Thammasat Review of Economic and Social Policy
Volume 6, Number 1, January – June 2020

Received: 12 March 2020
Revised: 1 May 2020
Accepted: 2 May 2020

Thailand's Personal Data Protection Act: An Understanding from the Perspectives of the European Privacy Law

Tanatas Bumpenboon[1]
Senior Analyst
Bank of Thailand
tanatasb@bot.or.th

[1] The opinions expressed in this publication are those of the author. They do not purport to reflect opinions or views of the author's affiliation or its members thereof. The presentation of material herein does not necessarily imply the expression of any opinion whatsoever, in whole or in part, of the Bank of Thailand.

ABSTRACT

The Thai Personal Data Protection Act B.E. 2562 (2019) (PDPA) is Thailand's first omnibus law that governs personal data protection in Thailand. It is predominantly based on the General Data Protection Regulation (Regulation 2016/679 or GDPR) of the European Union that came into force in 2016. Hence, there are several similarities between the two.

As PDPA's practicality and enforceability remain largely untested in Thailand since its major operative provisions will come into effect in the middle of 2020. Thus, the author therefore compares PDPA with GDPR by investigating into GDPR and its applicability to determine best data protection practices for a company that deals with provision of financial services.

For personal data protection, PDPA and GDPR require satisfaction of one or more legal bases in order for a company to collect and process data of an individual. Obtaining consent is often seen as one method of this. However, the author finds that obtaining a consent is a key but – oftentimes – not necessary. There are several other legal bases that are as strong, if not stronger, than consent, e.g. contractual relationship and legitimate interests. Despite validity of legitimate interests as a legal basis, its coverage and applicability are not well-defined and yet conclusive. The company has to consider and evaluate individual experiences and expectations, along with industry best practices to carefully determine whether such legitimate interests have been realized and prudently balanced against individual rights.

Keywords: Laws, Privacy, Data Protection

JEL Classification: D82, G20, K20

1. Introduction

Disruption is an inescapable challenge for all industries and one of the most notorious is data disruption (Accenture, 2019).[2] The inexorable march of big data has been relentless and the trend is irreversible.[3] It is the new oil whose value has been realized and harvested in all possible avenues. All kinds of businesses – from online retailers to offline conglomerate wholesalers – are mining this wealth of information to better serve their customers and such data is considered the main pathway to succeed.

Inundated with data, financial services are no different. The impact of data on financial institutions can hardly be overestimated.[4] Financial data – ranging from bank transactions to online loan applications – convey messages to banks about what their customers are doing and what products are of their interests. Data analytics enhances banks' performance by improving how they segment, target, acquire, and lastly retain customers. It helps banks expand their customer bases and gain insight that may lead to further marketing opportunities, including new products, and new communication channels. For

[2] Some are tackling the so-called 'disruption challenge' very well; while others are not. Among top 10,000 companies, as much as USD 41 trillion in enterprise value is already exposed to disruption today.

[3] Today, more data is generated in a 24-hour period than ever before (IBM, 2017) and by 2025, it is estimated that 463 exabytes of data will be created each day globally (equivalent to 212,765,957 DVDs daily) (World Economic Forum, 2019). The influx and outflow of data are originated from many sources, including but not limited to, personal devices, internet of things (IoT), machine learning and artificial intelligence (AI).

[4] Just as cloud, the rise of IoT further explodes the amount of customer data gathered from networks of products; whereas the rise of open architecture (such as Open APIs) allows financial institutions to collect valuable data about their customers from data stored at other entities as well.

example, targeted and customized loan products for businesses with seasonal sales, predicted by big data models.

The paper is organized as follows. In the previous section I briefly outlined the background of data disruption, and demonstrated the extended benefits of big data, the phenomenon has challenged regulators to balance the said benefits with an appropriate level of data privacy right. Section 2 then recapitulates data privacy laws in the global context along with their developments and legal similarities (or lack thereof) among different jurisdictions. Section 3 focuses on the Thai personal data protection law and Section 4 highlights its major obligations, namely consent and validity of legitimate interests to collect and process data. The author delves into the same provisions of GDPR and attempts to explore GDPR's interpretation regarding those provisions. Multiple case laws and administrative rulings are examined to determine the extent to which the concept of consent and legitimate interests are put into use. Finally, the author summarizes the lessons learned from GDPR and offers a guidance for companies, and in particular, financial institutions, to navigate through this labyrinth of personal data protection laws.

1. Data Privacy Laws in the Global Context

Data privacy laws have never been as important as they are today. The number of privacy laws worldwide has grown from 20 in the 1990s to more than 100 at the present (Deloitte, 2015; UNCTAD, n.d.). Some countries have sectoral coverage. That is, different industries or economic sectors have their own data privacy laws. For instance, prior to 2019, the Thai Financial Institutions Businesses Act, B.E. 2551 (2008) (FIBA) governs major issues relating to data privacy that involves financial institutions, whereas the Thai Telecommunications Business Act, B.E. 2544 (2001) (TBA)

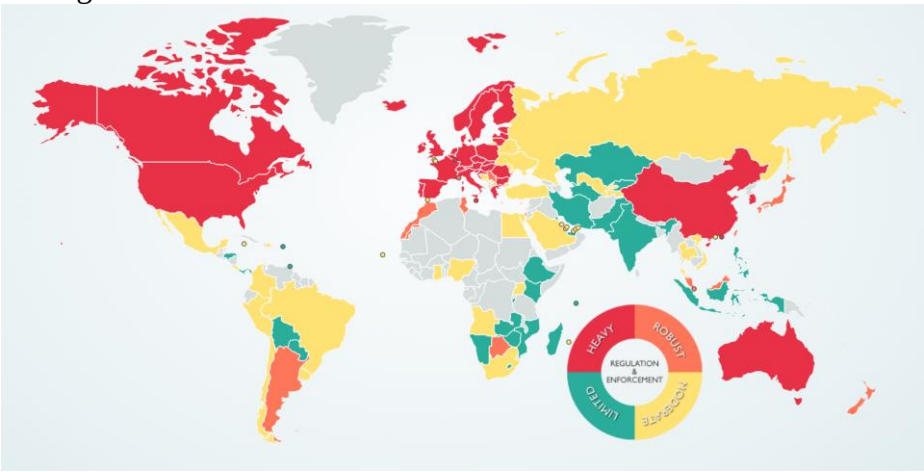
governs telecommunication data of individuals.[5] On the other hand, some countries have omnibus coverage, with a national data protection law in place of, or complementary to, provincial or sectoral regulations. In the global context, the paper primarily focuses on GDPR. It is the European new framework for data protection laws that replaced the previous 1995 omnibus data protection directive and aims to harmonize data privacy laws across Europe and be a governing law applicable to all member states. GDPR has fully come into force since May 25, 2018. It ensures that personal data can only be collected and managed under strict conditions.[6] Its obligations and implications toward data protection will be extensively discussed in Section 4.

While these data protection laws from different jurisdictions all benefit customers and preserve individual rights, there exist significant differences in beliefs and regulations concerning customer data around the world. These differences and their contrasting levels of rigidity burden companies who have to navigate through this labyrinth of inconsistency and, as things stand, will be one of the most challenging tasks going forward.

[5] The US has several sector-specific and some omnibus data privacy laws that are enforced by individual states. For example, the California Consumer Privacy Act of 2018 (CCPA) applies across all sectors and introduces an overarching privacy protection. However, its coverage – by nature of being a state law – is limited to within the state of California.

[6] As of 28 January 2020, the EU member states are also pushing reform on privacy regulation framework, the ePrivacy Directive. In the same fashion as GDPR, the proposed ePrivacy Directive ensures that all communications over public networks or electronic channels maintain respect for data privacy rights. It ensures that consent must be obtained before cookies are stored and used to enhance users' experiences in their computers.

Figure 1. Data Protection Law in Selected Jurisdiction



Source: DLA Piper, 2020

3. Personal Data Protection in Thailand

3.1 History of Personal Data Protection prior to 2019

Prior to 2019, before the Personal Data Protection Act, B.E. 2562 (2019) (PDPA), there was no single omnibus statutory law directly governing data privacy as well as the overarching issues of data protection in Thailand. However, the fundamental right to privacy has duly been recognized in the Constitution of Thailand while the general application of data protection and privacy is prescribed under the Civil and Commercial Code (CCC) and in some sectoral specific laws such as those governing financial services and telecommunication services.

The Constitution of Thailand codifies:

> Section 32. A person shall enjoy the rights of privacy ... Any act violating or affecting the right of a person … or exploitation of personal information in any manner whatsoever shall not be permitted, except by virtue of a provision of law enacted only to the extent of necessity of public interest.

The Constitution upholds the rights of privacy and the government could only deprive a person of stipulated rights pursuant to laws. The provision acts as a safeguard from arbitrary denial of rights by the government and balances interests of individuals whose rights were deprived of and public interests that the laws bring about.[7] However, for disputes among private entities and individuals, a court generally considers other bodies of laws – such as CCC or sectoral laws that impose specific obligations rather than the overarching concept in the Constitution (Decision of the Thai Supreme Court, 2015).

Among individuals, rights and duties of privacy including data privacy and data protection are applied through CCC under the principle of tort.

[7] The provisions are somewhat similar to those of the US Amendments, where no person shall be deprived of liberty – in this case privacy – without due process of law. For example, the US Supreme Court first recognized a zone of privacy in *Griswold v. Connecticut* that upheld marital privacy and struck down bans on contraception (Griswold v. Connecticut, 1965).
Pursuant to the Fifth Amendment and Fourteen Amendment of the US Constitution:

"No person shall be … nor be deprived of life, liberty, or property, without due process of law; …" (U.S. Const. amend. XIV)

"… No State shall make or enforce any law … nor shall any State deprive any person of life, liberty, or property, without due process of law; …" (U.S. Const. amend. XIV)

> Section 420. A person who, willfully or negligently, unlawfully injures the life, body, health, liberty, property or any right of another person, is said to commit a wrongful act and is bound to make compensation therefore.
>
> Section 421. The exercise of a right which can only have the purpose of causing injury to another person is unlawful.

Pursuant to CCC, when a company has a duty to maintain privacy and safeguard information of an individual, if the company fails to keep the information safe or fails to protect it from unauthorized access causing damages to the individual, the individual may bring a case against a company under CCC.

Aside from FIBA and TBA explained earlier, specific laws such as the Credit Information Business Act, B.E. 2545 (2012) (CIBA) also provide data protection and safeguard individual data rights with respect to credit information and credit-related financial activities. However, like FIBA and TBA, coverage of CIBA is limited to data regarding financial statuses and credit records from financial institutions and rights of individuals are restricted only to those stipulated therein. As a consequence, an individual is unable to exercise other rights *per se* that he is not entitled to. For example, pursuant to Section 25 of CIBA[8], an

[8] Section 25. For the purpose of protections given to the Owner of Information, the Owner of Information is entitled to: (1) right to know which of his or her Information is kept by the Credit Information Company; (2) right to check his or her Information; (3) right to request for correction of incorrect Information; (4) right to object when his or her Information is incorrect; (5) right to be informed the result of the checking of his or her Information within specified time; (6) right to know causes of refusal of the application for Credit or services from Financial Institution in the case that the Financial Institution uses Information of Credit Information Company as reason for refusal; (7) right to appeal to the Committee pursuant to Section 29 …

individual may not remove or withdraw his information from the credit bureau database since the law does not empower the individual accordingly (Decision of the Thai Supreme Court, 2009).

Despite the fact that several bodies of law are governing data protection and data privacy from different perspectives, attempts to enact an omnibus privacy law were made several times. In 2014, the Office of the Prime Minister first published the draft Data Protection Act in 2014 that provided criteria for collecting, using, and disclosing personal data. The 2014 draft granted personal data protection rights and established a Data Protection Committee. The draft underwent several rounds of changes and later was approved in principle by the Cabinet on 6 January 2015, but was further revised as proposed by the Council of State in May 2015. After several rounds of revision, in December 2018, the Council of State eventually approved the long-awaited draft Act and the National Legislative Assembly finally passed it into laws in 2019 (ETDA, 2020).

3.2 The Personal Data Protection Act, B.E. 2562 (2019) (PDPA)

PDPA is Thailand's first consolidated data protection law. It was published in the Thai Government Gazette on May 27, 2019 and has been in effect since May 28, 2019.[9] However, the main operative provisions on data protection and individual rights[10] will not come into force until after a one-year grace period from

[9] The unofficial English version of PDPA can be found here: https://www.etda.or.th/app/webroot/content_files/13/files/The%20Personal%20Data%20Protection%20Act.pdf

[10] Under Chapters 2, 3, 5, 6 and 7 and Section 95 and Section 96. Chapter 2: Personal Data Protection; Chapter 3: Rights of Data Subject; Chapter 5: Complaints; Chapter 6: Civil Liability; Chapter 7: Penalties and a few transitional provisions.

the publication date, i.e. May 27, 2020.[11] PDPA prescribes standards and practices on protection of personal data and issues relating to data privacy and imposes obligations on companies when collecting, using, and disclosing personal data.

4. Key Obligations and Practical Implications – from the Perspectives of GDPR

This section aims to delineate important aspects and illustrate key provisions of PDPA, which is largely based on GDPR. Most of GDPR's major provisions are considered new as there were no omnibus data protection laws in Thailand before. Hence, considering PDPA from the perspectives of GDPR will give companies, practitioners and individuals a better understanding on what implications PDPA could have on data protection and obligations that a company has to follow.[12]

Aside from analyzing GDPR to better understand PDPA, recognizing regional differences is equally important because customer data increasingly crosses sovereign boundaries. In the past, companies were often subject to regulation in a single jurisdiction (i.e. their domicile). Now they may need to account for their customers' locations, their storage centers, and data processing facilities when considering what

[11] As of April 22, 2020, due to the Coronavirus pandemic, the Digital Economy and Society Ministry is seeking to postpone enforcement of some of the main provisions under PDPA. Readers are advised to refer to official announcement or cabinet resolutions that may result in such delay or temporary suspension of PDPA. See more at https://www.bangkokpost.com/business/1905210/delay-mulled-for-personal-data-law-enforcement

[12] However, there are some provisions in PDPA that require further clarification by additional issuance of notifications and those secondary regulations. As a result, business practitioners and consumers are strongly recommended to keep updated.

regulations will apply to their activities. Particularly, for companies that engage foreign customers, process data internationally (including data of foreign entities processed domestically), or leverage multiple cloud-based service providers, identifying the appropriate jurisdictions may already be challenging.

The section then continues discussing the importance of obtaining relevant consent to proceed on data management. For businesses, it seems that obtaining valid customer consent ensures smooth and pleasant experiences for companies to manage customer data. However, it is unlikely the case that a company is capable of securing consent from all of its customers. That is, some of the customers might already lose contact with the company, while others might have established their relationship with the company long before PDPA was passed into laws. Hence, the company may need to rely on other legal bases to proceed with such customer data management. In this light, one of the less-rigid grounds that the company may turn to is 'legitimate interests'. Unfortunately, PDPA and the Thai juridical branch have not provided guidelines or court decisions on disputes relating to legitimate interests yet. Therefore, considering GDPR practices to gain an understanding on PDPA may provide the company with noteworthy insight, preparing and equipping the company with a greater understanding to duly collect and process customers' personal data.

4.1 Extraterritorial Jurisdiction

Jurisdiction is an aspect of state sovereignty, defined as juridical power and authority to hear, and adjudicate a dispute via exercising of relevant judicial power. Traditionally, domestic laws govern those who reside in a territory within a scope of sovereignity – not those outside, unless the laws

contain extraterritorial enforcement clauses. Therefore, by being a domestic law, PDPA *initially* applies to the collection, use, or disclosure of personal data by an entity[13] that is in Thailand regardless of where the collection, use or disclosure of personal data takes place.

Not only does PDPA enjoy its domestic application, it also extends its enforcement extraterritorially. PDPA's extraterritorial jurisdiction applies to entities outside Thailand under two circumstances: (1) the collection, use or disclosure of personal data are of individuals who are in Thailand, or (2) their activities relate to the offering of goods or services to or behavior of individuals in Thailand.[14] It is worth noting that PDPA specifically use the phrase 'in Thailand' rather than of the 'Thai nationality'. Therefore, PDPA also protects all individuals therein regardless of nationality. The extraterritorial application of GDPR takes the same approach. GDPR applies to the processing of personal data by companies established in the EU, regardless of whether the processing takes place in the EU. GDPR also applies if processing activities are related to the offering of goods or services to individuals in the EU or to the monitoring of behavior of individuals in the EU.[15]

One of the very first questions that a financial institution needs to carefully consider is whether PDPA is applicable to it. These extraterritorial jurisdictions warrant a thorough understanding to assess its applicability. In this light, PDPA formulates 3 layers to determine whether a company is subject to PDPA:

(1) is it located in Thailand?

[13] PDPA Section 6. An entity subject to PDPA under 2 categories: data controller and data processor.
[14] PDPA Section 5.
[15] GDPR Article 3.

(2) does it offer goods or services in Thailand?

(3) does it monitor behavior of individuals in Thailand?

Any affirmative statement to any question stated above means the financial institution is indeed subject to PDPA, which is applicable to most of the financial institutions in Thailand by nature. For a foreign bank located outside Thailand, consider a centralized function that conducts financial surveillance for fraud or Anti-Money laundering and Counter Terrorism Financing (AML/CFT) or an ordinary marketing material that seeks customer information. Pursuant to PDPA's extraterritorial application, if that foreign bank engages Thai customers, manages or monitors data of Thai residents (or any entity in Thailand), the bank will be subject to PDPA. Also, if that foreign bank is located in the EU, given its location and GDPR's intra-territorial enforcement, it must satisfy GDPR as well. On the other hand, a Thai bank that uses data of EU residents is likewise extraterritorially subject to GDPR; and because it is a Thai incorporated company, it needs to domestically comply with PDPA as well. Hence, many financial institutions, in particular those that conduct businesses internationally, will be subject to various data protection laws from different jurisdictions depending on their coverage, groups of customers, and data collected.

As a case in point, the Canadian company, AggregateIQ Data Services Ltd (AIQ), was issued a warning by the United Kingdom's (UK) Information Commissioner's Office (ICO).[16] AIQ was involved in targeting political advertising on social media to individuals whose information was supplied to them by various political parties and campaigns. After an

[16] The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. It exercises supervision on GDPR and domestic laws relating to data protection.

investigation by ICO, AIQ was found not to have adequately complied with GDPR.[17] However, the most interesting point about this dispute is that although AIQ is based in Canada, the UK's ICO still exercised its jurisdiction over AIQ that processed data of individuals in the UK and ruled that AIQ must erase all the personal data relating to UK individuals obtained without appropriate GDPR legal bases.

4.2 Legal Grounds

PDPA and GDPR share similar principles. That is, all personal data must be collected and processed *lawfully*, *fairly* and in a *transparent* manner.

Fairness and transparency mean that personal data shall be collected only to the extent necessary.[18] This does not mean that data collected has to always be essential. Rather, it must be a targeted and proportionate way of achieving the purpose taking into account of quantity and manner of data collected. Hence, neither is it sufficient nor reasonable to contend that data processing and data collecting are necessary because a company is operating in a particular way. In other words, the question is whether data collecting and data processing are necessities for the stated purpose, not whether it is a necessary part of the *business's choice* of method for pursing that purpose (ICO, n.d.).

On May 16, 2019, the Lithuanian Data Protection Supervisory Authority (VDAI) fined MisterTango, an

[17] Among others by: (1) not processing personal data in a way that the data subjects were aware of, (2) not processing personal data for purposes for which data subjects expected, (3) not having a lawful basis for processing, (4) not processing the personal data in a way for which it was originally collected, and (5) not issuing the appropriate fair processing information to those.

[18] PDPA Section 22 and GDPR Article 6.

electronic payment service provider for over EUR 61,500. The charge was for the lack of implementation of data minimization, disclosing personal data, and failing to report a breach. MisterTango processed more data than necessary to achieve its purposes, which was to carry out customer payments. In addition to the personal data necessary for the transaction,[19] the company also superfluously collected information on (1) dates of provision of unopened electronic invoices, their senders and amounts; (2) dates, topics and texts of unread notifications; (3) purposes, types, amounts of the loans; (4) names of the pension funds, accumulated units and amounts, value thereof; and (5) types of credits, due balances, amounts and dates of payments, numbers of the issued payment cards and amounts in such payment cards (VDAI, 2019).

One of the most interesting aspects in this decision is that VDAI issued its finding without assessment of the market practice within the payment industry, although there was no indication that the ruling would change if it did so. It simply indicated that MisterTango collected and processed excessive – and unnecessary – data in relation to executing the payments. Hence, the rule of thumb is to keep data collecting and data processing to the extent necessary and proportionate to the purpose a company aspires to achieve.

In addition to being fair and transparent, collection and processing are *lawful* only if a company possesses a lawful basis under relevant provisions, which are similar under both PDPA and GDPR.[20]

[19] such as customer's name and family name, ID, account number, currency, purpose of the transaction and it's code where applicable,

[20] PDPA defines personal data – to be protected – as any information relating to a person, which enables the identification of such person, whether directly or indirectly, but not including the information of deceased persons. Differing from the GDPR, PDPA does not specifically

In summary, a company may not collect, use, or disclose personal data without appropriate consent unless:

(1) for purpose relating to preparation of historical documents, research, or statistics, in which appropriate safeguard is put in place;

(2) for suppressing danger to a data subject's life;

(3) when processing is necessary for the performance of a contract;

(4) for the performance of a task carried out in the public interest by the data controller the achievement of the purpose relating to public interest research and statistics;

(5) for the legitimate interest of the data controller where such interest does not override those of the data subject; or

(6) is necessary for compliance with a law to which the data controller is subjected.[21]

Deciding which lawful basis applies is critical to ensure that data is lawfully collected and processed – and subsequent rights of individuals thereafter. A company must determine a lawful basis before starting to process personal data and it is important to be confident of the company's pick of the basis for the first time.[22] If the company finds that the chosen basis was inaccurate, it may be difficult to simply swap to a different one, even if a different basis could have actually applied from the start (ICO, n.d.).

address IP addresses, cookie identifiers and radio frequency identification tags as online identifiers that may be considered as personal data, such as IP addresses, cookie identifiers, and radio frequency identification tags.

[21] PDPA Section 24 and GDPR Article 6.

[22] No one basis should be considered always better, safer or more important than the others. Also, the company does not need to choose only one basis. More than one basis is allowed.

In Greece, PriceWaterhouseCoopers Business Solution SA (PWCBS) was fined EURO 150,000. The Hellenic Data Protection Authority (HDPA) held that PWCBS was responsible for failing to ensure of lawful, fair and transparent processing of its employees' personal data. Although PWCBS successfully obtained consent from its employees, HDPA ruled that their consent was invalid for two reasons: (1) PWCBS actually relied on other bases – not consent; and (2) consent was not freely given, regardless. HDPA clarified that the choice of consent as the legal basis was inappropriate, as the processing of personal data was directly linked to the performance of employment contracts, and was in compliance with its *legal obligation* to ensure smooth and effective operation of the company – warranting any other legal bases but not consent. Nevertheless, it had failed to notify the employees about those other legal bases, leading employees to misconstrue that their data processing was carried out under their consent. Furthermore, PWCBS failed to prove that consent was freely given providing the fact that there was significant imbalance of power between parties, one was an employer and the others were employees (Hellenic DPA, 2019).

Although PDPA does not specifically spell out 'lawfulness, fairness and transparency' like that of GDPR[23], such overarching principle appears throughout. Similar to GDPR, subsequent swap of legal basis to collect and process customer data is likely prohibited under PDPA as it requires that a company shall inform an individual of the purpose of the collection for use or disclosure of the individual data, including the purpose which is permitted without the individual's consent.[24] Therefore, even if a company does not

[23] GDPR Article 5(1)(a).
[24] PDPA Section 23.

need to obtain consent from an individual under certain legal bases, the company still needs to inform the individual of the purpose the individual's data is being use in any case.

4.2.1 Consent

As mentioned earlier, collecting and processing personal data are generally prohibited, unless it is expressly authorized by law under appropriate legal grounds, or an individual has consented to such collecting and processing. Consent *per se* allows companies to do just about anything with the individual data as long as it is considered valid and legitimately obtained. As a result, PDPA and GDPR specifically set out a high standard for consent as consent is one of several legal bases to collect and process data.[25] Pursuant to GDPR[26],

> … '[C]onsent' 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 …
>
> [Consent] should be given by a clear affirmative act ... This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent …
>
> In order to ensure that consent is freely given, consent should not provide a valid legal ground … where there is

[25] PDPA Section 19; GDPR Article 4 and its preamble.
[26] GDPR Preamble (32 and 43), Article 4.

> a clear imbalance between the data subject and the controller …

Unlike GDPR, PDPA does not provide definition of consent. However, it set out requirements on what a valid consent should be, which is quite similar to that of GDPR.[27]

> A request for consent shall be explicitly made … unless it cannot be done by its nature. In requesting consent from the data subject, the Personal Data Controller shall also inform the purpose of the collection, use, or disclosure of the Personal Data. Such request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an easily accessible and intelligible form and statements, using clear and plain language, and does not deceptive or misleading to the data subject in respect to such purpose. … In requesting consent from the data subject, the Data Controller shall utmost take into account that the data subject's consent is freely given…

In terms of consent, comparing to PDPA, GDPR provides clearer guidance as it requires that consent must be unambiguous and involve a clear affirmative action (an opt-in). It specifically prohibits pre-ticked opt-in boxes.[28] On the other hand, PDPA is silent on whether a 'boilerplate' consent form (sometimes include a pre-ticked opt-in consent) is valid as long as other requirements are satisfied. For example, the question remains on validity of a boilerplate consent provided under a clear manner, distinguishable from other matter, freely given, using plain and clear language.

For example, regarding financial institutions, the Bank of Thailand has issued the Notification on market conduct

[27] PDPA Section 19.
[28] GDPR Preamble (32)

allowing disclosure of customer data to other entities for marketing purpose as long as certain conditions are met. Among others, a bank must clearly notify customers that the disclosure is for marketing purposes. It must inform customers a list of recipients of data so that the customers can decide whether they will give their consent. The Notification further allows the bank to update a list of recipients of data to include additional parties but it must honor rights of the customers to *decline* the disclosure of data, and to raise their objection. That is, it is worth noting that that customers' consent is considered given to the disclosure of data if the customers do not raise any objection within the specified timeframe. Yet, there must be a process to ensure that the customers have been aware of that request (The Bank of Thailand Notification No. SVG. 1/2561, 2018).[29]

Nevertheless, both PDPA and GDPR requires that consent must be freely given. That is, a simple consent is not sufficient unless it is also proven that it is freely given. For example, consent of individuals in the context of employment relations cannot always be regarded as freely given due to the clear imbalance between the parties, namely the employer and the employees (Hellenic DPA, 2019).[30]

In 2019, Google LLC was fined EUR 50 million by the Commission Nationale de l'Information et des Libertes of

[29] The Bank of Thailand releases and updates Notifications from time to time. Therefore, it is recommended to keep the information up to date as the Bank of Thailand Notification, No. SVG. 1/2561 (2018), Re: Regulations on Market Conduct is released in 2018 before PDPA is enacted in 2019.

[30] Also, in Sweden, the Swedish Data Inspectorate fined a high school in the country after it trialed the use of facial recognition technology to monitor student attendance. The regulator determined that the school was responsible for processing sensitive personal data unlawfully. Although the consent is obtained, that that consent was invalid because there was an imbalance in power in the relationship between the school and its students.

France (CNIL) for various failings under GDPR. Pursuant to GDPR, consent must be sufficiently informed, specific, and unambiguous. It must also be granular (as separated from other parts of agreement and as requiring separate consent for separate things)[31] and obtained through a form of active acceptance. CNIL held that individual consent was not freely given. It was pre-opted in as it was a pre-ticked box. In addition, individuals were not given enough information about what their consent would mean in terms of the Google services they have been offered, why Google processed their personal data, and how long their data was kept. CNIL further clarified that it was not entirely the case that the information was not there. Rather, the ruling attacked accessibility of the information. That is, most of the information was there, but it was scattered via various different links (CNIL, 2019).

For consent, best practices for companies, and in particular financial institutions, are to ensure it is easy for customers to fully understand what the companies are doing with their data. A financial institution often requires customers to release their personal data to help them provide services. In most cases, a part of customer data is used for such services but other parts may be used for cross-selling other products and developing models for other uses. As previously mentioned, the company – financial institution included - may not collect, use, or disclose personal data without appropriate consent unless it is exempted by other legal bases. It follows that obtaining valid consent seems to be one of most viable ways to gain access to customer data. Therefore, a comprehensive privacy notice should be clear and concise, easily understandable, and be as accurate as possible about what data are being collected and why they are being used.

[31] Vague or blanket consent is not sufficient.

To further ensure that consent is freely given, the financial institution must avoid creating impression that there is imbalance in negotiation power between the customer and the financial institution. One suggested solution is to let the customer sign the notice or the agreement acknowledging that he is not forced into disclosing his personal data that is not directly related or considered unnecessary to the services or product he receives. Many financial institutions include a clause allowing the customer to refuse disclosing his data and that will not have any impact of his receiving of products and services. Lastly, the financial institution should inform customers of all legal bases they rely on for processing such data as well, as subsequently switching legal bases *ex post facto* will be considered unfair and misleading thus opposing the principle of accountability and transparency of PDPA.[32]

4.2.2 Legitimate Interests

PDPA and GDPR set a high standard for consent yet it is a common misconception that consent is required for all data processing. PDPA and GDPR lay down a principle that consent is appropriate if only companies can offer individuals

[32] For instance, consider a case where a financial institution decided to process customer data on the basis of consent, and obtained consent from individuals. An individual subsequently decided to withdraw their consent, as is their right. Even the financial institution could have originally relied on other legal grounds, it could not do so at a later date. It should have made clear to the individual from the start that there were other grounds to process such data as well, regardless whether consent was given. Leading the individual to believe that they had a choice was inherently unfair if that choice would be irrelevant. This could be done by obtaining consent and also simply indicating that the financial institution also possessed other legal grounds to process individual data. However, by failing to inform the individual of other legal bases, the financial institution may not process the individual data when the individual withdrew consent thereafter.

real choice and control over how they want their data to be used. As mentioned earlier, if a company cannot offer a genuine choice, consent will not be appropriate, and will not be considered legally valid. Consequently, requesting consent in such case is misleading and deemed unfair. Nevertheless, a company may not need consent if it can find other lawful bases as consent is not considered inherently better or more important than other alternatives. That is, if consent is difficult to obtain, a company may consider other alternatives.

Among those six legal bases,[33] the ground of legitimate interests seems to be the least self-explanatory, and, at the same time, a less-rigid basis that a company may turn to in the case that it fails to obtain consent.

> Pursuant to Article 6(1)(f) of GDPR,
> Processing shall be lawful if … [it] is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Similar provisions are also found in PDPA,[34]

[33] (1) for purpose relating to preparation of historical documents, research, or statistics, in which appropriate safeguard is put in place;
(2) for suppressing danger to a data subject's life;
(3) when processing is necessary for the performance of a contract;
(4) for the performance of a task carried out in the public interest by the data controller the achievement of the purpose relating to public interest research and statistics;
(5) for the legitimate interest of the data controller where such interest does not override those of the data subject; or
(6) is necessary for compliance with a law to which the data controller is subjected.

[34] PDPA Section 24.

> The Data Controller shall not collect Personal Data without the consent of the data subject, unless: … it is necessary for legitimate interests of the Data Controller or any other Persons or juristic persons other than the Data Controller, except where such interests are overridden by the fundamental rights of the data subject of his or her Personal Data …

A company can consider legitimate interests of its own, or any third party, including wider benefits to society (ICO, n.d.). However, both PDPA and GDPR balance their broad coverage of legitimate interests by weighing them with rights of individuals. To assess whether data processing will be lawful under this basis, the proposition can be broken down into a three-part test: *(1) Purpose test, (2) Necessity test, and (3) Balancing test* (ICO, n.d.; The Law Society, 2019; UCL, n.d.).

The purpose test requires that a company must pursue legitimate interests. A wide range of interests may be classified as legitimate interests. They can be a company's own interests or the interests of third parties, commercial interests as well as wider societal benefits. According to ICO, legitimate interests may be compelling or trivial. However, the more trivial they are, the more they will be considered overridden by individual rights in the balancing test (ICO, n.d.).[35] GDPR specifically provides a few cases whereby the uses of data are considered serving legitimate interests including: the processing of personal data to prevent fraud, to carry out direct marketing activities, to undertake internal administrative purposes, or to ensure network and information securities.

[35] Balancing test will be discussed later.

> … The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest. …[36]

> … Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. …[37]

> The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security … constitutes a legitimate interest of the data controller concerned.[38]

The necessity test means that the processing of data (in terms of manner and quantity) must also be a targeted and proportionate way of achieving the purpose. The processing will not be deemed necessary if there is another reasonable but less intrusive way to achieve the same result (UCL, n.d.). The test is very much aligned with the principle of GDPR, where data collecting and data processing must be carried out to the extent necessary.[39]

The Hungarian data protection authority (NAIH) levied a EUR 3,100 fine against a Hungarian financial institution for unlawfully rejecting a customer's request to have his phone

[36] GDPR Article 47.
[37] GDPR Article 48.
[38] GDPR Article 49.
[39] See also Section IV(2) Legal Grounds.

number erased after arguing that it was in the company's legitimate interest to process this data in order to enforce a debt claim against the customer. Applying the necessity test to assess whether there was legitimate interest, NAIH ruled that the customer's phone number was not necessary for the purpose of debt collection since the creditor could also communicate with the debtor by post. Keeping the superfluous phone number of the debtor therefore violated the principles of data minimization and purpose limitation, failing the necessity test as a result (NAIH, 2019).

NAIH also ruled that Tax IDs may not be used as client identifiers, since the practice was – similar to the collection of phone number – a violation of the GDPR's data minimization principle. In its ruling, the NAIH held that private entities can only process tax IDs with consent of the client or to fulfil their obligations to the tax authority, therefore also failing the necessary test (NAIH, 2019).

The principle of necessity is discussed in the N26 case from Germany. N26 is a German neobank (mobile bank) started as a FinTech and fully launched as a bank in 2016. N26 had collected and processed personal data of all former customers; some of them are proceeded without permission. The bank acknowledged that it had retained data relating to all former customers in order to maintain a blacklist, so that it would not make a new account available to these persons, safeguarding against money laundering. The Berlin Commissioner for Data Protection held that N26's practice of collecting and process personal data was illegal as the practice was beyond what considered necessary and not proportionate. In order to prevent a new bank account from being opened, only data of individuals who were actually suspected of money laundering should only be kept – not those of all former customers. (Berliner Beauftragte für Datenschutz und Informationsfreiheit, 2018)

The balancing test weighs a company's so-called legitimate interests against an individual's interests. What is challenging for the balancing test is individuals have distinguished interests that are subject to their characteristics, experiences, and relationship with a company. Hence, legitimate interests are more likely to be justified when a company uses data that an individual would reasonably expect and practically foresee and that have a minimal privacy impact. Where there is an impact on individuals, legitimate interests may still apply if a company can show there are even more compelling benefits to the processing and the impact on individuals is to the degree acceptable. In particular, if the individual would not reasonably expect the company to use data in a certain way, or it would cause the individual unwarranted harm, it is likely that the individual's interests would override those legitimate interests of the company (ICO, n.d.). It follows that pure economic interests or convenience are not considered legitimate interests and therefore cannot override the interests of the customer, in any case. (NAIH, 2019). In order to rely on legitimate interests to lawfully disclose personal data to a third party, the company should consider why the third party wants the information, whether the third party actually needs it, and what the third party will do with it (ICO, n.d.). Similarly, a company needs to demonstrate that the disclosure is justified, whereas the third party will be responsible for determine its lawful basis for its own processing (ICO, n.d.).

Equipped with data through customers' inquiry and customers' self-disclosure, a financial institution should avoid using legitimate interests if it is using personal data in ways that its customers do not understand and would not reasonably expect them being used (or if it thinks some customers would object if they are aware of its usage). The bank should also avoid this basis for data processing if it could cause

unwarranted harm, unless it is confident there is nevertheless a compelling reason to do so that justifies the impact.

5. Conclusion and What to Expect in the Future

The pinnacle of PDPA and GDPR is that data must be collected and processed lawfully, fairly and in a transparent manner. Obtaining consent provides a strong legal basis to collect and process data as it puts individuals in control, building trust and engagement. Valid consent should be considered a genuine customer-centric data management best practice. However, consent is appropriate if and only if a company can offer people real choice and control over the company's use of data. One major factor to determine validity of consent is therefore whether the consent is freely given. In order to be considered freely given, a company must take into account of an individual's understanding of consent language, scope, and clarity. In addition, consent will not be considered freely given if there is a clear imbalance of power between the individual and the company.

Consent is one lawful basis for collecting and processing data, but there are several alternatives. If obtaining consent is difficult, a company may turn to other legal grounds. Legitimate interests seem to be one of the lesser-rigid grounds to collect and process data as legitimate interests can be a company's own interests, a third party's interests, or as broad as other societal interests. Determining whether the company can rely on legitimate interests generally depends on the three-part test. That is, a company can claim legitimate interests when collection and processing of individual data are necessary for the purposes, and when comparing to interests, rights and freedom of an individual, there is sufficient overriding interests for the company to collect and process data.

Financial institutions in Thailand are beginning to feel the effect of either PDPA or GDPR – or in many cases, both – on their routine operations. PDPA and GDPR are comprehensive and omnibus in nature, and it would be easy to get overwhelmed by its reach and complexity. That said, the basic pillars of data protection remain. Data belongs to an individual – not a company. The individual possesses data rights – not the company.

One of the guiding principles to navigate through GDPR and PDPA is that the company should adopt approaches that incorporate privacy practice *by design and by default.* Privacy by design simply means that privacy should be a foundation of any systems, business processes and company products. It follows that a financial institution should design and provide an individual with a product that does not invade his or her privacy. Hence, the product should not require the individual's inputs of data that are deemed unnecessary for the product. Neither should it monitor other transactions nor unreasonably keep personal information of the individual for an extended period of time without legitimate interests.

In addition, privacy by default assures that a company should adopt practices that assume an individual will want to preserve the privacy of his or her information. Similarly, it follows that a financial institution should honor the principle of fairness and transparency. All of the consumer choices provided by the financial institution should be privacy-preserving by default, without the individual having to request. Email addresses, by default, should not be used for marketing and should not be shared with other companies without affirmative customer consent.

Finally, as regulations that focus on business processes that continuously change and evolve over time, PDPA and GDPR will likely necessitate a company to incorporate privacy by design and privacy by default into the company's

DNA, one that represents professional values and beliefs held by the company's executives and all of its personnel. Therefore, one of the best practices to encourage privacy by design and by default may begin with a simple step such as employee training and awareness raising. Appropriate tone at the top that prioritizes legitimate uses of customers data may be considered as a major driving force to increase customer trust overall.

References

Accenture (2019). Breaking through disruption. Retrieved from https://www.accenture.com/_acnmedia/thought-leadership-assets/pdf/accenture-breaking-through-disruption-embrace-the-power-of-the-wise-pivot.pdf

Bank of Thailand Notification No. SVG. 1/2561. (2018). Regulations on Market Conduct.

Berliner Beauftragte für Datenschutz und Informationsfreiheit. (2018). *Datenschutz und Informationssicherheit.* Retrieved from https://www.zaftda.de/tb-bundeslaender/berlin/695-tb-lfd-berlin-2018-ohne-drs-nr-vom-28-03-2019/file

Commission Nationale de l'Informatique et des Libertés (2019, January 21). Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC. Retrieved from https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf

Deloitte (2015). *Big Data: Mining a National Resource.* https://www2.deloitte.com/xe/en/pages/about-deloitte/articles/no-place-like-home/big-data.html

DLA Piper (2020). *Data Protection Laws of the World.* https://www.dlapiperdataprotection.com/

Electronic Transactions Development Agency (2020, May 11). Knowledge Sharing of Personal Data Protection [Thai]. Retrieved from https://www.etda.or.th/content/personal-data-protection-by-etda

Griswold v. Connecticut, 381 U.S. 479 (1965).

Hellenic Data Protection Authority (2019). Summary of Hellenic DPA'S Decision, 26/2019. Retrieved from https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/DECISIONS/SUMMARY%20OF%20DECISION%2026_2019%20(EN).PDF

IBM (2017). *Big data solutions.*

Information Comissioner's Office (n.d.). *Guide to the General Data Protection Regulation (GDPR).* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

The Law Society (2019, August 5). *Legitimate interests*. Retrieved from https://www.lawsociety.org.uk/support-services/practice-management/gdpr/gdpr-for-solicitors/legitimate-interests/

National Authority for Data Protection and Freedom of Information (2019). Hatarozat, NAIH/2019/2526/2 [Hungarian]. Retrieved from https://www.naih.hu/files/NAIH-2019-2526-2-H-hatarozat.pdf

State Data Protection Inspectorate (VDAI) (2019, May 16). Įmonės atsakomybės neišvengs – Lietuvoje skirta ženkli bauda už Bendrojo duomenų apsaugos reglamento pažeidimus [Lithuanian]. Retrieved from https://www.ada.lt/go.php/lit/Imones-atsakomybes-neisvengs--lietuvoje-skirta-zenkli-bauda-uz-bendrojo-duomenu-apsaugos-reglamento-pazeidimus-/1

Decision of the Thai Supreme Court, 5372/2552 (2009).

Decision of the Thai Supreme Court, 4893/2558 (2015).

U.S. Const. amend. XIV. (n.d.). The United States Constitution (Fourteenth Amendment).

University College London (n.d.). *Practical Data Protection Guidance Notices*. https://www.ucl.ac.uk/data-protection/guidance-staff-students-and-researchers/practical-data-protection-guidance-notices/legitimate

United Nations Conference on Trade and Development (n.d.). *Data Protection and Privacy Legislation Worldwide.* https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

World Economic Forum. (2019). *How much data is generated each day?* Retrieved from https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/