data privacy.

The GDPR, in Articles 44-50 includes detailed rules regarding cross-border data transfers essentially making such transfers possible in certain limited different circumstances. Data can be freely transferred to third-countries that have obtained a favourable (full) adequacy decision by the

European Commission (Article 45). However, only a small number of countries have so far obtained such approval. Data can also be freely transferred to any US businesses that have signed up to the EU-US Privacy Shield framework – a special agreement (a partial adequacy decision) put in place between the EU and the US following the end of the 'Safe Harbor' rules.

For transfers falling outside these special arrangements, the transfer must be based on one of the other grounds recognised in the GDPR:

- transfers subject to appropriate safeguards (Article 46);
- transfers based on binding corporate rules (Article 47); and
- transfers based on derogations for specific situations (Article 49), including where the data subject has explicitly consented to the proposed transfer, or where transfer is necessary for the performance of a contract between the data subject and the controller.

The Thai PDPA contains restrictions on cross-border data transfers. In particular, Section 28 states that:

> *In the event that the Personal Data Controller sends or transmits the Personal Data overseas, the relevant destination country or international organization that receives such personal data shall have sufficient personal data protection standards, and such act shall be performed in accordance with the rules for the protection of Personal Data as prescribed by the Committee in Section 16(5), except in the following cases:*
> *(1) where the law so prescribes;*
> *(2) where the consent of the Personal Data Owner has been obtained after the Personal Data Owner has been informed of the insufficient personal data protection standards of the relevant destination country or international organization that receives such personal data;*
> *(3) where it is necessary to comply with the contract under which the Personal Data Owner is a contracting party or it is necessary to use the Personal Data to comply with the Personal Data Owner's request before entering into such contract;*
> *(4) where it is the act in compliance with the contract between the Personal Data Controller and other persons or juristic persons for the interests of the Personal Data Owner.*
> *(5) where it is to prevent or stop harms to life, body or health of the Personal Data Owner or other persons when the Personal Data Owner is unable to give consent at such time;*
> *(6) where it is necessary to accomplish the missions having significant public interest.*
> *In the event that there is a problem of the sufficient personal data protection standards of the relevant destination country or international organization that receives such personal data, such problem shall be submitted to be determined by the Committee. The decision of the Committee may be reviewed when there is a new evidence to believe that the destination country or international organization that receives such personal data has development to have the sufficient personal data protection standards.*

9. Extraterritoriality

An email is sent from Germany to Sweden. The subject matter is a project in SE Asia where the software programme is developed in Estonia but where its use is governed by English law. There are many types of data involved. Could, hypothetically, these various data types be nationalized or localised? Can the entire sets of data be subject to one national legal system?

These jurisdictional issues reflect the complexity of trying to find an optimal approach to data flows, which do not (by their nature) recognize national boundaries. Many [4] are working on this but there is no simple answer.

Such everyday situations illustrate that on technical grounds is may not even be possible to localize or nationalize all data.

The WTO recognizes data as a kind of service; in that context its governance can be found in GATS. Generally speaking, GATS jurisprudence does not support (subject to exceptions), data localization. The special treatment of sensitive data sets such as medical and financial records do need to be recognized.

Cross border governance of data, it is suggested, requires some standardization. It would not help any nation's standing if personal data could be sent across borders (eg for processing, for deployment in another jurisdiction etc) without any regulation. At the opposite extreme, nationalizing or localizing data would not work either. The world has by and large moved to standard which requires the transferee jurisdiction to be at least as protective as the transferor jurisdiction.

Harmonisation in Cross Border Rules is thus desired. APEC Cross-Border Privacy Rules (CBPR) System www.cbprs.org offer one approach (see more about APEC in the next part of this Backgrounder).

Many, if not most, of the world's data privacy frameworks either expressly (see e.g. GDPR) or impliedly (see e.g. Singapore's *Personal Data Protection Act*) apply in an extraterritorial manner. Article 3 of the GDPR states:

> *1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.*
> *2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*
> > *(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*
> > *(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.*
> *3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.*

Similarly, Section 5 of the Thai PDPA states:

> *This Act shall apply to the collection, use or disclosure of Personal Data undertaken by Personal Data Controllers or Personal Data Processors who are in the Kingdom, regardless of whether such collection, use or disclosure are carried out in or outside the Kingdom.*
> *In the event that the Personal Data Controllers or Personal Data Processors are outside the Kingdom, this Act shall apply to the collection, use or disclosure of Personal Data of the Personal Data Owner who is in the Kingdom, undertaken by such Personal Data Controllers or Personal Data Processors in the following activities: (1) the offer of goods or services to the Personal Data*

[4] Including, notably, the Internet & Jurisdiction Policy Network

Owner who is in the Kingdom, regardless of whether the payment is made by the Personal Data Owner; (2) the monitoring of the Personal Data Owner's behavior in the Kingdom.

The key objectives of a provision dealing with the geographical reach of a data privacy law is to fulfil two distinct functions. Using the Thai *Personal Data Protection Act* as an example:

1) It should ensure that the *Personal Data Protection Act* provides adequate protection in the Kingdom of Thailand in relation to actors and activities overseas impacting the data privacy of the Thai people; and
2) It should ensure that the *Personal Data Protection Act* does not apply more broadly than is necessary.

As currently drafted, Section 5 is useful for the first of these purposes but less so for the latter. While its broad scope is not unusual amongst data privacy laws (and very similar to that of the GDPR), section 5 is clearly broader than it needs to be. This has several downsides:

1) As it covers many more controllers and processors than the enforcement authorities can possibly pursue, the application of the law becomes arbitrary and open to discrimination and abuse;
2) It undermines the international legitimacy of the *Personal Data Protection Act*;
3) It puts the *Personal Data Protection Act* at odds with aspects of international law (such as the doctrine of comity);
4) It puts unnecessary pressure to pursue the enforcement of the *Personal Data Protection Act* where not necessary for the protection of the Thai people; and
5) It adds to the risk of other States seeking to impose their laws in an overly broad manner thereby impacting Thai interests.

Section 5 appears to mirror parts of the EU GDPR Art. 3 with all its blemishes. (While GDPR Art 3 refers to processing outside the EU, Art 5 refers to collection, use or disclosure outside Thailand). Many have commented[5] that the GDPR provision does not well respect international law principles. In many cases, other countries or actors will claim to have jurisdiction and the legitimacy of enforcement actions may in those cases be called into question. Furthermore, any attempt at enforcing domestic law against foreign actors is associated with considerable practical problems. (Guidelines on GDPR Art 3 are expected to be published soon).

To illustrate, there is a considerable difference between requiring fair collection, use or disclosure of personal data (Chapter II) and imposing criminal liability (including jail terms) on foreigners having acted in their home States (Chapter VII – Part I). In the light of this, it is not appropriate to have a single test of extraterritoriality for the entire Act. Rather, under a best practice model, different jurisdictional hurdles are applied depending on the severity of impact on the foreign party, hence a kind of 'layered' approach may work.

Some rules (see e.g. sections 26 and 27) are aimed at preventing direct abuse, while other rules (see e.g. section 40) are aimed at more administrative goals. While it may be reasonable to ask a foreign company to abide by the first type of rules as soon as that foreign company collects data from Thai nationals (even in a once off transaction), the same limited degree of contact may not justify Thailand imposing on the company the duty of prepare items for examination by the

[5] Professor Dan Svantesson, Managing Editor of the Oxford Journal of International Data Privacy Law https://academic.oup.com/idpl, an expert advisor to the Internet &Jurisdiction Policy Network, has assisted JFCCT / EABC with information on cross border and extra territorial issues in the past. A useful reference on Art 3 (and other parts of GDPR) appears here: https://works.bepress.com/christopher-kuner/1/

Committee. When the Law applies to actors outside Thailand, the legal rules contained in the Law could be broken down into three layers (abuse-prevention layer, rights layer, and administrative layer) with different, incrementally demanding, jurisdictional rules attached to each layer. Adopting this structure would see the Law's approach to extra-territoriality reach greater harmonization.

One Service Provider's approach to managing Personal Data and Privacy – Telenor Group.

Need customers' trust to provide personalized services

Telenor experiences every day how connectivity changes people's life and work, and how businesses and societies are transformed by mobile technology. Personalization of products and services drives customer engagement and value creation. Data responsibility and privacy are most important. Telenor's aim is to be a trusted partner with strong integrity, reducing inequalities and delivering on safety, security and privacy. This trust has to be earned.

Technological advantages, such as artificial intelligence, the Internet of Things and 5G, will both generate and need large amounts of data to add value. The digital society provides endless opportunities, but also a need for secure data handling.

Building strong privacy frameworks in Asia and Europe

In order to conform to the GDPR requirements in Europe, for the past couple of years Telenor has conducted a GDPR readiness project in each European business unit, where all data processing activities have been mapped and appropriate procedures are in place at all stages. Privacy management has been strengthened in terms of both people and procedures.
Telenor has established an Asia Privacy Program to further strengthen data protection in Asian operations.

A major learning from privacy readiness projects in both Asia and Europe in the past years is that Telenor need to promote new privacy culture within each organization, with the aim of winning the hearts and minds of all employees who have a role to play in privacy governance. This is an ongoing process, but a solid foundation has been set

Ethical Artificial Intelligence

Artificial intelligence (AI) will impact nearly all sectors of economy and society. AI technologies will drive digitalization of existing industries and will enable the development of new industries and ways of doing things.

Telenor's ambition is to strengthen AI capabilities, both through applying AI techniques to our core products and operations, and also through taking on new positions. Internet of Things (IoT) is one of those prioritized areas in Telenor where new business models will emerge and be driven by AI.
The approach to data privacy (and all related aspects) is being upheld which these new technologies are being applied.

One of the Telenor efforts with regards ethical AI is participation in the EU-funded Horizon 2020 project application where the intention is to address scientific limits of AI systems and prioritize human-centered AI. This project focuses on how AI systems should allow humans to understand the reasons behind their decisions. Moreover it explores how AI researchers and practitioners using both data-driven and knowledge-based methods could guarantee safety, privacy and security of AI systems before deployment.

Wider issues relevant to the PDPA and privacy, security issues

1. Source of Thai law:

An unofficial English translation of the draft Personal Data Protection Law issued August/September is the reference (the draft referred to as the 'PDPA'). While as with all Thai laws, the official version is the original Thai version, the unofficial translation used is the best available source for current purposes. It is acknowledged that difference in meaning can occur through translation.

2. Harmony with other laws

A new draft Cybersecurity law has received considerable attention. One issue is whether it will have the effect of over-riding personal data rights.

Trust and confidence in administration is needed. How will the Personal Data Protection Commission be constituted? Will it be a government official heavy model, or will it be more consistent with a Multi-Stakeholder Model (MSM) style of governance, allowing more experts and private sector stakeholder. In the PDP context government is policy maker and user. In the Cybersecurity context, there are three roles:

Three Roles of Government	*What is should be*
Policy Maker, Rule Marker	Some critical infrastructure is in private hands. Needs multi-stakeholder model (MSM) of governance with private sector on board
User	Cybersecurity laws apply to all; Government actors should not be exonerated from complying with Personal Data Protection law or Cybersecurity law.
Operator of a Cybersecurity Command Centre	Direct management needs independence from policy making and independence from infra owners, but co-operation with private sector needed – MSM model.

3. The concept of Consultation

The organisers recommend good and meaningful consultation for any new laws or material changes to laws.

Article 77 of the Constitution lays out some basis for this, but by the nature of the Constitution, does not prescribe details. Details may be found in APEC's Good Regulatory Practices (GRP) and in the consultation practices of some economies. Consultation involves a number of steps, including: (i) feedback on a concept paper, (ii) issuance of a draft law, with explanation and feedback in two rounds of written submission with at least one public hearing, (iii) marked up changes with version and release date control, (iv) a regulatory impact assessment at an early stage in this process.

Good consultation educates user groups (business, individuals, government and civil society), and gets buy-in. Those participating may hire lawyers, economist, accountants, IT experts etc. Through buy in, user groups and the industry morally and intellectually 'owns' part of the law. Compliance and effective operation should thus be smoother.

The organisers commend the Ministry of Digital Economy and Society in particular the office of Permanent Secretary, for all efforts in arranging consultations.

4. APEC Privacy Framework

APEC (Asia Pacific Economic Co-operation) Privacy Framework dates from 2005[6]. It is a set of principles and implementation guidelines to establish effective privacy protections which avoid barriers to information flows, and ensure continued trade and economic growth in the APEC region. It relies on nine Information Privacy Principles. The Cross Border Privacy Rules (CBPR)[7] grew from the Privacy Framework.

Unlike the GDPR, which is a directly applicable regulation, CBPR is a voluntary system which does not displace or change domestic laws or regulations. IAPP has a useful comparison table [8]. One other notable difference is that CBPR applies to Controllers, not Processors whereas GDPR and PDPA apply to both. A participant (nation) must map its local law to the CBPR framework.

The APEC CBPR system requires participating businesses to develop and implement data privacy policies consistent with the APEC Privacy Framework. These policies and practices must be assessed as compliant with the minimum program requirements of the APEC CBPR system by an accountability agent. Once the PDPA becomes law, Thailand could join the APEC CBPR.

As IAPP notes, "The privacy enforcement authorities of a country that takes part in the system should have the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the CBPR program requirements" [9]

5. Some organisations involved in development of the personal data field

Internet & Jurisdiction Policy Network www.internetjurisdiction.net

Oxford Journal of International Data Privacy Law https://academic.oup.com/idpl

Thai Netizen Network https://thainetizen.org

International Association of Privacy Professionals https://iapp.org

APEC: Privacy Framework (originally published 2005), http://publications.apec.org/. Cross Border Privacy Rules www.cbprs.org

In Thailand, both JFCCT and EABC offer experience and advocacy in this area through their Digital Economy/ICT group.

[6] http://publications.apec.org/ with reviews and updates such as http://mddb.apec.org/Documents/2016/SOM/CSOM/16_csom_012app17.pdf
[7] www.cbprs.org
[8] https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules/
[9] See previous fn.

TABLE OF CONTENTS: PRIMER and BACKGROUNDER

PRIMER

BACKGROUNDER

Sponsored by

Telenor Group started more than 160 years ago as a national telecoms operator in Norway. It is one of the world's largest mobile telecommunications companies with operations in Scandinavia, Eastern Europe and Asia. Today Telenor has 172 million mobile customers across eight markets. Nine out of 10 of Telenor group customers are in Asia. www.telenor.com

Sponsored by

Based in Bangkok, DigiThai Software Group provides quality services to customers around the world. Because of our European core, we understand the new GDPR processes. DigiThai helps its customers identify, classify, discover, protect and profit from the data in their organizations, including biometrics data (fingerprints and face recognition metadata) and provide a range of IT related services. www.digithaigroup.com

Net Protection Concepts has been operating as system integrators in Thailand for more than ten years. Originally starting out as an IT security company NPC has evolved with specializations and expertise in network solutions, security & compliance (related to data in motion as well as data at rest), automation, messaging and analytics.

NPC partners with the industry's leading providers of proven technology such as Cisco Systems Inc. TIBCO Software Inc. and a few more.www.npc-international.net

Blackstone One is a cloud-based, fully automated, subscription model vulnerability scanner which uses automated remediation. www.blackstoneone.net

Data proliferation brings many new opportunities but also many downsides: more data breaches, more sophisticated cyber-attacks and more network management challenges. SentryWire detects intrusions, minimizes damage caused by breaches and enables packet level analysis of any incident, for as little as 20% of the cost of other systems, by providing up to months of authoritative packet capture history. Incident handling and forensic analysis starts with SentryWire. https://www.aximglobal.com/sentrywire.php

Supported By

Joint Foreign Chambers of Commerce in Thailand (JFCCT) www.jfcct.org

European Association for Business and Commerce (EABC)
www.eabc-thailand.org

Organised By

Thai-Swedish Chamber of Commerce – TSCC
www.swecham.com

Thai-Norwegian Chamber of Commerce - TNCC
www.norcham.com

Thai-Finnish Chamber of Commerce – TFCC
www.thaifin.org/

Danish-Thai Chamber of Commerce – Dancham
www.dancham.or.th