# CIVIL LIABILITY UNDER DATA PROTECTION LAWS: A COMPARATIVE STUDY BETWEEN THAILAND'S PERSONAL DATA PROTECTION ACT AND THE EU'S GENERAL DATA PROTECTION REGULATION

BY

MR. THEERACHIT JITKARUNAWONG

AN INDEPENDENT STUDY SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF LAWS IN BUSINESS LAWS (ENGLISH PROGRAM)
FACULTY OF LAW
THAMMASAT UNIVERSITY
ACADEMIC YEAR 2019

COPYRIGHT OF THAMMASAT UNIVERSITY

Ref. code: 25626101040100INS

# CIVIL LIABILITY UNDER DATA PROTECTION LAWS: A COMPARATIVE STUDY BETWEEN THAILAND'S PERSONAL DATA PROTECTION ACT AND THE EU'S GENERAL DATA PROTECTION REGULATION

BY

MR. THEERACHIT JITKARUNAWONG

AN INDEPENDENT STUDY SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF LAWS IN BUSINESS LAWS (ENGLISH PROGRAM)
FACULTY OF LAW
THAMMASAT UNIVERSITY
ACADEMIC YEAR 2019
COPYRIGHT OF THAMMASAT UNIVERSITY

Ref. code: 25626101040100INS

THAMMASAT UNIVERSITY

FACULTY OF LAW

INDEPENDENT STUDY

BY

MR. THEERACHIT JITKARUNAWONG

ENTITLED

CIVIL LIABILITY UNDER DATA PROTECTION LAWS: A COMPARATIVE STUDY BETWEEN THAILAND'S PERSONAL DATA PROTECTION ACT AND THE EU'S GENERAL DATA PROTECTION REGULATION

was approved as partial fulfillment of the requirements for the degree of Master of Laws in Business Laws (English Program)

on October 7, 2020

Chairman _____

(Assistant Professor Korrasut Khopuangklang, Ph.D.)

Member and Advisor _____

(Lasse Schuldt, Ph.D.)

Dean _____

(Assistant Professor Munin Pongsapan, Ph.D.)

| | |
|---|---|
| Independent Study Title | CIVIL LIABILITY UNDER DATA PROTECTION LAWS: A COMPARATIVE STUDY BETWEEN THAILAND'S PERSONAL DATA PROTECTION ACT AND THE EU'S GENERAL DATA PROTECTION REGULATION |
| Author | Mr. Theerachit Jitkarunawong |
| Degree | Master of Laws |
| Major Field/Faculty/University | Business Laws (English Program)<br>Faculty of Law<br>Thammasat University |
| Independent Study Advisor | Lasse Schuldt, Ph.D. |
| Academic Years | 2019 |

## ABSTRACT

The General Data Protection Regulation (GDPR) imposes new challenges for both public sector and private sector in ensuring the protection of personal data of the data subjects. With stricter rules come more responsibility and the risk of encountering a civil action for damages. Article 82 of the GDPR gives the data subject a right to receive compensation from the data controller and/or the data processor for any material damage or non-material damage suffered as a result of an infringement of the regulation. While Thailand just enact the Personal Data Protection Act (PDPA) in 2019 and it is postponed to fully enforce in 2020.

This independent study examines what could constitute a compensable non-material or immaterial damage and how the compensation could be determined according to the GDPR of the European Union (EU) and the PDPA of Thailand. This is done through the legal dogmatic method in order to compare civil liability between the GDPR and the PDPA. From the study, although the GDPR becomes a new standard requires the member states to implement, it has been found that a lot of discretion is left up to the member states themselves in the EU when it comes to

Ref. code: 25626101040100INS

assessing damage. However, damage is to be interpreted according to the principles laid down by the European Court of Justice and the member states also need to take into account the principles of equivalence and effectiveness. The data subject also has the right to full compensation for the damage suffered and the compensation needs to be proportionate in connection with the damage. On the other hand, when considering Section 77 and 78 of the PDPA, it makes difference with the GDPR in some respects, such as the term of damage and damages. When it comes to award damages especially for immaterial damage, however, it becomes necessary to determine overall damage and take into consideration the circumstances of each individual case.

**Keywords:** Civil Liability, Data Protection, PDPA, GDPR

Ref. code: 25626101040100INS

# ACKNOWLEDGEMENTS

During I am doing this independent study, there is an incident of Corona Virus epidemic 2019 (COVID-19). Most of the people are required to be home quarantined and maintain social distancing in order to prevent the spread of the virus. It would fundamentally change virtually all aspects of our lives.

With respect to this independent study, it could not have been completed without support and help from many people. firstly, I would like to express my sincere gratitude to Dr. Lasse Schuldt, my advisor for the valuable support and constructive recommendations on this study. His guidance helped me in all the time of research and writing of this study. He always encourages me and gives positive thinking to achieve this hard time. I could not have imagined having a better advisor.

Besides my advisor, I would like to thank Assistant Professor Dr. Korrasut Khopuangklang, Associate Professor Arnon Mamout, Ajarn Thitirat Thipsamritkul and Ajarn Chawin Ounpat for their insightful comments and ideas, also for the hard question which incented me to widen my research from various perspectives.

Last but not the least, I must express my very profound gratitude to my family and my friends for providing mt with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this independent study. This accomplishment would not have been possible without them. If there is a deficiency within this thesis, I openly accept any kinds of critics and suggestions that will be useful for the quality improvement of the author in the future. Hopefully with the information of this thesis can be beneficial to many people.

Mr. Theerachit Jitkarunawong

Ref. code: 25626101040100INS

# TABLE OF CONTENTS


| | Page |
|---|---|
| ABSTRACT | (1) |
| ACKNOWLEDGEMENTS | (3) |
| LIST OF ABBREVIATIONS | (7) |
| CHAPTER 1 INTRODUCTION | 1 |
| 1.1 Background and Issues | 1 |
| 1.2 Hypothesis | 4 |
| 1.3 Objectives of the Study | 4 |
| 1.4 Scope of the Study | 5 |
| 1.5 Research Methodology | 5 |
| 1.6 Expected outcome | 6 |
| CHAPTER 2 DATA PROTECTION DUTIES AND CIVIL LIABILITY UNDER THE GDPR | 7 |
| 2.1 Brief History of Data Protection | 7 |
| 2.2 Principles Relating to Processing of Personal Data | 8 |
| 2.2.1 Lawfulness, Fairness and Transparency | 9 |
| 2.2.2 Purpose Limitation | 10 |
| 2.2.3 Data Minimization | 10 |
| 2.2.4 Accuracy | 11 |
| 2.2.5 Storage Limitation | 11 |
| 2.2.6 Integrity and Confidentiality (Security) | 12 |
| 2.2.7 Accountability Principle | 13 |


Ref. code: 25626101040100INS

2.3 Relevant Parties 13
2.3.1 Controller 13
2.3.2 Processor 14
2.3.3 Individual 15
2.4 Civil Liability under the EU's GDPR 15
2.4.1 Damage 15
2.4.1.1 Material Damage 16
2.4.1.2 Immaterial Damage 16
2.4.2 Burden of Proof 17
2.4.3 Compensation 18
2.4.4 Exemption from Liability 21
2.5 Summary 22

CHAPTER 3 DATA PROTECTION DUTIES AND CIVIL LIABILITY UNDER THE PDPA 24

3.1 Brief History of the PDPA 24
3.2 Guideline on Lawful Basis for Processing Personal Data 25
3.2.1 Contract Basis 25
3.2.2 Consent Basis 26
3.2.3 Vital Interest Basis 27
3.2.4 Legal Obligation Basis 28
3.2.5 Public Task Basis 28
3.2.6 Legitimate Interest Basis 29
3.2.7 Archives/Research/Statistics Basis 30
3.3 Relevant Parties 31
3.3.1 Data Controller 31
3.3.2 Data Processor 31
3.3.3 Data Subject 32
3.4 Civil Liability under Thailand's PDPA 33

Ref. code: 25626101040100INS

3.4.1 Damage 33
3.4.2 Burden of Proof 33
3.4.3 Compensation 34
3.4.3.1 Actual Damages 34
3.4.3.2 Punitive Damages 34
3.3.4 Exemption from Liability 35
3.5 Summary 36

CHAPTER 4 ANALYSIS OF CONTENTIOUS ISSUES REGARDING CIVIL LIABILITY UNDER THE PDPA 39

4.1 Categories of Civil Liability 39
4.2 Theory of Civil Liability 40
4.2.1 Liability based on Fault 41
4.2.2 Liability without Fault 41
4.3 Definition of Damage 42
4.3.1 Material Damage 43
4.3.2 Immaterial Damage 44
4.4 Calculation of Damages 47
4.4.1 Actual Damages 48
4.4.2 Punitive Damages 49

CHAPTER 5 CONCLUSIONS AND RECOMMENDATIONS 52

5.1 Conclusions 52
5.2 Recommendations 54

REFERENCES 56

BIOGRAPHY 65

Ref. code: 25626101040100INS

# LIST OF ABBREVIATIONS

| Symbols/Abbreviations | Terms |
|---|---|
| CCC | Civil and Commercial Code |
| DPO | Data Protection Officer |
| EU | European Union |
| GDPR | General Data Protection Regulation |
| PDPA | Personal Data Protection Act |
| UK | United Kingdom |

# CHAPTER 1
# INTRODUCTION

## 1.1 Background and Issues

At the moment, if we are talking about the toughest privacy and security law in the world, the first law that we are thinking of might be "The General Data Protection Regulation". This regulation came into effect on 25 May 2018.[1] It tightens Europe already with strict laws concerning what companies are able or unable to perform with personal data of people and conversely, it gives an opportunity for those people to control over their own personal data such as how his/her data shall be collected and used. Moreover, the GDPR forces companies to justify every single thing that they control or process with personal data. Although the GDPR is European Union legislation, it has a huge effect on businesses outside the EU including the US, China and Thailand. It could affect everyone no matter where you are or where you live. For non-EU countries, they are concerned with the GDPR due to several businesses collect or use EU residents' data they also use companies based in the EU for services and processing data. If a company fails to comply with the GDPR, the penalty could be up to 20 of millions of euros or 4 % of annual turnover whichever is larger under Article 83 (5) GDPR.

The old laws were written before smartphones started collecting massive amounts of sensitive information for companies like Google and Facebook. In times of worldwide connection via the Internet, the fear of the transparent person is omnipresent. The GDPR gives organizations guidelines on what they can and cannot do with personal data. It also makes them give users more clarity over the kind of data being used and how companies will use it.

---

[1] GDPR.EU, 'What is GDPR, the EU's new data protection law?' <https://gdpr.eu/what-is-gdpr/> accessed 13 June 2020.

Ref. code: 25626101040100INS

Personal data under the GDPR are any data that can identify someone that is a name, phone number or age. In addition, the laws also include things like an IP address or location data. Even tighter rules apply for sensitive information such as sexual orientation, religion, health data and political opinions. They are particularly worth protecting under Article 4 (1) GDPR.

The way that a company is able to collect personal data from the data subjects is that the data subjects often have to opt in to allow a company to use and process their personal data. It means that only a few ticked boxes by the data subjects, a company is allowed to use such personal data according to a very long statement that people rarely to read. In fact, some parts of the contents contain in the statement are a risk of disadvantage for the data subjects. The storage and processing of personal data are, therefore, read by the data subjects and at least permitted with the consent of the person concerned.

The fact is even today many people often handle their personal data too lightly and ignore how valuable it can be for companies and authorities. Global data companies such as Google and Facebook collect data on the activities of users from the World Wide Web. These master data from the location data to information on purchasing behavior to contacts are mostly used for the placement of individualized advertising for the respective user and they ultimately generate millions in profits every year. Personal data is, therefore, worth money.[2]

In addition, misuse of this sensitive data can also have consequences under criminal law. For example, a person is able to access bank data and thus, access accounts without authorization, false documents can be created and sold by using personal data or ID numbers and so on. It is considered that such person commits offences Computer Crime Act B.E. 2550 under Article 5, 9 and 10 regarding

[2] Jullanar Alwazir, 'Google and Facebook, the Data Collecting Companies' <https://medium.com/jullanar-alwazir/google-and-facebook-the-data-collecting-companies-42dd5cb0e016> accessed 20 July 2020.

Ref. code: 25626101040100INS

the illegal access to other people's computer systems[3] and offences relating to counterfeit and alteration under Title VII, Chapter 3 and 4 of Thailand's Criminal Code.

On the other hand, there are many companies contact with data subjects in the EU. Hence, Thailand has been affected to issue a regulation in connection with protecting personal data. Subsequently, Personal Data Protection Act B.E. 2562 was published in the Government Gazette since 27 May 2019[4] and this Act shall come into force except for the provisions of Chapter II, Chapter III, Chapter V, Chapter VI, Chapter VII, and Section 95 and Section 96, which shall come into effect after the period of one year from the date of its publication in the Government Gazette under Section 2 of this Act. Therefore, PDPA shall become full of enforcement on 27 May 2020.

Unfortunately for data subjects, on 21 May 2020, there was the Royal Decree[5] provided exemption for a wide list of companies both government sectors and private sectors such as a company which operate business of banking, communication, construction, education, insurance, medical and public health, professional practices, real estate, tourism, transportation and etc. by making the provisions of Chapter II, Chapter III, Chapter V, Chapter VI, Chapter VII, and Section 95 and Section 96 will be ineffective from 27 May 2020 until 31 May 2021. It means that

---

[3] Nbtc Administrator, 'Hacker – Cybercrime', (2016) <http://1secure.nbtc.go.th/?p=318> accessed 2 August 2020.

[4] Pra Ratcha Bunyud Koom Krong Kormoon Suan Bookkon Por.Sor. 2562 [Personal Data Protection Act B.E. 2562], Government Gazette Vol. 136 Sec. 69 Kor (27 May 2019): 52. (พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, ราชกิจจานุเบกษา เล่มที่ 136 ตอนที่ 69 ก (27 พฤษภาคม 2562): 52.)

[5] Pra Ratcha Kridsadeka Kamnod Nuayngan Lae Kidchakarn Tee Pookuabkoom Kormoon Suan Bookon Mai Yoo Paitai Bungkub Hang Pra Ratcha Bunyud Koom Krong Kormoon Suan Bookkon Por.Sor. 2562 Por.Sor. 2563 [Royal Decree defining agencies and businesses that personal data controllers are not subject to the Personal Data Protection Act B.E. 2562 B.E. 2563], Government Gazette Vol. 137 Sec. 37 Kor (21 May 2020): 1. (พระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563, ราชกิจจานุเบกษา เล่มที่ 137 ตอนที่ 37 ก (21 พฤษภาคม 2563): 1.)

PDPA was postponed an enforcement for a year and the data subject is unable to obtain protection from this Act as well as data controller still does not have any responsibility.

However, once this Act comes into effect in 2021, if data controller and/or data processor breach(es) or violate(s) any duties and it is caused damage to data subject under the PDPA, there will be a liability even civil liability, criminal liability and administrative liability. In this independent study, it is focused mainly on civil liability in Chapter 6 Section 77 and Section 78, in which the data controller and/or the data processer have strict liability to the data subject. The issues are who have the burden of proof, how can data controller and/or data processer exempt from civil liability, how to define "damage" under Section 77 due to it is prescribed very broad and no particular definition despite, in the GDPR mentions both material damage and non-material damage or immaterial damage together with example definition in the recitals, and under Section 78, the court is able to impose punitive damages for data subject which the GDPR did not provide it.

## 1.2 Hypothesis

Even though the PDPA has been adopted substantially from the GDPR, but the standard for civil liability in case of infringement of the PDPA are not sufficiently clear and foreseeable. However, the study is expected to show that the PDPA does not provide for civil liability in the case of purely immaterial damage. This is expected to be a shortcoming of the Act as immaterial damage appears to be a frequent category of damage in cases of personal data protection violations.

## 1.3 Objectives of the Study

1.3.1 To study the basic concept of civil liability relevant to data protection laws.

1.3.2 To study general principles of data protection laws.

Ref. code: 25626101040100INS

1.3.3 To clarify the right to compensation for the data subject.

1.3.4 To compare and analyze civil liability under data protection laws both Thai's Personal Data Protection Act and the EU's General Data Protection Regulation.

1.3.5 To propose a measurement of awarding damages under the Personal Data Protection Act B.E. 2562.

**1.4 Scope of the Study**

This independent study mainly focuses on the basic concept in connection with civil liability, general overview of data protection, but without limitation to, compare and analyze concerning similarity and difference between Thai's Personal Data Protection Act especially Chapter 6 Civil Liability Section 77 – 78 and the EU's General Data Protection Regulation particularly on Chapter 8 Remedies, liability and Penalties Article 82 Right to Compensation and Liability.

In addition, because in 2020 there is no precedent case under Personal Data Protection Act B.E. 2562 for the court to consider yet, therefore, it is necessary to study other existing provisions similar to civil liability under Personal Data Protection Act B.E. 2562. For instance, the Civil and Commercial Code, the Product Liability Act B.E. 2551 and the Enhancement and Conservation of National Environmental Quality Act B.E. 2535 etc.

**1.5 Research Methodology**

The research methodology of this independent study is conducted by documentary research inclusive of related statutes or regulations in Thailand and the European Union, Thai and foreign textbooks, legal articles and journals, thesis or dissertation, Thai Supreme Court's decision, precedent case in the EU, qualitative expert interviews and garner other related sources both online and offline in order to draw the attention regarding civil liability under data protection laws and find out the

Ref. code: 256261010401001NS

difference between Thai's Personal Data Protection Act and the EU's General Data Protection Regulation.

**1.6 Expected Outcome**

1.6.1 To deeply understand civil liability under data protection laws.

1.6.2 To thoroughly understand principles concerning data protection laws and the responsibility of data controller and data processor.

1.6.3 To distinguish civil liability between Thai's Personal Data Protection Act and EU's General Data Protection Regulation.

1.6.4 To understand the right of data subject to seek compensation and damages with fairness.

1.6.5 To demonstrate an example scenario in case it happens in Thailand when PDPA fully comes into effect.

Ref. code: 25626101040100INS

# CHAPTER 2
# DATA PROTECTION DUTIES AND CIVIL LIABILITY UNDER THE GDPR

## 2.1 Brief History of Data Protection in the European Union

The protection of personal data, one of the privacy right, is a fundamental right expressed in Article 8 of the EU Charter of Fundamental Rights.[6] Furthermore, personal data of the EU citizen shall be protected under Article 16 of the Treaty on European Union and the Treaty on the Functioning of the European Union,[7] which also contains the legal basis for adopting rules for the protection of personal data. The purpose of the data protection regulation is to strengthen personal data protection rights of individuals and facilitate the free flow of personal data in the internal market. The personal rights are not absolute. There must always be a balance between the right of the individual and the right in freedom of others.[8]

In 1995, the European Data Protection (Directive 95/46/EC) on the protection of individuals in relevant to the processing of personal data and on the free movement of such data is adopted. It not only reharmonized legislation but also led to new differences. This directive is not directly binding on all European countries that is why the European Commission worked on the GDPR almost ten years. This resolution laid down one binding set of rules across the EU, included better rights for individuals increased liability and additional powers for supervisory authorities.[9] Subsequently, in 2016, the EU adopted the GDPR and it affects to several countries

---

[6] European Union Agency for Fundamental Rights, 'Article 8 – Protection of personal data' <https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data> accessed 20 July 2020.

[7] Article 16 of the Treaty on European Union and the Treaty on the Functioning of the European Union, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012E%2FTXT> accessed 20 July 2020.

[8] CIPPTraining, 'Origins and Historical Context of EU Data Protection Law' <https://www.youtube.com/watch?v=hFbmkFUFGpk> accessed 8 August 2020.

[9] ibid.

Ref. code: 25626101040100INS

all around the world that have relationship with the European countries. It replaces the Directive 95/46/EC which was adopted at the time when people frequently used internet for transferring information to each other. The GDPR is currently recognized as law across the EU. Member States are required to ensure that in their countries have a regulation following the GDPR and it is implementable within 2 years or by May 2018.[10] It leads to other countries all over the world attempt to comply with such regulations because such compliance may yield economic benefits.

In addition, the reason why the EU decided to establish a regulation to replace the Directive 95/46/EC was to create harmonization between Member States since it was found that there were differences in the implementation of the personal data protection in each country and the level of personal data protection between Member States was also different and inequal for the rights. The more different regulatory circumstance interrupted the free flow of information, the further governments and businesses are required to arrange specific resolution for increasing discontinued scenarios.[11]

## 2.2 Principles Relating to Processing of Personal Data

Data protection law requires compliance with several principles which are stipulated in Article 5 of the GDPR. An individual may bring an action or a lawsuit against the controller where he or she suffers damage as a result of a breach by the controller of one or more of the following principles.[12]

---

[10] European Data Protection Supervisor, "The History of the General Data Protection Regulation", <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en#:~:text=It%20replaces%20the1995%20Data%20Protection,their%20countries%20by%20May%202018.> accessed 24 July 2020.

[11] Alan Calder, EU GDPR A Pocket Guide second edition (IT Governance Publishing 2016), p.16.

[12] Peter Carey, Data Protection A Practical Guide to UK and EU Law (Oxford University Press 2018), p.32.

Ref. code: 25626101040100INS

### 2.2.1 Lawfulness, Fairness and Transparency

This principle apply to all processing of personal data and it can be divided into three elements: (1) to process personal data lawfully; (2) to process personal data fairly and (3) to process personal data transparently.[13]

Lawfulness of processing personal data is required the consent of the individuals or another lawfully basis under the GDPR, such as necessity to perform according to the contract, it is necessary for the purpose of legitimate interests of the controller, necessity to protect the vital interests of the individuals.[14]

Besides processing personal data lawfully, it is required to process fairly. This principle is in connection with the relationship between the controller and the individuals. Controllers shall notify the individuals what they are dealing with their personal data and the individuals must understand what is happening with their data. Moreover, the individuals have to know the risks and how to solve the problem when it is in breach.[15]

In a transparent manner, the controller is required to take any proper measure in order to collect personal data from the individuals and inform them how their personal data will be used before start processing. The transparency of processing required unambiguous and simple language to be clear for the individuals.[16]

However, processing of personal data by the controllers shall meet at least one of the lawfulness conditions contained in Article 6 of the GDPR and the processing of special category personal data is made lawful by one of the conditions imposed in Article 9 of the GDPR.

---

[13] ibid., p.33.

[14] Europe C and Rights EUAF, Handbook on European data protection law: 2018 Edition (Council of Europe 2018), p.117 – 118.

[15] ibid., p.118 – 119.

[16] ibid., p.119 – 121.

Ref. code: 25626101040100INS

### 2.2.2 Purpose Limitation

The individuals have to be acknowledged the purpose of processing personal data before the controller collect their personal data to process such data. The controller is able to collect data especially personal data from the individuals only for specific purpose and such purpose needs to be explicit or legitimate purpose. The Controller is unable to process the data in any manner that is incompatible with the purpose which informed to the individuals or out of scope that is unforeseeable.[17]

For example, An airline company collects personal data from passengers for operation the flight, such as name, age or any special requirements in need. If the airline company as the controller would like to use such data to promote according to marketing plan, use of data for irrelevant purpose will be considered as processing data without legal basis.[18]

### 2.2.3 Data Minimization

Although the controller can collect personal data within the purpose, personal data shall be adequate, relevant and limited to what is necessary related to the purposes for which they are processed.[19] The controller is required to ensure that the processing of personal data is sufficient to properly fulfil a legitimate purpose and not process data to fulfill by other means.[20]

For instance, when HR department on behalf of a company recruits new employee to a vacancy position. The applicant is required to send resume to the company and it contains several personal data, such as contract information, education, experience in order to reach qualifications. Once it is submitted, it means

---

[17] supra note 12, p.34 – 35.

[18] supra note 14, p.123 – 124.

[19] Recital 39 of the GDPR.

[20] Information Commissioner's Office (ICO), 'Principle (c): Data minimisation' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/> accessed 20 July 2020.

Ref. code: 25626101040100INS

that the company collects personal data, the employer should determine what data is in need for consideration in order to put the new employee to the vacancy position. After review what data is necessary, the unnecessary data shall be deleted in order to minimize data collection.[21]

### 2.2.4 Accuracy

Controllers do not only collect accurate data, but also needs to keep the data up to date and regarding inaccurate data, it shall be erased or rectified without delay. It is relatively similar to the equivalent provision in the Directive 95/46/EC.[22] Thus, the collected data is required to be kept checking regularly the accuracy of data because if data is inaccurate, it might be caused damage to the individual. An example, when a businessman desires to request for a credit from financial institute, it will usually check the credit information of the customer. If database in connection with the credit history is incorrect or out of date, such as the customer has an outstanding balance, despite he already paid, it will turn out that he has not good credit, this customer may suffer negative effects from this inaccurate data.[23]

### 2.2.5 Storage Limitation

This principle provides that personal data shall not be kept in database longer than necessity to the purposes of processing. The objective of this principle is that organizations do not retain obsolete data, and its wording in the GDPR is substantially similar to that contained in the Directive 95/46/EC.[24]

---

[21] Paul Voigt and Axel von dem Bussche, The EU General Data Protection Regulation (GDPR) A Practical Guide, (Switzerland: Springer International Publishing 2017), p.91.

[22] Information Commissioner's Office (ICO), 'Principle (d): Accuracy' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/> accessed 20 July 2020.

[23] supra note 14, p.301.

[24] supra note 12, p.38.

Ref. code: 25626101040100INS

Organizations should create Retention Policies in order to enforce storage limitation. There are a set of guidelines and standards that contain procedure to store and organize the data and set deadlines for erasure of unnecessary data.[25]

In addition, the important question for the controller is how long personal data will be kept, the answer depends on the purposes that the controller and the individual are agreed. Personal data also must be erased or anonymized when they are no longer needed it. However, right to erasure can be done by request from the individuals. Lastly, controller can keep personal data for longer, if they are only keeping it for legitimate purposes, such as public interest archiving, scientific or historical research, or statistical purposes.[26]

**2.2.6 Integrity and Confidentiality (Security)**

When the controller are given a trust by the individuals, they shall process their personal data in a manner that guarantees the proper security of personal data, including preventing unauthorized or illegal processing and accidental loss, destruction or damage by means of technical and organizational measures.[27]

In a compliance with the principle, it should not be considered only Article 5 of the GDPR, it is required to determine in conjunction with Article 32 of the GDPR, which provides security of processing personal data as well. This principle is similar to standard in the Directive 95/46/EC, but in the GDPR is the controller has more tasks, especially, in the serious case, the controller is required to inform or notify not only the related national regulator, but also individuals who are affected.[28]

---

[25] supra note 21, p.92.

[26] Information Commissioner's Office (ICO), 'Principle (e): Storage limitation' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/> accessed 20 July 2020.

[27] Article 5 (1) (f) of the GDPR

[28] supra note 12, p.39 – 40.

Ref. code: 25626101040100INS

Further to technical and organizational measures, it could be pseudonymizing data and encrypting personal data, such as the sentence "Mr. Theera Jitkaruna was born 18 February 1958, has two children, one boy and one girl" can be pseudonymized the information as following: "TJ 1958 has two children, one boy and one girl"; or "123abC has two children, one boy and one girl". It will be unable to identify Mr. Theera Jitkaruna and such data are more likely to be protected properly and safe from misconduct by third-party.[29]

### 2.2.7 Accountability Principle

The above-mentioned principles are applied to personal data but the accountability principle under Article 5 (2) of the GDPR specifically states responsibility of the controller or it means that the processor is excluded. In addition, the controller is also required to comply with all respective six principles in order to protect personal data of the individuals.[30]

However, although this principle does not mention directly to the processor, but it does not mean the processor will not have any obligation. There is a connection between the controller and the processor, such as keeping a record of processing operations and appointing a Data Protection Officer or DPO under Article 5 (2), 30 and 37 of the GDPR.[31]

## 2.3 Relevant Parties

### 2.3.1 Controller

It is not limited to the natural person; the juristic person can also be considered as a controller. Moreover, it does not matter that such person is in the private sector or public sector, public authority or agency can be a controller as well.

---

[29] supra note 14, p.131 – 132.

[30] supra note 12, p.40.

[31] supra note 14, p.136.

To determine who is the controller, it has to consider the purposes of the processing of personal data. In this regard, it can be done solely or jointly controller.[32]

The controller is the person who makes decisions in connection with processing personal data and control the personal data which are processed, and the controller shall be responsible for all actions arising from processing personal data that decided. In addition, being a controller, it actually has power to use personal data of the individuals, but the power shall be in the scope which is given by the individuals and the controller has to comply with accountability under the GDPR. However, if an individual is processing personal data not for commercial purposes but for personally purposes, it is not subject to the controller under the GDPR.[33] Where there are more than one controller jointly determine the purposes and means of processing personal data, they shall be considered as joint controllers.[34]

### 2.3.2 Processor

Regarding entity of the processor, it is considered like the controller which can be a natural person or legal person, public authority, agency or other body. The key is the processor is appointed or designated by the controller to process personal data on behalf of the controller.[35] As a consequence, the processor process data not for his or her own interests, but for the interests of the controller. Although in the process of processing data, the processor has to make personally decisions on each action, Article 29 of the GDPR prescribes the main idea that the

---

[32] Article 4 (7) of the GDPR.

[33] Information Commissioner's Officer (ICO), 'What are 'controllers' and 'processors'?' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/#:~:text=The%20GDPR%20defines%20a%20controller,the%20processing%20of%20personal%20data.> accessed 27 July 2020.

[34] Article 26 (1) of the GDPR.

[35] Article 4 (8) of the GDPR.

Ref. code: 25626101040100INS

processor or any relevant person, who is able to access the personal data, is not allowed to process personal data or use such data for any activities, but there are an exception which is the processor or such person conduct by the instruction of the controller. If the processor or such person perform out of scope or purpose which the controller has agreed with the individual, such processor or such person shall be liable like they are controllers.[36]

### 2.3.3 Individual

It is the data subject who own the personal data which the GDPR aims to protect. As a result, the individuals have several rights under Chapter 3 of the GDPR. For example, the data subject has the right to request for permission from the controller to access his or her personal data and when such data are transferred to a third country, the data subject has the right to be informed;[37] when the data subject is no longer to store his or her personal data with the controller, he or she shall have the right to erasure or it calls right to or forgotten which the personal data will be disappear in the system.[38]

## 2.4 Civil Liability under the EU's GDPR

### 2.4.1 Damage

Under Article 82 (1) of the GDPR explicitly mentions both material damage and non-material (immaterial) damage. As a result, when there are data breaches by the controller or the processor, the individual can claim for any damage and it is interpreted very broad especially intangible damage, such as unacceptable from social, damage in relevant to mental and loss of confidence.[39] In this regard,

---

[36] supra note 33.

[37] Article 15 of the GDPR.

[38] Article 17 of the GDPR.

[39] supra note 21, p.205.

Ref. code: 25626101040100INS

the individuals are supposed to be compensated for the damage that they have suffered from the act of the controller or the processor.[40]

However, the concept of damage under the GDPR shall be interpreted unrestrictedly. It is not only material damage, but also immaterial damage. Under Recital 75 of the GDPR, there are some examples of damage which assist to determine damage, such as social discrimination, financial loss in the business, identity theft or fraud, damage to the reputation of the individual, loss of confidentiality of personal data, or any other damage in connection with social or economic disadvantage. Apart from such examples, the data subjects or any individuals who are violated of their rights or obtain inappropriate protection of their personal data by the controller, it might be considered as damage as well.[41]

**2.4.1.1 Material Damage**

Material damage or pecuniary damage is damage related to tangible thing, such as loss of assets or property, loss of wages and it usually has a bill or a receipt, such as medical bills, invoice. The key is it can be calculated into monetary value.[42] Hence, material damage always has evidence to prove and the court will award easier than non-material damage.

**2.4.1.2 Immaterial Damage**

It is also called non-material or non-pecuniary damage or moral damage means that damage which is irrelevant to the property or income of

---

[40] Recital 146 of the GDPR.

[41] Thomas Schweiger, 'EUR 800,-- in non-material damages under Art 82 GDPR awarded by Austrian Court for the processing of party preferences without legal basis' (2019), <https://www.linkedin.com/pulse/eur-800-non-material-damages-under-art-82-gdpr-court-schweiger> accessed 2 August 2020.

[42] Stack Exchange, 'What counts as material or non-material damage under the GDPR?' <https://law.stackexchange.com/questions/28928/what-counts-as-material-or-non-material-damage-under-the-gdpr> accessed 28 July 2020.

Ref. code: 25626101040100INS

any person. This damage covers wide range of damage and most of the legal systems accept that violation of personal freedom can be considered as immaterial damage. It is internal appearance of human so that it is difficult to prove and have evidence.[43]

For example, the feeling of pain, anxiety, mental distress, and spiritual suffering or torment. It includes injury to feelings or dignity as well as loss of enjoyment or loss of future wages.[44] The situation can be like, when a customer deposit money in the bank and he does not want anybody know this matter especially his wife who lives in the same house. Later, he moves to other city and inform new address to the bank. One day, he requests the bank for his statement, the bank approves his request and send his statement to the old address. His wife receives the statement and then have an argument with him. He feels very stressed and unhappy since then. This is considered as immaterial damage arising from breach of accuracy principle by the controller.

### 2.4.2 Burden of Proof

The data subject or the individual is required to demonstrate three elements to establish a controller or a processor liable for compensation which are (1) the performance of an unlawful act, such as the controller failed to comply with any principle under the Article 5 of the GDPR or the processor process personal data out of purpose limitation; (2) the existence of damages or compensation; and (3) a causation between the first element which is unlawful act and the second element which is the damages incurred.[45]

Besides the data subject needs to prove the above three elements, he or she is also required to present to the court who is the controller and who is

---

[43] Arta Dauti, 'Compensation for Immaterial (Moral) Damage Due to Violation of Personality Rights in Kosovo' (2017), Acta Universitatis Danubius. Juridica 13 (3), p.104 – 120.

[44] ibid.

[45] Brendan Van Alsenoy, 'Liability under EU Data Protection Law from Directive 95/46 to the General Data Protection Regulation' (2016), p.274.

Ref. code: 25626101040100INS

the processor. This burden of proof is a little bit difficult for the data subject because all information is with the controller and processor.

Ultimately, the data subject has to demonstrate damages both from material damage, such as expense for recovery and immaterial damage, such as extreme anxiety. This issue is also difficult and challenge for the data subjects. The most of difficulty for the data subjects is that how they can find the relevant evidence which is able to find or accessible by the controller or its processor only. As the personal data processing is normally conducted or analyzed by back office.[46]

Notwithstanding, in term of the controller and the processor, they also have defense to exemption from liability under Article 82 (3) of the GDPR, the controller or the processor shall not be liable to the data subject if such controller or processor are able to prove that there is no way to be responsible for the event giving rise to the damage.

In this regard, it means that when the existence of damage caused by non-compliant processing of a controller or processor, and the data subject has the right to claim for compensation or damages. The liability depends on the degree of processing responsibility between controllers and processors.[47]

### 2.4.3 Compensation

In case a company or an organization which they are considered as a controller or processor violated any provisions of the GDPR, as a consequence of infringement, the relevant individuals are able to claim for compensation that they have suffered even material damage or immaterial damage. Both damage will be calculated into actual damages by evidence or imposed by the court. The GDPR ensures that individuals will be furnished with compensation or any damages, no matter how many controllers or processors involved in the processing of the

---

[46] ibid.

[47] Neil Patrick, 'Your GDPR "Duties of Proof" and Liability' <https://www.digitalistmag.com/finance/2018/03/19/your-gdpr-duties-of-proof-and-liability-05961632/> accessed 25 July 2020.

Ref. code: 25626101040100INS

personal data of individuals. Compensation and damages can be claimed directly to the competent domestic courts where the cause of action is occurred in connection with infringement or violation of regulation.[48]

In the GDPR, there is merely actual damages that individuals can claim from the controller or the processor because it does not mention punitive damages in any regulation. The reason why the GDPR does not stipulates punitive damages in civil sanction may be it already have very high fine penalty up to 20 million Euro or 4% of global turnover (whichever is the higher) on the company or the organization of the controller or processor that breach the GDPR.[49]

There is a precedent case in Austria which the fact is that the Austrian Post as the defendant in this case had unlawfully collected and sold personal data of millions of individuals to business partners which it is considered as the political affinity of millions of Austrians. Regarding data protection dispute, an Austrian lawyer filed a lawsuit against the Austrian Post on the basis of Article 82 of the GDPR and claimed damages in the amount of EUR 2,500. The plaintiff considered his alleged political opinion a special category of personal data, the storage of which requires the legal basis of his consent according to Article 9 of the GDPR. The plaintiff also added that the Austrian Post had not informed the plaintiff about this processing of his data. The plaintiff claimed that, as a result of that unlawful and negligent processing, he irretrievably lost control of his data and suffered immaterial damage.[50]

---

[48] European Commission, 'Can my company/my organisation be liable for damages?' <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/can-my-company-my-organisation-be-liable-damages_en#:~:text=Individuals%20can%20claim%20compensation%20if,reputational%20loss%20or%20psychological%20distress.> Accessed 24 July 2020.

[49] Garon Anthony, 'Can English Law Insurance Policies Cover Fines Imposed Under GDPR?' <https://www.natlawreview.com/article/can-english-law-insurance-policies-cover-fines-imposed-under-gdpr> accessed 2 August 2020.

[50] Stephan Winklbauer, 'Austrian Court Ruling on Immaterial Damages for GDPR Violation – A Mere Violation of Data Protection Regulations is not Enough' (EuroCloud, 8 June 2020) <

The Court of first instance held that the political affinity of individuals must be considered as a special category of personal data, since it reflects the political opinion of that person. The Austrian Post has neither been able to provide a legal basis for the processing of these special categories of personal data, nor has it informed the plaintiff about such processing. As a result, the Austrian Post was held liable for a material breach of Article 9 of the GDPR as well as Article 14 of the GDPR. Both infringements were considered to constitute a material impairment of the basic rights and freedoms of the plaintiff and the court awarded the plaintiff the amount of EUR 800 as immaterial damages.[51]

Later, the Court of Appeal entirely dismissed the action on the ground that the plaintiff had neither sufficiently claimed nor proved the immaterial damage caused by infringement of the defendant. A mere violation of data protection regulations, even if it has led to short-term negative thoughts, does not reach the materiality threshold for immaterial damages. In this case, the materiality threshold of the GDPR is interpreted that not every violation of the GDPR results in claims for immaterial damage but only those where the data subject must have experienced a noticeable disadvantage and it must be an objectively comprehensible impairment of personal rights with a certain weight.[52]

Apart from the above case in Austria, there is also an interesting case in the English courts between Lloyd and Google.[53] This case was, however, not yet based on the GDPR but on the UK's Data Protection Act 1998. The fact is that Richard Lloyd, as personal and on behalf of 4.4 million iPhone users alleged that Google breached data privacy of the data subjects by collecting and selling personal data to advertiser company without consent of the iPhone users, despite those users set private for such data. As a result, Lloyd brought class action on behalf the iPhone

---

https://eurocloud.org/news/article/austrian-court-ruling-on-immaterial-damages-for-gdpr-violation-a-mere-violation-of-data-protection/> accessed 27 September 2020.

[51] ibid.

[52] ibid.

[53] Lloyd v. Google LLC [2019] EWCA Civ 1599

users to the competent court in the UK and his mainly argument is that the data subjects got loss of control over their personal data because of infringement of Google as controller and processor. In this case, he did not claim for other material or immaterial damage, such as financial loss or distress.[54] Surprisingly, the Court of Appeal's unanimous judgment award Lloyd for compensation due to Google violates or breaches of data protection legislation. Such act of Google causes the data subjects a loss of control of personal data. The very interesting thing is that the Court of Appeal award for compensation without proof of distress or any material damage.[55]

### 2.4.4 Exemption from Liability

When the data subject brings a civil case to the court for claiming compensation or damages from a controller or a processor, it is not every case that the court will render an order in favor to the data subject. If a controller or processor can demonstrate that they have already comply with the principle of data protection and processing personal data correctly, they shall not be liable for any damages. For instance, when a data breach or data leak causes a high degree of risk to the data subjects and such controller or any involving processors had already notified the situation to the data subjects within appropriate time and without delay. The outcome is that the controller or processor may be exempt from this in particular circumstance.[56]

---

[54] Simon Orton, Giles Pratt, Rhodri Thomas, Rachael Annear and Emilio Salice, 'Lloyd v Google: A watershed moment for data protection damages claims?' <http://knowledge.freshfields.com/en/Global/r/4022/lloyd_v_google__a_watershed_moment_for_data_protection> accessed 29 July 2020.

[55] Inforrm's Blog, 'News: Supreme Court grants permission to appeal in Lloyd v Google LLC' <https://inforrm.org/2020/03/11/news-supreme-court-grants-permission-to-appeal-in-lloyd-v-google-llc/> accessed 29 July 2020.

[56] Tim Hickman, 'Obligations of controllers and processors under the GDPR' <https://events.lawsociety.org.uk/uploads/files/96495e21-6c88-464c-ac7c-023de4533db1.pdf> accessed 25 July 2020.

Ref. code: 25626101040100INS

## 2.5 Summary

The GDPR is continuously developed to protect personal data of individual or the data subject because there is a lot of cases that companies or organizations took advantage and abused from collecting personal data in the past until now. If a company or an organization would like to collect personal data of the data subject from the EU with any reasons, they will be considered as a controller or processor as the case may be, as a result, they are required to comply with regulations of GDPR and maintain the important principles of data protections laws. If it appears that there is any infringement of the GDPR, they have to notify the relevant data subjects within appropriate time. Otherwise, they will be liable for both material and immaterial damage.

Further to material damage, it is quite clear because it can be calculated in form of an amount of money. For example, a hospital collects personal healthcare data from a patient. The authorized director of the hospital is a controller. A processor is their staffs who have duty to use or process the personal healthcare data of the patient or the data subject. Such data can be considered as sensitive data which is required to be protected with high standard by the GDPR.[57] If such data is leaked because a controller or processor breach of any regulations of the GDPR, it is a trigger that the data subject is able to claim for compensation or damages. In this case, suppose that the data subject is fired by his or her employer because they know about his or her health status that risk being COVID-19 from the hospital. Definitely, the material damage would be severance pay of the data subject and damages by unfair termination which can be calculated by his or her salary from the date he or she is terminated until retirement.

Regarding immaterial damage such as suffer or distress which are mental injury that difficult to impose as amount of money and the court has to use his discretion to impose the amount of damages.

---

[57] GDPR register, 'Healthcare sector: How to Comply With GDPR?' <https://www.gdprregister.eu/gdpr/healthcare-sector-gdpr/> accessed 29 July 2020.

Ref. code: 25626101040100INS

Due to the GDPR widely opens for the data subject to present material damage and immaterial damage which are awarded by discretion of the court, consequently, the GDPR does not mention about punitive damages.

However, the GDPR is not only the beginning of regulating data protection but it also inspires many countries in the world to have data protection laws such as Brazil, Australia, Japan and Thailand. Although most of their regulations are similar to the GDPR, but there are still some aspects that are different from the GDPR.[58] In particular, civil liability in the PDPA of Thailand that will explain details in next chapter.

[58] Dan Simmons, '9 Countries with GDPR-like Data Privacy Laws' (2019), <https://insights.comforte.com/9-countries-with-gdpr-like-data-privacy-laws> accessed 19 September 2020.

Ref. code: 25626101040100INS

# CHAPTER 3
# DATA PROTECTION DUTIES AND CIVIL LIABILITY UNDER THE PDPA

## 3.1 Brief History of the PDPA

After the GDPR is officially regulated and the EU takes it as serious matter to comply with it, several countries expedite to regulate data protection laws in order to set standard similar to the GDPR including Thailand.

With the rapidly developing of technology and increasing of infringement of personal data and privacy rights, especially use of personal data is exploited or disclosed by abuse or without the consent of the data subject for commercial benefit and/or for the benefit of using personal data to commit various offenses such as fraud, defamation, etc. These problems inevitably affect the confidence in digital development for the economy and society according to government policy. Therefore, it is necessary for Thailand to enact the protection of personal data law to create a mechanism and provide protection in the same standard of other countries and to be consistent with the international standard so that it effectively solves the problem of a personal data breach and ease of obligation for relevant parties.[59]

When consider the aspect of basic rights and freedoms according to the constitution of Thailand, privacy rights are protected under Section 14 of the first constitution of Thailand (or Siam at that time)[60] until now, the latest constitution of Thailand B.E. 2560[61], privacy rights are still protected under Section 34 to 36.

---

[59] ETDA, Draft of the Personal Data Protection Act, <https://ictlawcenter.etda.or.th/de_laws/detail/de-laws-data-privacy-act> accessed 2 July 2020.

[60] Rattammanoon Hang Ratcha Arnachak Siam [Constitution of Siam], Government Gazette Vol. 49 (10 December 1932): 529. (รัฐธรรมนูญแห่งราชอาณาจักรสยาม, ราชกิจจานุเบกษา เล่ม 49 (10 ธันวาคม 2475): 529)

[61] Rattammanoon Hang Ratcha Arnachak Thai [Constitution of Thailand], Government Gazette Vol. 139 Sec. 40 Kor (6 April 2017): 1 (รัฐธรรมนูญแห่งราชอาณาจักรไทย, ราชกิจจานุเบกษา เล่ม 134 ตอนที่ 40 ก (6 เมษายน 2560): 1.)

Ref. code: 25626101040100INS

Besides the protection of privacy rights under the constitution, the Civil Commercial Code also protects the privacy rights according to tort liability or unlawful act under Section 420 to 423 and the Penal Code has provision regarding the offence of disclosure of confidential under Section 322 to 323, moreover, there is the offence of defamation under Section 326 to 333 as well.[62]

However, the turning point of protection of personal data in Thailand occurred in 1997, Official Information Act B.E. 2540 was enacted by which contains the definition of "personal information" under Section 4 for the first time in Thai law. In addition, it is prescribed protection of personal information by the government agencies in Chapter 3, Section 21 – 25.[63]

With regard to the PDPA, it appears that the Cabinet approved in principle the draft Personal Data Protection Act in 2017 which actually drafted since before 2015 until it is enacted in 2019.[64]

### 3.2 Guideline on Lawful Basis for Processing Personal Data

As the GDPR is a prototype of standard regulation with regard to data protection, in Thailand, there is no practical guideline yet so, it can study in the GDPR. Regarding lawful basis for processing personal data, in the PDPA, it appears in Section 24 of the PDPA and it is able to compare with lawfulness of processing under Article 6 of the GDPR.

#### 3.2.1 Contract Basis

Basically, the terms and conditions of the contract will be bind the parties upon they are not against the law.[65] When processing of personal data is

---

[62] Nakorn Sareerak, Kwam Pen Suantua [Privacy], (Bangkok: P.Press Co., Ltd., 2014), p.240. (นคร เสรีรักษ์, ความเป็นส่วนตัว, (กรุงเทพมหานคร: บริษัท พี.เพรส จำกัด, 2557), น.240.)

[63] ibid.

[64] supra note 4.

[65] Section 151 of the CCC.

Ref. code: 25626101040100INS

necessary to provide service according to the contract that agreed by the data controller and the data subject, such as process financial information in order to calculate bank interest or when it is required to process the personal data in order to comply with request of the data subject before enter into the contract, such as check information before open an account or request for loan from the bank, contract basis can be applied only general personal data not including sensitive data, if use contract basis for processing, it is not required additional consent from the data subject. In this regard, contract basis can be applied for merely general personal data, not including of sensitive data.[66] For instance, in the e-commerce website, address of consumer is needed in order to deliver goods or send receipt according to contract of sales, or in booking hotel website, credit card information is collected as a security before enter into reservation of a room contract, or a company has to collect information concerning bank account of an employee in order to pay salary in accordance with contract of labor.[67]

Processing data on the ground of contract is limited only the personal data of the data subject, it excludes data from the third-party. For example, in case of insurance agreement, processing data of spouse as an insured can be done by receiving consent or legitimate interest within the scope that is foreseeable and reasonable.[68]

### 3.2.2 Consent Basis

There is a Latin quote said that "*volenti non fit injuria*". It means that "to a willing person, no injury is done." This doctrine holds that a person who willingly puts himself or herself in a dangerous situation, such person has to accept

---

[66] Piyabutr Bunaramrueang, Piti Eiamchamroonlarp, Chawin Ounpat, and Thitirat Thipsamritkul, Thailand Data Protection Guidelines 2.0, publish 1 (Bangkok: Chulalongkorn University Publishing, 2019), p.54.

[67] ibid, p.55.

[68] supra note 66.

Ref. code: 25626101040100INS

the consequence and is unable to sue for any damages.[69] In Section 19 – 21 of the PDPA, it is provisions in relevant to giving consent under the PDPA. Basically, the data controller is unable to collect, use or disclose personal data, unless the data subject gives consent before or at that time.

The elements of consent are consist of (1) freely given due to giving consent needs to be related to the contract or providing service without any conditions; (2) informed consent, it shall be easily understandable for average person, simple, clear and plain, and easily accessible.[70]

To enable consent, it shall be meet requirements of consent. Consent shall be given before processing data and no conditions in providing services or in other words, it may say that consent is separate from contract without doubt. The data controller has to clearly declare the objective of processing data and give an opportunity to the data subjects to take affirmative action by physical motion, such as the data subjects have to swipe bar and click. In opposite, the data controller shall give an opportunity for the data subjects to withdraw the consent easily as well as giving consent at the first time.[71]

### 3.2.3 Vital Interest Basis

In the event that data processing is necessary to protect vital interest of the data subject or any other persons, such as preventing serious hazards that may be harmful to health and life by processing health data or sensitive data, the operator will be able to use this vital interest basis to process the data only if the data subject is in a condition that cannot express his or her consent and there is no other way to protect the lives of others without having to process this data.[72]

---

[69] Cornell Law School, 'definition of volenti non fit injuria' <https://www.law.cornell.edu/wex/volenti_non_fit_injuria> accessed 1 August 2020.

[70] Suthitinun Srirat, Consent in Data Protection Law, (a Thesis for the Degree of Master of Laws, Faculty of Law, Thammasat University, 2018), p.283 – 284.

[71] supra note 66, p.58 – 64.

[72] ibid, p.75.

Ref. code: 25626101040100INS

For example, a hospital reveals health data of the patient in order to help such person who need urgent and unconscious treatment, or public health agencies process data in connection with public infection to monitor epidemic situations.

### 3.2.4 Legal Obligation Basis

In case that data processing is necessary for the performance of duty that the data controller has by the law, which such data controller is usually non-governmental organizations, it shall clearly state that they are performing their duties or complying with orders of any government authority.[73]

This basis will not be applied if the data controller has the discretion to process the data to comply with the law, or there are other appropriate alternative for complying with the law other than the processing of personal data. In the case of processing according to this basis, the data subject is not entitled to delete, transfer data, or object to processing, e.g. processing data according to the order by the court, or the employer disclosed the salary information of the employees to the Revenue Department to clarify the details of the income and expenditure calculations of the business under Section 65 Revenue Code.[74]

### 3.2.5 Public Task Basis

The data controller or the data processor who are able to process the data according to public task basis are usually government officials or organizations, such as the Office of the Courts of Justice, Secretariat of the House of Representatives and the Senate Officials of various ministries that perform legal duties, including private agencies that perform the duty as the state has assigned for the public benefit according to the law, such as driving license examination services. The duties and responsibilities of the mission shall be clear and can refer to specific laws that give authority. However, public task basis will not be applied when

---

[73] ibid, p.76.

[74] ibid.

Ref. code: 25626101040100INS

government agency can process the data without using personal data, such as the Bank of Thailand is able to investigate information regarding debt of the citizen from statistics that received from commercial banks without identifying any person.[75]

In addition, in case the data controller or the data processor are government agency, it is not only Section 4 of the PDPA that need to be concerned, but also Section 23 (1) of Official Information Act B.E. 2540. Both provisions are consistent with principle of necessity to conduct legal instruments and the state authority according to Section 77 of the Constitution of the Kingdom of Thailand, as well as Regulatory Impact Assessment or RIA that might affect to the privacy rights of personal data of the data subject.[76]

### 3.2.6 Legitimate Interest Basis

The data controller or the data processor may process the personal data by claiming legitimate interest basis of the data controller and third-party but it shall be reasonable and not out of scope of expectation of the data subject. For instance, to deter crime and fraudulent, to use data for internal management of the company, to assist the state officer in order to achieve their mission or public task by not contrary to duty of confidentiality. However, processing personal data on legitimate interest basis makes the processing be broad and flexible. Hence, the data controller is required to use their discretion very carefully in order to weight between legitimate interest and benefits of the data subject (Legitimate Interest Assessments – LIA). The data controller shall specify what is legitimate interest and what is necessity of processing personal data. Moreover, the data controller has duty to protect rights and liberty of the data subject as well. Such discretion of the data controller is very risk to make a decision that the data controller may be liable in the future. On the other hand, the data controller is unable to claim that they process personal data by legitimate interest basis just because they already announce in the privacy policy. If the contents in the policy do

---

[75] ibid, p.77.

[76] ibid, p.77 – 78.

Ref. code: 25626101040100INS

not stipulate specifically and ensure that the data subject has a chance to read because it cannot be expected that everyone will read privacy policy in detail.[77]

To use legitimate interest basis for processing personal data, the data controller is supposed to ensure that it is necessary to process data, it is obviously legitimate interest and weight LIA by considering the following factors, namely: (1) characteristics of data and benefits. This may depend on the relationship between the data controller and the data subject in order to understand what the data subjects expect of data management. (2) Impacts and risks of processing data, such as disclosing information or data to other people and (3) measures to protect data and protect the rights and interests of the data subjects.[78]

Examples of processing personal data by using legitimate interest basis are: authentication of a customer, collect time sheets of lawyer in order to consider profit sharing, information about check in and check out from a hotel in order that if there is a dispute, the hotel is able to check and investigate the person who commit a crime or unlawful act.[79]

### 3.2.7 Archives/Research/Statistics Basis

In general, this basis is considered merely a method to achieve a purpose of processing personal data. It makes difference to another basis which focus on specific objective. To process personal by archives or research or statistics basis, it is unable to apply only this basis. In practice, it is required to apply along with other basis such as consent basis or legitimate interest basis because this basis does not solely appear in the GDPR. Otherwise, the processing may be inconsistent with international practice including the GDPR and it is risk to reach the breach of processing personal data.[80]

---

[77] ibid, p.79.

[78] ibid, p.80.

[79] ibid, p.82 – 83.

[80] ibid, p.84 – 85.

Ref. code: 25626101040100INS

## 3.3 Relevant Parties

### 3.3.1 Data Controller

It is an individual or juristic person that is authorized to make a decision on behalf of the organization concerning collect, use or disclose a personal data of the data subjects.[81] In a company, there will only one person or group of person that is able to control over the personal data or it may say that the person who is an authorized director of the company, he or she will be the data controller.

The data controller has duty toward the data subject to collect data only necessary reasons and lawful basis. When personal data is collected, the data controller can use such data within objective that has obtained consent from the data subject. Keep data update and ensure or investigate such personal data is corrective data at all time. Delete or remove data when the time of collecting is over. Inform the data subject immediately when the data controller knows that data is leak and last but not least establish DPO.[82]

### 3.3.2 Data Processor

It is an individual or juristic person who carry out in connection with collection, use or disclosure of a personal data in accordance with an order or in the name of data controller. In this regard, such individual and juristic person is not data controller.[83] In a company, it may have a number of data processors not only employee in the company, but also the other outsource that the company hire them to process or analyze personal data.

---

[81] Section 6 of the PDPA

[82] Surangkana Wayuparb, "Personal Data Protection", in Seminar on the topic of Personal Data Protection, by Electronic Transactions Development Agency (ETDA) at Auditorium Head office of Thai Airways International Public Company Limited Bangkok, 2019: p.10.

[83] supra note 81.

Ref. code: 25626101040100INS

The data processor has duty to use personal data within the scope of lawful basis and inform the data controller when find out that personal data of the data subject is leak.[84]

### 3.3.3 Data Subject

It is the person who is the owner of personal data. In the PDPA of Thailand, there is no definition for Data Subject, but this law protects merely an individual not include juristic person.

The data subject has rights to access their personal data at all time, request for copy, edit, delete or remove, control and limit the processing of personal data and object or refuse act of the data controller and the data processor.[85]

Regarding personal data, it is data or information related to a person which is able to be directly or indirectly identified a person but excluding data of the deceased person in particular.[86] Moreover, there is a kind of personal data that shall be protected in particular, it is sensitive data under Section 26 of the PDPA. For example, personal data in relevant to racial or ethnic origin, political opinion, religious or philosophical beliefs, criminal history, medical information, sexual orientation and etc.[87] These sensitive personal data is risk to be used for unfair discrimination, it is therefore protected with high standard.[88]

---

[84] supra note 82.

[85] supra note 81.

[86] ibid.

[87] infra note 90, p.4.

[88] Piyabutr Bunaramrueang, Piti Eiamchamroonlarp, Chawin Ounpat, and Thitirat Thipsamritkul, Thailand Data Protection Guidelines 1.0, publish 1 (Bangkok: Chulalongkorn University Publishing, 2018), p.19.

Ref. code: 25626101040100INS

## 3.4 Civil Liability under Thailand's PDPA

### 3.4.1 Damage

Under Section 77 of the PDPA of Thailand, it states only "damage" and there is no definition for it. Generally, damage that the court will clearly award damages for the injured party usually are monetary loss or material damage due to it can be calculated from receipts or any relevant documents. This case will be changed when damage is unable to be calculated in form of money which is non-material damage. It is a normal kind of damage that will be occurred when there is an infringement of the PDPA, actually, also other Acts.

### 3.4.2 Burden of Proof

Due to Section 77 of the PDPA is prescribed in line with Section 96 of Enhancement and Conservation of National Environmental Quality Act B.E. 2535,[89] which is strict liability principle, it is easier for the data subject to prove liability of

---

[89] **Section 96 of Enhancement and Conservation of National Environmental Quality Act B.E. 2535** states that if leakage or contamination caused by or originated from any point source of pollution is the cause of death, bodily harm or health injury of any person or has caused damage in any manner to the property of any private person or of the State, the owner or possessor of such point source shall be liable to pay compensation or damages therefor, regardless of whether such leakage or contamination is the result of a willful or negligent act of the owner or possessor thereof, except in case it can be proved that such pollution leakage or contamination is the result of:

(1) Force majeure or war;

(2) An act done in compliance with the order of the Government or State authorities;

(3) An act or omission of the person who sustains injury or damage, or of any third party who is directly or indirectly responsible for the leakage or contamination.

The compensation or damages to which the owner or possessor of the point source of pollution shall be liable according to the foregoing first paragraph shall mean to include all the expenses actually incurred by the government service for the clean-up of pollution arisen from such incident of leakage or contamination.

Ref. code: 25626101040100INS

data controller and/or data processor but it does not shift burden of proof at all, the data subject still needs to prove in connection with relationship between action and result.[90]

### 3.4.3 Compensation

#### 3.4.3.1 Actual Damages

It is an amount of damages which is imposed to compensate the damage that occurs to the injured party and he or she has to pay out of pocket losses or pay in advance, such as future medical expenses and loss of income.[91] Actual damages include material damage and immaterial damage. In addition, it is possible to charge the interest after complete calculating the total of actual damages. The rate of interest is 7.5 percent per annum since the date of violation.[92]

In case the data controller and/or the data processor fail to comply with the PDPA and it causes damage to the data subject, regardless of whether such noncompliance was exercised willfully or negligently, the data controller and/or data processor shall be liable for actual damages arising from the violation of the PDPA.[93]

#### 3.4.3.2 Punitive Damages

Under Section 78 of the PDPA, apart from actual damages that the data subject will receive absolutely when show evidence to the court. The

---

[90] Tanavat Kitikomolsuk, The Determination of Punitive Damages in the Law on Enhancement and Conservation of National Environmental Quality, (a Thesis for the Degree of Master of Laws, Faculty of Law, Thammasat University, 2018), p.121.

[91] ibid., p.13 – 15.

[92] Section 7 and 206 of the CCC.

[93] Jutharat Anuktanakul, Nuanporn Wechsuwanarux, Keiko Shirai and Kiratika Poonsombudlert, 'Personal Data Protection Act: A New Era of Privacy Rights in Thailand' <https://www.theworldlawgroup.com/writable/documents/news/Chandler-Data-Mar-2019.pdf> accessed 29 July 2020.

Ref. code: 25626101040100INS

court is also empowered to order the data controller or the data processor to pay punitive damages in addition to actual damages. However, such punitive damages shall not exceed two times of the actual damages that the court already considered. To determine punitive damages, the court will consider other factors as well, such as financial status of the data controller and/or the data processor, the gravity level of the data controller and/or the data processor that cause the damage.[94]

The principle of punitive damages is applied only the law is allowed. It is a remedy and penalty by law to prevent violation of the law.[95] In term of the PDPA, punitive damages will at least make the data controller and the data processor to reconsider when they are ignoring to comply with the PDPA.

**3.4.4 Exemption from Liability**

Under Section 77 of PDPA, the data controller or the data processor will not be liable when they can prove that damage is arising from force majeure or act of god which is the circumstance that no one is able to prevent although he or she put best effort to control,[96] such as the data controller is hacked by a hacker or fire accident that destroy all system and data base at the place that the data controller or the data processor collect personal data of the data subjects.

In addition, if damage is arising from the act of the data subject even action or omission, the data controller or the data processor will not be liable as well, such as the data subject requests the data controller to return personal data.

Last but not least, exemption from liability can be when the data controller of the data processor need to comply with an order from the government

---

[94] ibid.

[95] supra note 90, p.124 – 128.

[96] **Section 8 of the CCC** "Force majeure means any event the happening or pernicious result of which could not be prevented even though a person against whom it happened or threatened to happen were to take such appropriate care as might be expected from him in his situation and in such condition."

Ref. code: 25626101040100INS

agency which have power by the law such as the company has to deliver profile of employee to the court as per a summon of request for document.

Although civil liability under the PDPA provides strict liability that will be advantage for the data subjects, there is a concerning exemption from civil liability which is "*force majeure*" or act of god that appears in the Section 77 (1) of the PDPA. It does not have definition for this word. As a result, it is required to consider Section 8 of the CCC.

### 3.5 Summary

It cannot refuse that one of the most important reason that the PDPA is enact because of the GDPR. However, in the remark of the PDPA stipulates that the reason why enact the PDPA is because there are currently a lot of case with regard to infringement of privacy rights of the data subject and it makes data subjects feel distress, annoyed and some case establish of damage to the data subject. In addition, collecting personal data in the digital age, it is more convenience, faster and easier to be violated and finally it will cause damage to the overall economy.

As a result, the data controller and the data processor according to the PDPA shall be responsible to the personal data that they collect from the data subject. Although the PDPA has yet to enforce because of the Royal Decree, but everyone concerning to the PDPA is supposed to prepare the system of collecting and processing personal data and study precedent case which related to the GDPR in order to prevent violation of data protection regulations that may occur in the future.

In case the data controller or the data processor fails to comply with their duty under the PDPA, such as processing personal data according to the contract, obtain consent from the data subjects before processing personal data that out of expectation of the data subjects. As a consequence, the controller or the data processor who violate or breach any provisions of the PDPA and it causes damage, they shall be liable to the data subject under Section 77 of the PDPA without

Ref. code: 25626101040100INS

proving that such data controller or data processor had done with intention or gross negligence because this provision rules a principle of strict liability to the data controller and the data processor. However, the data controller and the data processor may be exempt from liability when they are able to prove that the cause of damage occurred because of act of god or the event that out of control by them, or it occurred by the data subject, such as the data subject actually disclose his or her personal data to third-party. Apart from this exception, the data controller or the data processor will not be liable if they can prove that what they have done because of compliance with order from the government officer that authorized by the law. In addition, the data subject can also claim for expenses that he or she paid to prevent damage that will occur or refrain from damage.

Furthermore, although "damage" in the PDPA is not concrete at all because it is too broad and does not provide definition for the damage, there is punitive damages under Section 78 of the PDPA which not appear in the GDPR. The court has discretion to determine the amount of punitive damage in addition to the actual damages, but it shall not exceed two times of the actual damages. To use discretion by the court, it is supposed to consider along with the circumstance of the situation. For instance, the level of damage that obtained by the data subject, financial status of the data controller and the data processor etc.

To sue the data controller or the data processor by the data subject, it could be done within three years since the data subject knows the damage but shall not exceed of ten years after the cause of infringement. The data subject is able to sue at the competent court which consider the head of office of the data controller or the data processor's company or organization according to the principle of domicile of the defendant, or the court that cause of action is occurred in the jurisdiction.

In Thailand, there is no precedent case to study yet, but the data subject can study from the several cases in the EU and it can be imagine that some problems that the data subject often encounter all the times, such as a call from insurance company that the data subject may not know that how they get the data

Ref. code: 25626101040100INS

subject's phone number or the case that the data subject receives advertisement from many companies which some of them, the data subject does not want it to appear in his or her device.

When the PDPA comes into force in full of provisions, it will resolve many problems that only the CCC may not reach to the civil liability and make it clearer in connection with damage and damages for the data subjects.



Ref. code: 25626101040100INS

# CHAPTER 4
# ANALYSIS OF CONTENTIOUS ISSUES REGARDING CIVIL LIABILITY UNDER THE PDPA

## 4.1 Categories of Civil Liability

Liability is occurred when there is a person who acts with fault which means that a person does something by intention or negligence and it causes damage to the other according to the principle of no liability without fault. This principle can be applied both civil case and criminal case.[97] In term of civil liability, it is a legal obligation that requires a party to pay for damages or to comply with the judgment by the court. It makes difference from criminal liability which is often brought by the public prosecutor for the sake of due process and crime control. Regarding civil liability, it is usually brought by a private party to sue for damages or injunctions or compensation. For example, in a car crash case, the owner of the car which is crashed can sue the driver who drives a car negligently in order to request for monetary damages and may be non-pecuniary damages if he/she can prove for it.

A civil liability is often spoken of a contractual liability or a tort liability. The issue of dispute is supposed to be that the defendant of a civil liability is either liable or not liable to the plaintiff. If the defendant shall be liable, he/she only needs to make remedies to the plaintiff in a manner of money. The defendant does not have to be imprison or fine or any other kinds of criminal penalty.

The standard of proof in a civil liability case is lower than in a criminal liability case. The standard of proof in criminal case is “beyond reasonable doubt”, while in a civil case is “proof on the balance of probability” or “on the balance of

---

[97] Sanunkorn Sodtipan, Kham Athibai Kodmai Laksana Lamerd Judkarnngannoksung Lae Lapmikuandai [Explanation of Tort Agency without Specific Authorization and Undue Enrichment], 8th edn (Bangkok: Winyuchon Publisher, 2018), p.27. (ศาสตราจารย์ ดร. ศนันท์กรณ์ โสตถิพันธุ์, คำอธิบายกฎหมายลักษณะละเมิด จัดการงานนอกสั่ง และลาภมิควรได้, พิมพ์ครั้งที่ 8 (กรุงเทพมหานคร: สำนักงานพิมพ์วิญญูชน, 2561), น.27.)

Ref. code: 25626101040100INS

preponderance".[98] The general rule is the party who claims has a duty to prove what such party claims but if there is a presumption in law favorable to a party, such part shall be required to prove only that the conditions entitling him/her to avail himself/herself of the presumption have been fulfilled.[99]

Further to civil liability under the PDPA, it is clear that the PDPA addresses to unlawful act by adopting strict liability since the draft of the PDPA.[100] In this regard, if the data controller or the data processor and the data subject have an agreement among them, when any party breaches the duty according to the agreement, it will be considered liability under such agreement as contractual liability. In addition, if it appears that the data controller or the data processor breaches the duty under any provisions of the PDPA, the data subject is able to claim for compensation under Section 77 and Section 78 of the PDPA as well because contractual liability and unlawful act will exist side-by-side.

**4.2 Theory of Civil Liability**

Due to this independent study focus on civil liability under the GDPR and the PDPA, it is supposed to be notion concerning tort liability or unlawful act and I would like to scope merely 2 theories as follows:

---

[98] Jarun Pakdeethanakul, Kham Athibai Kodmai Laksana Payan [Explanation of Evidence Law], 4th edn (Bangkok: The Thai Bar), p.303 – 306. (ศาสตราจารย์พิเศษ จรัญ ภักดีธนากุล, คำอธิบายกฎหมายลักษณะพยาน, พิมพ์ครั้งที่ 14 (กรุงเทพมหานคร: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, 2562), น. 303 – 306.)

[99] **Section 84/1 of the CCC** "Any party raise the facts in order to support his or her pleading, such party has burden to prove the facts, but if there is assumption in the law or assumption that it should be which appear from normal circumstance to be advantage to any party, such party shall prove only he or she had already completely complied with the conditions that he or she will obtain benefits from the assumption."

[100] supra note 59.

Ref. code: 25626101040100INS

### 4.2.1 Liability Based on Fault

Basically, “liability based on fault” or “no liability without fault” are the same principle that a person who act against the law shall be liable when damage is occurred intentionally or negligently to other party and such damage is caused by that person.[101] It appears as a general rule according to Section 420 of the CCC. Consequently, the party who bring to case to the court shall have burden of proof for 4 elements as follows:

a) The damage is occurred.
b) It is intentionally or negligently caused by a person.
c) It has causation between the action and damage (the relationship between cause and effect).
d) How much the party who causes damage shall pay for compensation to other party.

If the plaintiff us unable to prove such 4 elements, the court may not favor the plaintiff for compensation or damages. In some cases, to prove intention or negligence is very difficult and too much burden for the injured party, applying theory of fault may not be appropriate or suitable for the injured party. However, in those cases, the other principle of unlawful act shall be applied such as strict liability that will be explained accordingly.

### 4.2.2 Liability without Fault

It can be called “strict liability”. It means that a person who is violated by the law does not need to prove standard of care or negligence due to it

---

[101] Chitti Tingsapat, Kham Athibai Pramuan Kodmai Pang Lae Panich Reang Matra Waduay Judkarnngannoksung Lapmikuandai Lamerd Bup 2 Matra 395 – 452 [Explanation of Civil and Commercial Code Sort Section Concerning Agency without Specific Authorization Undue Enrichment Tort Book 2 Section 395 – 452], (Bangkok: Professor Chitti Tingsapat fund Facult of Law Thammasat University, 2014), p.71. (จิตติ ติงศภัทิย์, คำอธิบายประมวลกฎหมายแพ่งและพาณิชย์ เรียง มาตรา ว่าด้วยจัดการงานนอกสั่ง ลาภมิควรได้ ละเมิด บรรพ 2 มาตรา 395 – 452, (กรุงเทพมหานคร: กองทุน ศาสตราจารย์จิตติ ติงศภัทิย์ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2557), น.71.)

Ref. code: 25626101040100INS

is exception of the general rule which is “no liability without fault”. On the other hand, it can also be called “objective responsibility” or liability based on assumption of the law without proving fault of the person who act against the law.[102] This theory is used in order to solve the problem that the plaintiff cannot prove fault of the defendant whether he/she causes damage with intention or negligence. Then, the law is unable to protect rights of the injured party to obtain compensation from violation. Strict liability is stipulated in many specific laws. For instance, The Effectiveness of the Enhancement and Conservation of National Environmental Quality Act B.E. 2535, The Product Liability Act B.E. 2551 and Civil Liability for Oil Pollution Damage Caused by Ships Act B.E. 2560.[103]

Under Section 77 of the PDPA, strict liability is adopted to make civil liability be stronger than unlawful act under Section 420 of the CCC and make the data controller and the data processor shall be easily liable to the data subject for non-compliance of the PDPA.

**4.3 Definition of Damage**

Damage is loss or injury caused by intention or negligence of somebody. It can be caused by breach of contract such as loss of profit or income (positive interest) or breach of precontract such as loss of opportunity or time consume loss (negative interest). On the other hand, it also can be caused by breach of legal duty such as injury to someone’s life, body, freedom, property, or any rights including damage to reputation.[104]

---

[102] supra note 98, p.495.

[103] Cheera Poompuang, Naew Kid Mhai Keawkub Kwam Rub Pid Tang Lamerd Kong Akkachon [“New Concept Concerning Tort Liability of Private Sector”], Office of the Council of the State, p.2 – 3. (จีระ พุ่งพวง, “แนวคิดใหม่เกี่ยวกับความรับผิดทางละเมิดของเอกชน”, สำนักงานคณะกรรมการกฤษฎีกา, น.2 – 3.)

[104] supra note 98, p.28 – 29.

Ref. code: 25626101040100INS

**4.3.1 Material Damage**

It is relating to monetary compensation. The loss can be calculated into an amount of money. For example, the costs for health care, loss of income, and other costs incurred due to the accident. In many cases, the assessment of the damage can be complicated because it takes a long time to establish the damage.[105] On the other hand, it may say that material damage is not only the thing that occur and exist but also the thing that is expected to occur including the thing that will definitely occur in the future. For instance, damage is caused to someone's body and he or she needs to be cured at the hospital. In this regard, the damage shall not be too far from the incident.[106]

When the data controller or the data processor breach of any duty under the PDPA and it causes damage to the data subject, there will be at least material damage to file a case against them.

Supposed, the director of a company as employer and the data controller collects personal data from its employee or the data subject and the HR service provider as the data processor is assigned to process such data accordingly. Then, the HR service provider discloses the personal data of the employee to the employer and it causes that the employer terminates employment contract of the employee. As a result, the employee will have a loss of wages and unemployed. In this scenario, the HR service provider breaches of data protection. The material damage is loss of wage. Therefore, both the employer as the data controller and the HR service provider as the data processor shall have liability against the employee as the data subject under the PDPA.[107]

---

[105] Cees Van Dam, European Tort Law, (2nd edn, OUP 2013) p.346.

[106] Pongsakorn Sookchuen, Damage in Tort Law under the Thai Civil and Commercial Code, (a Thesis for the Degree of Master of Laws, Faculty of Law, Thammasat University, 2013), p.41.

[107] Chusert Supasitthumrong, 'The reach and liabilities of the Personal Data Protection Act' <https://www.bangkokpost.com/business/1741919/the-reach-and-liabilities-of-the-personal-data-protection-act> accessed 29 July 2020.

Ref. code: 25626101040100INS

The data controller and the data processor both are having duty to protect personal data of the data subject. When the data controller or the data processor breaches of such duty, it may cause damage to the data subject. Regarding material damage, the scenario can be like when the data controller obtains personal data from the data subject for one reason but the data controller does not use such personal data according to the reason, such personal data is used for advertisement and it makes the data subject loses his job. The expected income of the data subject and any other things that have receipt such as medical bill can be claimed as material damage by the data subject.

**4.3.2 Immaterial Damage**

The injured party may not be caused only pecuniary (material) loss but also non-pecuniary (immaterial) loss, such as pain and suffering and loss of amenities.[108] In Thailand, immaterial damage is not specifically defined in the CCC but it usually appear in the plaint of the plaintiff that claim for damages in other forms, such as distress, melancholy, isolation, and disappointed. The reason that the law does not define immaterial damage because the law may want to cut off problem of proof the damages and it gives too much discretion for the court.[109] The Supreme Court will award compensation for immaterial damage when the plaintiff is able to prove that there is not only material damage, but also immaterial damage under Section 446 of the CCC because if there is only immaterial damage, the Supreme Court may not favor for the plaintiff. In addition, immaterial damage needs

---

[108] ibid, p.399.

[109] Porntip Sudti-Autasilp, Kasiahai Tang Chitchai: Suksa Kodmai Laksana Lamerd Kong Aungkrid Lae German Preabteab Kub Kodmai Laksana Lamerd Kong Thai [Non-material Damages: Study Tort Laws in England and Germany Compare with Tort Laws in Thailand], (Course: "Executive judge in the Court of First Instance" No. 13, Judicial Training Institute of the Court of Justice, 2014), p.21 – 22. (พรทิพย์ สุทธิอรรถศิลป์, ค่าเสียหายทางจิตใจ: ศึกษากฎหมายลักษณะละเมิดของอังกฤษและเยอรมันเปรียบเทียบกับกฎหมายลักษณะละเมิดของไทย, (หลักสูตร "ผู้พิพากษาผู้บริหารในศาลชั้นต้น" รุ่นที่ 13, สถาบันพัฒนาข้าราชการฝ่ายตุลาการศาลยุติธรรม สำนักงานศาลยุติธรรม, 2557), น.21 – 22.)

Ref. code: 25626101040100INS

to be caused directly by the injury to the claimant. In case it is only indirect damage[110], such as the husband has no right to sue for mental damage caused by loneliness because he has lost a wife who used to make her husband's life happy from the person who caused his wife to die because of no ground by the law.[111]

Later, there is a case that the Supreme Court award immaterial damages for the plaintiff. The summary of the case is that although the defendant did not fire the firearms but the defendant used a firearm to intimidate the plaintiff as this causes damage to the plaintiff's health and hygiene of the plaintiff because it was shocking the plaintiff, causing psychological damage which is other damage apart from material damage under Section 446 of the CCC, the plaintiff has the right to claim compensation in this case.[112]

With regard to immaterial damage under data protection laws, it often happens when the data subject trusts the data controller and gives his personal data to the data controller. For instance, the data subject uses one social media platform and inputs his personal information by setting privacy as only the data subject can see the information. One day, the data controller or the data processor discloses that information to third-party and other people can reach the data subject with that information. The data subject will certainly feel uncomfortable and insecure that makes the data subject does not want to use any platform again. This can be a phobia of the data subject and it is considered as immaterial damages, the data subject shall be able to claim for damages, even though it is difficult to calculate.

Regarding non-material damage or immaterial damage, it may say that it is impossible to return everything back to the same but it still has

---

[110] ibid, p.25.

[111] Judgment of the Supreme Court No. 789/2502 (Assistant Department of Supreme Court Justice) <https://deka.supremecourt.or.th/> accessed 2 August 2020.

[112] Judgment of the Supreme Court No. 4571/2556 (Assistant Department of Supreme Court Justice) <https://deka.supremecourt.or.th/> accessed 2 August 2020.

Ref. code: 25626101040100INS

compensation.[113] When the PDPA is considered as specific law and there is not any provision concrete this issue, it is required to look into general provision which is unlawful act in the CCC. Basically, unlawful act appears in Section 420 of the CCC.[114] The dispute of immaterial damage under the PDPA might be right of privacy that is not provided explicitly in Section 420 of the CCC but it can be one of "any other right".[115] Right of privacy is an absolute rights arising from personal right and it shall be protected by the law.[116] Further to non-pecuniary loss, the closest provision is Section 446 of the CCC.[117] To apply this Section, it is required to have damage to body or health or liberty but it excludes any other right. Therefore, when the data subject would like to claim merely immaterial damage, the court may not award in favor of the data subject. This is the problem that need to be considered. Anyhow, to calculate the compensation, under Section 438 of the CCC[118] provides an essential guideline for the court to estimate the amount of damages, as pursued in the case, by making such awards based on the actual amount of damages suffered by the infringed party.

---

[113] Jakarin Khomase, Damages for Mental Injury Under Law of Torts, (a Thesis for the Degree of Master of Laws, Faculty of Law, Thammasat University, 2018), p.117 – 119.

[114] **Section 420 of the CCC** "A person who, willfully or negligently, unlawfully injures the life, body, health, liberty, property or any right of other people, shall commit a wrongful act and is bound to pay compensation therefore."

[115] supra note 107, p.72 – 74.

[116] ibid.

[117] **Section 446 of the CCC** "In the case of injury to the body or health of another, or in the case of deprivation of liberty, the injured person may also claim compensation for the damage which is non-pecuniary loss. The claim is not transferable, and does not pass to the heirs, unless it has been acknowledged by contract, or on action on it has been commenced."

[118] **Section 438 of the CCC** "The court shall determine the manner and the extent of the compensation according to the circumstances and the gravity of the wrongful act.
However, compensation may include restitution of the property of which the injured person has been wrongfully deprived or its value as well as damages for any injury caused."

Ref. code: 25626101040100INS

Interpretation of "damage" under Section 77 of the PDPA is supposed to be clear. As the guideline of the Supreme Court's decision appears that the court will not award the injured party for immaterial damage, unless there is a provision allow to claim for non-pecuniary damages like Section 4 of Liability for Damages Arising from Unsafe Products Act B.E. 2551.[119] However, there is a general rule in connection with non-pecuniary damages appear in Section 446 of the CCC but the difficulty is the court will not award solely for non-pecuniary damages. It shall have base or ground from material damage that the data subject has to prove for this.

On the other hand, there is a decision by the Court of Appeal Region 7, Department of environment case No. 3426/2550 (2007) in relevant to "damage" under Section 96 of Enhancement and Conservation of National Environmental Quality Act B.E. 2535 that when considering the act of the defendants and gravity of expanding of chemical, the court used his discretion to award not only material damage which is medical care, loss of property, but also immaterial damage which is loss of ability, distress and loss of quality of light. Such decision is quite favor to the group of plaintiffs and the total of damages is 29 million Baht.[120] It can see that that court is able to assess damages fairly and appropriately when the plaintiff can present the damage even material and immaterial damage.

Further to guideline of the Supreme Court of Thailand, the claim for damages from the action that cause immaterial damage is required to have a provision which allow the plaintiff to claim explicitly. However, when Section 77 of the PDPA does not define immaterial damage in particular and it needs to apply "any other right" in general unlawfully act under Section 420 of the CCC, the

---

[119] **Section 4 of Liability for Damages Arising from Unsafe Products Act B.E. 2551** "…"Mental damage" means pain, torture, phobia, anxiety, sorrow, shame or other similar types of mental damages."

[120] Krisanapol Na Thalang, Discretion of Imposing Damages in Environment Case, (Course: "Executive judge in the Court of First Instance" No. 11, Judicial Training Institute of the Court of Justice, 2013), p.26.

Ref. code: 25626101040100INS

Judgment of the Supreme Court in 2020 defined “any other right” that it is the right that is certified and protected by the law for the injured person and the defendant shall make the any other right of the plaintiff disappear. It makes the plaintiff has more burden of proof which are (1) what law protects the right and (2) how does it disappear.

### 4.4 Calculation of Damages

To calculate material damage is not difficult because it usually has an evidence, such as medical bills or receipt. But for immaterial damage, it is not easy to calculate. As a principle of unlawful act, when someone intentionally or negligently injures another person, he or she has to try to get the injured party return back to the former position that he or she was in before the injury. Most of the time that is impossible because of the nature of loss, but the court will impose damages as close as possible for the injured party.[121]

#### 4.4.1 Actual Damages

An amount awarded to the injured party to compensate for a proven injury or loss. Such damages are supposed to sufficient in amount to indemnify the injured party for the loss suffered. It can be estimated and monetarily compensated (pecuniary damages) or in some cases, it cannot be measured in money (non-pecuniary damages). Both material damage and immaterial damage will be counted as actual damages and it will be the base of calculation for punitive damages.

In connection with material damage which lead to calculate actual damages, it is clear that if the data subject as the plaintiff have documents such as a receipt or a bill, he or she is able to demand the amount of claim according to the amount which indicates in such documents. The problem is that if the incident

[121] Sununta Chankaew, Compensation in the Tort Case That Causing Non-Pecuniary Damage, <https://www.krisdika.go.th/data/activity/act225.pdf> accessed 2 August 2020.

Ref. code: 25626101040100INS

includes immaterial damage, how to calculate the damages? Especially, in the case that has only immaterial damage, how can the court award for damages?

As the Austria Post case in Chapter 2 of the study, the plaintiff shall not only demonstrate the disadvantage in his or her emotional life that was caused by the infringement of the GDPR and the resulting impairment of personality rights. In addition, the case-law of the Union Courts has also established as a condition for compensable damage that it must have been factual and certain. Consequently, there must be an actual impairment in the emotional in order for immaterial damages to be awarded under the GDPR. Even if it has led to short-term negative feelings, is not in itself a disadvantage that could lead to a claim for damages. Thus, a minimum of personal impairment must be demanded for the existence of immaterial damage.[122]

**4.4.2 Punitive Damages**

Damages awarded in addition to actual damages when the defendant acted with recklessness or gross negligence, malice or deceit. Punitive damages are intended to punish and deter violation in the future.

As punitive damages appears in Section 78 of the PDPA that the data subject can claim for punitive damages for twice of actual damages, it may help the court to calculate damages, when it is too difficult to calculate immaterial damage in the actual damages. For example, if the data subject can prove material damage in the amount of 1,000,000 Baht and cannot prove immaterial damage to receive compensation in the amount of 1,000,000 Baht, the court may award actual damages in the amount of 1,000,000 Baht for material damage and award punitive damages twice of actual damages which is 1,000,000 Baht as well. The total is the same and the method is different.

In Thai law, punitive damages are only permissible when the law expressly provides for it and currently, punitive damages are conducted to apply in

[122] supra note 50.

Ref. code: 25626101040100INS

several Acts. [123] For instance, Section 13 (3) of Trade Secret Act B.E. 2545[124], Section 16 of Promotion and Development of Quality of life of Persons with Disabilities Act, B.E. 2550[125], Section 42 of The Consumer Case Procedure Act B.E. 2551[126] and

---

[123] supra note 108, p.18 – 23.

[124] **Section 13 (3) of Trade Secret Act B.E. 2545** "(3) in case the evidence is clear that infringement of trade secret is conducted with willfully or maliciously causing the trade secrets to cease the quality of secrecy, the court may order the infringer to pay punitive damages in addition to the compensation granted under (1) and (2). However, it shall not exceed two times of the compensation under (1) or (2)"

[125] **Section 16 of Promotion and Development of Quality of life of Persons with Disabilities Act, B.E. 2550** "... Request according to paragraph one is not limited the right of the claimant to claim for damages on the ground of violation to the competent court and the court may impose other damages which is non-pecuniary to person with disability that is discriminated with unfair condition and if the discrimination with unfair condition to the person with disability is conducted with willfully or gross negligently, the court may impose punitive damages for the person with disability not exceed 4 times of actual damages ..."

[126] **Section 42 of The Consumer Case Procedure Act B.E. 2551** "If the cause of action arising from the business operator intentionally takes advantage from the consumer unfairly, or willingly causes damage to the customer, or gross negligent regardless of damage causing to the consumer, or act in a manner which contravenes the responsibility as a person having occupation or business which is trusted by the public, upon the judgment that the business operator pay the damages to the consumer, the court may order the business operator to pay punitive damages in addition to the actual damages imposed by the court as appropriated. In this regard, it shall take into account every circumstance, such as the damage to the consumer, the interest received by the business operator, financial status of the business operator, the mitigation of damage occurrence, as well as involving of the consumer.

The imposition of punitive damages under paragraph one, the court may impose not exceeding two times of the actual damages imposed by the court, but if the actual damage is not exceeding the amount of fifty thousand Baht, the court may impose punitive damages not exceeding five times of the actual damages imposed by the court."

Ref. code: 25626101040100INS

Section 11 (2) of Liability for Damages Arising from Unsafe Products Act B.E. 2551.[127]

[127] **Section 11 (2) of Liability for Damages Arising from Unsafe Products Act B.E. 2551** "If the facts appear that the business operator produced, imported, or sold the products, in sprite of awareness that the products were unsafe, or that the business operator was unaware, but committed gross negligence, or had awareness that the product was unsafe after it is produced, imported or sold the unsafe product without taking appropriate action to prevent damages from occurring, the court may order the business operator to pay punitive damages in addition to the amount of actual compensation imposed by the court, but not to exceed two times of the actual compensation. In this regard, it shall be considered along with circumstances, such as the severity of the damage obtained by the injured party, awareness of unsafety by the business operator, the period of time in which the business operator concealed the unsafety of the product, the actions taken by the business operator after becoming aware that the product was unsafe, the benefits received by the business operator, the financial status of the business operator, the mitigation of damage occurrence, as well as involving of the injured party."

Ref. code: 25626101040100INS

# CHAPTER 5
# CONCLUSIONS AND RECOMMENDATIONS

## 5.1 Conclusions

Since 1995 that the European Data Protection (Directive 95/46/EC) was created to harmonize the member states of the EU and set forth standard of data protection for the data subjects, it had been developed more than 20 years into the current version of the GDPR. From July 2018 to July 2020, course of overall sum of fines in cumulative reach 490 million Euro already.[128]

The GDPR is data protection law that regulates a compliance with personal data for organizations which deal with personal data of individuals. Although the GDPR is established by the EU, but it affects to several countries around the world including Thailand. It may say that the GDPR is a role model of data protection law to maintain principles namely: lawfulness, fairness and transparency, purpose limitation, accuracy, storage limitation, integrity, and confidentiality (security) and accountability.

In Thailand, the PDPA is designed to protect personal data of the data subject as well. This law is very new to Thailand and have not yet to be fully enforced. Anyone who is considered as data controller or data processor is required to adjust collecting data, setting privacy policy and compliance with the PDPA. Many organizations did not familiar with management of data like this and there are a lot of infringement of personal data. For instance, a bank collected personal data from its customer and sold to the insurance company then, the customer gets a stranger call from an insurance company. Currently, Thai people have more acquaintance with this law and somebody may see pop-up cookies policy or a small text file that

[128] GDPR Enforcement Tracker, 'Fines Statistics' <https://www.enforcementtracker.com/?insights> accessed 3 August 2020.

Ref. code: 25626101040100INS

a website stores on a device when visit the site [129] that need to be accepted or declined. It is one of requirements, if data controller would like to collect data from the data subject. In addition, there are other lawful basis for processing personal data e.g. public basis, legitimate interest basis and legal obligation basis.

With regard to liability under the GDPR and the PDPA, there are civil liability, administrative fines and criminal penalties. In this study, it focuses on merely civil liability by comparing both legislatives side by side especially in the aspect of immaterial damage that challenge Thai court determining right to compensate for the data subject.

Regarding the burden of proof, In the GDPR, the individual is required to prove the infringement of the controller or the processor. However, regarding the proof of fault, the burden of proof is shifted to the controller and/or the processor under Article 82 (3) of the GDPR. As for the PDPA, the data controller and/or the data processor shall be liable to the data subject only the damage is occurred from their action which is considered as strict liability regime, it assists the data subject to have less burden of proof by filing the case without proving the internal element. It does not matter that the data controller or the data processor willfully or negligently process personal data, only there is damage, it will establish liability for the data controller and the data processor.

In respect of damage, in the GDPR provides not only material damage but also immaterial damage, while the PDPA stipulates just “damage” that may make significantly difference for claiming damages. From the study, when consider the guideline of the precedent cases in the EU with regard to award damages for immaterial damage which is very high standard and the guideline of the Supreme Court of Thailand regarding immaterial damage, the PDPA is likely to not cover immaterial damage because the PDPA does not provide explicit definition of “immaterial damage” in any provisions. However, even though the PDPA does not separate material and non-material damage, but it allows the court to award punitive

[129] European Commission, ‘Cookies Policy’ <https://ec.europa.eu/info/cookies_en> accessed 3 August 2020.

Ref. code: 25626101040100INS

damages for two times of the actual damages, while the GDPR did not mention at all about punitive damages. In contrast, if any cases are brought to the court only immaterial damage, there will be no base to calculate actual damage and the court will be unable to award the plaintiff for punitive damages additionally.

Further to the exemption from liability, the PDPA is similar to the GDPR but the PDPA is stipulated in detail which are force majeure and compliance with the government agencies. However, the PDPA also prescribes limitation period for filing the case for 3 years after knowing the incident, it is longer than unlawful act under the CCC that is fair enough for the data subject.

Notwithstanding, the PDPA is currently postponed to 2021. I hope that it will come into force effectively and I expect that there will have an interesting case that the data subject is protected from infringement of the data controller and the data processor.

## 5.2 Recommendations

The recommendations tend to develop and improve the PDPA by studying from the GDPR as a role model in aspect of civil liability. I would like to recommend as follows:

The main issue of the study is immaterial damage that the PDPA does not provide clear definition of it and it causes that the court has to use discretion for interpretation on the word “damage” under Section 77 of the PDPA. As infringement of privacy rights will have much more protection under the PDPA, in addition, civil liability of under the CCC will be replaced by the PDPA, it should be prescribed explicit definition of “damage” in order to prevent narrow interpretation and the data subject will not be completely protected as it is a vital purpose of the data protection law because most of damage that occur to the data subject is immaterial damage. If only “damage” under the PDPA does not cover immaterial damage, the problem is that the PDPA has no enforcement to protect personal data of the data

Ref. code: 25626101040100INS

subject because it is unable to calculate for actual damage and absolutely cannot go to punitive damages.

Ref. code: 25626101040100INS

# REFERENCES

## Books and Articles

Brendan Van Alsenoy, 'Liability under EU Data Protection Law from Directive 95/46 to the General Data Protection Regulation' (2016).

Bunaramrueang P, Eiamchamroonlarp P, Ounpat C, and Thipsamritkul T, Thailand Data Protection Guidelines 1.0, publish 1, Bangkok: Chulalongkorn University Publishing, 2018.

Bunaramrueang P, Eiamchamroonlarp P, Ounpat C, and Thipsamritkul T, Thailand Data Protection Guidelines 2.0, publish 1, Bangkok: Chulalongkorn University Publishing, 2019.

Pakdeethanakul J, Kham Athibai Kodmai Laksana Payan [Explanation of Evidence Law], 4th edn, Bangkok: The Thai Bar (ศาสตราจารย์พิเศษ จรัญ ภักดีธนากุล, คำอธิบายกฎหมายลักษณะพยาน, พิมพ์ครั้งที่ 14 กรุงเทพมหานคร: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, 2562.)

Poompuang C, Naew Kid Mhai Keawkub Kwam Rub Pid Tang Lamerd Kong Akkachon ["New Concept Concerning Tort Liability of Private Sector"], Office of the Council of the State. (จีระ พุ่งพวง, "แนวคิดใหม่เกี่ยวกับความรับผิดทางละเมิดของเอกชน", สำนักงานคณะกรรมการกฤษฎีกา.)

Sareerak N, Kwam Pen Suantua [Privacy], Bangkok: P.Press Co., Ltd., 2014. (นคร เสรีรักษ์, ความเป็นส่วนตัว, กรุงเทพมหานคร: บริษัท พี.เพรส จำกัด, 2557.)

Sodtipan S, Kham Athibai Kodmai Laksana Lamerd Judkarnngannoksung Lae Lapmikuandai [Explanation of Tort Agency without Specific Authorization and Undue

Ref. code: 25626101040100INS

Enrichment], 8th edn, Bangkok: Winyuchon Publisher, 2018. (ศาสตราจารย์ ดร. ศนันท์กรณ์ โสตถิพันธุ์, คำอธิบายกฎหมายลักษณะละเมิด จัดการงานนอกสั่ง และลาภมิควรได้, พิมพ์ครั้งที่ 8, กรุงเทพมหานคร: สำนักงานพิมพ์วิญญูชน, 2561.)

Tingsapat C, Kham Athibai Pramuan Kodmai Pang Lae Panich Reang Matra Waduay Judkarnngannoksung Lapmikuandai Lamerd Bup 2 Matra 395 – 452 [Explanation of Civil and Commercial Code Sort Section Concerning Agency without Specific Authorization Undue Enrichment Tort Book 2 Section 395 – 452], Bangkok: Professor Chitti Tingsapat fund Facult of Law Thammasat University, 2014. (จิตติ ติงศภัทิย์, คำอธิบายประมวลกฎหมายแพ่งและพาณิชย์ เรียงมาตรา ว่าด้วยจัดการงานนอกสั่ง ลาภมิควรได้ ละเมิด บรรพ 2 มาตรา 395 – 452, กรุงเทพมหานคร: กองทุนศาสตราจารย์จิตติ ติงศภัทิย์ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2557.)

Van Dam C, European Tort Law, 2nd edn, OUP 2013.

**Thesis and Dissertations**

Calder A, EU GDPR A Pocket Guide second edition, IT Governance Publishing 2016.

Carey P, Data Protection A Practical Guide to UK and EU Law, Oxford University Press 2018.

Dauti A, ‘Compensation for Immaterial (Moral) Damage Due to Violation of Personality Rights in Kosovo’ (2017), Acta Universitatis Danubius. Juridica 13 (3).

Europe C and Rights EUAF, Handbook on European data protection law: 2018 Edition, Council of Europe 2018.

Khomase J, Damages for Mental Injury Under Law of Torts, a Thesis for the Degree of Master of Laws, Faculty of Law, Thammasat University, 2018.

Ref. code: 25626101040100INS

Kitikomolsuk T, The Determination of Punitive Damages in the Law on Enhancement and Conservation of National Environmental Quality, a Thesis for the Degree of Master of Laws, Faculty of Law, Thammasat University, 2018.

Na Thalang K, Discretion of Imposing Damages in Environment Case, Course: "Executive judge in the Court of First Instance" No. 11, Judicial Training Institute of the Court of Justice, 2013.

Sookchuen P, Damage in Tort Law under the Thai Civil and Commercial Code, a Thesis for the Degree of Master of Laws, Faculty of Law, Thammasat University, 2013.

Srirat S, Consent in Data Protection Law, a Thesis for the Degree of Master of Laws, Faculty of Law, Thammasat University, 2018.

Sudti-Autasilp P, Kasiahai Tang Chitchai: Suksa Kodmai Laksana Lamerd Kong Aungkrid Lae German Preabteab Kub Kodmai Laksana Lamerd Kong Thai [Non-material Damages: Study Tort Laws in England and Germany Compare with Tort Laws in Thailand], Course: "Executive judge in the Court of First Instance" No. 13, Judicial Training Institute of the Court of Justice, 2014. (พรทิพย์ สุทธิอรรถศิลป์, ค่าเสียหายทางจิตใจ: ศึกษากฎหมายลักษณะละเมิดของอังกฤษและเยอรมันเปรียบเทียบกับกฎหมายลักษณะละเมิดของไทย, หลักสูตร "ผู้พิพากษาผู้บริหารในศาลชั้นต้น" รุ่นที่ 13, สถาบันพัฒนาข้าราชการฝ่ายตุลาการศาลยุติธรรม สำนักงานศาลยุติธรรม, 2557.)

Voigt P and von dem Bussche A, The EU General Data Protection Regulation (GDPR) A Practical Guide, Switzerland: Springer International Publishing 2017.

Ref. code: 25626101040100INS

**Electronic Media**

Alwazir J, 'Google and Facebook, the Data Collecting Companies' <https://medium.com/jullanar-alwazir/google-and-facebook-the-data-collecting-companies-42dd5cb0e016>

Anthony G, 'Can English Law Insurance Policies Cover Fines Imposed Under GDPR?' <https://www.natlawreview.com/article/can-english-law-insurance-policies-cover-fines-imposed-under-gdpr>

Anuktanakul J, Wechsuwanarux N, Shirai K and Poonsombudlert K, 'Personal Data Protection Act: A New Era of Privacy Rights in Thailand' <https://www.theworldlawgroup.com/writable/documents/news/Chandler-Data-Mar-2019.pdf>

Article 16 of the Treaty on European Union and the Treaty on the Functioning of the European Union, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012E%2FTXT>

Chankaew S, Compensation in the Tort Case That Causing Non-Pecuniary Damage, <https://www.krisdika.go.th/data/activity/act225.pdf>

CIPPTraining, 'Origins and Historical Context of EU Data Protection Law' <https://www.youtube.com/watch?v=hFbmkFUFGpk>

Cornell Law School, 'definition of volenti non fit injuria' <https://www.law.cornell.edu/wex/volenti_non_fit_injuria>

ETDA, Draft of the Personal Data Protection Act, <https://ictlawcenter.etda.or.th/de_laws/detail/de-laws-data-privacy-act>

Ref. code: 25626101040100INS

European Commission, ‘Can my company/my organisation be liable for damages?’ <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/can-my-company-my-organisation-be-liable-damages_en#:~:text=Individuals%20can%20claim%20compensation%20if,reputational%20loss%20or%20psychological%20distress.>

European Commission, ‘Cookies Policy’ <https://ec.europa.eu/info/cookies_en>

European Data Protection Supervisor, “The History of the General Data Protection Regulation”, <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en#:~:text=It%20replaces%20the1995%20Data%20Protection,their%20countries%20by%20May%202018.>

European Union Agency for Fundamental Rights, ‘Article 8 – Protection of personal data’ <https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data>

GDPR.EU, ‘What is GDPR, the EU’s new data protection law?’ <https://gdpr.eu/what-is-gdpr/>

GDPR Enforcement Tracker, ‘Fines Statistics’ <https://www.enforcementtracker.com/?insights>

GDPR register, ‘Healthcare sector: How to Comply With GDPR?’ <https://www.gdprregister.eu/gdpr/healthcare-sector-gdpr/>

Hickman T, ‘Obligations of controllers and processors under the GDPR’ <https://events.lawsociety.org.uk/uploads/files/96495e21-6c88-464c-ac7c-023de4533db1.pdf>

Information Commissioner's Office (ICO), 'Principle (c): Data minimisation' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/>

Information Commissioner's Office (ICO), 'Principle (d): Accuracy' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/>

Information Commissioner's Office (ICO), 'Principle (e): Storage limitation' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/>

Information Commissioner's Officer (ICO), 'What are 'controllers' and 'processors'?' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/#:~:text=The%20GDPR%20defines%20a%20controller,the%20processing%20of%20personal%20data.>

Inforrm's Blog, 'News: Supreme Court grants permission to appeal in Lloyd v Google LLC' <https://inforrm.org/2020/03/11/news-supreme-court-grants-permission-to-appeal-in-lloyd-v-google-llc/>

Nbtc Administrator, 'Hacker – Cybercrime', (2016) <http://1secure.nbtc.go.th/?p=318>

Orton S, Pratt G, Thomas R, Annear R and Salice E, 'Lloyd v Google: A watershed moment for data protection damages claims?' <http://knowledge.freshfields.com/en/Global/r/4022/lloyd_v_google__a_watershed_moment_for_data_protection>

Patrick N, ‘Your GDPR "Duties of Proof" and Liability’ <https://www.digitalistmag.com/finance/2018/03/19/your-gdpr-duties-of-proof-and-liability-05961632/>

Schweiger T, ‘EUR 800,-- in non-material damages under Art 82 GDPR awarded by Austrian Court for the processing of party preferences without legal basis’ (2019), <https://www.linkedin.com/pulse/eur-800-non-material-damages-under-art-82-gdpr-court-schweiger>

Simmons D, ‘9 Countries with GDPR-like Data Privacy Laws’ (2019), <https://insights.comforte.com/9-countries-with-gdpr-like-data-privacy-laws>

Stack Exchange, ‘What counts as material or non-material damage under the GDPR?’ <https://law.stackexchange.com/questions/28928/what-counts-as-material-or-non-material-damage-under-the-gdpr>

Supasitthumrong C, ‘The reach and liabilities of the Personal Data Protection Act’ <https://www.bangkokpost.com/business/1741919/the-reach-and-liabilities-of-the-personal-data-protection-act>

Winklbauer S, ‘Austrian Court Ruling on Immaterial Damages for GDPR Violation – A Mere Violation of Data Protection Regulations is not Enough’ (EuroCloud, 8 June 2020) < https://eurocloud.org/news/article/austrian-court-ruling-on-immaterial-damages-for-gdpr-violation-a-mere-violation-of-data-protection/>

**Other Materials**

Judgment of the Supreme Court No. 73/2563 (Assistant Department of Supreme Court Justice) <https://deka.supremecourt.or.th/>

Judgment of the Supreme Court No. 4571/2556 (Assistant Department of Supreme Court Justice) <https://deka.supremecourt.or.th/>

Judgment of the Supreme Court No. 789/2502 (Assistant Department of Supreme Court Justice) <https://deka.supremecourt.or.th/>

Lloyd v. Google LLC [2019] EWCA Civ 1599.

Pra Ratcha Bunyud Koom Krong Kormoon Suan Bookkon Por.Sor. 2562 [Personal Data Protection Act B.E. 2562], Government Gazette Vol. 136 Sec. 69 Kor (27 May 2019): 52. (พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, ราชกิจจานุเบกษา เล่มที่ 136 ตอนที่ 69 ก (27 พฤษภาคม 2562): 52.)

Pra Ratcha Kridsadeka Kamnod Nuayngan Lae Kidchakarn Tee Pookuabkoom Kormoon Suan Bookon Mai Yoo Paitai Bungkub Hang Pra Ratcha Bunyud Koom Krong Kormoon Suan Bookkon Por.Sor. 2562 Por.Sor. 2563 [Royal Decree defining agencies and businesses that personal data controllers are not subject to the Personal Data Protection Act B.E. 2562 B.E. 2563], Government Gazette Vol. 137 Sec. 37 Kor (21 May 2020): 1. (พระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563, ราชกิจจานุเบกษา เล่มที่ 137 ตอนที่ 37 ก (21 พฤษภาคม 2563): 1.)

Rattammanoon Hang Ratcha Arnachak Siam [Constitution of Siam], Government Gazette Vol. 49 (10 December 1932): 529. (รัฐธรรมนูญแห่งราชอาณาจักรสยาม, ราชกิจจานุเบกษา เล่ม 49 (10 ธันวาคม 2475): 529)

Rattammanoon Hang Ratcha Arnachak Thai [Constitution of Thailand], Government Gazette Vol. 139 Sec. 40 Kor (6 April 2017): 1 (รัฐธรรมนูญแห่งราชอาณาจักรไทย, ราชกิจจานุเบกษา เล่ม 134 ตอนที่ 40 ก (6 เมษายน 2560): 1.)

Ref. code: 25626101040100INS

Wayuparb S, “Personal Data Protection”, in Seminar on the topic of Personal Data Protection, by Electronic Transactions Development Agency (ETDA) at Auditorium Head office of Thai Airways International Public Company Limited Bangkok, 2019.

# BIOGRAPHY

| | |
|---|---|
| Name | Mr. Theerachit Jitkarunawong |
| Date of Birth | March, 1990 |
| Educational Attainment | 2012: Bachelor of Sport Science, Chulalongkorn University<br>2016: Bachelor of Laws, Thammasat University<br>2019: Master of Law in Business Laws (English program), Thammasat University<br>2020: Barrister at Law, Thai Bar Association |
| Work Experiences | 2017 – Present:<br>Associate at Kanung & Partners Law Offices<br>2019 – Present:<br>Associate at Legal Guardians Co, Ltd. |

Publications

Theerachit Jitkarunawong, ‘Civil Liability under Data Protection Laws: A Comparative Study between Thailand's Personal Data Protection Act and the EU's General Data Protection Regulation’ (LL.M. Independent Study, Thammasat University, 2019)

Ref. code: 25626101040100INS