TDRI Quarterly Review, Vol. 38 No. 2 (June 2023): 3-16.

PREPARING TO DEAL WITH PERSONAL DATA PROTECTION MEASURES IN PLATFORM BUSINESSES*

*Khemmapat Trisadikoon***

The personal data collected is significant to platform businesses as part of their use of big data. In business, the more business owners know about consumers, the better they can offer products and services that meet their needs. However, the desire for data to respond to consumer needs may lead businesses to overlook or not give sufficient attention to personal data protection measures. Traditional personal data protection measures may need to respond adequately to current platform regulations and oversight of personal data use.

This article explains the impact of using personal data in platform businesses and proposes guidelines for regulating and overseeing the use of personal data in platform businesses.

1. INTRODUCTION

The rapid growth of platform businesses in the past 10 years has created unprecedented wealth in human history due to the large-scale economic environment of many related companies, the use of artificial intelligence (AI) technology in business operations, and the use of big data to meet consumer demand. These factors have led to platform businesses growing economically more than traditional businesses. At the same time, this has created challenges different from those traditional businesses.

2. THE ECONOMY OF PLATFORM BUSINESSES AND THE USE OF PERSONAL DATA

In the past decade, global platform businesses have grown tremendously. In 2021, among the top 10 companies with the highest market value in the world, seven of them were digital platform companies,[1] which increased from just one in 2006.[2] In the context of Thailand, the market value of digital platform businesses has continuously grown from 18 billion baht in 2015 to 900 billion baht in 2021, with digital platforms playing a significant role in the e-commerce industry with a trade value

** Summary and additional information from Somkiat Tangkitvanich and others, The Study on Impact and Regulatory Policy Proposal of Digital Platform in Thailand (Office of the National Higher Education, Science, Research, and Innovation Policy Council, 2022).*

*** Mr. Khemmapat Trisadikoon is Senior Researcher, Law for Development, Thailand Development Research Institute; email: khemmapat@tdri.or.th.*

[1] *Statista, The 100 largest companies in the world by market capitalization in 2022 [online], accessed April 30, 2023, from www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/.*

[2] *The Economist, The rise of the superstars [online], accessed April 30, 2023, from www.economist.com/special-report/2016/09/15/the-rise-of-the-superstars.*

of approximately 600 billion baht, accounting for 8 percent of the total retail trade. The online advertising market is worth approximately 20 billion baht, accounting for 20 percent of the total advertising market. The value of food delivery through apps is approximately 50 billion baht, accounting for 8 percent of the entire food industry.[3] As can be seen, the expansion of platform businesses has greatly benefited the economy, as mentioned above. On the other hand, it has also raised concerns about the potential impact of platform business practices, including using personal data.

At present, platform businesses have been collecting and using a large amount of users' personal data for profiling purposes in order to offer products and services that meet the needs of users. This is particularly true for businesses that offer free services, in which case users may provide their personal data in lieu of payment. In some cases, the service providers not only do not charge for the services, but also provide some benefits in exchange for users providing personal data to the platform or consenting to the use of their personal data for the platform's benefit.

Platform businesses have been collecting and using many users' data for profiling purposes to offer products and services that meet users' needs; this is particularly true for businesses that offer free services, in which case users may provide their data instead of payment. In some cases, the service providers not only do not charge for the services but also provide some benefits in exchange for users providing personal data to the platform or consenting to use their data for the platform's benefit.

The reason why consumers are not yet aware of the excessively low cost of privacy is due to information asymmetry between businesses and consumers. Consumers are not sure exactly what personal data the business is collecting and how the collected data will be used, including whether appropriate measures are in place to prevent leaks, resulting in an underestimation of the cost. In addition, companies may take advantage of consumer behavior biases that seek to avoid the difficulty of reading lengthy and complex documents or notifications, and may not adjust the default settings, fully allowing them to collect data.

In addition, the low-cost evaluation of personal data also includes not considering the impact of disclosing personal data on others (data externality), which can be both positive and negative.[4] This means that information about a consumer's purchase of a product or service can indicate the possibility of another group of consumers purchasing similar products and services. However, the latter group of consumers may not provide information about their preferences for these products and services.

The key issue in protecting personal data on business platforms is balancing the use of data for business benefits and preserving the data subject's privacy.

[3] *Prichart Chokkerd, Food delivery in 2021 had a total value of over 50 billion baht, expanding over 24% year-over-year [online], accessed April 30, 2023, from https://brandinside.asia/k-research-analysis-on-food-delivery-expand-in-2021/; and Brandinside, Restaurant businesses in 2022 face high risk and must be small-sized to reach customers and be highly flexible in order to have a chance to survive [online], accessed April 30, 2023, from https://brandinside.asia/restaurant-business-2021/.*

[4] *D. Bergemann, Bonatti, A. and Gan, T. (2022), The economics of social data. The RAND Journal of Economics, 53: 263-296. Accessed from https://ssrn.com/abstract=3459796.*

3. CHALLENGES IN PROTECTING PERSONAL DATA IN PLATFORM BUSINESSES

In Thailand, the challenge of protecting personal data in platform businesses lies outside the law, as Thailand has enacted the Personal Data Protection Act of 2019 based on such principles as the General Data Protection Regulation (GDPR) of the European Union. However, the challenge of protecting personal data in platform businesses lies in enforcing data protection laws. There are at least three challenges in protecting personal data in platform businesses, which are as follows:

3.1 Communication guidelines with consumers on the Internet

Communicating with consumers is essential in enforcing personal data protection. Generally, laws and guidelines for regulating the use of personal data require businesses that use personal data to communicate transparently and not burden consumers excessively. This involves providing information about collecting, using, and disclosing personal data and requires communication to be friendly toward consumers. The problem that arises is that some companies intend to disclose details about the use of data with language that is lengthy and difficult to understand, forcing consumers to spend a long time understanding it, or block some content on their websites to force consumers to give consent to the use of tracking technology, which is called a "cookie wall."

In addition, this unfriendly communication may result in consumers not paying attention and granting businesses access to personal data without caution or consent, especially in the current era, where some platform applications have expanded to become "super apps," performing multiple activities on the same platform.

3.2 Appropriate measures to prevent data leakage

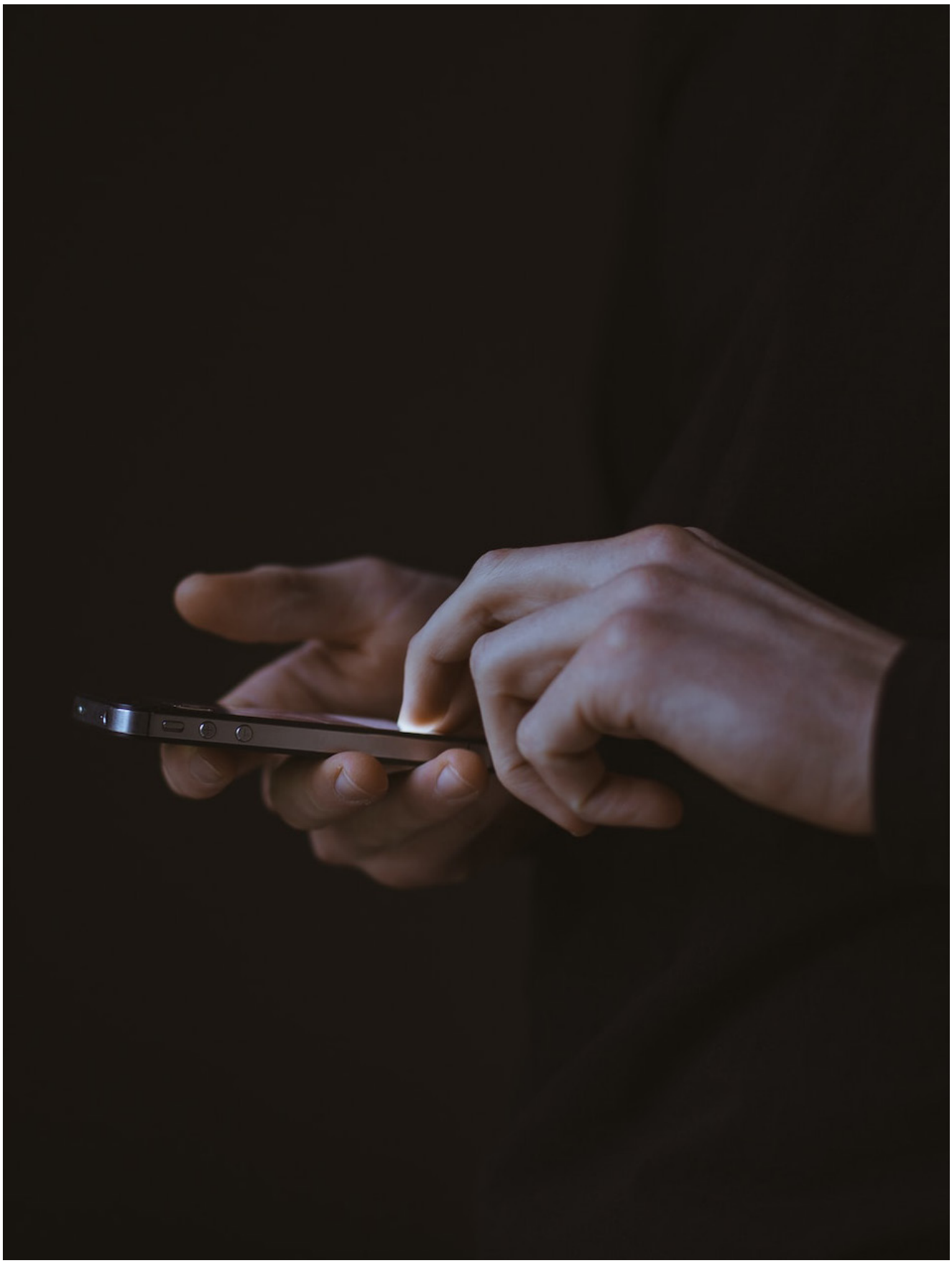
Appropriate measures to prevent data leakage are becoming more of a concern in Thailand. At the same time, it may be difficult for consumers to understand and evaluate the appropriateness of a company's storage methods. This is partly due to the need for more standards for protecting personal data.

3.3 Non-compliance with cross-border personal data protection laws

Platforms often transmit data across borders, which may result in inadequate personal data protection due to lower data protection standards in some countries. The Japanese Internet company LINE Corporation has been investigated for providing consumer data to partner companies in China without notifying consumers as required by law. In addition, Chinese laws grant authorities, especially security agencies, extensive power, with lower levels of personal data protection than in Japan.[5] Therefore, the problem of non-compliance with cross-border personal data protection laws needs to be addressed, and guidelines should be established for platforms transmitting data across borders.

The challenges in all three aspects are essential issues that need to be studied, with solutions put forward to address these problems.

[5] *Nikkei Asia, Line silently exposed Japan user data to China affiliate [online], accessed April 30, 2023, from https://asia.nikkei.com/Business/Companies/Line-silently-exposed-Japan-user-data-to-China-affiliate.*



4. PERSONAL DATA PROTECTION UNDER THAI LAW

Thailand enacted the Personal Data Protection Act of 2019 as a general law for protecting personal data for various organizations, including platform businesses. The law is based on models such as the GDPR of the European Union, and its content is more than 70 percent similar to that regulation.[6]

The principle of this law is to create responsibility, transparency, and fairness toward the owners of personal data throughout the process of collecting and using data. It assigns duties to organizations that collect data (referred to as data controllers under the law), starting from clearly stating the purpose of collecting and using personal data, setting the principles of collecting personal data to the extent necessary and not exceeding the purpose that has been communicated to the data owners, ensuring the security of personal data, and deleting personal data when they are no longer necessary. Companies are responsible for monitoring and creating channels for data owners to exercise their rights under the law.

One more thing is that this law has defined the responsibilities of not creating excessive burdens for personal data owners in collecting and using personal data. That is, the law provides guidelines for collecting and using personal data legally, without requiring consent as the only method of collecting and using personal data, but the law acknowledges the use of personal data that is consistent with daily life activities, such as collecting and using data from contracts,[7] or collecting or using personal data by considering the balance between the rights of personal data owners and the benefits of the company (legitimate interest).[8] These guidelines are accepted to be fair and not to create excessive burdens for personal data owners compared with collecting data by requesting consent, which may have negative consequences for personal data owners from collecting personal data without reason. This may also create opportunities for violating the rights of personal data owners in cases where the company may use broad and unclear language to request consent.

In addition, the law provides data subjects with certain rights to manage and control their data. These include the right to be informed about the collection, use, and disclosure of personal data, the right to access personal data to ensure its accuracy, and the right to withdraw consent or object to processing personal data. As the data controller, the company must comply with these rights, which can lead to the cessation of the collection, use, and disclosure of personal data.[9]

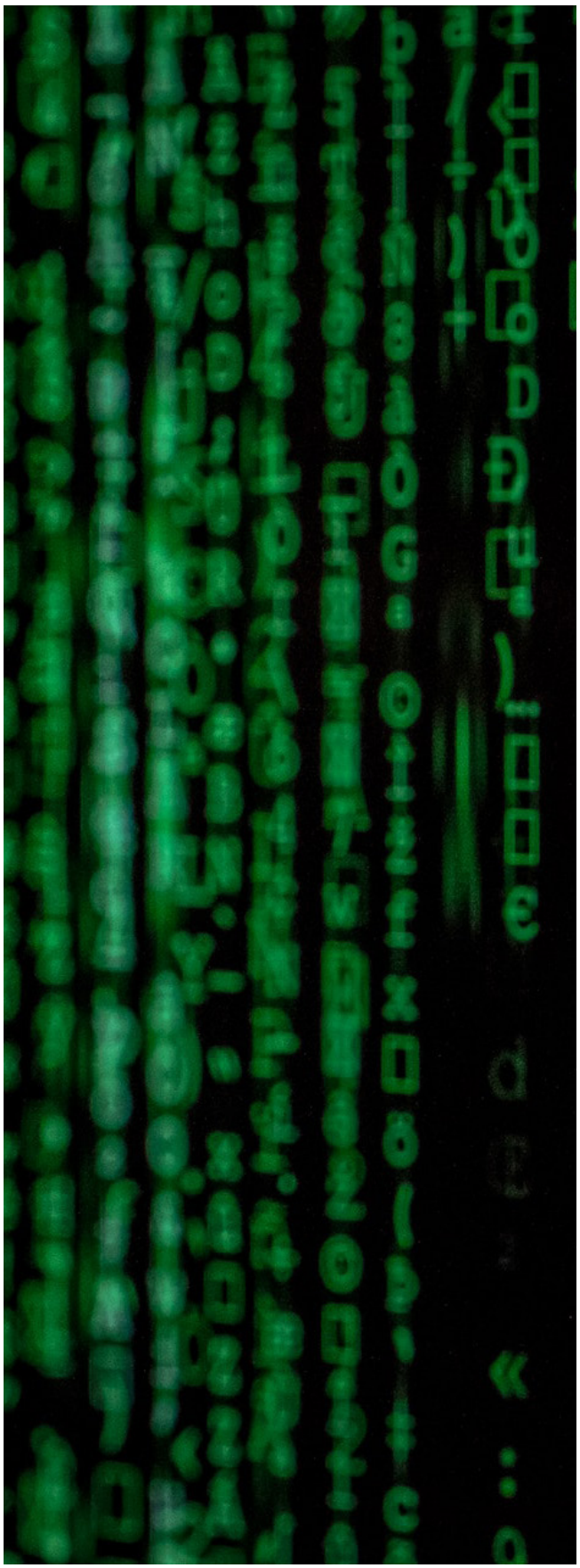
One important aspect that this law stipulates is expanding the scope of law enforcement to cover actions outside of the country or jurisdiction (extraterritoriality scope) to protect the movement of personal data to other countries and prevent loopholes in the protection of personal data. This can be achieved by requiring the destination country

[6] *Alexis Kateifides and others, Comparing Privacy Laws: GDPR v. Thai Personal Data Protection Act [online], accessed April 30, 2023, from https://www.dataguidance.com/sites/default/files/gdpr_v_thailand_updated.pdf.*

[7] *Personal Data Protection Act of 2019, Section 24 (3).*

[8] *Ibid., Section 24 (5).*

[9] *See Personal Data Protection Act of 2019, Section 19, Section 23, Section 30, and Section 34.*



or company to have a standard of personal data protection equivalent to that under Thai law. In addition, the law also requires companies that use the personal data of Thai people but need offices in Thailand to appoint a representative to communicate with the supervisory agency. If these companies violate the law, they should be punished accordingly.

However, when examining Thailand's readiness to enforce the law, the law has only established criteria rules for data protection for just five issues, and there are only two guidelines related to data protection (see the table below). This is relatively minimal, raising concerns that the law may not adequately protect the right to privacy. One reason is that the Personal Data Protection Act of 2019 has only recently been enacted after a two-year delay in enforcing the law.[10]

[10] *The Act came into effect on June 1, 2022; see the Royal Decree specifying the agencies and businesses that are not subject to the Personal Data Protection Act of 2019 (Second Amendment) of 2021.*

Table: Criteria rules and guidelines announced by the Personal Data Protection Commission (PDPC) (as of February 2023)

Regulations concerning PDPC Office and Commission	
1.	Regulations of the PDPC on the Criteria for Qualifications of Officers and Personnel Under the Personal Data Protection Act
2.	Regulations of the PDPC on the Specification of Identification Cards for Officers Under the Personal Data Protection Act
3.	Regulations of the PDPC on the Criteria and Procedures for Selecting the Chairman and Qualified Commission Members of the Conduct Commission for the PDPC Office
4.	Regulations of the PDPC on the Criteria and Procedures for Selecting the Chairman and Qualified Commission Members of the Supervisory Commission for the PDPC Office (Second Amendment)
5.	Regulations of the PDPC on the Criteria and Procedures for Selecting the Chairman and Qualified Commission Members of the Supervisory Commission for the PDPC Office
Regulations on Established Criteria Rules for Data Protection	
1.	Regulations of PDPC on the Exemption of the Record of Processing Activities for Small and Medium-sized Enterprise Data Controllers
2.	Regulations of the PDPC on the Criteria and Methods for Creating and Maintaining Records of Activities Related to the Processing of Personal Data by Data Processors
3.	Regulations of the PDPC on the Measures to Ensure the Security of Data Controllers
4.	Regulations of the PDPC on the Criteria for Considering the Administrative Fine of Expert Commission
5.	Regulations of the PDPC on the Submission, Non-acceptance, Termination of Consideration, and Time Limit for Considering Complaints
Guideline form PDPC	
1.	Guidelines for Obtaining Consent from Data Subjects Under the Personal Data Protection Act of 2019
2.	Guidelines for Notifying the Purposes and Details of Personal Data Collection from Data Subjects Under the Personal Data Protection Act of 2019

Source: Somkiat Tangkitvanich and others.

The problem arising from the lack of adequate data protection standards is that some private companies may take advantage of personal data without being accountable to the users, or some companies may need adequate data security systems. Meanwhile, individuals whose personal data has been violated may not be aware of the damage incurred immediately or may need more resources and expertise to conduct their investigation, leading to a lack of compensation for any damage suffered from the breach.

In addition, if we consider specifically platform businesses that collect and use personal data intensively, there are at least four urgent concerns as follows:

4.1 Transparent and ethical collection and use of personal data for consumers

There is a trend for platforms to collect an enormous amount of personal data. However, some businesses may have detailed and hard-to-understand privacy notices and block access to specific website content until the consumer agrees to use tracking technology (cookie wall). In addition, platforms are also trending toward expanding their business across different industries by sharing personal data among companies within the same group. For example, a food delivery platform may expand its business by providing loans using the drivers' income data as a database for loan services. This raises concerns about whether such data usage is beyond the stated purposes or without the consent of the individuals.[11]

At present, although the Personal Data Protection Commission has guidelines for informing the purposes and details of collecting personal data from data subjects, as well as guidelines for obtaining consent from data subjects under this Act, the practices are focused on positive behaviors rather than negative ones to be avoided. For example, using personal data collection technology or tracking user behavior on websites and applications such as cookies does not emphasize the sharing of data among companies in the same group, which should have guidelines to promote transparency in the collection and use of personal data.

4.2 Security and prevention of personal data leakage

The platforms store a large amount of consumer data, but some may need appropriate measures to ensure security, leading to data breaches. Although there are currently guidelines for data security, these guidelines provide only a framework and factors to consider in maintaining data security. There are no recommended methods or technologies to ensure clarity for businesses.[12]

4.3 Cross-border transfer of personal data

The platform may transfer personal data to companies and countries that do not have the same level of personal data protection as Thailand.[13]

[11] *See Somkiat Tangkitvanich and others, The Study on Impact and Regulatory Policy Proposal of Digital Platform in Thailand (Office of the National Higher Education, Science, Research, and Innovation Policy Council, 2022), pp. 76-80.*

[12] *See Regulations of the PDPC on the Measures to Ensure the Security of Data Controllers.*

[13] *Other countries and areas, such as the European Union, have announced reliable "Whitelist" names. This clarifies which countries can send personal data through certified and supervised agencies.*

4.4 Exemption from enforcing personal data protection laws in government agencies

On July 5, 2022, the Cabinet drafted a royal decree that would exempt the enforcement of the Personal Data Protection Act of 2019[14] for government agencies using personal data. The royal decree would not apply to government agencies that collect and use personal data for national security or public interest purposes. However, this exemption could create many exceptions and potentially have adverse impacts on the privacy protection standards for Thai citizens, which differ from those of other countries. Transferring personal data from other countries to Thailand may challenge digital businesses.

The abovementioned issue reflects the problem of enforcing the Personal Data Protection Act of 2019 in Thailand, particularly in digital platform businesses. To bridge this gap, Thailand should study the principles of personal data protection and experiences from other countries. This guideline will help improve the regulation and supervision of personal data usage on digital platforms within the country.

5. GUIDELINES FOR THE PROTECTION OF PERSONAL DATA AND INTERNATIONAL EXPERIENCE

Under this topic, we shall consider approaches to protecting personal data in other countries, both in terms of legal principles and experiences related to protecting personal data in platform businesses in different countries.

5.1 Principle of data protection

The key objective of personal data protection is to balance consumers' right to privacy and the business benefits derived from using personal data, as well as national security. There are three regulatory models for personal data protection: the first emphasizes responsibility toward data subjects, the second allows companies to pursue business benefits freely, and the third prioritizes national security through state control.[15]

The first model emphasizes creating accountability toward the owner of personal data. An example of this type of law is the GDPR of the European Union and United Kingdom, which prioritize the privacy rights of data subjects. Businesses and government agencies that benefit from personal data are responsible for implementing appropriate measures to protect personal data and enable the owner of personal data to easily exercise their rights in managing personal data, including understanding the purposes of data collection and use, refusing to allow the use of personal data, requesting the transfer of personal data, or requesting the deletion of personal data.[16]

[14] *Thai Government, Summary of the news from the Cabinet Resolution on July 5, 2022 [online], accessed April 30, 2023, from www.thaigov.go.th/news/contents/details/56572?fbclid=IwAR3urkjQeTG60Xuu0gDYBT6rBmBityC30hJwHTtQncP8bEmGGPfCz30DdrA.*

[15] *Martina Francesca Ferracane and Erik van der Marel, Regulating Personal Data: Data Models and Digital Services Trade, p. 6 [online], accessed April 30, 2023, from https://openknowledge.worldbank.org/server/api/core/bitstreams/0b4562ce-777f-567b-8247-9441ec24a26c/content.*

[16] *Information Commissioner's Office (ICO), How do we comply with the cookie rules? [online], accessed April 30, 2023, from https://ico.org.uk/for-organisations/guide-topecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/.*

In addition, GDPR has also attempted to balance personal data use with the data subject's rights. The law may exempt certain rights of the data subject for collecting and using certain types of personal data. For example, data subjects may not be able to request deletion or refuse the use of personal data that is necessary for government tax agencies to comply with tax laws or for collecting personal data to prevent or control epidemics such as COVID-19, or for verifying financial data of suspected persons involved in terrorism or money laundering.[17]

However, these exemptions do not lead to the exemption of the overall protection of the rights of all state agencies. For instance, state agencies responsible for tracking and preventing the spread of COVID-19 still must prevent personal data from being leaked and cannot use such data for other purposes. They also must take other measures as specified in the GDPR.[18]

Another aspect is that GDPR allows private companies to collect and use personal data without explicit consent if it does not violate the data subject's privacy rights too much. For example, they collect cookies necessary for website performance.[19]

The second model is the freedom of disclosure, allowing companies to seek business benefits freely. An example is the United States, where the federal and state governments have almost no laws protecting personal data that specify the company's responsibility and the data subject's rights. Companies can benefit from personal data without consent and use such data for purposes not notified to consumers in advance. Meanwhile, the data subject may claim damages for privacy violations citing consumer protection laws that do not specifically address data protection.[20] This situation may result in inadequate protection for the data subject. However, some states, such as California and Virginia, have begun to enact data protection laws like GDPR.[21]

The third model is the state's control of personal data activities, which prioritizes national security. An example is China, which enacted the Personal Information Protection Law (PIPL) in 2021 to protect personal data. However, the law grants authority to state officials to access private sector databases for reasons related to national security without complying with personal data protection

[17] *European Data Protection Supervisor (EDPS), EDPS Survey on Covid-19 related processing activities by EUIs [online], accessed April 30, 2023, from https://edps.europa.eu/system/files/2022-03/22-03-03_covid_survey_rreport_en.pdf; and Data Protection Act 2018, Schedule 1.*

[18] *Ibid.*

[19] *ICO, What are the rules on cookies and similar technologies? [online], accessed April 30, 2023, from https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-the-rules-on-cookies-and-similar-technologies/#rules9.*

[20] *The data protection system in the United States is a "patchwork system" that lacks a central law but relies on multiple laws at both the federal and state levels, and is dispersed in laws that regulate branch-specific businesses. See Khemmapat Trisadikoon, A Study of the Necessity of and Approaches to the Preparation of Personal Data Protection Guidelines [online], accessed April 30, 2023, from https://tdri.or.th/wp-content/uploads/2022/07/Volume-37-Number-2-June-2022.pdf.*

[21] *See Office of the Attorney General, California Consumer Privacy Act (CCPA) [online], accessed April 30, 2023, from https://oag.ca.gov/privacy/ccpa; and Sarah Rippy, Virginia passes the Consumer Data Protection Act [online], accessed April 30, 2023, from https://iapp.org/news/a/virginia-passes-the-consumer-data-protection-act/.*

measures.[22] There have been observations about the behavior of the Chinese government accessing consumer data and various algorithms from platform companies such as Tencent, Alibaba, and ByteDance, which owns the TikTok application.[23]

In addition, the Chinese government tends to tighten control over personal data in response to the activities of private companies that may affect the state's security. Previously, the Chinese government was concerned about registering Didi Global. This ride-hailing app collects screen image data from more than 12 million users, including the recording of facial images of more than 107 million users. By entering the United States stock market, the app would have to disclose information to the United States government, which would have impacts on the Chinese government's stability.[24]

From all the above, the Thai companies' approach to balancing the use of personal data with privacy rights following the GDPR guidelines seems appropriate. Furthermore, in the context of the current global landscape, most platforms are trying to adapt to the GDPR's privacy protection standards of the European Union. The GDPR of the European Union has legally binding provisions that extend beyond the European Union's borders to safeguard its citizens. To safeguard personal data, exporting it to countries or companies that have lower standards than the European Union is restricted unless consent or supportive measures are acquired. If data protection standards fall below those set by the GDPR, it will increase business costs.[25]

5.2 International experience

Two foreign experiences are worth studying: the case studies of the European Union and the United Kingdom. These countries have implemented the GDPR, which is a principle-based regulation. It requires companies to have measures to ensure processing security without specifying any methods or techniques. Each private company can design privacy protection measures appropriate to its business, considering costs and available technology, which allows for flexibility in work while still protecting the privacy rights of personal data owners. At the same time, the law can adapt to changing situations and technologies.

The essential factors that lead to successful law enforcement are using "soft laws" and self-regulation mechanisms, such as developing guidelines and codes of conduct that provide principles, application guidelines, good examples, and behaviors to avoid that could violate the law. However, these tools do not have a legal status that requires strict adherence to their excellent examples, which allows companies to choose measures that

[22] *See Xu Ke and other, Analyzing China's PIPL and how it compares to the EU's GDPR [online], accessed April 30, 2023, from https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr/*

[23] *Annabelle Liang, Chinese Internet giants hand algorithm data to government [online], accessed April 30, 2023, from https://www.bbc.com/news/business-62544950.*

[24] *Eva Dou and Pei-Lin Wu, China fines Didi $1.2 billion for breaking data-security law [online], accessed April 30, 2023, from https://www.washingtonpost.com/world/2022/07/21/china-didi-fine-data-security/. In addition, this measure has also been certified as a prohibition on companies collecting or using such data in Article 10 of the PIPL law.*

[25] *Marco Luisi, GDPR as a Global Standards? Brussels' Instrument of Policy Diffusion [online], accessed April 30, 2023, from https://www.e-ir.info/2022/04/09/gdpr-as-a-global-standards-brussels-instrument-of-policy-diffusion/.*

comply with their principles and develop appropriate measures for their business characteristics.

The advantage of using these tools is that they create clarity in complying with the law and interpretation and serve as preliminary guidelines on how law enforcement agencies think. Ensuring transparency and fairness in collecting and using personal information is crucial, along with establishing standards for maintaining security and transferring data across borders. It is particularly essential for businesses operating on a platform.

The European Data Protection Board has issued 55 guidelines and is currently listening to feedback on another 11 guidelines.[26] Drafting these guidelines involves a consultation process and public hearing to receive input and suggestions for improvement from companies that may request further clarity or may have conflicting opinions.

An example practice of platform businesses is collecting data unfairly through a "cookie wall," which is an obstacle that blocks access to website services created by companies. This obstacle disappears only when users consent to use cookie technology to collect and track their behaviors. To obtain consent for cookies, companies must avoid using a cookie wall as it is illegal. Instead, they can explore other ways to obtain consent following correct practices.[27]

Data protection supervisory authorities also support the private sector in developing business ethics. This is done by allowing the private sector to develop their business ethics and having the supervisory authorities review and approve them. An exciting example of business ethics is the EU Cloud Code of Conduct, which protects personal data on European cloud systems. Supervisory authorities in Belgium support this. Leading cloud service providers, including companies in the Alibaba Cloud and Google Cloud platforms, have signed up to comply with this code of conduct. These guidelines and standards ensure data security on the cloud and give clear direction on preventing data breaches for digital platform businesses that store data on their own cloud systems or third-party service providers.[28]

Apart from using tools to comply with the law in the private sector, based on the experience of GDPR enforcement in the European Union, another critical issue is the role of regulatory agencies that need to work proactively. More than self-regulation alone is needed to protect personal data because companies have incentives to benefit from personal data, while the cost of accessing and verifying consumer data breaches is relatively high. Therefore, to help consumers, regulatory agencies must investigate and monitor business sector activities using personal data. For example, the Office of the Data Protection Commissioner of Ireland investigated cross-border data transfers of the TikTok app. This investigation was proactive without any complaints, but the committee assessed the risk of data transfer between countries because a Chinese company owns the app. The data were

[26] *Data as of February 2022.*

[27] *Guidelines 05/2020 on consent under Regulation 2016/679.*

[28] *See EU Cloud Code of Conduct, Alibaba Cloud adheres to the EU Cloud Code of Conduct [online], accessed April 30, 2023, from https://eucoc.cloud/en/detail/alibaba-cloud-adheres-to-the-eu-cloud-code-of-conduct; and Google, EU Cloud Code of Conduct [online], accessed April 30, 2023, from https://cloud.google.com/security/compliance/eu-cloud-code-of-conduct.*

sent to a country with weaker data protection laws, so the company may have to increase its efforts to protect it. In addition, the committee is concerned about the processing of personal data of children under 18 and the problem of verifying the age of individuals under age 13, which may not comply with GDPR.[29]

Another example is the British Information Commissioner's Office (ICO), which has studied the impact of using AdTech on user privacy. For instance, collecting user data and behavior from various sources to create user profiles for personalized advertising may lead to inappropriate use of such data or presenting products or services that may harm consumers. The problem with this type of technology is that data collect from multiple sources, such as "third-party cookies," make it difficult to attribute responsibility to the data controller or processor.[30] As a result, ICO has consulted with the Interactive Advertising Bureau (IAB UK) and marketing platforms to improve the privacy-friendliness of AdTech.[31]

In addition, regulatory agencies should provide opportunities for businesses to consult and negotiate, such as in the case of ICO collaborating with Google to develop a privacy sandbox on the Android system to develop targeted advertising techniques that are privacy friendly. The office provided legal advice and assistance.[32] Developing under this regulatory sandbox mechanism would enable businesses to innovate while protecting consumer privacy at the same time.

6. SUGGESTIONS FOR LEGAL IMPROVEMENTS

In protecting personal data in platform businesses, the government and the Personal Data Protection Office should maintain a balance between protecting the privacy rights of consumers and the business benefits and national security. This should be based on international standards to facilitate data transfer across borders and appropriate practices should be implemented. The government and the Personal Data Protection Office should take the following actions:

(1) Enforce the law according to the principles of the Personal Data Protection Act of 2019, maintaining a balance between the privacy rights of consumers and the business benefits and national security, like the GDPR of the European Union, which will be the global standard in the future.

(2) Repeal the exemption of personal data protection law for government agencies that would adversely affect the privacy rights of the public and platform businesses in the country.

---

[29] *Data Protection Commission, Irish DPC submits Article 60 draft decision on inquiry into TikTok [online], accessed April 30, 2023, from https://www.dataprotection.ie/en/news-media/irish-dpc-submits-article-60-draft-decision-inquiry-tiktok-0.*

[30] *ICO, Update Report into Adtech and Real Time Bidding [online], accessed April 30, 2023, from https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf.*

[31] *IAB UK, IAB UK's response to ICO's adtech and real time bidding: Update Report [online], accessed April 30, 2023, from https://www.iabuk.com/news-article/iab-uks-response-icos-adtech-and-real-time-bidding-update-report.*

[32] *ICO, ICO's Opinion on Data Protection and Privacy Expectations for Online Advertising Proposals [online], accessed April 30, 2023, from https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/02/ico-statement-on-the-google-privacy-sandbox/.*

(3) Accelerate the promotion of self-regulation of good platform businesses by issuing guidelines and encouraging the development of business ethics, particularly urgent issues, such as:

- Accelerating the development of practices regarding the proper notification of privacy and consent for the use of data storage technology, monitoring user behavior on websites and applications, as well as the practice of using data in addition to the first purpose that reports for platforms that expand cross-sector operations by sharing data between companies within the group, which the Office of the Personal Data Protection Committee may clarify by preparing examples of different situations where consent or behavior should or should not be required consent.
- Supporting the development of security and prevention ethics for preventing data leaks for large platforms, or maybe certified by international ethics for data protection on cloud systems in the European Union.
- Developing practices for evolving company policies and protective measures when sending data to countries with lower protection standards than Thailand.

(4) Conduct aggressive monitoring of the operations of platforms that may pose high risks to consumer privacy, such as checking platforms that are expanding into "super apps" to see if they share data among companies within the conglomerate correctly and examining platforms that may transfer data to destination countries with lower protection standards than Thailand. The office may conduct aggressive inspections by using algorithms that the platform businesses use.

(5) Open opportunities for platform business companies to receive consultation from the Office of the Personal Data Protection Commission for discussion between platform business companies using the "regulatory sandbox" supervision method to allow platform business companies to innovate while considering the privacy rights of data subjects.