

Individual Control over Alternative Credit Data via Notice-and-Consent Mechanism under the Thai Personal Data Protection Law

Kriengsak Areejitkasame

Individual Control over Alternative Credit Data via Notice-and-Consent Mechanism under the Thai Personal Data Protection Law^{*}

Kriengsak Areejitasame^{**}

Abstract

The purpose of this research paper is to find an effective way to provide the data subject with proper individual control over personal information via notice-and-consent mechanism in the processing of alternative credit data under the Thai personal data protection law.

This study employed a qualitative research method by (1) reviewing the origin, legal concept, and practice of the protection of personal data by providing the data subject with individual control over personal information via notice-and-consent mechanism; (2) examining the criteria and elements in law that determine notice-and-consent mechanism relating to the processing of alternative credit data; and (3) analyzing and evaluating whether the Thai personal data protection law properly provides the data subject with individual control over personal information via notice-and-consent mechanism in the processing of alternative credit data by comparing the Thai law with international measures, frameworks, laws, and relevant cases.

^{*}The research article is a part of dissertation “Protection of Alternative Credit Data: A Comparative Legal Analysis.” This dissertation has been approved by a graduate school as partial fulfillment of the requirement for the Doctor of Philosophy in Economic Law Program at Shanghai University of Finance and Economics. Professor Song Xiaoyan is an advisor. Professor Shen Wei, Professor Liao Zhimin, Professor Wu Wenfang, Professor Hu Yuan, and Associate Professor Liu Yang are examiners.

^{**}Student in Doctor of Philosophy in Economic Law Program, Shanghai University of Finance and Economics, Shanghai, China. E-mail: kriengsakareed@hotmail.com

Received 23 March 2022, Revised 2 May 2023, Accepted 23 May 2023.

This study found that (1) the legal concept of granting individual control over personal information, especially via notice and consent has long been playing a key role in information privacy law, and widely adopted in credit process; (2) the processing of alternative credit data presents the risks of failure to inform, lack of freedom to choose and decide, and improper reuse and repurpose that undermine individual control; (3) although the Thai Personal Data Protection Act (PDPA), 2019 (B.E. 2562) has provided fair individual control over personal information relating to alternative credit data processing, it still has certain limitations, including inflexible and impractical notice and consent, and lack of clear guidance on subsequent use of personal data. This study, therefore, recommends the relevant Thai authorities to impose stricter requirements under the PDPA or issue financial regulations that focus on the data subject's understandability, establish greater resilient, substantive, and consumer-centric notice and consent, and ensure the controller's accountability.

Keywords: individual control over personal information, notice-and-consent mechanism, processing of alternative credit data

1. Introduction

At present, personal data protection law focuses on protecting personal data by providing individual control over personal information particularly via notice-and-consent mechanism. Personal data protection law requires financial institutions collecting alternative credit data to provide notice and consent by offering the data subject to read the privacy policy containing terms and conditions of personal data processing, and request for consent from the data subject. The legal concept underlying this approach is to give individual control over one's own information.

The collection, use and disclosure of alternative credit data also mainly rely on notice-and-consent mechanism. Alternative credit data in this study refers to any non-traditional data that the lender uses for an assessment of the borrower's potentiality and willingness to pay back loans, including such data as utility payment, mobile usage, geolocation, social network analysis, etc. These alternative credit data normally cover sensitive personal data that requires careful treatment and safeguards; otherwise, the unauthorized or improper use of such data can undermine the data subject's fundamental rights and freedom.

Although the approach of providing individual control over personal information has been widely adopted in the collection of personal data, including alternative credit data, literature found deficiencies of such approach. Studies focusing on evaluating approaches to empower the data subject's control especially via notice and consent in the US or EU data protection law, found that this approach cannot truly provide control owing to individual's lack of informed and rational choices, and structural problems from too many companies collecting and using personal data.¹ Besides, individual cannot give free and informed consent because of the complexity,

¹Daniel J. Solove, "Privacy self-management and the consent dilemma," *Harvard Law Review* 126, 7 (May 2013): 1880-1881.

long-period retention, implication of the volume of big data, and the passive role of consent and that sum of individual decisions may not benefit the society as a whole.²

Furthermore, there has not been literature analyzing and evaluating the criteria and elements of individual control over personal information relating to the processing of alternative credit data under the Thai legal personal data protection framework. The existing Thai literature mostly focused on general legal problems of data protection, or traditional credit data under the credit information business law, including the scope of credit information that should be expanded to reflect the borrower's creditworthiness,³ the misuse of credit information in employment,⁴ general principles, and scope of personal data and sensitive data in the protection of personal data in the financial and banking sector.⁵

This study, therefore, attempts to examine the legal criteria and elements that determine individual control over personal information especially via notice-and-consent mechanism under the Thai personal data protection law with a primary focus on the processing of alternative credit data. This study proposes modifications to the legal concept of individual control over personal information under the Thai personal data protection law and suggests amendments to the Thai law in order to properly provide proper individual control over personal information in the processing of alternative credit data. It recommends that notice-and-consent mechanism under the PDPA be supplemented by transparency and understandability requirement as a prerequisite, as well as the elements of flexibility, practicality, and consumer focus.

²Robert H. Sloan and Richard Warner, "Beyond notice and choice: Privacy, norms, and consent," **Journal of High Technology Law** 14, 2 (March 2013): 370-414.

³Wilairat Y., "Problems on "Credit Information" under the Law Relating to Credit Information Business," (M.A. thesis, Thammasat University, 2017), p. 100.

⁴Srichola S. and Tipayanee P., "Legal Issues Related to Credit Information on the Use of Credit Information for Other Purposes," **DPU Graduate Studies Journal** 4, 3 (March 2016): 215-226.

⁵Khaosanit D., "Legal Measures in Private Data Protection : Case Study in Finance and Banking of Commercial Bank," (M.A. thesis, Dhurakij Pundit University, 2018), p. 111.

2. Objective

This study attempts to find an effective way to properly provide the data subject with individual control over personal information via notice-and-consent mechanism in the processing of alternative credit data under the Thai personal data protection law.

3. Methodology

By employing qualitative research, regarding whether the existing Thai personal data protection legislation provides proper individual control over personal information via notice-and-consent mechanism in the processing of alternative credit data, this study (1) reviewed the origin, legal concept, and practice of the protection of personal data by providing the data subject with individual control over personal information via notice-and-consent mechanism; (2) examined the criteria and elements in law that determine notice-and-consent mechanism relating to the processing of alternative credit data; and (3) analyzed and evaluated whether the Thai personal data protection framework properly provides the data subject with individual control over personal information via notice-and-consent mechanism in the processing of alternative credit data. It employed comparative legal analysis of the Thai law and foreign personal data protection measures, frameworks, and laws among the most influential international and regional developments, including the Council of Europe (CoE), Organization for Economic Co-operation and Development (OECD), Asia-Pacific Economic Cooperation (APEC) as well as privacy laws and regulations in the European Union (EU) and the United States (US), which are regarded as international and regional norms of conduct for information privacy. The evaluation and comparative results were further combined and analyzed to propose modifications to the relevant legal concept and also make recommendation for amending the Thai personal data protection legislation. The examined materials include technical reports, literature, legal texts, international frameworks and measures, textbooks, and law cases and data protection authorities' decisions, both in Thailand and foreign countries.

4. The Legal Concept of Providing Individual Control over Personal Information

4.1 Privacy and Personal Data Protection as Individual Control Over Personal Information

Several authors give a definition of privacy as individual control over personal information. Warren and Brandeis' definition of privacy as the right to one's personality is deemed as the cornerstone of data protection as the right to privacy as control over personal information.⁶ In addition, Alan Westin and Parent also have similar views on privacy protection. Alan Westin similarly defined privacy as the ability to determine for ourselves when, how, and to what extent information about us is communicated to others.⁷ Later, William Parent defined privacy as not sharing unrecorded personal information with others, and Parent emphasized that privacy is a moral value for those who value freedom and individuality.⁸ For Parent, personal information is the fact that most people do not want to reveal about themselves, such as salary, sexual orientation or health. Parent assumed that documented personal information, such as in public publications or court records, is considered a public record that should not be considered privacy invasion at any time. Fried also discussed that privacy "is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves".⁹ Meanwhile, Miller described privacy as "the individual's ability to control the circulation of information relating to him".¹⁰

⁶Samuel D. Warren, Louis D. Brandeis "The right to privacy," **Harvard Law Review** 14, 5 (December 1890): 193-220.

⁷Alan F. Westin, "Privacy and freedom," **Washington and Lee Law Review** 25, 1 (March 1968): 166-170.

⁸William A. Parent, "Privacy, Morality and the Law," **Philosophy and Public Affairs**, 12, 4 (October 1983): 269-288.

⁹Charles Fried, "Privacy," **Yale Law Review** 77, 3 (January 1968): 475-493.

¹⁰Arthur R. Miller, **The Assault on Privacy-Computers Data Banks and Dossiers** (Ann Arbor, MI: The University of Michigan Press, 1971), p. 190.

Additionally, individual control regarding a person has a strong linkage to other fundamental values, including dignity, privacy, and autonomy.¹¹

Privacy as individual control concept also gains significance in many nations' information privacy laws and practice. The German constitutional court asserted the importance of individual control by judging that a person shall be able to predict with reasonable certainty about his information in certain areas that is known to social context and estimate the knowledge of information receiving parties; otherwise, he is crucially inhibited in his freedom to plan or to decide freely and without being subject to any pressure influence.¹² Most data protection laws around the world provide individual control using notice and consent.¹³ In the European Union, consent is the most common basis for legitimizing data processing as defined in Article 7 of the Data Protection Directive.¹⁴ In the US, notice and consent is the main principle used in privacy regulation for a long time and also a core principle in Fair Information Practice.¹⁵ In court practice, the German Supreme Court viewed that a person has the right "to determine for himself whether his personal data should be divulged

¹¹Helen Nissenbaum, "Privacy as contextual integrity," *Washington Law Review* 79, 1 (February 2004): 119-158. Daniel J. Solove, *The future of reputation: Gossip, rumor, and privacy on the internet*, (New Haven: Yale University Press, 2007), p. 130.; Alan F. Westin, op. cit.

¹²Bundesverfassungsgericht U. V., *zum Volkszählungsgesetz 1983* [Online], available URL: <https://freiheitsfoo.de/files/2013/10/Census-Act.pdf>, 1983 (December, 15).

¹³Omer Tene and Jules Polonetsky, "Big data for all: Privacy and user control in the age of analytics," *Northwestern Journal of Technology and Intellectual Property* 11, 5 (April 2013): 240-272.

¹⁴Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995.; Article 29 Working Party, "Opinion 15/2011 on the Definition of Consent, Article 29," 13 July 2011.

¹⁵The White House, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," 1 February 2012.; Colin J. Bennett, *Regulating privacy: Data protection and public policy in Europe and the United States* (New York: Cornell University Press, 1992), p. 263.

or utilized”¹⁶ In the case of *Tournier v. Bank of England*,¹⁷ the court considered that the bank cannot disclose confidential data of the consumer without the consumer’s consent.

4.2 Individual Control via Notice-and-Consent Mechanism

Notice-and-consent mechanism represents individual control over personal information in that a person has an ability to determine when and how others may collect personal data and how to use it.¹⁸ Notice refers to the privacy policy or terms and conditions of data processing and rights of individuals. Consent is an act of the data subject in agreeing with the terms and conditions. In other words, notice provides information on terms and conditions regarding the collection, analysis, use or dissemination of personal data; while, consent represents the data subject’s right to accept or reject such terms and conditions.¹⁹

In the online and digital financial services sphere, notice-and-consent mechanism is widely adopted in the form of presenting a privacy policy to the consumer and request them to accept the terms and conditions of personal data processing by giving consent. Most personal data protection laws and business practices focus on giving individual control over personal information via notice-and-consent mechanism in order to determine whether the data controller can collect personal data and use in which way. For example, the EU GDPR requires the data controller to obtain consent from the data subject before or at the time of collection of personal sensitive data. Consent is also one of the six lawful bases for personal data processing.

¹⁶Riedel Eibe, “New Bearings in German Data Protection. Judgement of the Federal Constitutional Court, Karlsruhe, of 15 December 1983,” *Human Rights Law Journal* 94, 101 (January 1984): 94-116.

¹⁷*Tournier v National Provincial Bank of England*, 1 K.B. 461, 1924.

¹⁸Alan F. Westin, op. cit.

¹⁹Robert H. Sloan and Richard Warner, op. cit.

5. Key Attributes and Risks to Individual Control in the Processing of Alternative Credit Data

5.1 Key Attributes of the Processing of Alternative Credit Data Relating to Individual Control over Personal Information

5.1.1 Obscurity

In this study, obscurity essentially refers to insufficient transparency and explainability owing to certain characteristics of the model and analysis, including proprietary nature of the analytic models, changing logic of analysis, and difficulty to explain the outcomes from the model. Transparency is not only developed by the disclosure and sharing of information, but more importantly by continuous dynamic intercommunication between organization and stakeholders.²⁰ Although transparency has many evolving definitions, it is interrelated with accountability, secrecy, privacy, efficiency, and effectiveness²¹ Therefore, companies have to carry out certain actions in order to verify if consumers understand their transparency policy and how they use consumers' information.²² Some organizations are not transparent regarding the treatment of consumers' information, such as the information accessed by the third party; thus, it appears that consumers highly expect to be well informed about their online activity and how their data are used by the firm.²³

Understanding the algorithms or models used to process alternative credit data is important but not straightforward. Today's 'big' alternative credit data that relies on algorithms bring the issue of modularity. Modularity means different modules perform different parts of the task and merge the results to arrive at the

²⁰Antonino Vaccaro and Peter Madsen, "Corporate dynamic transparency: the new ICT-driven ethics?," **Ethics and information technology** 11, 2 (June 2009): 113-122.

²¹Ball C., "What is transparency?," **Public Integrity** 11, 4 (September 2009): 293-308.

²²Nill A. and Aalberts R., "Legal and Ethical Challenges of Online Behavioral Targeting in Advertising," **Journal of Current Issues & Research in Advertising** 35, 2 (July 2014): 126-146.

²³Granados N. and Gupta A., "Transparency strategy: Competing with information in a digital world," **MIS quarterly** 37, 2 (June 2013): 637-641.

final result.²⁴ Although each module is understandable, putting them together creates complexity. For example, a credit scoring algorithm may include a module that scores the customer's total debt burden, payment history, and the customer's possible profitability. The consumer's previous payment records may enter all these modules, but how the record affects the final credit decision may not be clear. For example, a record of pre-payments may be helpful for scoring based on payment history, but because this consumes the income that can be used to pay for new loans, it may reduce the score in the total debt burden module.

5.1.2 Automation

There are two key types of automation referred in this study: automated decision-making and profiling. Automated decisions are decisions made by computer processing systems without any human involvement, typically based on inferences produced by profiling using machine learning models applied to big data. Meanwhile, profiling is the automated processing of personal data to evaluate, analyze or predict likely aspects of a person's interests, personal preferences, behavior, performance at work, economic situation, health, reliability, location or movements. Automated decision-making can be used for inferences and predictions in the case of alternative credit data. There are merits that accurate default prediction and personalize credit pricing are beneficial for both lenders and borrowers.²⁵ When a lender can accurately predict default, they can determine a cutoff for extending a loan or price risk accordingly, reducing a loss for lenders.²⁶

²⁴Koene A. Clifton, C., Hatada Y. Webb H., and Richardson, R., **A governance framework for algorithmic accountability and transparency** [Online], available URL: [https://www.europarl.europa.eu/stoa/en/document/EPRS_STU\(2019\)624262](https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2019)624262), 2019 (April, 4).

²⁵Gillis T. B., **False dreams of algorithmic fairness: The case of credit pricing**, (Cambridge: Harvard University Press, 2020) 37-40.

²⁶Phillips R., "Optimizing prices for consumer credit," **Journal of Revenue and Pricing Management** 12, 4 (July 2013): 360-77.; Staten M., "Risk-Based Pricing in Consumer Lending," **Journal of Law, Economics & Policy** 11, 1 (March 2015): 33-58.

5.1.3 Open Data

Having an open data platform allows service providers or financial institutions to access potential customer data without having to store it. Customer data is shared to third party service providers via secure channels to offer a choice of financial products or services. In requesting access to such information, the client authorizes third party providers to access or store information necessary to provide financial products or services. In essence, open data platform allows data sharing of the bank's customer data to other third-party service providers. In addition, the data shared through open data platform will not only include account information, but will also include alternative credit data from other sources that can be analyzed to gain an insight into the customer's financial behavior. Therefore, the approach to protecting personal data in this open data platform is very important to increase trust and control over of the customer in the context of data sharing for finance.²⁷

5.2 Risks to Individual Control over Personal Information from the Processing of Alternative Credit Data²⁸

5.2.1 Failure to Inform

1) Insufficient Information

Insufficient information means that a data subject has not received the information necessary to make informed decisions about the collection, collection, use, and sharing of personal data, or is unable to make appropriate decisions regarding the rights as a data subject. Insufficient information may arise from the fact that

²⁷World Bank, **The Role of Consumer Consent in Open Banking: Financial Inclusion Support Framework** [Online], available URL: <https://documents.worldbank.org/curated/en/099425002082230437/pdf/P1705050aeb8e704f088260f228802b73b8.pdf>, 2021 (December, 15).

²⁸Citron D. K. and Solove D. J., "Privacy harms," **Boston University Law Review** 102, 3 (April 2022): 793-863. This study follows Citron and Solove's classification of autonomy harms but does not take into account chilling effects because chilling effects often refer to the government acts that inhibit people from engaging in certain civil liberties, such as free speech, political participation or religious activities, which are rather outside of the scope of this study.

the data controller does not provide complete information or provides unclear information, such as the purpose of the information use, data storage period, data sharing, the right to correct or delete data or even the right to withdraw consent. In certain cases, data controllers may not be able to disclose to their owners technical or intellectual property information, such as information about the algorithm or logic used in analyzing or predicting data, or even certain factors used in assessing such data as customer credit scoring. To ensure that consent is informed, data controllers should provide as much information as possible about the purposes for which the data will be used, including relevant risk information and negative or positive impacts.

2) Unawareness

Unawareness here refers to the fact that the data subject does not have sufficient awareness of the collection, use or sharing of their personal data. Awareness element comes from the concept of individual control as the degree to which a person is aware of a situation and has conscious intentions and is able to initiate, stop, or keep the situation.²⁹ In the case of financial services, financial institutions may have many obscure channels to collect personal data, including customer interactions in chat and phone channels, social media data, or even using third party data such as credit bureaus. Furthermore, when giving consent at the time of offering services, the data owner may not be sufficiently conscious of allowing the data controller to use sensitive or financial data, or share to other service providers.

3) Complexity of Information

Complexity of information refers to the processing of personal data that is difficult for the data subject to understand or data that the data controller is unable to explain in understandable language. Profiling and automated decision-making processes often make information too complex to understand. Most of such decisions

²⁹Van Ooijen I. and Vrabec H. U., “Does the GDPR enhance consumers’ control over personal data? An analysis from a behavioural perspective,” **Journal of Consumer Policy** 42, 1 (March 2019): 91-107.

are made using algorithmic models, artificial intelligence or machine learning which are often based on complicated assumptions or factors or advanced techniques of analysis. In this study, the focus is on the complexity of using big data analytics or advanced algorithmic models that are often complex both in terms of explaining the overall model and explaining the logic of the results, inference or prediction from the analysis.

5.2.2 Lack of Freedom to Choose and Decide

1) Coercion

Coercion is the pressure or limitation on an individual's freedom to choose or act. In data privacy, the data subject may be coerced to consent to the collection, use or disclosure of personal data with no other options, such as refusal or subject-specific consent. From time to time, the data subject may be requested to accept terms and conditions or data processing activities that are not essential to the provision of the service. Besides, the data subject may be compelled that personal data be collected or processed in an automated way without human involvement.

2) Manipulation

Manipulation refers to inappropriately influencing an individual's behavior or decisions. Big data collection together with predictive and inference capability allows the data controller to understand and predict consumer behavior. Profiling and automated decision-making in effect will categorize individuals and put some restrictions on types or prices of certain products or services according to the data subject's preferences or the specific need at that time. This will deprive the data subject of the freedom to choose goods or services as they should be. A clear example of using consumer data for manipulation is the Cambridge Analytica incident, where personal data was purchased from Facebook for psychological analysis and used to help Donald Trump become President of the US.³⁰

³⁰Lapowsky I., **How Cambridge Analytica Sparked the Great Privacy Awakening** [Online], available URL: <https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening>, 2019 (March, 17).

3) Limitation of Choices

The data subject's ability to control concept emphasizes the role of choice and individual self-determination over other values.³¹ Where a service provider focuses on offering tailor products or services, it may deprive the user of ample comparable options. In terms of information, the data subject may fall into a filter bubble where the information received by the user is based on the specific or behavioral information of the data subject without presenting all available necessary information. As a result, the data subject is unable to obtain sufficient information or product selection from other sources before making a decision to use service.

5.2.3 Improper Reuse and Repurpose

1) Lack of Control

In some circumstances, the data subject may not be able to choose whether to properly handle personal data or limit the use of personal data. Digital platforms have made important decisions on the collection and flow of personal data, and the public has been increasingly going through “digital resignation,” feeling unable to control their data and just accepting the loss of control.³² When the credit results of analysis or processing come out, the data subject may not have the right to object to the decisions or to request human intervention or review on such results or even to limit the scope of the data use obtained from such analysis. In the case of open data platform, consumers may not be able to control the sharing of personal data to third parties, particularly the sharing of data subsequently after it has been shared with the first third party.

2) Unfulfilled Promise

Unfulfilled promises may arise from non-compliance with the terms and conditions on the collection, use or sharing of personal data that the data

³¹Lazaro C. and Metayer D. L., “Control over personal data: True remedy or fairy tale,” **SCRIPTed: A Journal of Law, Technology and Society** 12, 1 (June 2015): 3-34.

³²Draper N.A. and Turow J., “The corporate cultivation of digital resignation,” **New Media & Society** 21, 8 (August 2019): 1824-1839.

subject provided when the data subject was initially accessed. This type of harm prevents individuals from making preferred choices or getting results according to their own decisions. For example, the data subject may not be able to limit the data use by the subsequent third-party service providers within the scope of the purpose for which it was provided to the first service provider.

6. Comparative Analysis of the Criteria and Elements of Individual Control over Personal Information under the Thai and Foreign Laws, Frameworks, and Cases

6.1 Transparency as a Prerequisite for Individual Control

Transparent information is necessary in that the data subject should be informed when personal data is collected or accessed so that the data subject is aware of the important matters and the conditions or guidelines for processing personal data, including the purposes for which the data is collected, type of the data collected, the storage period, the third party to whom the data will be disclosed, etc. Once the data subject has all the necessary information, he or she can appropriately make an informed decision concerning personal data processing.

6.1.1 Principle of Transparency

With regard to transparency in the processing of personal data by the controller, in principle, the Thai legal framework, including the PDPA, does not explicitly state the principle of transparency or requirements. Nevertheless, the CoE Convention 108+ and the General Data Protection Regulation (GDPR) clearly state transparency principles in terms of processing personal data and the way in which it is distributed, including situations in which it is necessary to provide such information to the data subject.

Under the CoE Convention 108+, personal data has to be processed fairly and in a transparent manner.³³ Data controller has to provide the data subjects

³³CoE Convention 108+ 2018, Article 5, 4 (a.) – Legitimacy of data processing and quality of data.

necessary information in order to ensure fair and transparent processing of the personal data, including legal basis and the purposes of the intended processing, the categories of personal data processed, the recipients or categories of recipients of the personal data, and the means of exercising the rights.³⁴

The GDPR requires that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency).³⁵ The GDPR, Recital 58 stipulated the principle of transparency with an emphasis on the characteristics of information addressed to the public or the data subject that shall be concise, easily accessible and easy to understand, and that clear and plain language and, may include visualization where appropriate. The form of such information can be in an electronic form including providing in a website. The GDPR emphasizes that this principle is necessary for the data subject to know and understand by whom personal data is being collected and for what purpose, especially in situations where there is a large number of parties involved with the use of complex technology as in the case of online advertising.³⁶

6.1.2 Right to be Informed and Access

The PDPA has clear provisions in terms of the right to be informed and right to access, which are in accordance with international law and principles.

The right to be informed is prescribed under Section 23 of the PDPA. In collecting the personal data, the data controller shall inform the data subject, before or at the time of such collection, of (1) the purpose of the collection for use or disclosure of the personal data; (2) notification of the case where the data subject must provide his or her personal data for compliance with a law, or contract; (3) the personal data to be collected and the retention period; (4) the categories of persons or entities to whom the collected personal data may be disclosed; (5) information, address, and the contact channel details of the data controller; and (6) the rights of the data subject.

³⁴CoE Convention 108+ 2018, Article 8 – Transparency of processing.

³⁵General Data Protection Regulation 2018, Art. 5, 1 (a.).

³⁶Ibid., Recital 58.

Apart from the right to be informed, the data subject is entitled to request access and obtain a copy of the personal data related to him or her, which is under the responsibility of the data controller, or to request the disclosure of the acquisition of the personal data obtained without his or her consent within 30 days after receiving the request.³⁷ The controller can reject such request only in the case where the rejection is subject a law or a court order, or such access and obtaining a copy of the personal data would adversely affect the rights and freedoms of others.³⁸

Under the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Privacy Guidelines), right to be informed is specified as openness principle that refers to a readily available general policy indicating developments and practices about personal data, including the practice to acquire, collect, store or use and the purpose of the use of personal data.³⁹ The APEC Privacy Framework stipulates that when collecting data, the data controller shall provide notice to data subjects on specific purposes, third parties to whom data may be received, choices and means that data subjects will be able to limit the use and disclosure and access and correction of personal data.⁴⁰ The controller is also required to take all reasonably practicable steps to provide the notice either before or at the time of collection; otherwise, as soon after as is practicable.

Under CoE Convention 108+, the data subject has the right to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her, the communication in an intelligible form of the data processed, all available information on their origin, on the preservation period as well as any other information that the controller is required to provide in order to ensure the transparency of processing.⁴¹

³⁷Personal Data Protection Act 2019, Thailand, Section 30.

³⁸Ibid., Section 30.

³⁹OECD Privacy Guidelines 2013, Art. 12.

⁴⁰APEC Privacy Framework 2005, Art. 21.

⁴¹CoE Convention 108+ 2018, Article 9 (b.) – Rights of the data subject.

Furthermore, the data subject has the right to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her.⁴² Similarly, under APEC Privacy Framework, the data subject is able to obtain from the data controller regarding the holding of personal data and can have access to personal data within a reasonable timeframe and manner and understandable form.⁴³

The GDPR imposes a duty on data controllers to ensure that data subjects know how personal data will be used before data processing.⁴⁴ The controller is also required to allow the data subject to access the data even after processing or access per request.⁴⁵ In addition, the controller must explain to the data subject in a way that is easily accessible about the process of processing personal data, including the specific purpose, which must be notified at the beginning of the collection, using plain and clear language and informing about the risks, rules, safeguards and rights of data processing.⁴⁶

6.1.3 Case

1) *Smaranda Bara and Others v. Președintele Casei Nationale de Asigurări de Sănătate, Casa Natională de Administrare Fiscală (ANAF)*:⁴⁷ the right to be informed of sharing and processing of personal data

In this case, personal tax information relating to self-employed income was passed from the national tax agency to the national health insurance fund on the basis that there was money owed to the health insurance. The key issue of this case was whether the data subject had to be informed in advance about

⁴²Ibid., Article 9 (c.) – Rights of the data subject.

⁴³APEC Privacy Framework 2005, Art. 29 (a), (b).

⁴⁴General Data Protection Regulation 2018, Art. 12, 13 and 14.

⁴⁵Ibid., Art. 15.

⁴⁶Ibid., Recital 39.

⁴⁷*Smaranda Bara and Others v. Casa Natională de Asigurări de Sănătate and Others*, CJEU, C-201/14, 2015.

the identity of the data controller and the purpose of sharing personal data before the data could be processed. The Court of Justice of the European Union (CJEU) ruled that when a government agency transfers personal data to another government agency for further processing, the data subject must be informed about the sharing and processing of such data.

By the same token, if a financial institution plans to transmit or share alternative credit data with another service provider through an open data platform, the financial institution must notify the data subject at the time of data collection or access. In the case of sensitive personal data, consent must be obtained by giving information about the transfer of data to third parties, type of data, and the purpose of the information. Furthermore, if the personal data is processed for a new purpose that is significantly changed from that initially declared, the data controller must obtain new consent to the data subject. The GDPR prescribes a guidance on purpose compatibility test and lays out factors to consider, including the linkage between the previous and new purpose, and the context surrounding data processing.⁴⁸ However, the Thai PDPA does not provide any guidance on such matter.

6.2 Notice-and-consent Mechanism

6.2.1 Consent Requirement under the Thai Legislation

The PDPA has requirements for obtaining consent from a data subject prior to the collection, use and disclosure of personal data and this must be done explicitly. Under Section 19 of the PDPA, the data controller shall not collect, use, or disclose personal data, unless the data subject has given consent prior to or at the

⁴⁸In order to check whether the new purpose is compatible with the original purpose, a compatibility test should be conducted. There are four key factors that the data controller needs to consider: the relationship between the original purpose and the new purpose, the context in which the data was collected and the reasonable expectation of the data subject, the nature of the data and the impact of the subsequent processing on the data subject, and the safeguards applied by the controller. See General Data Protection Regulation 2018, Recital 50.

time of such collection, use, or disclosure.⁴⁹ A request for consent shall be explicitly made in a written statement, or via electronic means, unless it cannot be done by its nature. When requesting consent, the PDPA also requires that it state its purpose and define the essential elements of obtaining consent. The 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 deceive or mislead the data subject in respect to such purpose.⁵⁰

The consent of the data subject must be freely given. In requesting consent from the data subject, the data controller shall utmost take into account that the data subject's consent is freely given. Also, the entering into the contract, including any provisions of the service shall not be a condition to obtaining consent for the collection, use, or disclosure of personal data that is not necessary or not related to such contract entering, including the provisions of the service. The data subject may withdraw his or her consent at any time. The withdrawal of consent shall be as easy as to giving consent, unless there is a restriction of the withdrawal of consent by law, or the contract which gives benefits to the data subject. However, the withdrawal of consent shall not affect the collection, use, or disclosure of personal data that the data subject has already given consent legally. In the event that the withdrawal of consent will affect the data subject in any manner, the data controller shall inform the data subject of such consequences of consent's withdrawal. If requested for the data subject's consent which is not in accordance with those prescribed above shall have no binding effect on the data subject and shall no longer enable the data controller to collect, use, or disclose the personal data.

⁴⁹Except the case where it is permitted to do so by the provisions of this Act or any other laws.

⁵⁰In this regard, the Committee may require the data controller to request for data subject's consent in accordance with the form and statements as prescribed by the Committee. See the PDPA 2019, Section 19.

6.2.2 Consent as a lawful basis for Processing of Personal Data

The OECD Guideline and APEC Privacy Framework state in the similar way that data collection must be limited by lawful and fair means, with the knowledge of the data subject or obtaining the consent of the data subject as appropriate.⁵¹ In addition, the data controller must obtain consent from the data subject before personal data is disclosed or used for purposes other than the purpose for which the data subject was originally notified.⁵²

Under CoE Convention 108+ and the GDPR, consent is one of the six lawful bases for processing personal data. The other five lawful bases are contract, legal obligation, vital interest, public task, and legitimate interests.⁵³ In addition, explicit consent is also be required for the processing of sensitive personal data for one or more specified purposes.⁵⁴ The GDPR also stipulates that consent must be given with a clear affirmative act of the data subject's agreement to the processing of his or her personal data either as an action or as a statement.⁵⁵ The data subject must be able to withdraw consent at any time.⁵⁶ However, a written declaration, such as terms and conditions of service must contain clear and plain language in an easily accessible format.⁵⁷ The data subject must explicitly give consent to the processing of sensitive data.⁵⁸ Consent cannot be taken from silence, pre-ticked boxes, pre-completed forms

⁵¹OECD Privacy Guidelines 2013, Art. 7; APEC Privacy Framework 2005, Art. 25 (a).

⁵²OECD Privacy Guidelines 2013, Art. 10 (a) ; APEC Privacy Framework 2005, Art. 24.

⁵³General Data Protection Regulation 2018, Art. 6 (1).

⁵⁴Ibid., Art. 9 (2) (a)

⁵⁵Ibid., Art. 7.

⁵⁶Ibid.

⁵⁷Ibid.

⁵⁸According to General Data Protection Regulation 2018, Art. 9 (1), sensitive data refers to special categories of personal data which reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

or inactivity.⁵⁹ The Thai PDPA has also established consent as one of the lawful bases for personal data processing.

6.2.3 Elements of Valid Consent

The EU GDPR defines consent as any freely given, specific, informed and unambiguous indication of the data subject's wishes.⁶⁰ Valid consent must include elements of freely given, specific, informed and unambiguous.⁶¹ Free consent means that the data subject has free expression of an intentional choice, that the choice can be exercised without deception, intimidation, coercion, or significant negative consequences for not giving consent. To be called freely given consent, the data subject must have free choice, or must be able to refuse or withdraw consent without detriment.⁶² In case of employment context, for instance, if the employer wants to process the employee's personal data for purposes other than the performance of employment contract, such as recreational activities or relationship with other organizations, the employee should be able to reject to give consent without any negative consequences. Furthermore, the consent shall not be conditional on the processing of personal data that is not necessary for the performance of the contract.⁶³ For example, if the data controller provides goods and services that are conditional on consent to share the data subject's personal data to third parties, this is not considered freely given consent because such consent to share personal data is not necessary for the performance of the contract.

Informed consent means that the data subject has sufficient information to make a decision or make that choice. The message that appears to the data subject should be easy to understand and accurate, at least the data subject

⁵⁹General Data Protection Regulation 2018, Recital 32; Explanatory Report of CoE Convention 108+ 2018, para. 42.

⁶⁰General Data Protection Regulation 2018, Art. 4 (11); CoE Convention 108+ 2018, Art. 5 (2).

⁶¹General Data Protection Regulation 2018, Art. 4 (11). See also CoE Convention 108+ 2018, Art. 5 (2).

⁶²General Data Protection Regulation 2018, Recital 42.

⁶³Ibid., Art. 7 (4).

should be aware of identity of the controller, types of data, purpose of processing, the recipients of data, the right of data subject.⁶⁴ Besides, the information should be in clear and easy to understand language without technical jargons or terms that should be generally incomprehensible.⁶⁵ Specific consent basically means consent is specific to the purpose of processing.⁶⁶ Consent must be obtained from the data subject for one or more specific consent.⁶⁷ In the event that the data processing is subject to any changes for a different purpose, the data subject must give consent again. The three main elements of specific consent are specific to the purpose, sufficient details in the consent request, and clear separation of information on data processing and other matters.⁶⁸ Unambiguous consent is that the data subject has to obviously give consent to a particular data processing from the data subject's statement or a clear affirmative action. Consent can be collected via a written or recorded oral statement or electronic means.⁶⁹ All consent has to be given in an unambiguous way, meaning that there should be no doubt that the data subject wished to express the agreement to allow personal data processing.⁷⁰ Safeguards should be ensured that the data subject is aware of the fact and extent of such consent giving.⁷¹

It is obvious that in the PDPA, consent is one of the legal bases prior to the collection, use and disclosure of personal data and also obtaining consent before collecting sensitive data. The essential elements of consent according

⁶⁴General Data Protection Regulation 2018, Recital 42; Article 29 Working Party, "Working Document on the processing of personal data relating to health in electronic health records (EHR)," 15 February 2007.

⁶⁵Article 29 Working Party, "Opinion 15/2011 on the Definition of Consent, Article 29," 13 July 2011.

⁶⁶Ibid.

⁶⁷General Data Protection Regulation 2018, Article 6(1)(a).

⁶⁸Article 29 Working Party, "Guidelines on Consent under Regulation 2016/679," (6 July 2018).

⁶⁹Ibid.

⁷⁰General Data Protection Regulation 2018, Art. 4 (11).

⁷¹Ibid., Recital 42.

to the PDPA are explicit, understandable, straightforward, freely given, and can withdraw at any time.⁷² Besides, although the PDPA does not have informed and specific consent requirements, the PDPA does require the data controller to provide necessary information to the data subject as discussed in the areas of the right to be informed, particularly in respect of identity of the data controller, purpose of data processing, and the right to withdraw consent.⁷³

6.2.4 Cases

1) *Tournier v. National Provincial and Union Bank of England*:⁷⁴
disclosure of information without consent

Tournier was a client of the National Provincial and Union Bank of England. His account was in overdraft and he agreed to pay the bank in installments. The bank's manager then called the Tournier's employer to inquire about his address. During the conversation, the manager disclosed Tournier's unpaid checks to Tournier's employer. The employer subsequently refused to renew Tournier's employment contract. Tournier, then, filed a lawsuit in the Court of Appeal. The Court held that the bank was liable for breach of contract between the bank and the customer. This was implied from the contractual term that the bank would not disclose to third parties without the customer's expressed or implied consent the status of the customer's account or transactions with the bank or any related customer's information, unless the bank is requested by a court, the disclosure is for a public duty, or to protect the bank's own interests. These four conditions are known as the principles of the conditions where the bank can disclose the customer's information. This case represents the lawful bases of the PDPA and the GDPR that cover the four principles. The laws also provide additional requirements in the terms of vital interests, contractual relationships and legitimate interests.

⁷²Personal Data Protection Act 2019, Thailand, Section 19.

⁷³*Ibid.*, Section 23.

⁷⁴*Tournier v National Provincial Bank of England*. 1 K.B. 461, 1924.

2) *Deutsche Telekom AG v. Bundesrepublik Deutschland*:⁷⁵ specific consent

In this case, the telecom provider requested consent on publication of the data subject's personal data, but the data subject did not have options on specific publishers. The issue was whether the telecom provider needed to request a new consent from the data subject with the specified name of the recipients of the personal data. The CJEU ruled that consent did not need to be renewed before submitting data to directories since this is specifically related to the purpose of the publication of personal data, but not relevant to choosing any specific providers. Besides, the disclosure of the specific publication for personal data itself could be detrimental to the data subject.

Article 13 of the GDPR requires that the data controller disclose information to the data subject, including to the recipients or categories of recipients of the personal data, if any. The GDPR does not require the data controller to reveal the recipients of personal data identity, but can choose to inform the categories of recipients or the name or identity of the recipients. Similarly, the PDPA also requires the data controller to provide information of the categories of persons or entities to whom the collected personal data may be disclosed, but not specific third parties.⁷⁶

3) *Clearview AI*:⁷⁷ not obtaining consent before the collection and use of personal data

The Clearview AI company has developed a search engine that uses images to search. Clearview AI collects images from websites and social media networks

⁷⁵*Deutsche Telekom AG v. Bundesrepublik Deutschland*, CJEU, C-543/09, 2011.

⁷⁶Personal Data Protection Act 2019, Thailand, Section 23.

⁷⁷*Commission nationale de l'Informatique et des Libertés* (CNIL - French Data Protection Authority), **Restricted Committee Deliberation No. SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI** [Online], available URL: https://www.cnil.fr/sites/default/files/atoms/files/deliberation_of_the_restricted_committee_no_san-2022-019_of_17_october_2022_concerning_clearview_ai.pdf, 2022 (October, 17).

that do not require logging into accounts and extracts images from videos available on the public platforms from individuals via Clearview AI's facial recognition software. In May 2020, the National French data protection authority investigated and later on November 26, 2021 imposed financial penalty of 20 million euros. One of the breaches is unlawful processing of personal data according to Article 6 of the GDPR. Processing of personal data must be on a lawful basis. The company did not obtain consent from the consumer before collecting and use of the consumer's images in its facial recognition software. The PDPA also requires the data controller to inform the data subject of the collection of personal data and as for the collection or sensitive data, explicit consent must be obtained as well.

7. Limitations of the Thai Legal Personal Data Protection Legislation

7.1 Limits of Notice-and-consent Mechanism

7.1.1 Consent as Right Waiving and Lack of Accountability

The notice-and-consent mechanism is a data protection practice that allows consumers to obtain information and at the same time have control over personal information. For instance, the PDPA requires explicit consent before the collection and processing of sensitive data. However, this approach may not be sufficient to properly protect the right to data privacy, since consent by a data subject can be deemed that the data subject is willing to waive the right to data privacy or even other constitutional rights.⁷⁸ Furthermore, the data controller may not have sufficient accountability since the controller may issue a privacy notice and request consent solely to comply with legal requirements without being in good faith in protecting the personal data of the data subject.

7.1.2 Impracticality of Valid Consent

As mentioned earlier, the PDPA only specifies that the controller has to obtain explicit consent, inform the purpose of the collection, use, or disclosure of

⁷⁸Daniel J. Solove, op. cit.

the personal data, using clear and plain language, and does not deceive or mislead the data subject in respect to such purpose, and also the consent of the data subject must be freely given. However, such requirements are rather subjective and requires appropriate interpretation in certain cases. For instance, in case the lender employs advanced algorithmic models composing of wide-ranging factors for assessing creditworthiness of the borrower, the content of the privacy policy to request for consent can be lengthy, complex or providing even insufficient information for the data subject. Although the PDPA imposes an obligation on the controller to give the data subject access to information and the right to be informed, the data subject may not be aware or understand, and the data controller may provide information that is too technical or inadequate for the data subject to make informed decisions on personal information. In some cases, the data controller itself may not be able to explain or lack understanding on the result of such credit model, such as the result generated from machine learning that discovers certain complex relationship among the factoring affecting creditworthiness in the model.

7.1.3 Lack of Negotiation Power

When the data subject receives privacy policies or terms and conditions, the PDPA does not provide the data subject with certain power or options to negotiate on such terms. Besides, as the data controllers are mostly large companies providing services, such as commercial banks or fintech companies, to a large number of customers, it is very difficult for the consumer to propose changing on the terms of privacy policy. To help address this issue, the EU lawmaker issues additional guidance for elements of specific consent, including specific to the purpose, sufficient details in the consent request, and clear separation of information on data processing and other matters.⁷⁹ From this elements, in case the controller or the lender requests to collect alternative credit data from the data subject with one or more purposes, the lender needs to clearly specify a particular terms and

⁷⁹Article 29 Working Party, “Guidelines on Consent under Regulation 2016/679,” (6 July 2018).

conditions of the privacy policy for each purpose and also provides opportunity for the data subject to choose to accept or reject certain consent.

7.1.4 Difficulty in Assessing Trade-off

One of the key purposes of consent requirement is to give the data subject opportunity to assess the trade-off between the benefits of giving personal information and the loss of personal privacy. Data subjects weigh the risks associated with the release of personal information to a controller against expected benefits, such as financial rewards, personalization, and social benefits.⁸⁰ However, in a practical situation, the data subject may not be able to thoroughly consider the cost and benefit, understand or even read the terms and conditions before giving consent, the data subject, therefore, cannot assess trade-offs between giving personal data and benefits from the controller's products or services due to certain limitations, such as limited reading time, the potential risks of giving consent, expected benefits etc.

7.2 Lack of Clear Guidance on Repurpose of Data Processing

In the case of an open data platform with subsequent sharing of personal data, if it is shared to multiple third-party service providers or if the purpose of use is changed multiple times, the data subject will incur new consent burdens. The PDPA does prevent the controller from the processing of personal data for the purpose different from the originally informed purpose unless the data subject has been informed of such new purpose, and the consent is obtained prior to the time of collection, use, or disclosure. Although this is a clear requirement on repurpose, the PDPA does not provide a clear guidance on how to differentiate that the new purpose is different from the original purpose. Unlike the PDPA, the GDPR prescribes a guidance on purpose compatibility test that the controller has to consider certain factors, including any linkage or relationship between the original and the new purpose, the context of personal data collection and the data subject's reasonable expectation,

⁸⁰Smith H. J., Dinev T., and Xu H., "Information privacy research: An interdisciplinary review," *MIS Quarterly* 35, 4 (December 2011): 989–1016.

the nature of the data, the consequences of further processing for data subjects, and the availability of appropriate safeguards for further processing operations.⁸¹

8. Conclusion and Discussion

Individual control over personal information is one of the top concepts cited by many authors and philosophers in the field of information privacy law. That an individual has control of one's own information means that an individual can choose and decide who does what and how with his own information. Thus, this individual control concept fosters other value of privacy, including autonomy and freedom, and self-determination. When referring to individual control over personal information in terms of personal data protection law, literature often concludes that individual control is essentially provided via notice-and-consent mechanism. However, the processing of alternative credit data brought emerging risks to this approach, including failure to inform, lack of freedom to choose and decide, and improper reuse and repurpose.

From the comparative analysis and assessment of the personal data protection legal framework related to the processing of alternative credit data in Thailand, it is evident that the Thai personal data protection law insufficiently provides individual control over personal information via notice and consent. The Thai legal framework mainly focuses on the use of notice-and-consent mechanisms, which still have many limitations. For instance, where the data subject gives consent to the collection of personal data, the data subject may be deemed to have waived the right to data privacy without negotiating power on the privacy policy offered by the data controller. Besides, in the case of repurpose or use of personal data for new purposes, the law does not provide clear guidelines on assessing whether such repurpose requires the new consent of the data subject.

⁸¹General Data Protection Regulation 2018, Recital 50 and Art. 6 (4); Explanatory Report of CoE Convention 108+ 2018, para. 49.

9. Recommendation

This study recommends that notice-and-consent mechanism under the PDPA be supplemented by the following elements of control over personal information.

9.1 Enhanced Transparency with the Data Subject's Understandability

Transparency element is a prerequisite for control over personal information. Before a data subject can have control over personal information, he or she must have complete, sufficient and understandable information to be able to make informed decisions regarding the collection, processing and sharing of personal information. Transparency in this study means transparency from both the data controller perspective and the data subject perspective. The data controller shall provide the data subject with all necessary information on data processing and including rights regarding personal data, in a complete and explainable manner. This is particularly the case when data is processed using advanced analytic models. As a data subject, while receiving such information, one must be aware and have an appropriate level of cognition in order to be able to make informed decisions about the processing activities of personal information appropriately.

Therefore, this study suggests that the relevant Thai authorities establish the concept of understandability of the data subject under the PDPA or issue an explicit financial regulations relating to alternative credit data protection. The data controller shall ensure that processing of personal data can be described clearly in all cases, especially those that use advanced analytics or artificial intelligence to analyze, predict or produce results that could have a significant impact on the data subject, such as receiving credit, making a job decision, etc. Such results should include both an explanation of the model used in terms of logic, factors, or weights of the factors used in the analysis and must explain about the origin and the resulting factors, and how it can be improved or changed. For example, the data subject should know how their credit scores using automated or algorithm models come from and how to improve such scores. This study also recommends to take into account the data

subject's literacy regarding data protection and rights which shall be protected by law as well. In this case, the data controller may test the data subject's knowledge or consider other useful personal data that could demonstrate the privacy literacy of the data subject, such as education level, age, occupation, etc.

9.2 Flexible, Substantive, and Consumer-Centric Notice-and-Consent Mechanism

In order to reinforce the significant role of notice and consent in representing the data subject's control over personal information, in addition to valid consent elements, including freely given, unambiguous, specific, understandable, this study recommends that the PDPA, especially under Section 19, be amended to allow flexibility in terms of negotiation, emphasize on the controller's accountability or the substance of the terms and conditions rather than focusing only for the sake of compliance. The law should require the controller to consider the characteristics or literacy of each particular group of the consumer. In certain cases that the data processing involves a high chance of producing privacy risks to the data subject, the notice and consent should give room for the data subject to negotiate or provide the data subject with sufficient choices on the privacy policy, such as the coverage of sensitive data collected and used, or the scope of data processing activities or even the categories or name of the third parties to whom the data will be shared. Besides, the data processing activities may be segregated by the type of data and purposes so that the data subject can choose or negotiate on each processing activity conveniently.

Furthermore, data controllers should be encouraged to be accountable and be aware of the importance of protecting personal data according to good principles, not only focusing on making notice and consent for compliance with the law or regulation, but should look for ways or measures that help protect the personal data of responsible consumers. In this case, the principle of 'privacy by default' should be established under the PDPA to emphasize on the proactive role of the data controller to establish data protection measures, including providing evident choices to individuals, keeping personal data in confidential unless the data subject

allows, providing sufficient individual rights, as well as always adhere to principles, such as data minimization and purpose limitation before the data processing begins.⁸²

In addition, the data controller should be required to take a consumer-centric approach by taking into account the data subject's literacy, characteristics and surrounding context in obtaining consent from the data subject. When the controller issues privacy notice and asks for consent from the individual, the controller should keep in mind that the content and information sent to the individual should match with their level of understanding or literacy on the data collected or particular purposes or means of data processing. If certain groups of individuals show that they require especially understandable and explainable language in the privacy notice, the controller should facilitate appropriate measures, including offering additional links of knowledge or explanation in their notice, or revising the notice to be more straightforward and suitable for each group of consumers. Besides, the controller should be required to consider the data subject's real situation when giving consent, including the means used (e.g. mobile apps or computer), and the sense of urgency when using such particular service. To illustrate, if the consumer is in dire need to get a particular loan, he or she will have no sufficient time to thoroughly read a complex and lengthy privacy policy before giving consent.

As for the case of open data platform, consumer's consent as well as the relevant laws and regulations also play a crucial role in granting the consumer's control. Although, banks and financial institutions are generally required to maintain confidentiality of customer data, there are exceptions in cases where the customer

⁸²General Data Protection Regulation, Article 25(2) specifies the requirements for data protection by default that "The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."

has given consent to the disclosure of that information. One of the objectives of open data platform is to provide more control of the account information and also to determine the data receiving parties. The study, thus, suggests that the Thai financial regulator issue an explicit regulation or guideline for obtaining consent, including informing the customer of the type of data to be collected, the purpose of the data collection, the retention period, the list or types of service providers to whom the data will be received, and consumer's authentication. These elements are essential to maintain individual control over alternative credit data shared among service providers in open data platforms.

Bibliography

- Ball C. “What is transparency?.” **Public Integrity** 11, 4 (September 2009): 293-308.
- Bennett Colin J. **Regulating privacy: Data protection and public policy in Europe and the United States**. New York: Cornell University Press, 1992.
- Bundesverfassungsgericht U. V. **zum Volkszählungsgesetz 1983** [Online]. Available URL: <https://freiheitsfoo.de/files/2013/10/Census-Act.pdf>. 1983 (December, 15).
- Citron D. K. and Solove D. J. “Privacy harms.” **Boston University Law Review** 102, 3 (April 2022): 793-863.
- Commission nationale de l’Informatique et des Libertés* (CNIL - French Data Protection Authority). **Restricted Committee Deliberation No. SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI** [Online]. Available URL: https://www.cnil.fr/sites/default/files/atoms/files/deliberation_of_the_restricted_committee_no_san-2022-019_of_17_october_2022_concerning_clearview_ai.pdf, 2022 (October, 17).
- Daniel J. Solove. “Privacy self-management and the consent dilemma.” **Harvard Law Review** 126, 7 (May 2013): 1880-1881.
- Draper N.A. and Turow J. “The corporate cultivation of digital resignation.” **New Media & Society** 21, 8 (August 2019): 1824-1839.
- Fried C. “Privacy.” **Yale Law Review** 77, 3 (January 1968): 475-493.
- Gillis T. B. **False dreams of algorithmic fairness: The case of credit pricing**, (Cambridge: Harvard University Press, 2020).
- Granados N. and Gupta A. “Transparency strategy: Competing with information in a digital world.” **MIS Quarterly** 37, 2 (June 2013): 637-641.
- Khaosanit D. “Legal Measures in Private Data Protection : Case Study in Finance and Banking of Commercial Bank.” M.A. thesis, Dhurakij Pundit University, 2018.
- Koene A. Clifton, C., Hatada Y. Webb H., and Richardson, R. **A governance framework for algorithmic accountability and transparency** [Online]. Available URL: [https://www.europarl.europa.eu/stoa/en/document/EPRS_STU_\(2019\)624262](https://www.europarl.europa.eu/stoa/en/document/EPRS_STU_(2019)624262), 2019 (April, 4).

- Lapowsky I. **How Cambridge Analytica Sparked the Great Privacy Awakening** [Online]. Available URL: <https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening>, 2019 (March, 17).
- Lazaro C. and Metayer D. L. "Control over personal data: True remedy or fairy tale." **SCRIPTed: A Journal of Law, Technology and Society** 12, 1 (June 2015): 3-34.
- Miller A. R. **The Assault on Privacy-Computers Data Banks and Dossiers**. Ann Arbour, MI: The University of Michigan Press, 1971.
- Nill A. and Aalberts R. "Legal and Ethical Challenges of Online Behavioral Targeting in Advertising." **Journal of Current Issues & Research in Advertising** 35, 2 (July 2014): 126-146.
- Parent William A. "Privacy, Morality and the Law." **Philosophy and Public Affairs**, 12, 4 (October 1983): 269-288.
- Phillips R. "Optimizing prices for consumer credit." **Journal of Revenue and Pricing Management** 12, 4 (July 2013): 360-77.
- Riedel Eibe. "New Bearings in German Data Protection. Judgement of the Federal Constitutional Court, Karlsruhe, of 15 December 1983." **Human Rights Law Journal** 94, 101 (January 1984): 94-116.
- Sloan Robert H., and Richard Warner. "Beyond notice and choice: Privacy, norms, and consent." **Journal of High Technology Law** 14, 2 (March 2013): 370-414.
- Smith H. J., Dinev T., and Xu H. "Information privacy research: An interdisciplinary review." **MIS Quarterly** 35, 4 (December 2011): 989-1016.
- Solove Daniel J. **The future of reputation: Gossip, rumor, and privacy on the internet**. New Haven: Yale University Press, 2007.
- Srichola S. and Tipayanee P., "Legal Issues Related to Credit Information on the Use of Credit Information for Other Purposes." **DPU Graduate Studies Journal** 4, 3 (March 2016): 215-226.
- Staten M. "Risk-Based Pricing in Consumer Lending." **Journal of Law, Economics & Policy** 11, 1 (March 2015): 33-58.
- Tene O. and Polonetsky J. "Big data for all: Privacy and user control in the age of analytics." **Northwestern Journal of Technology and Intellectual Property** 11, 5 (April 2013): 240-272.

- Vaccaro A. and Madsen P. “Corporate dynamic transparency: the new ICT-driven ethics?.” **Ethics and information technology** 11, 2 (June 2009): 113-122.
- Van Ooijen I. and Vrabec H. U. “Does the GDPR enhance consumers’ control over personal data? An analysis from a behavioural perspective.” **Journal of Consumer Policy** 42, 1 (March 2019): 91-107.
- Warren S. and Brandeis L. “The right to privacy.” **Harvard Law Review** 14, 5 (December 1890): 193-220.
- Westin Alan F. “Privacy and freedom.” **Washington and Lee Law Review** 25, 1 (March 1968): 166-170.
- Wilairat Y. “Problems on “Credit Information” under the Law Relating to Credit Information Business.” M.A. thesis, Thammasat University, 2017.
- World Bank. **The Role of Consumer Consent in Open Banking: Financial Inclusion Support Framework** [Online]. Available URL: <https://documents.worldbank.org/curated/en/099425002082230437/pdf/P1705050aeb8e704f088260f228802b73b8.pdf>, 2021 (December, 15).
- Article 29 Working Party. “Guidelines on Consent under Regulation 2016/679.” (6 July 2018).
- Article 29 Working Party. “Opinion 15/2011 on the Definition of Consent, Article 29.” 13 July 2011.
- Article 29 Working Party. “Working Document on the processing of personal data relating to health in electronic health records (EHR).” 15 February 2007.
- Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 1995.
- The White House. “Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy.” 1 February 2012.
- Asia-Pacific Economic Cooperation Privacy Framework 2005.
- Convention for the protection of individuals with regard to the processing of personal data.

Council of Europe. **Convention 108+ Convention for the protection of individuals with regard to the processing of personal data** [Online]. Available URL: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf, 2022 (April, 25).

European Union General Data Protection Regulation 2018.

Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 2013.

Personal Data Protection Act 2019 (B.E. 2562), Thailand.

WP29 Opinion 15/2011 on the definition of consent (WP 187).

Deutsche Telekom AG v. Bundesrepublik Deutschland, CJEU, C-543/09, 2011.

Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others, CJEU, C-201/14, 2015.

Tournier v National Provincial Bank of England. 1 K.B. 461, 1924.

