ปัญหาทางกฎหมายเกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562: ศึกษากรณีหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 39

โดย

ณฐพร วิริยะลัพภะ

วิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตาม

หลักสูตรนิติศาสตรมหาบัณฑิต

คณะนิติศาสตร์

บัณฑิตวิทยาลัย มหาวิทยาลัยรังสิต

ปีการศึกษา 2562

LEGAL ISSUES RELATING TO THE PERSONAL DATA PROTECTION ACT B.E. 2562: A CASE STUDY ON THE DUTY OF DATA CONTROLLERS ACCORDING TO SECTION 39

BY

NATAPOHN WIRIYALAPPA

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS FOR

THE DEGREE OF MASTER OF LAWS

FACULTY OF LAW

GRADUATE SCHOOL, RANGSIT UNIVERSITY

ACADEMIC YEAR 2019

วิทยานิพนธ์เรื่อง

ปัญหาทางกฎหมายเกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562: ศึกษากรณีหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 39

โดย

ณฐพร วิริยะลัพภะ

ได้รับการพิจารณาให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญานิติศาสตรมหาบัณฑิต

มหาวิทยาลัยรังสิต
ปีการศึกษา 2562

ผศ.ดร.ภูมิ มูลศิลป์
ประธานกรรมการสอบ

ศ.พิเศษ วิชา มหาคุณ
กรรมการ

ดร.ธเนศ สุจารีกุล
กรรมการและอาจารย์ที่ปรึกษา

บัณฑิตวิทยาลัยรับรองแล้ว

(ผศ. ร.ต. หญิง ดร. วรรณี ศุขสาตร)
คณบดีบัณฑิตวิทยาลัย
5 มิถุนายน 2563

Thesis entitled

LEGAL ISSUES RELATING TO THE PERSONAL DATA PROTECTION ACT B.E.2562: A CASE STUDY ON THE DUTY OF DATA CONTROLLERS ACCORDING TO SECTION 39

by

NATAPOHN WIRIYALAPPA

was submitted in partial fulfillment of the requirements
for the degree of Master of Laws

Rangsit University
Academic Year 2019

Asst. Prof. Dr. Poom Moolsilpa
Examination Committee Chairperson

Prof. Vicha Mahakun
Member

Thanes Sucharikul, S.J.D.
Member and Advisor

Approved by Graduate School

(Asst.Prof.Plt.Off. Vannee Sooksatra, D.Eng.)
Dean of Graduate School
June 5, 2020

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จได้เนื่องด้วยความช่วยเหลือและความกรุณาอย่างยิ่งของบุคคลหลายท่านซึ่งไม่สามารถนำมากล่าวในที่นี้ได้ทั้งหมด ผู้มีพระคุณท่านแรกที่ผู้เขียนขอกราบพระคุณเป็นอย่างยิ่งคือ ดร.ธเนศ สุจารีกุล ที่ได้ให้ความกรุณาสละเวลาอันมีค่ารับเป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ พร้อมทั้งได้สละเวลาอันมีค่าเป็นอย่างยิ่งเพื่อให้ความรู้ คำแนะนำ และแนวทางที่เป็นประโยชน์ต่อการศึกษาในการทำวิจัยในครั้งนี้จนกระทั่งวิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ด้วยดี

ผู้เขียนขอขอบคุณคณะกรรมการในการสอบทุก ๆ ท่าน ที่ได้สละเวลาอันมีค่าอย่างยิ่งในการเป็นกรรมการสอบวิทยานิพนธ์รวมถึงให้คำแนะในการตรวจสอบและแก้ไขวิทยานิพนธ์

อีกทั้งผู้เขียนขอขอบคุณ นายก่อเกียรติ บุญนวล ที่คอยช่วยเหลือทุก ๆอย่างและอยู่เคียงข้างจนวิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยดี

สุดท้ายนี้ผู้เขียนขอขอบคุณนายไพรัช วิริยะลัพภะ และ ฐิติพร วิริยะลัพภะ ที่สนับสนุนการศึกษาและให้กำลังใจอยู่เคียงข้างผู้เขียนมาโดยตลอด

อนึ่ง หากวิทยานิพนธ์ฉบับนี้มีคุณค่าและมีประโยชน์ต่อการศึกษาค้นคว้าของผู้ที่สนใจอยู่บ้างผู้เขียนขออุทิศให้แก่บุพการี คณาจารย์ ตลอดจนผู้แต่งตำรา บทความต่าง ๆ ที่ผู้เขียนได้ใช้ศึกษาค้นคว้า หากมีความบกพร่องประการใดผู้เขียนขอน้อมรับไว้แต่เพียงผู้เดียว

ณฐพร วิริยะลัพภะ
ผู้วิจัย

5806304 : ณฐพร วิริยะลัพภะ

ชื่อวิทยานิพนธ์ : ปัญหาทางกฎหมายเกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562: ศึกษากรณีหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา39

หลักสูตร : นิติศาสตรมหาบัณฑิต

อาจารย์ที่ปรึกษา : ดร. ธเนศ สุจารีกุล

บทคัดย่อ

วิทยานิพนธ์ฉบับนี้มีวัตถุประสงค์เพื่อศึกษาถึงบทบัญญัติ แนวคิดและความเป็นมาของพระราชบัญญัติข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อค้นหาเจตนารมณ์ของกฎหมายและปัญหาทางกฎหมายที่อาจเกิดขึ้นจากการบังคับใช้กฎหมาย ทั้งค้นหาแนวทางและข้อเสนอแนะในการปรับปรุงกฎหมาย โดยวิทยานิพนธ์ฉบับนี้ใช้วิธีการวิจัยเชิงคุณภาพ มุ่งเน้นการวิเคราะห์ข้อมูลเชิงเนื้อหาทางนิติศาสตร์จากกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล โดยการรวบรวมและค้นคว้าจากตำรา เอกสาร บทความ วารสาร วิทยานิพนธ์ ข้อมูลจากอินเตอร์เน็ตทั้งภาษาไทยและภาษาอังกฤษ

วิทยานิพนธ์ฉบับนี้พบว่า หน้าที่ของผู้ประกอบกิจการในการบันทึกข้อมูลส่วนบุคคลของลูกค้าและลูกจ้างเป็นภาระอย่างมากนับแต่กระบวนการบันทึกที่ใช้เทคนิค มีความซับซ้อน และมีความเสี่ยงที่ต้องรับผิดตามกฎหมาย ดังนั้นกิจการขนาดใหญ่และขนาดเล็กจำเป็นต้องจ้างผู้เชี่ยวชาญทั้งทางด้านกฎหมายและเทคนิคเพื่อให้คำปรึกษาในกระบวนการบันทึก แม้ว่ากฎหมายจะมีบทบัญญัติผ่อนปรนให้แก่กิจการขนาดเล็กก็ตาม แต่บทบัญญัติบางส่วนยังคงมีปัญหาในวลีที่ไม่มีความชัดเจน เช่น กิจการขนาดเล็ก “อาจได้รับการยกเว้น” จากหน้าที่ดังกล่าว และผู้ประกอบกิจการมีหน้าที่บันทึกเพียงข้อมูลซึ่ง “มีความเสี่ยง” ที่จะกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล อย่างไรก็ตามปัญหาอาจเกิดจากวลีที่ว่า “อาจได้รับยกเว้น” และ “มีความเสี่ยง” มีความหมายอย่างไร ซึ่งความไม่ชัดเจนของวลีทั้งสองดังกล่าวก่อให้เกิดความไม่แน่นอน และความกังวลกับบุคคลทุกฝ่ายที่เกี่ยวข้อง ด้วยเหตุดังกล่าว ผู้เขียนจึงมีความเห็นว่าบทบัญญัติบางส่วนโดยเฉพาะอย่างยิ่งวลีทั้งสองข้างต้นควรได้รับการแก้ไขให้มีความชัดเจน เพื่อให้การตีความกฎหมายเป็นไปในทางเดียวกัน

(วิทยานิพนธ์มีจำนวนทั้งสิ้น 136 หน้า)

คำสำคัญ: ข้อมูลส่วนบุคคล, กระบวนการบันทึก, กิจการขนาดเล็ก

ลายมือชื่อนักศึกษา ..... ลายมือชื่ออาจารย์ที่ปรึกษา .....

5806304	:	Natapohn Wiriyalappa
Thesis Title	:	Legal Issues Relating to the Personal Data Protection Act B.E. 2562: A Case Study on the Duty of Data Controllers According to Section 39
Program	:	Master of Laws
Thesis Advisor	:	Thanes Sucharikul, S.J.D.

Abstract

The main objective of this Thesis is to study the provisions, concepts, and evolution of the Personal Data Protection Act of B.E. 2562. It also purposes to delve into the spirits of the Act, and to dig up possible legal issues which may arise from the actual application of the Act, as well as to find ways and means to improve the Act. This Thesis is a legal qualitative analysis of the Act. It will employ data from various sources, including text books, articles, journals, theses, information from the Internet, both in Thai and English.

The Thesis finds that the duty of enterprises to record personal data of clients and employees are very onerous since recording processes are very technical, complicated, and prone to legal liability. Therefore, the enterprises, large and small, have to employ both technical and legal specialists to assist them in the recording processes. Although the Act has lenient provisions applicable to small enterprises, some of the provisions are problematic since they are ambiguous, such as the small enterprises "may be exempted" from the duty aforesaid, and they have the duty to record only the "data which are "likely or prone" to affect personal rights and liberty of the owners of the data". However, the problems may occur as to what the phrases "may be exempted" and "likely or prone" mean. These are the texts of the Act which are ambiguous, and thus they allow subjective appraisal and interpretation by all persons involved. The said texts of the Act also create uncertainty and apprehension on the part of all the enterprises. The Author of this Thesis, therefore, is of the opinion that some provisions of the Acts, including in particular the texts mentioned above, be amended to make them clearer, and thus amendable to their objective application.

(Total 136 pages)

Keywords: Personal Data, Recording processes, Small enterprises

Student's Signature …..... Thesis Advisor's Signature .....

สารบัญ

สารบัญ (ต่อ)

สารบัญ (ต่อ)

สารบัญตาราง

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ข้อมูลเกี่ยวข้องกับการดำเนินชีวิตของมนุษย์ในทุก ๆ ด้าน ถือเป็นหัวใจหลักของการทำงานและการทำธุรกิจทุกประเภท ข้อมูลยังเป็นแหล่งความรู้ที่นำมาใช้ประกอบการพิจารณาหรือประกอบการตัดสินใจในทุก ๆ เรื่อง อาทิเช่น การจัดซื้อจัดจ้าง การลงทุน การพิจารณาปรับเลื่อนขั้นเงินเดือน หรือการพิจารณาอนุมัติต่าง ๆ[1] เมื่อทุกอย่างบนโลกใบนี้ล้วนเป็นข้อมูล ข้อมูลจึงเปรียบเสมือนเครื่องมือชิ้นสำคัญที่จะทำให้ธุรกิจประสบความสำเร็จ ดังที่ไคลฟ์ ฮัมบี (Clive Humby) นักเศรษฐศาสตร์ชาวอังกฤษ (Britain) ได้กล่าวว่า “ข้อมูลคือน้ำมัน” หรือ “Data is the new oil”[2] ซึ่งในขณะนั้นประมาณ ปี พ.ศ. 2549 ความคิดดังกล่าวยังไม่ได้รับการยอมรับ เพราะการดำเนินธุรกิจในขณะนั้นมักจะมุ่งเป้าไปที่ผู้บริโภคที่อาศัยอยู่ในประเทศของผู้ประกอบกิจการเท่านั้น ขนาดของข้อมูลที่จำเป็นในการวิเคราะห์ และประมวลผล เพื่อทราบทิศทางของตลาดจึงมีขนาดไม่ใหญ่นัก แต่ในปัจจุบันด้วยเทคโนโลยีทางด้านโทรคมนาคม และเทคโนโลยีการขนส่งได้พัฒนาไปอย่างมาก ทำให้การติดต่อสื่อสาร การส่งสินค้า หรือการเดินทางระหว่างประเทศเป็นไปได้อย่างสะดวก รวดเร็ว ผู้ประกอบกิจการภายในประเทศก็เริ่มขยายธุรกิจของตนออกไปต่างประเทศมากยิ่งขึ้น ดังนั้น จึงมีความจำเป็นที่ผู้ประกอบกิจการจะต้องทราบข้อมูลเกี่ยวกับพฤติกรรมของผู้บริโภคภายในประเทศก่อนที่ผู้ประกอบกิจการจะตัดสินใจลงทุนขยายกิจการนั้น

ในยุคดิจิทัล (Digital Age) การดำเนินกิจกรรมต่าง ๆ ถูกขับเคลื่อนด้วยเทคโนโลยี วิถีชีวิตของผู้คนเริ่มผูกติดกับโลกออนไลน์ การสื่อสารกันในโลกออนไลน์ที่ผู้คนทั่วทุกมุมโลกสามารถติดต่อถึงกันอย่างสะดวกและรวดเร็ว ได้ขยายตัวจนกลายเป็นเครือข่ายทางสังคม (Social

---

[1] จาก *ข้อมูลหมายถึงหัวใจหลักของการทำงาน*, 2558. ลิขสิทธิ์ 2558 โดย IM2Market. สืบค้นจาก https://www.im2market.com/2015/11/14/2031

[2] From Data is not the new oil, by Samuel, F., 2019, Copyright 2019 by Samuel, F. Retrieved from https://towardsdatascience.com/data-is-not-the-new-oil-bdb31f61bc2d

Network) และขยายวงกว้างไปสู่การดำเนินกิจกรรมในเชิงธุรกิจ โดยนักธุรกิจส่วนใหญ่มองว่าเครือข่ายทางสังคมเป็นเครื่องมือเชื่อมต่อและสร้างมูลค่าทางธุรกิจได้ ไม่ว่าจะเป็นการซื้อขายสินค้าบริการ หรือการโฆษณาธุรกิจผ่านเครื่องมือออนไลน์ เสมือนผู้ประกอบกิจการมีหน้าร้านที่ทุกคนบนโลกสามารถเข้าถึงได้ การเชื่อมต่อกันทางธุรกิจในโลกออนไลน์นี้ย่อมมีการไหลเวียนของข้อมูลจำนวนมหาศาล (Big Data) เช่น ชื่อ นามสกุล หมายเลขบัตรประจำตัวประชาชน หรือหมายเลขบัตรเครดิต ข้อมูลการเข้าเว็บไซต์ เป็นต้น ข้อมูลเหล่านี้ล้วนเป็นข้อมูลส่วนบุคคลที่ผู้ประกอบกิจการได้เก็บรวบรวม และนำมาวิเคราะห์เพื่อให้ทราบถึงพฤติกรรมของผู้บริโภค และใช้ประโยชน์ในการเข้าถึงเป้าหมายเพื่อโฆษณาสินค้า หรือเพื่อดำเนินกิจกรรมทางธุรกิจอย่างอื่น เช่น ในกรณีของบริษัทกูเกิล (Google) ที่เริ่มต้นจากการทำเว็บไซต์ค้นหาข้อมูล (Search Engine) ให้รองรับการค้นหาได้หลายภาษา จึงมีผู้ใช้งานจากทั่วทุกมุมโลก ปัจจุบันพบว่ามีผู้ใช้บริการของกูเกิลมากกว่า 5,000 ล้านครั้งต่อวัน[3] ทำให้จำนวนข้อมูลที่เก็บได้จากคำค้นหา (Keyword) มีจำนวนมากพอที่จะนำมาวิเคราะห์ ประมวลผล เพื่อทราบว่าผู้คนมีความสนใจเกี่ยวกับสินค้า หรือบริการใด และทำตัวเป็นสื่อกลางโฆษณาสินค้า หรือบริการนั้นให้ตรงกับกลุ่มเป้าหมาย[4] หากเปรียบข้อมูลมีค่าดั่งน้ำมัน กูเกิลก็เปรียบเสมือนโรงกลั่นข้อมูลที่ผลิตข้อมูลได้อย่างมหาศาล แล้วขายข้อมูลที่กลั่นออกมาในรูปแบบของโฆษณา[5] ทำให้ในปัจจุบันปัจจุบันกูเกิลมีรายได้จากการโฆษณาเป็นหลัก[6] คำค้นหาที่เกิดจากการค้นหาของผู้ใช้บริการกูเกิลนั้น มีลักษณะเป็นข้อมูลทั่วไปที่ไม่สามารถระบุตัวบุคคลได้ กูเกิลจึงสามารถเก็บรวบรวมข้อมูลดังกล่าวได้โดยไม่ต้องขออนุญาตจากผู้ใช้บริการ ซึ่งการนำ

[3] From *63 Fascinating Google Search Statistics*, by Aleksandra, 2017, Copyright 2017 by Aleksandra. Retrieved from https://seotribunal.com/blog/google-stats-and-facts/

[4] จาก *ประวัติ Google (กูเกิล) ความเป็นมา มีมาอย่างไร*, 2556. ลิขสิทธิ์ 2556 โดย Modify. สืบค้นจาก https://www.modify.in.th/1772

[5] From *The world's most valuable resource is no longer oil, but data*, by David Parkins, 2017, Copyright 2017 by David Parkins. Retrieved from https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

[6] From *Top 10 Companies and Brands Owned by Google as of 2017*, by Juan D. R., 2017, Copyright 2017 by Juan David Rodriguez. Retrieved from https://learn.stashinvest.com/companies-brands-owned-google

ข้อมูลส่วนบุคคลมาใช้โดยไม่ได้รับอนุญาตจากเจ้าของข้อมูลย่อมเป็นการละเมิดสิทธิความเป็นส่วนตัว[7] อันเป็นสิทธิมนุษยชนขั้นพื้นฐานที่ควรได้รับความคุ้มครอง

ปัจจุบันประเทศต่าง ๆ ทั่วโลก ให้ความสำคัญกับสิทธิความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล หรือข้อมูลส่วนตัว ดังจะเห็นได้จากการผลักดันกฎหมายคุ้มครองข้อมูลส่วนบุคคลของแต่ละประเทศให้มีผลใช้บังคับเพื่อคุ้มครองสิทธิเกี่ยวกับข้อมูลส่วนบุคคล โดยการที่ผู้ใดจะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้อื่น จะต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และได้รับความยินยอมจากผู้นั้นเสียก่อน ดังนั้น ผู้ประกอบกิจการที่จะนำข้อมูลส่วนบุคคลมาวิเคราะห์เพื่อประโยชน์ในเชิงธุรกิจ ก็มีหน้าที่ต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และได้รับความยินยอมจากเจ้าของข้อมูลนั้นเสียก่อน อย่างไรก็ตาม ขั้นตอนในการขอความยินยอมเป็นเพียงหลักการคุ้มครองข้อมูลส่วนบุคคลประการหนึ่งเท่านั้น ผู้ประกอบกิจการในฐานะที่เป็นผู้เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลยังมีหน้าที่รับผิดชอบจัดมาตรการต่าง ๆ ให้เป็นไปตามหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลประการอื่น การบันทึกรายการต่าง ๆ จึงเป็นมาตรการหนึ่งที่ถือเป็นความรับผิดชอบของผู้ประกอบกิจการ และจัดเป็นภารกิจภายใต้หลักความรับผิดชอบ (Accountability) อันเป็นหลักการคุ้มครองข้อมูลส่วนบุคคลที่สำคัญอีกที่ผู้ประกอบกิจการจะต้องปฏิบัติตาม เพื่อทำให้เกิดความโปร่งใสในการดำเนินหน้าที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพราะการบันทึกรายการข้อมูลจะทำให้เห็นภาพรวมได้ว่าผู้ควบคุมข้อมูลซึ่งเป็นผู้ประกอบกิจการเอาข้อมูลไปใช้ทำอะไรบ้าง

ในประเทศไทยได้ถูกยกระดับสู่ระบบดิจิทัลกันอย่างกว้างขวางในหลายภาคส่วนทั้งในภาครัฐและภาคเอกชน ดังจะเห็นได้จากกลุ่มธุรกิจการเงินการธนาคารที่ประเทศไทยมีอัตราการเข้าถึงการบริการทางการเงินแบบดิจิทัลสูงที่สุดในโลก จึงทำให้เจ้าของข้อมูลเริ่มหันมารับรู้ถึงความเสี่ยงด้านความปลอดภัยและความเป็นส่วนตัวของข้อมูลในโลกออนไลน์โดยความเสี่ยงดังกล่าวไม่ได้มาจากกลุ่มอาชญากรไซเบอร์เท่านั้น แต่ยังรวมถึงความหละหลวมขององค์กรธุรกิจ

---

[7] จาก *รายงานการศึกษาวิจัยฉบับสมบูรณ์ เรื่อง ปัญหาและมาตรการทางกฎหมายในการรับรองและคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว* (น. 6), โดย สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ, 2558, กรุงเทพฯ: ดอกเบี้ย. ลิขสิทธิ์ 2558 โดย สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ.

ด้วย[8] สำหรับการให้ความคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายของประเทศไทย ตามรัฐธรรมนูญแห่งราชอาณาจักรไทย ได้รับรอง และคุ้มครองมิให้นำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ เว้นแต่จะได้รับยกเว้นตามกฎหมาย[9] กล่าวคือเป็นการห้ามนำข้อมูลส่วนบุคคลไปใช้ประโยชน์โดยเด็ดขาด เว้นแต่มีกฎหมายบัญญัติไว้โดยเฉพาะยกเว้นให้นำข้อมูลส่วนบุคคลของบุคคลอื่นไปใช้ได้ ซึ่งปัจจุบันประเทศไทยมีกฎหมายที่เกี่ยวกับข้อมูลส่วนบุคคลคือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้นำกรอบการคุ้มครองข้อมูลขององค์การร่วมมือและพัฒนาทางเศรษฐกิจ (The Organization for Economic Cooperation and Development หรือ OECD) ในเรื่อง Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data[10] และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation หรือ GDPR) มาเป็นแนวทางในการร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล มีการกำหนดให้ผู้ประกอบกิจการที่ต้องการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะต้องทำการขอความยินยอมจากเจ้าของข้อมูล โดยการขอความยินยอมจากเจ้าของข้อมูลจะต้องแจ้งให้ทราบถึงวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ทั้งนี้การขอความยินยอมต้องไม่มีเงื่อนไข หากการขอความยินยอมโดยมีเงื่อนไขที่ไม่มีความจำเป็นหรือไม่มีความเกี่ยวข้องสำหรับการเข้าทำสัญญาซึ่งรวมถึงการให้บริการใด ๆ ย่อมไม่มีผลผูกพันเจ้าของข้อมูล และไม่ทำให้ผู้ควบคุมข้อมูลสามารถทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้[11] แม้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยจะมีหลักการคุ้มครองข้อมูลส่วนบุคคลที่เป็นสากลก็ตาม แต่เมื่อพิจารณารายละเอียดเกี่ยวกับการบันทึกรายการข้อมูลแล้ว ปรากฏว่าการบันทึกรายการเป็น

---

[8] จาก *หนุนธุรกิจปรับตัวรับ พรบ.คุ้มครองข้อมูลส่วนบุคคล*, โดย ฐานเศรษฐกิจ, 2562. ลิขสิทธิ์ 2562 โดย ฐานเศรษฐกิจ. สืบค้นจาก https://www.thansettakij.com/content/401625

[9] รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธรศักราช 2562 มาตรา 32 บัญญัติว่า “บุคคลย่อมมสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ”

[10] จาก *การคุ้มครองข้อมูลส่วนบุคคล (Data Privacy) ของหน่วยงานภาครัฐ*, โดย สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, 2557. ลิขสิทธิ์ 2557 โดย สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. สืบค้นจาก http://www.etcommission.go.th/ article -dp-topic-dp.html

[11] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19

มาตรการหนึ่งภายใต้หลักความรับผิดชอบ (Accountability) ซึ่งเป็นหลักการสำคัญของการคุ้มครองข้อมูลส่วนบุคคล ที่จะทำให้การดำเนินการที่เกี่ยวกับการบันทึกรายการข้อมูลส่วนบุคคลมีความโปร่งใส

การที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 39 บัญญัติให้ผู้ควบคุมมีหน้าที่ต้องจัดทำบันทึกรายการ เพื่อให้เจ้าของข้อมูลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตรวจสอบ แต่รายละเอียดของรายการที่ให้ผู้ควบคุมต้องจัดทำบันทึกนั้นมีความไม่ชัดเจน อาทิ รายการเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล ตามมาตรา 39(3) กฎหมายไม่ได้ระบุว่าต้องมีรายละเอียดอย่างไร ทั้งในส่วนของข้อยกเว้นที่กำหนดให้ผู้ประกอบกิจการขนาดเล็กไม่ต้องจัดทำบันทึกรายการ ซึ่งมาตรา 39 วรรคสาม บัญญัติโดยใช้คำว่า “อาจยกเว้นมิให้นำมาใช้บังคับกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก...” ทำให้เกิดข้อสงสัยว่ากรณีใดบ้างที่จะยกเว้นให้ผู้ประกิจการขนาดเล็กไม่ต้องจัดทำบันทึก นอกจากนี้ในส่วนข้อยกเว้นของข้อยกเว้นมีการบัญญัติที่ไม่ชัดเจนโดยกฎหมายใช้คำว่า “...ข้อมูลมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล...” โดยไม่ได้กำหนดว่าความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลมีลักษณะเป็นอย่างไรและไม่ได้กำหนดเอาไว้ว่า “...กิจการที่เก็บรวบรวมข้อมูลส่วนบุคคลเป็นครั้งคราว...” มีลักษณะเป็นอย่างไร การบัญญัติกฎหมายที่ไม่ชัดเจนเช่นนี้ส่งผลให้เกิดความสับสนกับผู้ที่ต้องปฏิบัติตามอีกทั้งอาจทำให้เจ้าของข้อมูลไม่ได้รับความคุ้มครองที่เพียงพอ จึงสมควรได้รับการแก้ไขเพื่อให้กฎหมายคุ้มครองข้อมูลส่วนบุคคลเกิดประสิทธิภาพและเป็นไปตามเจตณารมณ์ของกฎหมายในการป้องกันการละเมิดสิทธิของเจ้าของข้อมูลอย่างแท้จริง

สำหรับวิจัยฉบับนี้จำกัดการศึกษาอยู่ที่มาตรา 39 ซึ่งเป็นเรื่องที่เกี่ยวกับการบันทึกรายการต่าง ๆตามที่มาตรา39 กำหนดไว้ และข้อยกเว้นไม่ต้องทำการบันทึกรายการซึ่งเป็นมาตราที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแต่ยังคงมีปัญหาอยู่กล่าวคือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ยังมีความไม่ชัดเจนทั้งการใช้ภาษาที่เข้าใจยากทำให้เกิดความสับสนกับผู้ที่ต้องปฏิบัติตามจึงสมควรได้รับการแก้ไข

1.2 วัตถุประสงค์การวิจัย

1.2.1 เพื่อศึกษาถึงแนวความคิดและความเป็นมาของหลักการจัดทำบันทึก

1.2.2 เพื่อศึกษาเกี่ยวกับแนวทางทฤษฎีของการคุ้มครองข้อมูลส่วนบุคคล

1.2.3 เพื่อเปรียบเทียบหลักเกณฑ์ของกฎหมายไทยและของต่างประเทศ

1.2.4 เพื่อค้นหาปัญหาของการคุ้มครองข้อมูลส่วนบุคคลที่เกิดขึ้นในประเทศไทยพร้อมทั้งข้อเสนอแนะแนวทางแก้ไขที่สามารถคุ้มครองข้อมูลส่วนบุคคลได้จริง

1.3 สมมติฐานการวิจัย

กฎหมายคุ้มครองข้อมูลของประเทศไทยกำหนดให้ผู้ประกอบกิจการที่เป็นผู้ควบคุมข้อมูลต้องจัดทำบันทึกที่มีรายการต่าง ๆ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 39 เพื่อให้เจ้าของข้อมูลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้ แต่รายการที่กฎหมายกำหนดนั้นมีรายละเอียดที่เกินความจำเป็นสำหรับการตรวจสอบ ทั้งการจัดทำบันทึกจำเป็นต้องจ้างผู้เชี่ยวชาญเพื่อลดความเสี่ยงจากโทษปรับที่กฎหมายกำหนดไว้ในอัตราที่สูงถึง 1 ล้านบาท ทำให้ผู้ประกอบกิจการต้องแบกรับภาระค่าใช้จ่ายเกินสมควร แม้กฎหมายจะยกเว้นไม่ให้ผู้ประกอบกิจการขนาดเล็กต้องจัดทำบันทึกก็ตาม แต่ข้อยกเว้นดังกล่าวกลับบัญญัติโดยใช้คำว่า “อาจยกเว้น” โดยไม่มีหลักเกณฑ์อื่นใดประกอบเพื่อทำให้ข้อยกเว้นมีความชัดเจน ดังนั้น เพื่อไม่ให้ผู้ประกอบกิจการต้องแบกรับภาระค่าใช้จ่ายที่ไม่จำเป็น และเพื่อให้กิจการขนาดเล็กได้รับประโยชน์จากข้อยกเว้นอย่างแท้จริงจึงควรแก้ไขกฎหมายให้มีความชัดเจน

1.4 กรอบแนวคิดการวิจัย

วิทยานิพนธ์ฉบับนี้มุ่งศึกษาเฉพาะมาตรา 39 ที่เกี่ยวกับนิติสัมพันธ์ระหว่างเจ้าของข้อมูลและผู้ควบคุมข้อมูลในเรื่องของบันทึกรายการและข้อยกเว้นไม่ต้องทำบันทึกรายการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยศึกษาวิเคราะห์หลักการคุ้มครองข้อมูลส่วนบุคคลจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation) สหราชอาณาจักร (The Data Protection Act 2018) สหรัฐอเมริกา และประเทศสิงคโปร์ (Personal Data Protection Act 2012) เปรียบเทียบกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.5 นิยามศัพท์

การประมวลผลข้อมูล หมายถึง การดำเนินการใด ๆ ซึ่งประกอบไปด้วยข้อมูลส่วนบุคคลหรือชุดของข้อมูลส่วนบุคคล ไม่ว่าจะได้ดำเนินการโดยอัตโนมัติหรือไม่ก็ตาม การดำเนินการดังกล่าวได้แก่ การเก็บรวบรวม การบันทึก การจัดระเบียบ การวางโครงสร้าง การปรับเปลี่ยนหรือแก้ไข การเผยแพร่ หรือวิธีอื่น ๆ ที่ทำให้สามารถนำไปใช้งานได้ การจัดวางหรือการจัดกลุ่มข้อมูล การจำกัดสิทธิ ตลอดจนการลบ หรือทำลายข้อมูลส่วนบุคคล

เจ้าของข้อมูล หมายถึง เจ้าของข้อมูลส่วนบุคคล

บุคคล หมายความว่า บุคคลธรรมดา

ผู้เก็บรักษาข้อมูล หมายถึง ผู้ควบคุมข้อมูล

ผู้ควบคุม หมายถึง ผู้ควบคุมข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูล หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

บทที่ 2

แนวความคิดและหลักการของการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับบันทึก

การวิจัยฉบับนี้มีวัตถุประสงค์เพื่อศึกษาถึงหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 39 กล่าวคือกฎหมายกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดทำบันทึกรายละเอียดต่าง ๆ ไว้เพื่อเป็นหลักฐานให้แก่เจ้าของข้อมูลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตรวจสอบ แต่เพื่อให้เข้าใจถึงความสำคัญของการจัดทำบันทึกจำเป็นที่จะต้องศึกษาถึงแนวความคิดของการคุ้มครองข้อมูลส่วนบุคคล หลักการคุ้มครองข้อมูลส่วนบุคคล และลักษณะของผู้ควบคุมซึ่งมีหน้าที่จัดทำบันทึกเสียก่อน ตลอดจนศึกษาถึงแนวความคิดและหลักการของบันทึก เพื่อให้เข้าใจถึงผลกระทบอันเกิดจากหน้าที่การจัดทำบันทึกจนต้องมีการยกเว้นหน้าที่ดังกล่าวในบางกรณี

2.1 แนวความคิดและที่มาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

2.1.1 แนวความคิดเกี่ยวกับการคุ้มครองสิทธิมนุษยชน

แนวความคิดเกี่ยวกับการคุ้มครองสิทธิมนุษยชนมีมาตั้งแต่สมัยโบราณ ซึ่งแต่เดิมเป็นแนวคิดที่โน้มเอียงไปในทางจำกัดอำนาจของกษัตริย์ หรือผู้มีอำนาจปกครองที่มีมากจนเกินไป โดยบรรดานักปราชญ์ในสมัยกรีกหรือสมัยโรมันถือว่าสิทธิมนุษยชนเป็นสิทธิที่เกิดขึ้นตามธรรมชาติมนุษย์ไม่ได้ทำขึ้น และมีอำนาจอยู่เหนือมนุษย์ แนวความคิดเกี่ยวกับสิทธิตามธรรมชาตินี้มีอิทธิพลเป็นอย่างมาก และได้ถูกถ่ายทอดจากนักปราชญ์ไปสู่บรรดานักการเมือง และประชาชนทั่วไป จนทำให้เกิดปฏิกิริยาทางการเมืองเพื่อต่อต้านและจำกัดอำนาจของกษัตริย์ หรือผู้มีอำนาจปกครอง ไม่ว่าจะเป็นการปฏิวัติ หรือการประกาศอิสรภาพของดินแดนที่อยู่ใต้การปกครองของประเทศอื่น กระทั่งต้องจัดทำข้อตกลงระหว่างประชาชนและผู้ใช้อำนาจปกครองในรูปแบบของเอกสารรับรองสิทธิเสรีภาพของประชาชนไว้ ดังปรากฏในสมัยของพระเจ้าจอห์น (John) แห่งอังกฤษ พระองค์เกิดขัดแย้งกับพวกพระและขุนนาง เพราะพระองค์ใช้อำนาจเกินขอบเขตไป พวกพระและขุนนางจึงบังคับให้พระองค์ลงพระปรมาภิไธยในเอกสารฉบับหนึ่ง เมื่อ ค.ศ. 1215 ซึ่งเรียกว่า “Great Charter” หรือ มหากฎบัตรแมกนาคาร์ตา (Magna Carta) อันเป็นเอกสารที่ให้ความคุ้มครองสิทธิเสรีภาพแก่

ราษฎรชาวอังกฤษ หรือปรากฏจากเอกสาร The Declaration of Independence ที่บรรดามลรัฐของสหรัฐอเมริกาต้องการเป็นเอกราชไม่ยอมขึ้นอยู่กับอังกฤษเป็นเหตุให้เกิดสงครามขึ้น จนกระทั่งมีประกาศเอกสารฉบับนี้ลงวันที่ 4 กรกฎาคม ค.ศ. 1776 มีข้อความว่า “เราถือความจริงซึ่งได้ประโยชน์แก่ตัวเองแล้วว่า มนุษย์เราเกิดมาย่อมเท่าเทียมกัน และต่างก็ได้รับสิทธิบางประการซึ่งไม่อาจโอนให้แก่กันได้มาจากพระเจ้า กล่าวคือสิทธิในชีวิต สิทธิในเสรีภาพ และสิทธิในการแสวงหาความสุขและเพื่อที่จะป้องกันสิทธิเหล่านี้ จึงได้จัดตั้งขึ้นซึ่งรัฐบาลได้รับอำนาจอันชอบธรรมด้วยความยินยอมของประชาชนผู้อยู่ใต้ปกครอง เมื่อเป็นเช่นนี้หากรัฐบาลดำเนินการปกครองไปในทางที่เป็นปรปักษ์ต่อหลักการดังกล่าวเมื่อใด เมื่อนั้นก็เป็นสิทธิของประชาชนที่จะเปลี่ยนแปลงหรือเลิกล้มรัฐบาลนั้นเสียได้ และกลับสถาปนารัฐบาลใหม่ขึ้นตามที่เห็นว่าจะทำให้เขาได้รับความปลอดภัยและยังความผาสุกให้เกิดขึ้นมากที่สุด”[12]

ในบางกรณีผู้มีอำนาจปกครองก็มีเจตนาให้การรับรองสิทธิแก่ประชาชนด้วยตนเอง ปรากฏหลักฐานในปี ค.ศ. 1292 (พ.ศ. 1835) จากหลักศิลาจารึกซึ่งพ่อขุนรามคำแหงได้ทรงจารึกขึ้นเพื่อให้เสรีภาพทางการค้า สิทธิยื่นเรื่องราวร้องทุกข์ ซึ่งในสมัยของพ่อขุนรามคำแหงนั้นตรงกับสมัยพระเจ้าเอ็ดวาร์ดที่ 1 แห่งอังกฤษ อันเป็นสมัยปฏิรูปอันยิ่งใหญ่สำหรับระบบกฎหมาย และรัฐสภาของอังกฤษ และเป็นสมัยของพระเจ้าฟิลิป เลอ เบ็ล แห่งฝรั่งเศส ซึ่งเป็นระยะที่กฎหมายโรมัน และรัฐสภาเริ่มมีบทบาทแทนที่อิทธิพลของสันตะปาปา[13]

ในศตวรรษที่ 17 แนวความคิดเรื่องการคุ้มครองสิทธิมนุษยชน ซึ่งแต่เดิมถือเป็นเรื่องภายในของแต่ละประเทศ ได้เปลี่ยนมาเป็นความร่วมมือกันระหว่างประเทศเพื่อหาแนวทางการคุ้มครองสิทธิมนุษยชนให้ดีขึ้น ประกอบกับเหตุการณ์สงครามโลกครั้งที่ 2 ได้นำมาซึ่งความสูญเสียชีวิตและทรัพย์สินของประเทศคู่สงครามอย่างมหาศาล จึงได้มีการจัดตั้งองค์กรสหประชาชาติขึ้นจนมีการผลักดันแนวทางคุ้มครองสิทธิมนุษยชนขึ้นมาคุ้มครองมนุษยชาติ จนกระทั่งเมื่อวันที่ 15 เมษายน ค.ศ. 1945 ก็ได้มีการประชุมใหญ่สหประชาชาติ ลงมติรับรองกฎบัตรสหประชาชาติ ให้สมาชิกมีพันธกรณีต่าง ๆ ร่วมกัน การรับรองสิทธิมนุษยชนก็เป็นพันธกรณีหนึ่งที่ทำให้เกิดปฏิญญา

---

[12] จาก *สิทธิมนุษยชนในสังคมโลก* (น.5-13), โดย กุลพล พลวัน, 2547, กรุงเทพฯ: สำนักพิมพ์นิติธรรม. ลิขสิทธิ์ 2547 โดย กุลพล พลวัน.

[13] จาก กุลพล พลวัน, *อ้างแล้วเชิงอรรถที่ 12* (น.17-18).

สากลว่าด้วยสิทธิมนุษยชน[14] และเมื่อวันที่ 10 ธันวาคม ค.ศ. 1948 (พ.ศ. 2491) สหประชาชาติได้ประกาศปฏิญาณสากลว่าด้วยสิทธิมนุษยชน จำแนกสิทธิที่ได้รับการคุ้มครองออกเป็น 2 ประเภท[15] คือ

ประเภทที่หนึ่ง สิทธิของพลเมืองและสิทธิทางการเมือง (Civil and Political Rights) เป็นการกล่าวถึงสิทธิตามธรรมชาติที่มีมาแต่เดิม ประกอบด้วย สิทธิในทางอิสรภาพแห่งการเคลื่อนไหว (The Rights to Freedom of Movement) สิทธิที่จะเป็นเจ้าของทรัพย์สินโดยลำพังหรือร่วมกับผู้อื่น (The right to own property alone as well as in association with others) สิทธิที่จะทำการสมรส (The rights to marry) สิทธิในความเสมอกันตามกฎหมายและสิทธิที่จะได้รับการพิจารณาที่เป็นธรรมถ้าถูกกล่าวหาว่ากระทำผิดอาชญาใด ๆ (The rights to equality before the law and to fair trial of accused of any crime) สิทธิในความเป็นอยู่ส่วนตัว (The rights to privacy) สิทธิในเสรีภาพแห่งการนับถือศาสนา (The rights to free speech and peaceful assembly) สิทธิที่จะลี้ภัย (The rights to asylum) การกระทำที่ถือว่าไม่ชอบด้วยกฎหมาย เช่น การเป็นทาส (slavery) การทรมาน (torture) และการกักขังตามอำเภอใจ (Arbitrary Detention) เป็นต้น ฯลฯ

ประเภทที่สอง สิทธิทางเศรษฐกิจและสังคม (Economic and Social Rights) ประกอบด้วย สิทธิในการศึกษา สิทธิที่จะจัดตั้งสหพันธ์กรรมกร สิทธิในมาตรฐานการครองชีพอันเพียงพอสำหรับสุขภาพและความเป็นอยู่ดีของตนและครอบครัว สิทธิในการพักผ่อนและเวลาว่าง รวมทั้งการจำกัดเวลาทำงานตามสมควรและวันหยุดงานเป็นครั้งคราวโดยได้รับสินจ้าง เป็นต้น ฯลฯ

2.1.2 แนวความคิดเกี่ยวกับสิทธิความเป็นอยู่ส่วนตัว

สำหรับสิทธิในความเป็นอยู่ส่วนตัวจัดเป็นสิทธิประเภทสิทธิของพลเมืองและสิทธิทางการเมือง ซึ่งรับรองไว้ในปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ข้อ 12 ว่า “บุคคลใด ๆ จะถูกแทรกแซงโดยพลการในชีวิตส่วนบุคคล ในครอบครัว ในเคหสถานหรือในการสื่อสาร หรือจะถูกลบลู่ในเกียรติยศและชื่อเสียงมิได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองตามกฎหมายต่อการ

---

[14] จาก กุลพล พลวัน, *อ้างแล้วเชิงอรรถที่ 12* (น.19-24).

[15] จาก กุลพล พลวัน, *อ้างแล้วเชิงอรรถที่ 12* (น.34).

แทรกแซงสิทธิ หรือการลบหลู่ดังกล่าวนั้น”[16] ปฏิญญาสากลข้อนี้ให้ความคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวไว้อย่างกว้างขวางและครอบคลุมถึงสิทธิต่าง ๆ หลายประการ ได้แก่[17]

(1) ความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลหรือข้อมูลส่วนตัว (Information Privacy) เป็นการให้ความคุ้มครองข้อมูลส่วนบุคคล

(2) ความเป็นส่วนตัวในชีวิตร่างกาย (Bodily Privacy) เป็นการให้ความคุ้มครองในชีวิตร่างกายของบุคคลในทางกายภาพที่จะไม่ถูกดำเนินการใด ๆ อันละเมิดความเป็นส่วนตัว อาทิ การทดลองพันธุกรรม หรือการทดลองยา เป็นต้น

(3) ความเป็นส่วนตัวในการติดต่อสื่อสาร (Communication Privacy) เป็นการให้ความคุ้มครองในความปลอดภัย และความเป็นส่วนตัวในการติดต่อสื่อสารทางจดหมาย โทรศัพท์ ไปรษณีย์อิเล็กทรอนิกส์ หรือวิธีการติดต่อสื่อสารอื่นใดที่ผู้อื่นจะล่วงรู้มิได้

(4) ความเป็นส่วนตัวในดินแดนหรืออาณาเขต (Territorial Privacy) เป็นการกำหนดขอบเขตหรือข้อจำกัดที่บุคคลอื่นจะบุกรุกเข้าไปในสถานที่ส่วนตัวมิได้ ทั้งนี้รวมทั้งการติดกล้องวีดิโอ และการตรวจสอบรหัสประจำตัวบุคคล (ID Checks)

แม้ “ความเป็นส่วนตัว” จะครอบคลุมถึงสิทธิหลายประการ แต่ความเป็นส่วนตัวที่นานาประเทศต่างให้ความสำคัญอย่างมากคือ “ความเป็นส่วนตัวในข้อมูลส่วนบุคคล” ทั้งนี้ เพราะ

---

[16] Universal Declaration of Human Right 1984 Article 12. “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

[17] จาก *รายงานฉบับสมบูรณ์โครงการศึกษาและพัฒนาแนวทางการคุ้มครองข้อมูลส่วนบุคคลภายใต้ประชาคมอาเซียน* (น.8-9), โดย สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, 2558, กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์. ลิขสิทธิ์ 2558 โดย สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์. สืบค้นจาก http://www.oic.go.th/FILEWEB/CABIWEBSITE/DRAWER01/GENERAL/DATA0007/00007559.PDF

ความก้าวหน้าทางเทคโนโลยีที่สามารถประมวลผลได้อย่างรวดเร็ว และจัดเก็บข้อมูลได้อย่างเป็นระบบส่งผลให้การติดต่อสื่อสารและการเผยแพร่ข้อมูล สามารถเคลื่อนย้ายและเชื่อมโยงกันได้โดยสะดวกรวดเร็ว ไม่จำกัดเวลาและสถานที่อีกต่อไป ซึ่งเป็นได้ทั้งโอกาสและภัยคุกคาม จึงจำเป็นต้องจัดวางกลไกให้มีความสัมพันธ์ระหว่างสิทธิความเป็นส่วนตัว เสรีภาพในการเคลื่อนไหวของข้อมูล และการเปิดเผยข้อมูล ให้มีความเหมาะสม เพื่อป้องกันการนำเทคโนโลยีสารสนเทศไปใช้ในทางมิชอบ หรือนำไปใช้ในทางทุจริตจนทำให้บุคคลที่เป็นเจ้าของข้อมูลนั้นได้รับความเสียหาย อันเป็นการละเมิดและก้าวล่วงในความเป็นส่วนตัวของบุคคลอื่น หรือการแทรกแซงต่อข้อมูลส่วนบุคคลโดยไม่คำนึงถึงสิทธิขั้นพื้นฐานของประชาชน อันเป็นการคุกคามความเป็นส่วนตัวของประชาชน ซึ่งอาจส่งผลกระทบต่อความสงบสุขของสังคมได้ในที่สุด ทำให้หลายประเทศเกิดแนวคิดในการให้ความคุ้มครองข้อมูลอย่างจริงจัง เพื่อป้องกันภัยคุกคามต่อความเป็นส่วนตัวของข้อมูลส่วนบุคคลโดยมีบทบัญญัติเป็นกฎหมายเฉพาะเพื่อคุ้มครองข้อมูลส่วนบุคคล หรือมีบทบัญญัติที่คุ้มครองของมูลส่วนบุคคลอยู่ในกฎหมายอื่น หรือมีการกำกับดูแลตนเอง (Self-Regulation) เป็นต้น

ต่อมาในปี ค.ศ. 1949 ได้มีการรวมกลุ่มกันของ 47 ประเทศก่อตั้งเป็นสภายุโรป (the Council of Europe) [18] มีจุดมุ่งหมายเพื่อส่งเสริมมาตรฐานของกฎหมาย สิทธิมนุษยชน การพัฒนาประชาธิปไตย หลักนิติธรรมระหว่างมวลสมาชิก ในส่วนการคุ้มครองสิทธิมนุษยชนได้มีการตกลงทำอนุสัญญายุโรปว่าด้วยสิทธิมนุษยชน (The European Convention on Human Rights หรือ ECHR) หรือเรียกอีกชื่อหนึ่งว่าอนุสัญญาว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน (Convention for the Protection of Human Rights and Fundamental Freedoms) ได้ร่างขึ้นในปี ค.ศ. 1950 และมีผลบังคับใช้วันที่ 3 กันยายน ค.ศ. 1953 โดยอนุสัญญาฉบับนี้ยืนยันสิทธิตามหลักของปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal protected human rights หรือ UDHR) UDHR และ ECHR เป็นกฎหมายที่พัฒนาขึ้นในยุคที่ไม่มีทั้งคอมพิวเตอร์และอินเตอร์เน็ต ต่อมาการพัฒนาเทคโนโลยีสารสนเทศก่อให้เกิดประโยชน์อย่างมากต่อผู้คนทั้งในด้านคุณภาพชีวิต การพัฒนาคุณภาพสังคมและนวัตกรรม ในขณะเดียวกันก็กระทบต่อสิทธิในความเป็นอยู่ส่วนตัว สภายุโรปจึง

---

[18] สภายุโรป (Council of Europe หรือ CoE) เป็นองค์การระหว่างรัฐบาลส่วนภูมิภาคที่ตั้งขึ้นในปี ค.ศ. 1949 (พ.ศ. 2492) เพื่อส่งเสริมสิทธิมนุษยชน ประชาธิปไตย และหลักนิติธรรม มีรัฐสมาชิกทั้งหมด 47 ประเทศ เป็นองค์กรระหว่างประเทศที่เป็นอิสระต่อสหภาพยุโรปที่มีสมาชิก 28 ประเทศ

เห็นความจำเป็นที่จะต้องจัดทำรายละเอียดเกี่ยวกับกฎเกณฑ์ในการให้ความคุ้มครองแก่ข้อมูลของบุคคล โดยประมาณกลางปี ค.ศ. 1970 คณะรัฐมนตรีแห่งสภายุโรป (Committee of Ministers of the Council of Europe) ได้ดำเนินการรวบรวมปัญหาต่าง ๆ ที่เกิดขึ้นเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล จนกระทั่งในปีค.ศ. 1981 อนุสัญญาว่าด้วยการคุ้มครองบุคคลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลโดยอัตโนมัติ (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data)[19] หรือเรียกว่า "Convention 108"[20] เป็นอนุสัญญาที่คุ้มครองบุคคลจากการประมวลผลข้อมูลส่วนบุคคลโดยมิชอบไม่ว่าการประมวลผลนั้นจะดำเนินการโดยภาคเอกชนภาครัฐ หรือศาลซึ่งมีอำนาจบังคับใช้กฎหมาย และในขณะเดียวกันยังมีวัตถุประสงค์เพื่อควบคุมการไหลเวียนข้อมูลส่วนบุคคลข้ามพรมแดนด้วย[21]

ต่อมาภายหลังสงครามเย็น ในปี ค.ศ. 1990 ฝรั่งเศสและเยอรมนีเสนอให้มีการจัดตั้งสหภาพการเมืองของยุโรปจนนำไปสู่การลงนามในสนธิสัญญากรุงมาสตริคต์ (Treaty of Maastricht หรือ Treaty on the European Union) เพื่อจัดตั้งสหภาพยุโรป (European Union หรือ EU) ขึ้นในปี ค.ศ. 1992 โดยมีวัตถุประสงค์เพื่อให้มีการกำหนดนโยบายด้านการต่างประเทศและความมั่นคงตลอดจนการใช้เงินสกุลยูโรร่วมกัน ปัจจุบัน EU มีรัฐสมาชิกจำนวน 28 ประเทศ[22] สำหรับแนวทางการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปมีพื้นฐานมาจากอนุสัญญาว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานแห่งสภายุโรป โดยมีการออกคำสั่งฉบับที่ 95/46/EC (Directive

---

[19] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No.108, 1981.

[20] Convention 108 เป็นลำดับที่ของข้อผูกพันทางกฎหมายระหว่างประเทศที่ออกโดยสภายุโรป

[21] From *Handbook on European data protection law* (pp.18-24), by European Union Agency for Fundamental Rights and Council of Europe, 2018, Luxembourg: Office of the European Union, Copyright 2018 by European Union Agency for Fundamental Rights and Council of Europe.

[22] จาก *สหภาพยุโรป/กรอบความร่วมมือพหุภาคี: สหภาพยุโรป(The European Union-EU)*, โดย กรมยุโรป กระทรวงการต่างประเทศ, 2563. ลิขสิทธิ์ 2563 โดย กระทรวงการต่างประเทศ. สืบค้นจาก http://www.mfa.go.th/ europetouch/th/other/8331/89715-สหภาพยุโรป-(The-European-Union---EU).html

95/46/EC) ว่าด้วยการคุ้มครองบุคคลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลและเสรีภาพในการเคลื่อนไหวของข้อมูล (on the protection of individuals with regard to the processing of personal data and on the free movement of such data) ได้กำหนดให้ประเทศสมาชิกให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับที่เทียบเท่ากัน

ในขณะที่องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (The Organization for Economic Cooperation and Development หรือ OECD)[23] ซึ่งเป็นองค์กรระหว่างประเทศอีกองค์กรหนึ่งที่ให้ความสำคัญในเรื่องของสิทธิในข้อมูลส่วนบุคคล ได้ทำการปรับปรุงปฏิญญากรุงโซลว่าด้วยอนาคตเกี่ยวกับเศรษฐกิจดิจิทัล ค.ศ. 2008 (Seoul Declaration for the Future of the Internet Economy) ให้มีแนวทางการคุ้มครองสิทธิความเป็นส่วนตัวครอบคลุมถึงสิทธิในข้อมูลส่วนบุคคล โดยการกำกับดูแลของคณะมนตรีแห่ง OECD ได้รับรองให้มีแนวทางปฏิบัติในการคุ้มครองความเป็นส่วนตัวและการไหลเวียนข้อมูลส่วนบุคคลข้ามพรมแดน (Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data) เมื่อปี ค.ศ. 2013[24] ซึ่งกำหนดให้รัฐสมาชิกสนับสนุนและคุ้มครองสิทธิขั้นพื้นฐาน (Fundamental Values) เกี่ยวกับความเป็นส่วนตัว สิทธิในปัจเจกชน เสรีภาพ และอิสระในการไหลเวียนของข้อมูลข่าวสาร และระมัดระวังความเสี่ยงที่จะเกิดขึ้นต่อการละเมิดสิทธิความเป็นส่วนตัวอันเนื่องมาจากการขยายตัวของนวัตกรรมที่มีการใช้ข้อมูลส่วนบุคคลเพื่อประโยชน์ทางเศรษฐกิจและสังคมมากขึ้น ตลอดจนคำนึงถึงการไหลเวียนของข้อมูลส่วนบุคคลที่ขยายตัวผ่านเครือข่ายทั่วโลกเพื่อร่วมกันปรับปรุงและเสริมสร้างกรอบการ

---

[23] OECD เป็นองค์กรระหว่างประเทศ โดยมีสมาชิกประกอบด้วยประเทศออสเตรเลีย ออสเตรีย เบลเยียม แคนนาดา ชิลี สาธารณรัฐเช็ค เดนมาร์ก เอสโตเนีย ฟินแลนด์ ฝรั่งเศส เยอรมนี กรีซ ฮังการี ไอซ์แลนด์ ไอร์แลนด์ อิสราเอล อิตาลี ญี่ปุ่น เกาหลีใต้ ลักเซมเบิร์ก แมกซิโก เนเธอแลนด์ นิวซีแลนด์ นอร์เวย์ โปแลนด์ โปรตุเกส สาธารณรัฐสโลวัก สโลวีเนีย สเปน สวีเดน สวิสเซอร์แลนด์ ตรุกี สหราชอาณาจักร และสหรัฐอเมริกา

[24] From *The OECD Privacy Framework* (น .2-3), by Organisation for Economic Co-operation and Development, 2013, Copyright 2013 by Organisation for Economic Co-operation and Development. Retrieved from https://www.oecd.org/sti/ieconomy/oecd_privacy_ framework .pdf

คุ้มครองความเป็นส่วนตัวระหว่างหน่วยงานที่เกี่ยวข้อง ทั้งให้มีการประเมินความเสี่ยงเพื่อพัฒนานโยบายและวิธีการป้องกันคุ้มครองความเป็นส่วนตัว[25]

2.1.3 การแทรกแซงสิทธิความเป็นอยู่ส่วนตัว

แม้ว่าสิทธิในความเป็นอยู่ส่วนตัวถือเป็นสิทธิมนุษยชนขั้นพื้นฐาน แต่ในบางกรณีรัฐจำเป็นต้องเข้าแทรกแซงสิทธิในความเป็นอยู่ส่วนตัว โดยวัตถุประสงค์หรือเหตุผลที่ให้อำนาจรัฐเข้าแทรกแซงสิทธิความเป็นส่วนตัวโดยชอบด้วยกฎหมาย มีดังต่อไปนี้[26]

(1) เพื่อคุ้มครองสิทธิของบุคคลอื่น เนื่องจากทุกคนมีสิทธิและเสรีภาพอย่างเท่าเทียมกัน สิทธิ เสรีภาพของบุคคลหนึ่งย่อมมีข้อจำกัดอยู่ที่สิทธิและเสรีภาพของบุคคลอื่น ๆ ดังนั้น การละเมิดผลประโยชน์ของบุคคลอื่นก็ดี การทำให้เกิดความเสียหายแก่บุคคลอื่นก็ดี หรือการทำให้เกิดความเสียเปรียบแก่บุคคลที่สามก็ดี กรณีดังกล่าวจึงเป็นการละเมิดสิทธิของบุคคลอื่น ดังนั้น สิทธิบุคคลอื่นจึงได้รับการรับรองโดยกฎเกณฑ์ของรัฐ และถือเป็นข้อจำกัดของสิทธิและเสรีภาพของบุคคลประการหนึ่ง

(2) เพื่อความมั่นคงในการดำรงอยู่และเพื่อความสามารถในการทำภาระหน้าที่ของรัฐเป็นเหตุผลอันชอบธรรมสำหรับการจำกัดสิทธิและเสรีภาพตามธรรมชาติของบุคคลได้

(3) เพื่อประโยชน์สาธารณะ ข้อนี้นับว่าเป็นเหตุผลที่สำคัญประการหนึ่งในการจำกัดสิทธิเสรีภาพโดยลักษณะของ “ประโยชน์สาธารณะ” คือ การตอบสนองความต้องการของคนส่วนใหญ่

สำหรับการพิจารณาว่าขอบเขตที่รัฐจะเข้าแทรกแซงสิทธิและเสรีภาพของปัจเจกบุคคลจะกระทำได้เพียงใดนั้น มีเกณฑ์สำคัญที่ใช้ในการพิจารณา ได้แก่ หลักการจำกัดสิทธิและเสรีภาพเท่าที่จำเป็น (Necessity)หรือหลักพอสมควรแก่เหตุ หรือหลักความได้สัดส่วน

---

[25] จาก Organisation for Economic Co-operation and Development, *อ้างแล้วเชิงอรรถที่ 24* (น.11-12).

[26] จาก สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ, *อ้างแล้วเชิงอรรถที่ 7* (น.15).

(Proportionality)หรือเรียกอีกชื่อหนึ่งว่า หลักห้ามมิให้กระทำเกิดกว่าเหตุซึ่งเป็นหลักที่มีความสำคัญอย่างยิ่งในการนำมาใช้ควบคุมการใช้อำนาจของรัฐที่มีผลกระทบต่อสิทธิและเสรีภาพของประชาชน โดยที่มาของหลักการดังกล่าวนั้น มาจากหลักกฎหมายของสหพันธ์สาธารณรัฐเยอรมนีและเป็นหลักกฎหมายที่ได้รับการยอมรับอย่างกว้างขวางในสหภาพยุโรป[27]

หลักความได้สัดส่วน เป็นหลักที่ถือว่ามีความสำคัญโดยเฉพาะอย่างยิ่งต่อศาลรัฐธรรมนูญของสหพันธ์สาธารณรัฐเยอรมนี นับตั้งแต่ทศวรรษที่ 1950 ศาลรัฐธรรมนูญสหพันธ์ได้นำหลักการดังกล่าวมาใช้เป็นเกณฑ์ในการพิจารณาในกรณีที่มีการจำกัดสิทธิและเสรีภาพของประชาชน โดยถือว่าเป็นหลักเกณฑ์ตามรัฐธรรมนูญที่นำมาใช้ตรวจสอบความชอบด้วยกฎหมายของการกระทำของรัฐทุกประเภทโดยภาระหน้าที่หลักของหลักความได้สัดส่วนนั้นมิได้มีความหมายมุ่งหมายเฉพาะการจำกัดการแทรกแซงของอำนาจรัฐเท่านั้น แต่หากตีความหลักความได้สัดส่วนอย่างถูกต้องแล้ว หลักความได้สัดส่วนนั้น นอกเหนือจากจะเป็นหลักการในทางเนื้อหาที่ห้ามมิให้มีการใช้อำนาจอย่างอำเภอใจแล้ว ยังเป็นเกณฑ์มาตรฐานที่เป็นสาระสำคัญในการควบคุมตรวจสอบตามรัฐธรรมนูญอีกด้วย โดยสาระสำคัญของหลักความได้สัดส่วนนั้น มีสาระสำคัญอยู่ 3 ประการ คือ[28]

(1) ความเหมาะสมของมาตรการหรือวิธีการสำหรับวัตถุประสงค์อันใดอันหนึ่งโดยหลักความเหมาะสม หมายความถึงสภาพการณ์ซึ่งรัฐได้ทำการแทรกแซงและภายในสภาพการณ์นั้นรัฐจะต้องคำนึงถึงการทำให้บรรลุวัตถุประสงค์ที่ได้กำหนดไว้ โดยมาตรการนั้นวางอยู่บนสมมติฐานที่ได้รับการยอมรับหรือเป็นมาตรการที่ได้แสดงให้เห็นอย่างแจ้งชัดว่ามีความเป็นไปได้ที่จะบรรลุวัตถุประสงค์ดังกล่าว

(2) ความจำเป็นของมาตรการหรือวิธีการ ศาลรัฐธรรมนูญของสหพันธ์ ได้อธิบายหลักความจำเป็นว่า มาตรการใดมาตรการหนึ่งจะมีความจำเป็นเมื่อไม่สามารถที่จะเลือกมาตรการอื่นใดที่มีผลเช่นเดียวกับมาตรการที่เลือกได้ อีกทั้งมาตรการนั้นเป็นมาตรการที่มีผลกระทบต่อสิทธิขั้นพื้นฐานน้อยที่สุดโดยการตรวจสอบความจำเป็นของมาตรการอันใดอันหนึ่งนั้น มีเงื่อนไขพื้นฐาน

---

[27] จาก สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ, *อ้างแล้วเชิงอรรถที่ 7* (น.16).

[28] จาก สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ, *อ้างแล้วเชิงอรรถที่ 7* (น.6-17).

อยู่ที่การพิจารณาความเหมาะสมของมาตรการนั้น เฉพาะมาตรการที่มีความเหมาะสมเท่านั้นถึงจะนำไปสู่การตรวจสอบตามหลักความจำเป็น

หลักความจำเป็นมีความสำคัญอย่างยิ่งในการควบคุมการใช้อำนาจมหาชนที่มีผลกระทบต่อสิทธิขั้นพื้นฐาน ซึ่งเคยมีกรณีตัวอย่างที่เกิดขึ้นในปี ค.ศ. 1968 ที่กรุงเบอร์ลิน เจ้าหน้าที่ตำรวจได้ออกคำสั่งห้ามมิให้มีการเดินขบวน แต่ก็มีบุคคลกลุ่มเล็ก ๆ ได้นำโปสเตอร์แผ่นเล็ก ๆ ไปติดที่โคมไฟตามถนน และสถานที่อื่น ๆ เพื่อเชิญชวนให้ประชาชนมาร่วมเดินขบวนในวันเวลาและสถานที่ ที่ปรากฏในแผ่นโปสเตอร์นั้น ตำรวจได้ทำการจับกุมบุคคลซึ่งทำการติดแผ่นโปสเตอร์นั้น โดยได้ควบคุมตัวบุคคลผู้นั้นไว้จนกระทั่งถึงวันที่มีการเดินขบวน และต่อมาได้มีการร้องไปยังศาลปกครองชั้นสูงของเบอร์ลิน ศาลได้วินิจฉัยว่าการจับกุมบุคคลดังกล่าวนั้นไม่มีความจำเป็นสำหรับการรักษาความสงบของสังคม เพราะการริบแผ่นประกาศดังกล่าวนั้นถือว่าเป็นการเพียงพอแล้ว

(3) ความได้สัดส่วนในความหมายอย่างแคบ หรือความสมเหตุสมผลระหว่างผลกระทบที่เกิดขึ้นกับประโยชน์ที่ได้จากการดำเนินการตามมาตรการดังกล่าว ได้แก่ การได้รับผลกระทบอันเกิดจากการแทรกแซงในเสรีภาพของปัจเจกบุคคลจะต้องไม่อยู่นอกเหนือจากขอบเขตความสัมพันธ์ของประโยชน์อันเป็นเป้าหมายของสาธารณะที่กำหนดไว้ ประโยชน์ที่ได้จากการดำเนินการตามมาตรการนั้นจะต้องมีน้ำหนักมากกว่าผลเสียที่เกิดจากมาตรการดังกล่าว ศาลรัฐธรรมนูญสหพันธ์เคยวินิจฉัยไว้ว่ามาตรการอันใดอันหนึ่งจะต้องไม่ก่อให้เกิดภาระแก่ผู้ได้รับผลกระทบจนเกินกว่าขอบเขต และผลกระทบที่เกิดขึ้นนั้นจะต้องเป็นไปอย่างมีเหตุผล ดังนั้น หลักความได้สัดส่วนจึงเป็นการยืนยันถึงความสมควร หรือความสมเหตุสมผล

หลักความได้สัดส่วนตามหลักกฎหมายของประเทศสหพันธ์สาธารณรัฐเยอรมนีนั้นถือว่าเป็นหลักกฎหมายมหาชนทั่วไปที่มิได้บัญญัติไว้เป็นลายลักษณ์อักษรแต่อย่างใด แต่ได้รับการยอมรับว่าเป็นหลักกฎหมายทั่วไปอย่างกว้างขวาง มิใช่เฉพาะแต่ในประเทศสหพันธ์สาธารณรัฐเยอรมนีเท่านั้นยังรวมถึงออสเตรเลีย สาธารณรัฐฝรั่งเศส สวิตเซอร์แลนด์ และประเทศอื่น ๆ นอกจากนั้นยังได้รับการยอมรับว่าเป็นหลักกฎหมายในกฎหมายระหว่างประเทศ โดยเฉพาะอย่างยิ่งเป็นหลักที่ได้รับการยอมรับจากสหภาพยุโรป ทั้งนี้ เพราะรากฐานของหลักความได้สัดส่วนนั้นมี

พื้นฐานมาจากหลักความยุติธรรม อันเป็นพื้นฐานของหลักกฎหมายทั่วไป และเป็นหลักที่คำนึงถึงความยุติธรรมทั้งในส่วนของปัจเจกบุคคลและความยุติธรรมต่อสังคมโดยรวมด้วย[29]

2.1.4 ที่มาของการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย

ประเทศไทยเป็นประเทศหนึ่งที่ได้ออกเสียงสนับสนุนในที่ประชุมสมัชชาใหญ่แห่งสหประชาชาติรับรองปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights หรือ UDHR) และได้รับรองสิทธิความเป็นอยู่ส่วนตัวไว้ในกฎหมายสูงสุดของประเทศตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2534 แก้ไขเพิ่มเติม (ฉบับที่ 5) พ.ศ. 2538 มาตรา 47 ดังนี้[30]

"สิทธิของบุคคลในครอบครัว ชื่อเสียง หรือความเป็นอยู่ส่วนตัว ย่อมได้รับความคุ้มครอง การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความ หรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชนอันเป็นการกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ หรือชื่อเสียง และความเป็นอยู่ส่วนตัว จะกระทำมิได้เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณชน..."

แนวคิดของความจำเป็นที่ต้องมีการคุ้มครองข้อมูลส่วนบุคคลโดยบทบัญญัติแห่งกฎหมายได้เริ่มปรากฏให้เห็นจากมติคณะรัฐมนตรีเมื่อวันที่ 28 กุมภาพันธ์ พ.ศ. 2539 ที่ได้เห็นชอบต่อนโยบายเทคโนโลยีสารสนเทศ (ไอที 2000) ที่เสนอโดยกระทรวงวิทยาศาสตร์เทคโนโลยีและสิ่งแวดล้อม ซึ่งมีจุดมุ่งหมายสำคัญเพื่อพัฒนาสังคมและ เสริมสร้างความแข็งแกร่งทางธุรกิจอุตสาหกรรม และการค้าระหว่างประเทศ ในการก้าวเข้าสู่สังคมสารสนเทศซึ่งเป็นยุคเศรษฐกิจใหม่แห่งศตวรรษที่ 21 โดยหนึ่งในมาตรการที่สำคัญคือ การปฏิรูปกฎหมายเทคโนโลยีสารสนเทศ (Information Technology Law) ซึ่งประกอบด้วยกฎหมาย 6 ฉบับ ได้แก่ กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายเกี่ยวกับลายมือชื่อทางอิเล็กทรอนิกส์ กฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ กฎหมายเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์ กฎหมายเกี่ยวกับการคุ้มครองข้อมูล

---

[29] จาก สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ, อ้างแล้วเชิงอรรถที่ 7 (น.17).

[30] จาก *การเปิดเผยข้อมูลส่วนบุคคลโดยธนาคารพาณิชย์กับมาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคล*, โดย ปิยะพร วงศ์เบี้ยสัจจ์, 2552, วิทยานิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิตย์.

ส่วนบุคคล และกฎหมายที่ออกเพื่อรองรับบทบัญญัติแห่งรัฐธรรมนูญว่าด้วยการพัฒนาโครงสร้างพื้นฐานสารสนเทศให้ทั่วถึงและเท่าเทียมกัน[31]

เมื่อประเทศไทยประกาศใช้รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 ที่ถือว่าเป็นรัฐธรรมนูญที่ส่งเสริมและคุ้มครองสิทธิเสรีภาพของประชาชนมากฉบับหนึ่ง ก็ยังคงมีการสืบทอดหลักเกณฑ์การรับรองและให้ความคุ้มครองแก่สิทธิในความเป็นอยู่ส่วนตัวในข้อมูลส่วนบุคคลโดยปรากฏในมาตรา 34และ มาตรา58 แห่งรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 ดังนี้

มาตรา 34 กำหนดว่า สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นส่วนตัว ย่อมได้รับความคุ้มครอง การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีการใดไปยังสาธารณชน อันเป็นการละเมิดหรือกระทบสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นส่วนตัวจะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณ

มาตรา 58 “บุคคลย่อมมีสิทธิได้รับทราบข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานราชการ หน่วยงานของรัฐ รัฐวิสาหกิจ หรือราชการท้องถิ่น เว้นแต่การเปิดเผยข้อมูลนั้นจะกระทบต่อความมั่นคงของรัฐความปลอดภัยของประชาชน หรือส่วนได้เสียอันพึงได้รับความคุ้มครองของบุคคลอื่น ทั้งนี้ตามกฎหมายบัญญัติ”[32]

ต่อมาได้มีการยกเลิกรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 และประกาศใช้รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 แทน ซึ่งได้มีการแก้ไขเพิ่มเติมการให้ความคุ้มครองจากการแสวงหาประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคล ตามมาตรา 35 ดังนี้

---

[31] จาก สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, *อ้างแล้วเชิงอรรถที่ 17* (น.10).

[32] จาก *ความเป็นส่วนตัว ความคิด ความรู้ ความจริงและพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย* (น. 243-244), โดย นคร เสรีรักษ์, 2557, กรุงเทพฯ: พี.เพรส. ลิขสิทธิ์ 2557 โดย นคร เสรีรักษ์.

“การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชนอันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวจะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณะ

บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวกับตน ทั้งนี้ ตามที่กฎหมายบัญญัติ” [33]

ปัจจุบันประเทศไทยก็มีการประกาศใช้รัฐธรรมนูญแห่งราชอาณาจักรไทยพุทธศักราช 2560 ในหมวด 3 สิทธิและเสรีภาพของปวงชนชาวไทยในมาตรา 32 กำหนดให้การนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่จะได้รับยกเว้นตามกฎหมาย กล่าวคือเป็นการห้ามนำข้อมูลส่วนบุคคลไปใช้ประโยชน์โดยเด็ดขาด เว้นแต่มีกฎหมายบัญญัติไว้โดยเฉพาะยกเว้นให้นำข้อมูลส่วนบุคคลของบุคคลอื่นไปใช้ได้ ซึ่งเป็นบทบัญญัติเพื่อคุ้มครองสิทธิความเป็นส่วนตัว รวมถึงข้อมูลส่วนบุคคลมิให้ถูกละเมิดตลอดทั้งเพื่อกำกับและควบคุมรัฐในเรื่องการเปิดเผยข้อมูลของปัจเจกบุคคลต่อสาธารณะ[34]จากข้อยกเว้นดังกล่าวจึงทำให้ต้องมีการบัญญัติ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลขึ้นมาเพื่อให้เป็นไปตามที่รัฐธรรมนูญกำหนดเอาไว้

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยเกิดขึ้นจากแนวคิดที่ต้องการรักษาดุลยภาพระหว่างเสรีภาพในการติดต่อสื่อสาร สิทธิในความเป็นส่วนตัว และความมั่นคงแห่งรัฐ และพัฒนากฎหมายคุ้มครองข้อมูลเกี่ยวกับบุคคลให้เป็นระบบและสอดคล้องกับกฎหมายของประเทศไทยที่ใช้อยู่ในปัจจุบัน และที่จะมีขึ้นในภายหน้า และสอดคล้องกับกฎเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลของนานาอารยประเทศที่เป็นที่ยอมรับอยู่ในปัจจุบัน ซึ่งผ่านการยกร่างหลายครั้ง โดยการยกร่างครั้งแรกได้ยกร่างขึ้นตามแนวทาง Directive 95/46/EC ของสหภาพยุโรป โดยเน้นที่ประเทศอิตาลีเป็นหลัก รวมทั้งประเทศอื่น ๆ ในภาคพื้นยุโรปด้วย เนื่องจากประเทศอิตาลีเป็นประเทศที่มีระบบประมวลกฎหมายเช่นเดียวกับประเทศไทย ประกอบกับประเทศในภาคพื้นยุโรปมีพัฒนาการ

---

[33] จาก ปิยะพร วงศ์เบี้ยสัจจ์, *อ้างแล้วเชิงอรรถที่ 30* (น.38).

[34] จาก *ความมุ่งหมายและคำอธิบายประกอบรายมาตราของรัฐธรรมนูญแห่งราชอาณาจักรพุทธศักราช 2560* (น.47), โดย สำนักงานเลขาธิการสภาผู้แทนราษฎร, กรุงเทพฯ: สำนักงานเลขาธิการสภาผู้แทนราษฎร, 2562. สืบค้นจาก https://www.parliament.go.th/ ewtcommittee/ewt/draftconstitution2/download/article/article_20191021103453.pdf

เกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลแล้วในระดับหนึ่ง อย่างไรก็ตามในการประชุมพิจารณาร่างกฎหมายตามแนวทางดังกล่าวพบว่ากลไกหรือหลักการของกฎหมายบางประการจำเป็นต้องพิจารณาอย่างรอบคอบ เนื่องจากการให้ความคุ้มครองข้อมูลส่วนบุคคลที่ได้รับผลกระทบจากพัฒนาการทางเทคโนโลยีค่อนข้างเป็นเรื่องใหม่ ดังนั้น การนำกลไกที่เข้มงวดมาบัญญัติเป็นกฎหมายอาจก่อให้เกิดปัญหาทางปฏิบัติในการบังคับใช้กฎหมายได้ ด้วยเหตุนี้จึงได้มีการปรับเปลี่ยนแนวทางของการยกร่างกฎหมายเสียใหม่[35]

การยกร่างครั้งต่อมา เป็นการศึกษากฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศอื่น ๆ เพิ่มเติมนอกเหนือจากสหภาพยุโรปและประเทศภาคพื้นยุโรปได้แก่ กฎหมายของออสเตรเลีย ฮ่องกง และนิวซีแลนด์ ที่แม้จะมีกำหนดหลักการใกล้เคียงกับกฎหมายของสหภาพยุโรปก็ตาม แต่ก็มีหลักเกณฑ์และกลไกการให้ความคุ้มครองข้อมูลส่วนบุคคลในอีกรูปแบบหนึ่งที่มีกลไกการใช้บังคับไม่เข้มงวดมากจนเกินไป นอกจากนี้กฎหมายดังกล่าวยังได้กำหนดกลไกการกำกับดูแลตนเอง โดยให้ผู้ซึ่งเก็บหรือรวบรวมข้อมูลสามารถที่กำหนด หรือวางหลักเกณฑ์ในทางปฏิบัติที่สอดคล้องกับการดำเนินงานของตนเองได้ ซึ่งการบัญญัติกฎหมายในแนวทางนี้ค่อนข้างมีความยืดหยุ่น และน่าจะเหมาะสมกับประเทศไทยซึ่งยังอยู่ในช่วงเริ่มต้นของการพัฒนาการให้ความคุ้มครองข้อมูลส่วนบุคคล[36] เมื่อศึกษาจากเอกสารประกอบการพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... ในปี พ.ศ. 2556 พบว่าได้มีการนำเอาหลักการคุ้มครองข้อมูลส่วนบุคคลตามแนวทางของ OECD มาใช้[37]

จนกระทั่งสหภาพยุโรปได้ประกาศใช้บังคับกฎหมายคุ้มครองข้อมูลส่วนบุคคล (General Data Protection Regulation หรือ GDPR) เมื่อปี ค.ศ. 2016 และมีผลบังคับใช้เดือนพฤษภาคม ปี ค.ศ. 2018 ซึ่งมีบทบัญญัติที่สำคัญเกี่ยวกับการโอนข้อมูลส่วนบุคคลข้ามพรมแดนโดยกำหนดว่าจะโอนข้อมูลไปยังประเทศนอกสหภาพยุโรปได้ต่อเมื่อ ประเทศนั้นมีการให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอ รัฐบาลชุดที่นำโดย พลเอก ประยุทธ์ จันทรโอชา จึงให้

---

[35] จาก ปิยะพร วงศ์เบี้ยสัจจ์, *อ้างแล้วเชิงอรรถที่ 30* (น.40).

[36] จาก ปิยะพร วงศ์เบี้ยสัจจ์, *อ้างแล้วเชิงอรรถที่ 30* (น.40).

[37] จาก *เอกสารประกอบการพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... อ.พ. 6/2556 สมัยสามัญทั่วไป* (น. 66), โดย สำนักงานเลขาธิการสภาผู้แทนราษฎร, 2556, ลิขสิทธิ์ 2556 โดย สำนักงานเลขาธิการสภาผู้แทนราษฎร. สืบค้นจาก http://www. parliament.go.th/library

ความสำคัญโดยมีการจัดลำดับว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.... เป็นกฎหมายที่มีความสำคัญเร่งด่วน[38] จนเมื่อวันที่ 27 พฤษภาคม พ.ศ. 2562 ประเทศไทยได้ประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2.2 ความหมายและลักษณะของข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลเป็นคำที่มีความหมายกว้างและหลาย ๆ ประเทศมีการแบ่งข้อมูลส่วนบุคคลที่แตกต่างกันออกไป เพื่อให้เกิดความเข้าใจคำว่าข้อมูลส่วนบุคคลมากยิ่งขึ้น จึงต้องทำการศึกษาความหมาย และประเภทของข้อมูล โดยมีรายละเอียดดังนี้

2.2.1 ความหมายของข้อมูลส่วนบุคคล

การศึกษานิยามของคำว่า “ข้อมูลส่วนบุคคล” (personal data) มิใช่เพียงเพื่อให้เกิดความชัดเจน และทราบถึงขอบเขตของการให้ความคุ้มครองเท่านั้น แต่นิยามของข้อมูลส่วนบุคคลยังสะท้อนถึงแนวความคิดในการให้ความคุ้มครองสิทธิความเป็นอยู่ส่วนตัวที่เป็นข้อมูลส่วนบุคคล ซึ่งมีทั้งองค์กรระหว่างประเทศ และกฎหมายของประเทศต่าง ๆ ได้ให้นิยามไว้ ดังนี้

2.2.1.1 องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organization for Economic Co-operation and Development) หรือ (OECD) นิยามคำว่า “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลใด ๆ อันระบุตัวหรืออาจระบุตัวบุคคลได้[39]

---

[38] จาก *รายงานผลการดำเนินการ โครงการพัฒนามาตรการในการดำเนินการ การพิจารณาความเหมาะสม ความเป็นไปได้ เพื่อจัดนำแนวทาง ขั้นตอนและวิธีการในการเข้าร่วมหรือทำความตกลงตามกรอบว่าด้วยการคุ้มครองความเป็นส่วนตัวของ APEC* (น. 77), โดย สถาบัน วิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, 2557, กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์. ลิขสิทธิ์ 2557 โดย สถาบัน วิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์. สืบค้นจาก http://www.oic.go.th/web2017/iwebform_viewer.asp?i=21111%2E14129605112112151111211

[39] Guidelines governing the protection of privacy and transborder flows of personal data

1 (b) “Personal data” means any information relating to an identified or identifiable individual (data subject).

2.2.1.2 สหภาพยุโรป (European Union: EU) ได้นิยามคำว่า “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลข่าวสารใด ๆ อันระบุหรือสามารถระบุเกี่ยวถึงบุคคลได้ (เจ้าของข้อมูล) ไม่ว่าทางตรงหรือทางอ้อม โดยเฉพาะอย่างยิ่งการอ้างอิงถึงการระบุตัวตน เช่น ชื่อ เลขบัตรประจำตัวประชาชน ข้อมูลตำแหน่งที่อยู่ หรือการระบุตัวตนออนไลน์ หรือการระบุลักษณะเฉพาะของบุคคลอย่างหนึ่งอย่างใดที่ประกอบไปด้วยลักษณะเฉพาะทางกายภาพ สรีรวิทยา พันธุกรรม สภาพจิตใจ สภาพเศรษฐกิจ สภาพวัฒนธรรมหรือสังคม[40]

2.2.1.3 กฎหมายคุ้มครองข้อมูลของประเทศสหราชอาณาจักร หรือ Data Protection Act 1998 ได้ให้คำนิยามของคำว่า “ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลที่เกี่ยวข้องกับตัวบุคคลธรรมดาที่มีชีวิตอยู่ผู้ซึ่งอาจสามารถถูกบ่งชี้ตัวบุคคลโดยอาศัย (1) ข้อมูลนั้นเอง หรือ (2) ข้อมูลนั้นเองประกอบกับข้อมูลอื่นที่อยู่ในความครอบครองของผู้ควบคุมดูแลข้อมูล ทั้งนี้ รวมถึงข้อมูลเกี่ยวกับการแสดงความคิดเห็นเกี่ยวกับตัวบุคคลธรรมดา และการแสดงเจตนาของผู้ควบคุมหรือบุคคลอื่นที่เกี่ยวกับบุคคลธรรมดานั้นด้วย[41]

2.2.1.4 กฎหมายคุ้มครองความเป็นส่วนตัวของประเทศสหรัฐอเมริกา หรือ Privacy Act 1974 ได้นิยามคำว่า “บันทึกข้อมูลส่วนบุคคล” (Record) หมายถึง การบันทึกใด ๆ การจัดเก็บรวบรวม หรือการจัดกลุ่มข้อมูลเกี่ยวกับบุคคล ซึ่งเก็บรักษาไว้โดยหน่วยงานรัฐบาลกลาง โดยรวมถึงข้อมูลเกี่ยวกับการศึกษา ข้อมูลเกี่ยวกับธุรกรรมทางการเงิน ประวัติทางการแพทย์ และ

---

[40] Regulation (EU) 2016/679 (General Data Protection Regulation) Article 4 (1) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

[41] Data Protection Act 1998 “Personal data means data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.”

ประวัติอาชญากรรม หรือประวัติการทำงาน และข้อมูลนั้นได้ระบุชื่อหรือหมายเลขประจำตัว สัญลักษณ์ หรือรหัสบ่งชี้อื่น ๆ ซึ่งสามารถแสดงได้ว่าหมายถึงบุคคลใด เช่น ลายนิ้วมือ หรือแผ่นบันทึกเสียง หรือภาพถ่าย เป็นต้น[42]

2.2.2 ประเภทของข้อมูลส่วนบุคคล

การศึกษาประเภทของข้อมูลอาจจำแนกได้หลายวิธีซึ่งการวิจัยฉบับนี้ได้จำแนกข้อมูลออกเป็น 2 ประเภท ได้แก่ข้อมูลที่ไม่เป็นข้อมูลส่วนบุคคลและข้อมูลที่เป็นข้อมูลส่วนบุคคลซึ่งมีรายละเอียด ดังต่อไปนี้

1) ข้อมูลที่ไม่เป็นข้อมูลส่วนบุคคล คือ ข้อมูลที่หน่วยงานหรือองค์กรทั้งหลายไม่ต้องขอความยินยอมเพื่อที่จะเก็บรวบรวม ใช้ หรือเปิดเผย ที่เป็นข้อมูลสำหรับการติดต่อทางธุรกิจ ทั้งนี้ต้องไม่ใช่ข้อมูลติดต่อทางธุรกิจที่ทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม ตัวอย่างเช่น[43]

1.1) เลขทะเบียนบริษัท

1.2) ข้อมูลสำหรับการติดต่อทางธุรกิจที่ไม่ได้ระบุถึงตัวบุคคล เช่น หมายเลขโทรศัพท์ หรือ แฟกซ์ที่ทำงาน, ที่อยู่สำนักงาน, อีเมล์ที่ใช้ในการทำงาน, อีเมล์ของบริษัท เช่น info@companay.com เป็นต้น

---

[42] Privacy Act 1974 “Record means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education,financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.”

[43] จาก Thailand Data Protection Guidelines 1.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (น.25), โดย ปิยะบุตร บุญอร่ามเรือง, ปิติ เอี่ยมจำรูญลาภ, ชวิน อุ่นภัทร และ ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล, 2561, กรุงเทพฯ:จุฬาลงกรณ์มหาวิทยาลัย. ลิขสิทธิ์ 2561 โดย ปิยะบุตร บุญอร่ามเรือง, ปิติ เอี่ยมจำรูญลาภ, ชวิน อุ่นภัทร และ ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล.

1.3) ข้อมูลนิรนาม (Anonymized Data) หรือข้อมูลแฝง (Pseudonymous Data) หมายถึง ข้อมูลหรือชุดข้อมูลที่ถูกทำให้ไม่สามารถระบุตัวบุคคลได้อีกโดยวิธีการทางเทคนิค

1.4) ข้อมูลผู้ตาย

2) ข้อมูลที่เป็นข้อมูลส่วนบุคคล สามารถแบ่งความคุ้มครองออกเป็น 2 ประเภท คือ คือ ข้อมูลส่วนบุคคลทั่วไป (Non–Sensitive Personal Data) และข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) โดยข้อมูลแต่ละประเภทมีลักษณะดังนี้[44]

2.1) ประเภทข้อมูลส่วนบุคคลทั่วไป คือ ข้อมูลเกี่ยวกับบุคคลผู้เป็นเจ้าของข้อมูลซึ่งสามารถบ่งชี้เฉพาะเจาะจงไปยังเจ้าของข้อมูลได้ ตัวอย่างเช่น[45]

2.1.1) ชื่อ-นามสกุล หรือชื่อเล่น

2.1.2) เลขประจำตัวประชาชน เลขหนังสือเดินทาง เลขบัตรประกันสังคม เลขใบอนุญาตขับขี่ เลขประจำตัวผู้เสียภาษี เลขบัญชีธนาคาร เลขบัตรเครดิต (การเก็บเป็นภาพสำเนาบัตรประชาชน หรือสำเนาบัตรอื่น ๆ ที่มีข้อมูลส่วนบุคคลที่กล่าวมาย่อมสามารถใช้ระบุตัวบุคคลได้โดยตัวมันเองจึงถือเป็นข้อมูลส่วนบุคคล)

2.1.3) ที่อยู่ อีเมล์ เลขโทรศัพท์

2.1.4) ข้อมูลอุปกรณ์ หรือเครื่องมือ เช่น IP address, MAC address, Cookie ID

---

[44] จาก *ข้อความคิดว่าด้วยข้อมูลข่าวสารส่วนบุคคล* (น.83), โดย ศิริกุล ภู่พันธ์, 2548, วิทยานิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์.

[45] จาก ปิยะบุตร บุญอร่ามเรือง, ปิติ เอี่ยมจำรูญลาภ, ชวิน อุ่นภัทร และ ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล, *อ้างแล้วเชิงอรรถที่ 43* (น.24).

2.1.5) ข้อมูลทางชีวมิติ (Biometric) เช่น รูปภาพใบหน้า ลายนิ้วมือ ฟิลม์เอกซเรย์ ข้อมูลสแกนม่านตา ข้อมูลอัตลักษณ์เสียง ข้อมูลพันธุกรรม

2.1.6) ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์ โฉนดที่ดิน

2.1.7) ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลข้างต้นได้ เช่น วันเกิดและสถานที่เกิด เชื้อชาติ สัญชาติ น้ำหนัก ส่วนสูง ข้อมูลตำแหน่งที่อยู่ (location) ข้อมูลทางการแพทย์ ข้อมูลการศึกษา ข้อมูลทางการเงิน ข้อมูลการจ้างงาน

2.1.8) ข้อมูลหมายเลขอ้างอิงที่เก็บไว้ในไมโครฟิล์ม แม้ไม่สามารถระบุไปถึงตัวบุคคลได้แต่หากใช้ร่วมกับระบบดัชนีข้อมูลอีกระบบหนึ่งก็จะสามารถระบุไปถึงตัวบุคคลได้ ดังนั้น ข้อมูลในไมโครฟิล์มจึงเป็นข้อมูลส่วนบุคคล

2.1.9) ข้อมูลการประเมินผลการทำงาน หรือ ความเห็นของนายจ้างต่อการทำงานของลูกจ้าง

2.1.10) ข้อมูลบันทึกต่าง ๆ ที่ใช้ติดตามตรวจสอบกิจกรรมต่าง ๆ ของบุคคล เช่น Log file

2.1.11) ข้อมูลที่สามารถใช้ในการค้นหาข้อมูลส่วนบุคคลอื่นในอินเตอร์เน็ต

2.2) ประเภทข้อมูลที่มีความอ่อนไหว คือ ข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคลแต่มีความละเอียดอ่อน และสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม จึงจำเป็นต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ กล่าวคือ เป็นข้อมูลประเภทที่หากมีการเปิดเผยอาจก่อให้เกิดผลกระทบต่อความรู้สึกของเจ้าของข้อมูล หรือประชาชนทั่วไป เป็นข้อมูลที่ก่อให้เกิดความขัดแย้ง ก่อให้เกิดผลกระทบต่อชื่อเสียงหรือเกียรติคุณของเจ้าของข้อมูล หรือเป็นข้อมูลซึ่งหากมีการเปิดเผยอาจก่อให้เกิดการตั้งข้อรังเกียจหรือเลือกปฏิบัติหรือเกิดอันตรายต่อ

เจ้าของข้อมูล โดยเจ้าของข้อมูลประสงค์ที่จะเก็บข้อมูลประเภทดังกล่าวไว้เป็นความลับ ตัวอย่างเช่น[46]

2.2.1) เชื้อชาติ

2.2.2) เผ่าพันธุ์

2.2.3) ความคิดเห็นทางการเมือง

2.2.4) ความเชื่อในลัทธิ ศาสนา หรือปรัชญา

2.2.5) พฤติกรรมทางเพศ

2.2.6) ประวัติอาชญากรรม

2.2.7) ข้อมูลสุขภาพร่างกาย หรือข้อมูลสุขภาพจิต

2.2.8) ข้อมูลอื่นใดซึ่งกระทบความรู้สึกของประชาชน

เมื่อพิจารณาข้อมูลที่มีความอ่อนไหวที่ได้กล่าวมาข้างต้น พบว่าการใช้หรือการเปิดเผยข้อมูลแต่ละข้อมูลส่งผลกระทบต่อเจ้าของข้อมูลที่แตกต่างกันไปตามแต่ประเภทของข้อมูล โดยสามารถแบ่งได้ออกเป็น 3 ระดับ ดังนี้[47]

ระดับหนึ่ง ข้อมูลข่าวสารประเภทที่มีความอ่อนไหวระดับต่ำ (Low Sensitivity) ข้อมูลประเภทนี้เป็นข้อมูลที่เกี่ยวข้องกับบุคล เป็นข้อมูลที่มีความอ่อนไหวเนื่องด้วย

---

[46] จาก ปิยะบุตร บุญอร่ามเรือง, ปิติ เอี่ยมจำรูญลาภ, ชวิน อุ่นภัทร และ ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล, *อ้างแล้วเชิงอรรถที่ 43* (น.26)

[47] จาก ปิยะพร วงศ์เบี้ยสัจจ์, *อ้างแล้วเชิงอรรถที่ 30* (น.19-29).

ข้อมูลเหล่านี้อาจช่วยทำให้ได้มาซึ่งข้อมูลที่มีระดับความอ่อนไหวสูงยิ่งขึ้นไป เช่น ชื่อสกุล วันเดือนปีเกิด สัญชาติ เพศ ที่อยู่ สถานภาพการแต่งงาน ชื่อนายจ้าง สถานที่ทำงาน อาชีพ เป็นต้น

ระดับสอง ข้อมูลข่าวสารประเภทที่มีความอ่อนไหวระดับกลาง (Moderate Sensitivity) เป็นข้อมูลที่มีความอ่อนไหวมากในแง่ที่มีโอกาสที่จะก่อให้เกิดความเสียหายเมื่อข้อมูลถูกนำเอาไปใช้ในทางที่ผิด ข้อมูลประเภทนี้ครอบคลุมข้อมูลประเภทที่เกี่ยวกับความคิดเห็นของบุคคล ซึ่งมีความครอบคลุมทุกเรื่องของชีวิต ข้อมูลที่มีความอ่อนไหวระดับปานกลางไม่ควรถูกเก็บรวบรวมโดยสิ้นเชิง เช่น หมายเลขประกันสุขภาพ ลายนิ้วมือ เชื้อชาติ วันแต่งงาน สาเหตุการหย่าร้าง เงินเดือน การล้มละลายของบุคคล ภาษีที่จ่าย กรมธรรม์ประกันชีวิต วันที่เข้าศึกษาและวันที่จบการศึกษา การตัดสินว่ากระทำความผิด ผลการลงโทษโดยคำสั่งศาล เป็นต้น

ระดับสาม ข้อมูลข่าวสารที่มีความอ่อนไหวระดับสูง (High sensitivity) ข้อมูลประเภทนี้ได้แก่ ข้อมูลรายละเอียดส่วนตัวของบุคคลในส่วนที่เกี่ยวข้องกับประวัติทางการแพทย์ พฤติกรรมทางเพศ หรือข้อเท็จจริงด้านอื่น ๆ ในชีวิตของบุคคลซึ่งสามารถกล่าวได้ว่าเป็นเรื่อง “ส่วนตัว” หรือ “ลับเฉพาะ” สำหรับข้อมูลประเภทความอ่อนไหวระดับสูงนี้ เหตุผลความจำเป็นที่จะต้องปกปิดข้อมูลมีความเหมาะสมมากที่สุด และเป็นข้อมูลที่ไม่ควรมีการเก็บโดยสิ้นเชิง เช่น ภาวะสุขภาพของร่างกาย ผลตรวจเลือดว่าเป็นโรคที่ติดต่อได้ ผลตรวจสุขภาพ ความผิดปกติทางจิต ข้อมูลที่ไม่ใช่ข้อเท็จจริงเกี่ยวกับบุคคลที่บันทึกโดยตำรวจ หรือได้รับมาจากผู้ให้เบาะแส เป็นต้น

ข้อมูลส่วนบุคคลทั่วไปแตกต่างจากข้อมูลส่วนบุคคลที่มีความอ่อนไหวซึ่งเป็นข้อมูลที่มีลักษณะพิเศษกว่า คือ ข้อมูลส่วนบุคคลประเภทที่มีความอ่อนไหวหากมีการเปิดเผยจะกระทบถึงความรู้สึกของประชาชนทั่วไปในทางลบต่อชื่อเสียงเกียรติคุณ และการเปิดเผยอาจก่อให้เกิดอันตรายต่อบุคคลได้ เช่น การเปิดเผยเชื้อชาติบางเชื้อชาติอาจนำมาซึ่งความไม่ปลอดภัยในชีวิตและทรัพย์สินของบุคคลได้ ดังนั้น โดยทั่วไปแล้วกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลแทบทุกประเทศจึงเคร่งครัดกับข้อมูลประเภทนี้มากกว่าข้อมูลส่วนบุคคลทั่วไป โดยกำหนดห้ามมิให้มีการเก็บรวบรวมข้อมูล ห้ามใช้และห้ามประมวลผลข้อมูลประเภทนี้ ไม่ว่ากรณีใด ๆ เว้นแต่มีกฎหมายบัญญัติไว้เป็นการเฉพาะ

2.2.3 การประมวลผลข้อมูลส่วนบุคคล

ก่อนที่จะศึกษาหลักการคุ้มครองข้อมูลส่วนบุคคล ตลอดจนหลักการจัดทำและเก็บรักษาบันทึก จำต้องพิจารณาถึงลักษณะของการกระทำใด ๆ ต่อข้อมูลส่วนบุคคลที่อาจกระทบต่อสิทธิของเจ้าของข้อมูล ซึ่งลักษณะของการกระทำต่อข้อมูล เช่น การเก็บ รวบรวม การบันทึก การกระทำต่อข้อมูลดังกล่าวอาจเรียกได้ว่าเป็น “การประมวลผล” ซึ่งการประมวลผลมีวิธีการหลายรูปแบบโดยมีรายละเอียดดังนี้

แนวความคิดของการประมวลผลข้อมูลส่วนบุคคลอาจศึกษาได้จากบทนิยามของคำว่า “การประมวลผล”(processing)ซึ่งปรากฏในกฎหมายของสหภาพยุโรป และกฎหมายของสภายุโรป โดยเมื่อกล่าวถึงการประมวลผลข้อมูลส่วนบุคคล หมายถึงการดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลไม่ว่าจะดำเนินการ โดยอัตโนมัติหรือไม่ก็ตาม เช่น การเก็บรวบรวม การบันทึก การจัดระบบองค์กร การจัดโครงสร้าง การเก็บรักษา การดัดแปลงหรือเปลี่ยนแปลง การแก้ไข พิจารณา ใช้ เปิดเผยโดยการส่ง เผยแพร่ หรือโดยวิธีอื่นใดในลักษณะเดียวกัน การจัดวางหรือผสมเข้าด้วยกัน การจำกัด ลบ หรือทำลาย[48]

การกระทำที่ถือว่าเป็นการประมวลผลปรากฏจากคำพิพากษาของศาลยุติธรรมสหภาพยุโรป (Court of Justice of the European Union หรือ CJEU) ซึ่งได้วินิจฉัยกรณีการกระทำใด ๆ ที่ถือเป็นการประมวลผลข้อมูลส่วนบุคคลไว้ดังนี้

1) ในคดีระหว่าง *František Ryneš v. Úřad pro ochranu osobních údajů* ศาลวินิจฉัยว่ากล้องวงจรปิด (CCTV) เป็นระบบที่ติดตั้งเพื่อคุ้มครองทรัพย์สิน การที่กล้องวงจรปิดที่นาย Ryneš นำมาติดตั้งไว้ที่บ้านได้บันทึกและเก็บภาพคนทำหน้าต่างบ้านของเขาแตกไว้ ถือได้ว่า

---

[48] GDPR Article 4(2) “Definitions processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.”

นาย Ryneš ได้กระทำการประมวลผลข้อมูลแล้ว และเป็นการประมวลผลข้อมูลโดยอัตโนมัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป[49]

2) กรณีที่นาย Manni ขอให้ลบข้อมูลการจัดอันดับบริษัทจำกัดด้านอสังหาริมทรัพย์ที่เลิกกิจการ (Liquidation) โดยอ้างว่าข้อมูลดังกล่าวเชื่อมโยงกับข้อมูลส่วนบุคคลของเขาและทำให้ชื่อเสียงของเขาเสียหาย ศาล CJEU ถือว่าการเผยแพร่และเก็บรักษาข้อมูลการจัดอันดับบริษัทเป็นประโยชน์ต่อสาธารณะซึ่งผู้มีอำนาจชอบที่จะเก็บรักษาข้อมูลและดำเนินการประมวลผลข้อมูลส่วนบุคคลได้ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล[50]

สำหรับการจำแนกวิธีการประมวลผลข้อมูลส่วนบุคคลอาจแยกออกเป็น

1) การประมวลผลข้อมูลโดยอัตโนมัติ (Automate Data Processing) เป็นการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลไม่ว่าทั้งหมดหรือบางส่วนโดยใช้อุปกรณ์ช่วยในการประมวลผล เช่น การทำให้ข้อมูลซึ่งไม่สามารถระบุถึงตัวบุคคลได้โดยเฉพาะเจาะจงไม่ว่าจะเป็นชื่อของบุคคล หมายเลขโทรศัพท์ หรืองานอดิเรกไปปรากฏบนเว็บเพจ[51] รวมถึงการเก็บรักษาข้อมูลบนเซิร์ฟเวอร์[52] และการเก็บรวบรวม บันทึก และจัดตำแหน่งข้อมูลอย่างต่อเนื่องและเป็นระบบของ

---

[49] From Judgment of European Court retrieved system. (2014b). Case 212/13. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62013CJ0212&from=EN

[50] From Judgment of European Court retrieved system. (2017). Case 398/15. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1590534459389&uri=CELEX:62015CJ0398

[51] From Judgment of European Court retrieved system. (2003). Case 101/01. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1590535498929&uri=CELEX: 62001CJ0101

[52] เซิร์ฟเวอร์ (Server) คือคอมพิวเตอร์ชนิดหนึ่งที่มีไว้สำหรับเก็บข้อมูลเพื่อแสดงเว็บไซต์

เครื่องมือช่วยค้นหาข้อมูล (Search Engine) ในระบบอินเตอร์เน็ตเหล่านี้ถือเป็นการประมวลผลข้อมูลโดยอัตโนมัติ[53]

2) การประมวลผลข้อมูลโดยตรง (Non-automated Data Processing) เป็นการประมวลผลข้อมูลส่วนบุคคลโดยมีการดำเนินการเก็บรวบรวมข้อมูล วางโครงสร้างหรือรูปแบบของข้อมูลด้วยตนเองเพื่อให้เกิดความสะดวกและรวดเร็วนการค้นหาข้อมูล เช่น กรณีที่นายจ้างเก็บแฟ้มข้อมูลของลูกจ้างที่ลาออกไปโดยเรียงลำดับรายชื่อของลูกจ้างตามตัวอักษร เป็นต้น[54]

สำหรับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ได้ให้คำนิยามของ “การประมวลผล” แต่เมื่อพิจารณาบทนิยามตามมาตรา 6 คำว่า “ผู้ควบคุม” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และคำว่า “ผู้ประมวลผลข้อมูล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุม ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุม จากบทนิยามดังกล่าวจะเห็นได้ว่าการที่กฎหมายกำหนดให้ผู้ควบคุม และผู้ประมวลผลข้อมูลให้เป็นผู้ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ซึ่งการดำเนินการดังกล่าวถือเป็นการประมวลผลข้อมูลตามความหมายของ “การประมวลผล” แห่ง GDPR ดังนั้นเมื่อเปรียบเทียบกับบทนิยามของคำว่าการประมวลผลตาม GDPR แล้วการประมวลผลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงจำกัดอยู่เพียงการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเท่านั้น มิได้มีความหมายกว้างขวางดังเช่นคำว่าการประมวลผลตามบทนิยามของ GDPR ไม่

---

[53] From Judgment of European Court retrieved system. (2014a). Case 131/12. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1590535376164&uri=CELEX: 62012CJ0131

[54] From *Handbook on European data protection law* (p.100), by European Union Agency for Fundamental Rights and Council of Europe, 2018, Luxembourg: Office of the European Union, Copyright 2018 by European Union Agency for Fundamental Rights and Council of Europe.

2.3 หลักการคุ้มครองข้อมูลส่วนบุคคลตามกรอบขององค์การระหว่างประเทศ

เนื่องจากข้อมูลส่วนบุคคลเป็นสิ่งสำคัญในการประกอบธุรกิจ การดำเนินธุรกิจต่าง ๆ ล้วนต้องอาศัยข้อมูลเป็นสิ่งสำคัญ ประเทศหลายประเทศจึงให้ความสำคัญเกี่ยวกับข้อมูลส่วนบุคคลโดยมีการนำหลักการคุ้มรองตามกรอบองค์การระหว่างประเทศ เช่น หลักการคุ้มครองข้อมูลส่วนบุคคลของ UN หลักการคุ้มครองข้อมูลส่วนบุคคลของ OECD หลักการคุ้มครองข้อมูลส่วนบุคคลของ APEC และ หลักการคุ้มครองข้อมูลส่วนบุคคลของ EU มาเป็นแนวทางในการร่างกฎหมาย เพื่อเข้าใจหลักการคุ้มครองข้อมูลส่วนบุคคลตามกรอบขององค์กรระหว่างประเทศได้ดียิ่งขึ้นจึงควรศึกษาหลักการคุ้มครองข้อมูลส่วนบุคคลตามกรอบองค์การระหว่างประเทศต่าง ๆ ซึ่งมีรายละเอียดดังต่อไปนี้

2.3.1 หลักการคุ้มครองข้อมูลส่วนบุคคลของ UN [55]

แนวทางนี้ได้จัดทำขึ้นเมื่อวันที่ 14 ธันวาคม 1990 โดยสมัชชาใหญ่แห่งสหประชาชาติได้มีมติกำหนดแนวทางในการประมวลผลแฟ้มข้อมูลส่วนบุคคลทางคอมพิวเตอร์ (Guideline Concerning Computerized Personal Data Files) ขึ้น เพื่อให้ประเทศสมาชิกปฏิบัติตามหลักเกณฑ์ในการกำหนดมาตรฐานขั้นต่ำเกี่ยวกับการบัญญัติกฎหมายภายในของรัฐ เกี่ยวกับข้อมูลส่วนบุคคลคือ “แนวทางในการควบคุมข้อมูลส่วนบุคคลที่จัดเก็บด้วยคอมพิวเตอร์” (Guidelines for the Regulation of Computerized Personal Data Files) ซึ่งมีหลักดังนี้

2.3.1.1 หลักความชอบด้วยกฎหมายและความเป็นธรรม (Principle of lawfulness and Fairness) ข้อมูลส่วนบุคคลจะต้องไม่ถูกเก็บรวบรวม หรือประมวลผลด้วยวิธีการที่ไม่เป็นธรรมหรือไม่ชอบด้วยกฎหมายและการใช้ข้อมูลส่วนบุคคลจะต้องไม่ขัดกับวัตถุประสงค์และหลักการของกฎบัตรสหประชาชาติ

---

[55] จาก สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, *อ้างแล้วเชิงอรรถที่ 38* (น.70-71)

2.3.1.2 หลักความถูกต้อง (Principle of Accuracy) ในการเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องมีการตรวจสอบอย่างสม่ำเสมอว่ากระทำด้วยความถูกต้อง ข้อมูลมีความสมบูรณ์ทันสมัยอยู่เสมอ และเก็บได้ภายในระยะเวลาเท่าที่จะมีการประมวลผลหรือใช้ข้อมูลเหล่านั้น

2.3.1.3 หลักการระบุวัตถุประสงค์โดยเฉพาะเจาะจง (Principle of the purpose-specification) จะต้องมีการระบุวัตถุประสงค์ในการจัดเก็บและเงื่อนไขของการใช้ประโยชน์ข้อมูลที่เก็บตามวัตถุประสงค์ซึ่งชอบด้วยกฎหมายโดย

1) เก็บรวบรวมเพียงเท่าที่เกี่ยวข้อง และเหมาะสมกับวัตถุประสงค์ที่ระบุไว้

2) ข้อมูลส่วนบุคคลจะต้องไม่ถูกใช้หรือเปิดเผย เว้นแต่ได้รับความยินยอมจากบุคคลที่เกี่ยวข้อง

3) ระยะเวลาที่จัดเก็บข้อมูลส่วนบุคคลจะต้องไม่เกินกว่าระยะเวลาที่การดำเนินการตามวัตถุประสงค์ที่ระบุไว้ได้สำเร็จลง

2.3.1.4 หลักการเข้าถึงข้อมูล (Principle of Interested-person access) เจ้าของข้อมูลมีสิทธิที่จะได้รู้ว่ามีการประมวลผลข้อมูลข่าวสารที่เกี่ยวกับตน โดยได้รับข้อมูลในรูปแบบที่เข้าใจได้ในเวลาอันสมควรและปราศจากค่าใช้จ่าย และสามารถขอให้แก้ไขหรือลบในกรณีมีการเก็บข้อมูลโดยไม่ชอบด้วยกฎหมาย ไม่จำเป็น หรือมีการเก็บข้อมูลโดยไม่ถูกต้อง ข้อกำหนดแห่งหลักการนี้ให้บังคับใช้กับบุคคลทุกคน โดยไม่คำนึงถึงสัญญาติหรือถิ่นที่อยู่

2.3.1.5 หลักการไม่เลือกปฏิบัติ (Principle of Non-discrimination) ห้ามเก็บรวบรวมข้อมูลซึ่งอาจทำให้เกิดการเลือกปฏิบัติที่ขัดต่อกฎหมาย เช่นข้อมูลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ สีผิว พฤติกรรมทางเพศ ความคิดเห็นทางการเมือง การนับถือศาสนา ความเชื่อทางปรัชญา หรือความเชื่ออื่น ๆ รวมทั้งข้อมูลการเป็นสมาชิกสหภาพ หรือสมาคมทางการค้า

2.3.1.6 การกำหนดข้อยกเว้น (Power to Make Exceptions) ข้อยกเว้นจากหลักการข้อที่ 1-4 อาจกำหนดได้ในกรณีจำเป็นเพื่อรักษาความมั่นคงของชาติ ระเบียบ สังคม สาธารณสุข หลักคุณธรรม และสิทธิและเสรีภาพของบุคคลอื่น ข้อยกเว้นจากหลักการข้อที่ 5 อาจ

เป็นกรณีเพื่อการป้องกันการเลือกปฏิบัติ ภายใต้ข้อบัญญัติของปฏิญญาสากลว่าด้วยสิทธิมนุษยชน หรือกลไกของกฎหมายอื่น ๆ ที่เกี่ยวกับการคุ้มครองสิทธิมนุษยชนและการป้องกันการเลือกปฏิบัติ

2.3.1.7 หลักการรักษาความปลอดภัย (Principle of Security) จะต้องมีการรักษาความปลอดภัยข้อมูลที่จัดเก็บ เพื่อป้องกันอันตรายทั้งจากภัยธรรมชาติ การสูญหายหรือเสียหาย การทำลายโดยบุคคล การเข้าถึงโดยปราศจากอำนาจ การใช้ในทางที่ผิด หรือการทำลายโดยไวรัสคอมพิวเตอร์

2.3.1.8 การกำกับดูแล (Supervision and Sanctions) กฎหมายของประเทศต่าง ๆ จะต้องระบุหน่วยงานที่รับผิดชอบในการควบคุม ดูแล และให้คำแนะนำเกี่ยวกับการปฏิบัติตามหลักการนี้

2.3.1.9 การส่งข้อมูลข้ามพรมแดน (Transborder Data Flows) การส่งข้อมูลระหว่างประเทศจะสามารถกระทำได้ในกรณีที่ประเทศสองประเทศ หรือมากกว่าสองประเทศ มีกลไกในการคุ้มครองสิทธิความเป็นส่วนตัวในระดับเดียวกัน

2.3.1.10 ขอบเขตการใช้ข้อปฏิบัติ (Field of Application) หลักปฏิบัติดังกล่าวควรได้มีการปฏิบัติใช้สำหรับข้อมูลในภาครัฐ และเอกชนที่จัดเก็บด้วยคอมพิวเตอร์ (Computerized Files) เช่นเดียวกับการจัดเก็บด้วยวิธีการอื่น ๆ ที่มีการปรับปรุงให้เหมาะสมกับเอกสารที่จัดเก็บด้วยมือ (Manual Files)

2.3.2 หลักการคุ้มครองข้อมูลส่วนบุคคลของ OECD[56]

การคุ้มครองข้อมูลส่วนบุคคลตามแนวทางขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD Guideline on the Protection of Privacy and Transborder Flows of Personal Data) เกิดขึ้นในปี ค.ศ. 1980 (พ.ศ. 2523) ซึ่งมีการวางหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลขึ้นอย่างเป็นรูปธรรม และเป็นหลักเกณฑ์ที่ประเทศส่วนใหญ่ให้การยอมรับว่าเป็นหลักเกณฑ์พื้นฐาน

---

[56] จาก สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, *อ้างแล้วเชิงอรรถที่ 38* (น.61-62).

เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่สำคัญ และนำไปบัญญัติเป็นกฎหมายภายในของตน กฎเกณฑ์ของแนวทางฉบับนี้เป็นแนวปฏิบัติขั้นต่ำของหลักการเพื่อให้ประเทศสมาชิกได้นำไปปฏิบัติในแต่ละประเทศ แนวปฏิบัตินี้ไม่ได้แยกระหว่างหน่วยงานของรัฐและหน่วยงานเอกชน และไม่ได้แยกว่าเป็นการประมวลผลข้อมูลเกี่ยวกับบุคคลโดยวิธีการอัตโนมัติหรือโดยวิธีการประมวลผลด้วยมือ ซึ่งมีหลักการคุ้มครองข้อมูลส่วนบุคคลดังต่อไปนี้

2.3.2.1 หลักข้อจำกัดในการเก็บรวบรวมข้อมูล ข้อมูลส่วนบุคคลที่จัดเก็บจะต้องได้มาโดยวิธีการที่ถูกต้องและชอบด้วยกฎหมาย โดยต้องให้บุคคลผู้เป็นเจ้าของข้อมูลรับทราบและยินยอมในการจัดเก็บข้อมูล

2.3.3.2 หลักคุณภาพของข้อมูล ข้อมูลส่วนบุคคลที่จัดเก็บต้องเป็นข้อมูลที่มีความเกี่ยวข้องกับวัตถุประสงค์ในการใช้ และต้องเป็นข้อมูลที่ถูกต้อง สมบูรณ์ และถูกต้องตรงตามความเป็นจริงอยู่เสมอ

2.3.2.3 หลักการกำหนดวัตถุประสงค์ ต้องมีการกำหนดวัตถุประสงค์ในการจัดเก็บข้อมูลส่วนบุคคลก่อนที่จะมีการจัดเก็บข้อมูลนั้น

2.3.2.4 หลักการจำกัดการใช้ข้อมูล การใช้ข้อมูลจะกระทำได้โดยขัดต่อวัตถุประสงค์ในการจัดเก็บมิได้ เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูล หรือได้รับอนุญาตตามเงื่อนไขที่กฎหมายกำหนด

2.3.2.5 หลักการรักษาความปลอดภัย ต้องจัดให้มีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูลเพื่อป้องกันความเสื่อมเสีย การเข้าถึง การทำลาย การใช้ การเปลี่ยนแปลงแก้ไข หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

2.3.2.6 หลักการเปิดเผยข้อมูล ต้องกำหนดวิธีการทั่วไปในการเปิดเผยข้อมูล รูปแบบของการเปิดเผย หลักเกณฑ์ในการขอให้มีการเปิดเผยข้อมูล ซึ่งต้องไม่เป็นการกระทบต่อความเป็นอยู่ส่วนตัวของเจ้าของข้อมูล

2.3.2.7 หลักการมีส่วนร่วมของปัจเจกบุคคล กำหนดให้ปัจเจกชนมีสิทธิต่าง ๆ ดังต่อไปนี้

1) มีสิทธิได้รับการแจ้งว่ามีข้อมูลของตนจัดเก็บอยู่

2) มีสิทธิตรวจสอบข้อมูลของตนที่มีผู้จัดเก็บ

3) มีสิทธิขอให้แก้ไขข้อมูลที่ไม่ถูกต้อง

4) มีสิทธิปฏิเสธไม่ให้มีการจัดเก็บข้อมูลของตน

2.3.2.8 หลักความรับผิดชอบ กำหนดความรับผิดในกรณีมีการละเมิดข้อมูลส่วนบุคคลของตน

2.3.3 หลักการคุ้มครองข้อมูลส่วนบุคคลของ APEC[57]

การกำหนดกรอบการคุ้มครองข้อมูลส่วนบุคคลของเอเปค (APEC Privacy Framework) มีเพื่อส่งเสริมเศรษฐกิจการค้าเสรีระหว่างสมาชิก โดยให้สมาชิกซึ่งมีกฎหมายและวิธีการดำเนินงานในการคุ้มครองข้อมูลส่วนบุคคลที่มีความแตกต่างกันสามารถนำไปปรับใช้ให้เหมาะสม วัตถุประสงค์ของกรอบการคุ้มครองฯ กำหนดมาตรฐานขั้นต่ำในการคุ้มครองข้อมูลส่วนบุคคล (Minimum Privacy Standard) เพื่อสนับสนุนการส่งผ่านข้อมูลภายในเขตเศรษฐกิจสมาชิก (Free Flow of Personal Data)[58]

ในช่วงก่อนปี ค.ศ. 2003 (พ.ศ. 2546) การพัฒนากฎหมายและระเบียบเกี่ยวกับข้อมูลส่วนบุคคลของเอเปคยังอยู่ในวงจำกัดจนกระทั่งในปี ค.ศ. 2003 รัฐบาลออสเตรเลียได้เสนอแก่ที่

---

[57]จาก สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, *อ้างแล้วเชิงอรรถที่ 38* (น.71-72).

[58] จาก สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, *อ้างแล้วเชิงอรรถที่ 38* (น. 92).

ประชุมให้เอเปคนำแนวทางการคุ้มครองข้อมูลส่วนบุคคลขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD guidelines of 1981) มาเป็นแนวทางในการกำหนดกรอบการคุ้มครองฯ ของเอเปค หลังจากที่ผ่านการพิจารณาและแก้ไขร่าง การประชุมระดับรัฐมนตรี (APEC Ministerial Meeting) ที่ประเทศชิลี ได้ประการกรอบการคุ้มครองข้อมูลส่วนบุคคลในเดือนพฤศจิกายน ค.ศ. 2004 (พ.ศ. 2547) วัตถุประสงค์หลักของกรอบการคุ้มครองฯ คือรักษาความปลอดภัยและความต่อเนื่องของข้อมูลที่ส่งผ่านธุรกรรมอิเล็กทรอนิกส์ทั้งในภาคธุรกิจ ผู้บริโภค และรัฐบาล และเพิ่มประสิทธิภาพและลดค่าใช้จ่ายในการส่งผ่านข้อมูล ในขณะเดียวกัน ก็ช่วยลดข้อจำกัดในการไหลเวียนของข้อมูลส่วนบุคคลระหว่างประเทศในเขตเศรษฐกิจของสมาชิก ซึ่งมีหลักการที่สำคัญ 9 ข้อ ซึ่งมีสาระสำคัญโดยสรุปดังนี้

1) หลักการป้องกันอันตราย (Preventing Harm) เพื่อเป็นการรักษาผลประโยชน์ของบุคคลในเรื่องสิทธิความเป็นส่วนตัว จึงต้องมีการกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลเพื่อป้องกันการใช้ข้อมูลโดยมิชอบ และป้องกันความเสียหายที่จะเกิดจากการใช้โดยมิชอบ ไม่ว่าจะเป็นการเก็บ การใช้ และการส่งต่อ

2) หลักการแจ้งให้ทราบ (Notice) ต้องแจ้งเจ้าของข้อมูลอย่างชัดเจนว่าจะมีการเก็บข้อมูลส่วนบุคคล วัตถุประสงค์การเก็บ ประเภทบุคคลหรือองค์กรที่ข้อมูลส่วนบุคคลอาจได้รับการเปิดเผย ต้องแจ้งสิทธิของเจ้าของข้อมูลและมาตรการที่จะใช้ในการจำกัดการใช้ การเปิดเผย การเข้าถึง และการแก้ไข ทั้งนี้ต้องแจ้งก่อนหรือในขณะที่เก็บหรือเร็วที่สุดหลังการจัดเก็บ

3) หลักจำกัดการเก็บข้อมูล (Collection Limitation) ต้องมีการจัดเก็บอย่างจำกัดเท่าที่เป็นไปตามวัตถุประสงค์ของการเก็บ การเก็บต้องทำโดยวิธีที่ถูกกฎหมาย และวิธีที่เป็นธรรมและเหมาะสม โดยได้แจ้งต่อและได้ขอคำยินยอมจากเจ้าของข้อมูลแล้ว

4) หลักการใช้ข้อมูลเฉพาะตามวัตถุประสงค์ (Uses of Personal Information) ข้อมูลที่เก็บไว้จะเอาไปใช้ได้เฉพาะตามวัตถุประสงค์ของการเก็บเท่านั้น เว้นแต่ได้รับคำยินยอมจากเจ้าของข้อมูลหรือเป็นไปตามข้อยกเว้นตามที่กฎหมายกำหนด

5) หลักการมีทางเลือก (Choice) เจ้าของข้อมูลมีสิทธิเลือกว่าจะยินยอมให้มีการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลของตน

6) หลักความสมบูรณ์ของข้อมูล (Integrity of Personal Information) ข้อมูลที่จัดเก็บต้องมีความถูกต้อง สมบูรณ์ เป็นปัจจุบัน ตามความจำเป็นและตามวัตถุประสงค์การเก็บ

7) หลักความปลอดภัย (Security Safeguards) ต้องมีมาตรการคุ้มครองข้อมูลอย่างเหมาะสมเพื่อป้องกันอันตรายที่อาจเกิดขึ้น ไม่ว่าจะเป็นการสูญหาย เสียหาย การเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การทำลายโดยไม่ได้รับอนุญาต การใช้ ปรับเปลี่ยนแก้ไข เปิดเผยโดยมิชอบ

8) หลักการเข้าถึงและแก้ไขข้อมูล (Access and Correction) เจ้าของข้อมูลมีสิทธิรับรู้ว่ามีการเก็บข้อมูลส่วนบุคคลของตนหรือไม่ และมีสิทธิเข้าถึงข้อมูลของตน และมีสิทธิขอให้ตรวจสอบความถูกต้องและขอให้ปรับปรุงแก้ไข เพิ่มเติมหรือทำลายข้อมูลของตน

9) หลักความรับผิดชอบ (Accountability) ผู้เก็บข้อมูลจะต้องรับผิดชอบการจัดมาตรการต่าง ๆ ให้เป็นไปตามหลักเกณฑ์ดังกล่าว การส่งข้อมูลส่วนบุคคลไปยังบุคคลหรือองค์การอื่น ๆ ไม่ว่าภายในประเทศหรือส่งไปยังต่างประเทศ จะต้องได้รับคำยินยอมจากเจ้าของข้อมูล และจะต้องมีมาตรการที่เหมาะสมที่ประกันได้ว่าบุคคลหรือองค์กรที่ได้รับข้อมูลไปแล้ว จะเก็บรักษาข้อมูลให้เป็นไปตามหลักเกณฑ์นี้

เมื่อพิจารณาหลักการคุ้มครองตามแนวทางของ APEC เปรียบเทียบกับหลักการคุ้มครองตามกรอบระหว่างประเทศอื่นจะพบว่า APEC Privacy Framework ไม่ได้มีลักษณะผูกพันตามกฎหมายในฐานะสนธิสัญญาระหว่างประเทศ ไม่ได้สร้างเงื่อนไขด้านเวลา และไม่ได้สร้างระบบการลงโทษ หรือหน่วยงานตรวจสอบ การยอมรับและปฏิบัติตามมาตรฐานนี้ตั้งอยู่บนหลักของความสมัครใจ หลักเกณฑ์ต่าง ๆ ของ APEC นั้นเน้นไปที่การคุ้มครองข้อมูลส่วนบุคคลและความเป็นส่วนตัวในบริบทของการค้าระหว่างประเทศในลักษณะที่สามารถเกิดขึ้นได้จริงในภูมิภาค กรอบของ APEC ได้เพิ่มหลักการสำคัญสองประการที่ OECD Guidelines ไม่ได้เน้นย้ำมากนัก นั่นคือหลักการป้องกันอันตรายและหลักการมีทางเลือก เพราะหลักการมีทางเลือกนั้น หากนำไปปฏิบัติอย่างเคร่งครัดน่าจะช่วยนำไปสู่การคุ้มครองอย่างแท้จริงได้ เพราะในสภาพความเป็นจริงแล้ว แม้จะใช้หลักความยินยอมหรือหลักการแจ้งวัตถุประสงค์เป็นมาตรฐาน แต่ภาคธุรกิจก็มักจะใช้การเก็บข้อมูลส่วนบุคคลเป็นเงื่อนไขในการให้บริการต่าง ๆ หรือใช้การแจ้งวัตถุประสงค์กว้าง ๆ ทั้งที่ไม่จำเป็นเสมอไป ถ้าหากผู้บริโภคต้องการจะใช้บริการก็จำเป็นจะต้องให้ข้อมูลส่วนบุคคลแก่

ผู้ประกอบการโดยทางเลือกของผู้บริโภคมีจำกัดเพียงแค่จะให้หรือไม่ให้เท่านั้น ทั้งที่ในความเป็นจริงสามารถสร้างตัวเลือกให้ผู้บริโภคเลือกเองได้ว่าต้องการจะให้ข้อมูลในระดับใด ซึ่งก็จะช่วยป้องกันการนำข้อมูลไปใช้โดยไม่จำเป็นหรือเกินวัตถุประสงค์ นอกจากนี้การสร้างทางเลือกตามความต้องการของผู้บริโภค ยังเป็นการเพิ่มประสิทธิภาพในการใช้ข้อมูลที่ได้มาให้เกิดประโยชน์สูงสุดสำหรับตัวผู้ประกอบธุรกิจเองด้วย กล่าวคือ ผู้ประกอบธุรกิจจะสามารถทราบได้ว่าผู้บริโภครายใดต้องการและเต็มใจรับบริการแบบใดบ้าง ทำให้ลดต้นทุนในการทำการตลาดและลดต้นทุนการเก็บรักษาข้อมูลที่ไม่จำเป็น และไม่สร้างความรำคาญใจให้กับผู้บริโภคโดยใช่เหตุ อันจะทำให้เกิดความไว้วางใจ และความสัมพันธ์อันดีระหว่างผู้ประกอบการและผู้บริโภคในระยะยาว[59]

นอกจากนี้ APEC Privacy Framework ถูกออกแบบมาให้ใช้ได้ทั้งภาครัฐและเอกชน หลักการทั้ง 9 ประการสามารถนำไปใช้เป็นต้นแบบในการออกกฎหมายกำกับการดูแลหน่วยงานภาครัฐ หรือนำไปเป็นหลักการควบคุมตนเองของภาคเอกชนได้ด้วย[60]

อย่างไรก็ตาม กรอบการคุ้มครองฯ ของเอเปคถูกนำไปเรียบเทียบกับการคุ้มครองข้อมูลส่วนบุคคลภายใต้ข้อบังคับของสหภาพยุโรป และการคุ้มครองข้อมูลส่วนบุคคลตามข้อตกลง (Convention) ของรัฐสภาแห่งยุโรป (Council of Europe) ซึ่งกรอบการคุ้มครองฯ มีความแตกต่างที่ชัดเจนกับแนวปฏิบัติของยุโรปในหลักการข้อที่ 1 และ 9 กล่าวคือ กรอบการคุ้มครองฯ ไม่ครอบคลุมประเด็นสำคัญ อาทิ การประมวลผลโดยวิธีอัตโนมัติ (Automated Processing) ซึ่งถือเป็นประเด็นสำคัญในการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป และรัฐสภาแห่งยุโรป นอกจากนั้นนักวิชาการและนักกฎหมายได้วิจารณ์เกี่ยวกับจุดบกพร่องในการคุ้มครองการจัดเก็บและใช้ข้อมูลส่วนบุคคลที่กำหนดในกรอบการคุ้มครองฯ กล่าวคือ กรอบการคุ้มครองฯ ไม่ได้แก้ไขจุดอ่อนที่มีในแนวปฏิบัติเกี่ยวกับข้อมูลส่วนบุคคลขององค์กรเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD) อาทิ กรอบการคุ้มครองฯ อนุญาตให้มีการใช้ข้อมูลระดับทุติยภูมิสำหรับการใช้ข้อมูลที่มีวัตถุประสงค์ในการใช้งานที่สอดคล้องหรือเกี่ยวข้องกัน หลักการจำกัดการจัดเก็บข้อมูลก็ไม่ได้แก้ไขช่องว่างที่ปรากฏในแนวปฏิบัติขององค์กรเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา

---

[59] จาก สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, *อ้างแล้วเชิงอรรถที่ 38* (น.88).

[60] จาก สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, *อ้างแล้วเชิงอรรถที่ 38* (น.89).

(OECD) แม้ว่ากรอบการคุ้มครองฯ ได้ปรับปรุงแนวปฏิบัติของ OECD โดยการเพิ่มเติมในส่วนของการแจ้งเจ้าของข้อมูลในการจัดเก็บ เปิดเผย เข้าถึงและแก้ไข แต่ในส่วนของการกำหนดข้อยกเว้นในการอนุญาตให้จัดเก็บและใช้ข้อมูล กรอบการคุ้มครองฯ กลับกำหนดมาตรฐานที่ต่ำกว่าแนวปฏิบัติของ OECD และไม่ได้ระบุหลักการกำหนดวัตถุประสงค์ (Purpose Specification) และหลักการเปิดเผยข้อมูล (Openness Principle) ที่ถือเป็นหลักการสำคัญในแนวปฏิบัติของ OECD[61]

อนึ่งการนำหลักการทั้ง 9 ประการที่บัญญัติไว้ในกรอบการคุ้มครองฯ ของเอเปค ดังกล่าวมาปฏิบัติกรอบของเอเปคไม่ได้มีการกำหนดรูปแบบหรือมาตรฐานในการนำไปใช้งาน และไม่ได้กำหนดให้สมาชิกต้องตรากฎหมายเฉพาะแต่ประการใด ซึ่งกรอบการคุ้มครองฯ ได้กำหนดแนวทางในการนำกรอบการคุ้มครองฯ ไปใช้งานในลักษณะข้อแนะนำที่สมาชิกสามารถนำไปปรับใช้ให้เหมาะสม โดยแบ่งออกเป็นการใช้งานภายในเขตเศรษฐกิจ และการใช้งานระหว่างประเทศ สำหรับการนำกรอบการคุ้มครองฯ ไปปฏิบัติภายในเขตเศรษฐกิจของสมาชิก สมาชิกสามารถเลือกใช้รูปแบบและวิธีการที่เห็นว่าเหมาะสมกับการดำเนินงาน ซึ่งสามารถกระทำได้โดยการตรากฎหมาย การดำเนินของหน่วยงานภาครัฐ หรือการที่เอกชนและภาคธุรกิจกำหนดกฎเกณฑ์ขึ้นใช้เอง หรือเป็นการผสมผสานรูปแบบและวิธีการที่กล่าวมาทั้งหมด ทั้งนี้ ควรมีหน่วยงานหรือองค์กรที่เป็นผู้รักษาการตามกรอบการคุ้มครองฯ และเป็นศูนย์รวมของการดำเนินการและประสานงานภายในเขตเศรษฐกิจ โดยการคุ้มครองความเป็นส่วนตัวผ่านการใช้งานกรอบการคุ้มครองฯ จะต้องไม่ขัดขวางการรักษาความมั่นคงความปลอดภัยของสาธารณะและพันธกิจของนโยบายสาธารณะของสมาชิก[62]

2.3.4 หลักการคุ้มครองข้อมูลส่วนบุคคลของ EU

แนวทางการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปเกิดขึ้นมาจากอนุสัญญาของสภายุโรป (the Council of Europe) โดยให้สหภาพยุโรปจัดให้มีการคุ้มครองบุคคลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลโดยอัตโนมัติ (Commission Recommendation : Relating to the

---

[61] จาก สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, *อ้างแล้วเชิงอรรถที่ 38* (น. 93-94).

[62] จาก สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, *อ้างแล้วเชิงอรรถที่ 38* (น. 94).

Council of Europe Convention for the Protection of individuals with regard to Automatic Processing of Personal Data) เพื่อประกันสิทธิขั้นพื้นฐานของประชาชน ภายใต้การกำกับดูแลของคณะกรรมาธิการแห่งประชาคมเศรษฐกิจยุโรปได้กำหนดให้ประเทศสมาชิกให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับที่เทียบเท่ากัน โดยใช้กฎระเบียบฉบับที่ 2016/679 (Regulation (EU) 2016/679) หรือที่เรียกว่า กฎระเบียบการคุ้มครองข้อมูลทั่วไป (the General Data Protection Regulation หรือ GDPR) ที่ออกโดยสภายุโรปและคณะมนตรีแห่งสหภาพยุโรปเป็นแนวทางในการยกร่างกฎหมายทั้งนี้ เพื่อให้กฎหมายอยู่ในลักษณะเป็นเอกภาพทั่วทั้งยุโรป

GDPR เป็นกฎระเบียบที่ว่าด้วยการคุ้มครองบุคคลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล และว่าด้วยการไหลเวียนข้อมูลโดยอิสระ ซึ่งพัฒนามาจากข้อบังคับสหภาพยุโรปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (EU Directive 95/46/EC) โดยถือว่าข้อมูลส่วนบุคคลเป็นสิทธิขั้นพื้นฐานในเรื่องความเป็นอยู่ส่วนตัวที่พลเมืองยุโรปทุกคนควรได้รับการปกป้องคุ้มครอง[63] โดย GDPR มีการปรับปรุงหลักเกณฑ์ต่าง ๆ ให้ทันสมัยขึ้น ซึ่งมีหลักการพื้นฐาน 7ประการดังนี้[64]

2.3.4.1 หลักความชอบด้วยกฎหมาย (Lawfulness) ความเป็นธรรม (Fairness) และความโปร่งใส (Transparency) บัญญัติไว้ในมาตรา 5 (1) (a) แห่ง GDPR ว่า “ข้อมูลส่วนบุคคลจะต้องประมวลผลโดยชอบด้วยกฎหมาย เป็นธรรม ในลักษณะที่โปร่งใสต่อเจ้าของข้อมูล”[65] หลักการพื้นฐานทั้ง 3 ประการนี้ค่อนข้างมีความคาบเกี่ยวกันโดยเฉพาะในเรื่องที่เกี่ยวกับการเก็บรวบรวม และใช้ข้อมูลส่วนบุคคล ซึ่งต้องอาศัยฐานของกฎหมาย (Lawful Basis) ทั้ง 6 ประการอันได้แก่ ฐานความยินยอม (Consent) ฐานสัญญา (Contract) ฐานหน้าที่ตามกฎหมาย (Legal Obligation) ฐานประโยชน์สำคัญต่อชีวิต (Vital Interest) ฐานภารกิจของรัฐ (Public Task) และฐาน

---

[63] มาตรา 8(1) แห่งกฎบัตรว่าด้วยสิทธิขั้นพื้นฐานแห่งสหภาพยุโรป (the Charter of Fundamental Rights of the European Union) และมาตรา 16(1) แห่งอนุสัญญาว่าด้วยหน้าที่ของสหภาพยุโรป (the Treaty on the Functioning of the European หรือ TFEU)

[64] From *Guide to the General Data Protection Regulation (GDPR)* (pp.14-48), by Information Commissioner’s Office, 2018a. Retrieved from https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf.

[65] GDPR Article 5 (1)(a). “Personal data shall be (a) processed lawfully, fairly and in a transparent manner in relation to the data subject.”

ประโยชน์อันชอบธรรม Legitimate Interest) และเพื่อหลีกเลี่ยงการละเมิดหลักการพื้นฐานดังกล่าว การประมวลผลข้อมูลส่วนบุคคลจำเป็นจะต้องระบุฐานของกฎหมายที่ใช้ในการประมวลผลข้อมูลส่วนบุคคลไว้ด้วย เช่น การเปิดเผยประวัติสุขภาพเพื่อช่วยเหลือผู้ป่วยประสบอุบัติเหตุทางรถยนต์ที่ต้องการการรักษาอย่างเร่งด่วนและหมดสติ เป็นการประมวลผลข้อมูลโดยอาศัยฐานประโยชน์สำคัญต่อชีวิต ดังนั้น หากการเปิดเผยข้อมูลส่วนบุคคลที่กระทำโดยปราศจากฐานของกฎหมายทั้ง 6 ประการแล้ว ย่อมเป็นการกระทำที่ละเมิดต่อหลักความชอบด้วยกฎหมาย ความเป็นธรรม และความโปร่งใส

นอกจากนี้หลักความชอบด้วยกฎหมายยังหมายความรวมถึงความชอบด้วยบทบัญญัติแห่งกฎหมายทั้งทางแพ่งและทางอาญา ดังนั้นการพิจารณาว่าจะเป็นการละเมิดต่อหลักความชอบด้วยกฎหมายหรือไม่ ไม่ได้จำกัดเฉพาะการประมวลผลที่เกี่ยวข้องกับการกระทำความผิดทางอาญาเท่านั้น แต่ยังหมายความรวมถึงการประมวลผลที่ทำให้เกิดผลเป็นการฝ่าฝืนหน้าที่ในการรักษาความลับ การขยายอำนาจตามกฎหมายหรือเป็นการใช้อำนาจโดยมิชอบ เป็นการละเมิดลิขสิทธิ์ เป็นการฝ่าฝืนข้อตกลงตามสัญญา หรือฝ่าฝืนต่อกฎหมายว่าด้วยสิทธิมนุษยชน เมื่อเกิดเหตุการประมวลผลโดยไม่ชอบด้วยกฎหมายขึ้น GDPR ได้ให้สิทธิแก่บุคคลในอันที่จะลบข้อมูลนั้นหรือจำกัดสิทธิในการประมวลผลข้อมูลนั้นได้

หลักความชอบธรรม โดยทั่วไปเป็นเรื่องเกี่ยวกับการจัดการข้อมูลส่วนบุคคลซึ่งประชาชนทั่วไปควรจะคาดหมายถึงความเหมาะสมในการจัดการนั้นได้ และต้องไม่ใช้ข้อมูลส่วนบุคคลไปในทางที่ไม่เป็นธรรมต่อเจ้าของข้อมูล แม้การใช้ข้อมูลนั้นจะได้มีการระบุฐานของการประมวลผลข้อมูลส่วนบุคคลไว้แล้วก็ตาม แต่ถ้าการประมวลผลนั้นขาดความชอบธรรม ก็ถือว่าเป็นการละเมิดต่อหลักการพื้นฐานนี้ ดังนั้นการประเมินว่าการประมวลผลข้อมูลส่วนบุคคลใดมีความชอบธรรมหรือไม่ จำเป็นที่จะต้องพิจารณาว่าการประมวลผลข้อมูลนั้นมีโอกาสที่จะกระทบต่อประโยชน์ของบุคคลใดบุคคลหนึ่งหรือไม่เพียงใด เช่น การเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประเมินความรับผิดทางภาษี หรือเพื่อกำหนดค่าปรับในความผิดทางอาญา แม้เจ้าหน้าที่ของรัฐจะอ้างว่าเป็นการใช้ข้อมูลอย่างเหมาะสมก็ตาม แต่การใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ดังกล่าวอาจเป็นเหตุให้เกิดความเสียหายต่อบุคคลได้ จึงถือว่าเป็นการใช้ข้อมูลส่วนบุคคลที่ไม่เป็นธรรม

หลักความโปร่งใสเป็นหลักการที่มีมูลฐานมาจากหลักความเป็นธรรม ซึ่งการประมวลผลด้วยความโปร่งใสเป็นหลักการที่กำหนดให้ต้องมีการแจ้งถึงการประมวลผลข้อมูลส่วน

บุคคลให้แก่เจ้าของข้อมูลทราบอย่างชัดเจน เปิดเผย และซื่อตรงตั้งแต่เริ่มต้น โดยจะต้องแจ้งรายละเอียดของผู้ที่เกี่ยวข้องกับการประมวลผล ทั้งวัตถุประสงค์และเหตุผลที่เหมาะสมในการใช้ข้อมูลส่วนบุคคลด้วยภาษาที่เข้าใจง่ายและมีความชัดเจน และต้องจัดให้มีมาตรการตรวจสอบถึงการปฏิบัติตามหลักความโปร่งใสได้เมื่อมีการร้องขอจากเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้อง หลักความโปร่งใสจึงมีผลต่อการตัดสินใจของเจ้าของข้อมูลที่จะพิจารณาอนุญาตให้มีการเก็บรวบรวม หรือใช้ข้อมูล นอกจากนั้นในกรณีของการประมวลผลลับหลัง (Invisible Processing) ที่ไม่ได้ทำการเก็บรวบรวมข้อมูลส่วนบุคคลมาจากเจ้าของข้อมูลโดยตรง แต่ได้รับข้อมูลส่วนบุคคลมาจากแหล่งอื่น ทำให้เจ้าของข้อมูลไม่ทราบถึงการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคล เพื่อให้เป็นไปตามหลักความโปร่งใส ผู้ที่ทำการประมวลผลลับหลังมีหน้าที่จะต้องแจ้งให้เจ้าของข้อมูลทราบถึงการประมวลผลนั้น

2.3.4.2 หลักการจำกัดวัตถุประสงค์ (Purpose Limitation) บัญญัติไว้ในมาตรา 5 (1) (b) แห่ง GDPR ว่า “การระบุวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลต้องมีความชัดเจน และชอบด้วยกฎหมาย และไม่ดำเนินการประมวลผลข้อมูลส่วนบุคคลด้วยวัตถุประสงค์ที่ไม่อาจยอมรับได้ เว้นแต่วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อประโยชน์สาธารณะ เพื่อการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ตามที่บัญญัติไว้ในมาตรา 89 (1) ให้ถือว่าการประมวลผลด้วยวัตถุประสงค์ดังกล่าวเป็นวัตถุประสงค์ที่ยอมรับได้”[66]

การดำเนินการตามหลักการจำกัดวัตถุประสงค์ เป็นหน้าที่ของผู้ควบคุมที่จะต้องระบุรายละเอียดของวัตถุประสงค์การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างชัดเจนไว้เป็นลายลักษณ์อักษร ไม่ว่าจะอยู่ในรูปแบบของเอกสาร หรือทางอิเล็กทรอนิกส์ โดยรายละเอียดของวัตถุประสงค์การเก็บรวบรวมข้อมูลส่วนบุคคลให้ระบุไว้ในส่วนนโยบายความเป็นส่วนตัวในลักษณะของรายละเอียดที่แยกออกมาต่างหากจากข้อความอื่น ๆ เพื่อให้เจ้าของข้อมูลเห็นได้อย่างชัดเจน นอกจากนั้นผู้ควบคุมหรือผู้ประมวลผลข้อมูลยังมีหน้าที่ทางเอกสารในการจัดทำและเก็บรักษา

---

[66] GDPR Article 5 (1)(b). “Personal data shall be: (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.”

บันทึกรายละเอียดวัตถุประสงค์ของกิจกรรมการประมวลผล เว้นแต่เจ้าของข้อมูลได้ทราบถึงรายละเอียดของวัตถุประสงค์ของการเก็บรวบรวมเพื่อนำข้อมูลส่วนบุคคลนั้นไปประมวลผลอยู่แล้ว ก็ไม่จำต้องระบุวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลไว้ในส่วนของนโยบายความเป็นส่วนตัว

ในส่วนของการจัดทำและเก็บรักษาบันทึกรายละเอียดวัตถุประสงค์ของกิจกรรมการประมวลผลนั้น GDPR บัญญัติไว้ในมาตรา 30 กำหนดให้ผู้ควบคุม หรือผู้ประมวลผลข้อมูลมีหน้าที่จัดทำและเก็บรักษาบันทึกกิจกรรมการประมวลผลโดยระบุรายละเอียดของวัตถุประสงค์ในการประมวลผลแต่ละครั้งไว้ในรูปแบบของเอกสาร แต่หน้าที่ในการจัดทำและเก็บรักษาบันทึกรายละเอียดวัตถุประสงค์ของกิจกรรมการประมวลผลในรูปแบบเอกสารดังกล่าวผู้ควบคุมไม่ต้องแจ้งให้เจ้าของข้อมูลทราบอีกครั้งหนึ่งหากเป็นการประมวลผลที่อยู่ภายในขอบวัตถุประสงค์เดิม

สำหรับผู้ควบคุมที่ได้รับการยกเว้นให้ไม่ต้องจัดทำและเก็บรักษาบันทึกกิจกรรมการประมวลผลตามมาตรา 30 วรรคห้าแห่ง GDPR ผู้ควบคุมนั้นยังมีหน้าที่จัดทำวัตถุประสงค์การเก็บรวบรวมข้อมูลส่วนบุคคลไว้ในส่วนของนโยบายความเป็นส่วนตัว อย่างไรก็ตามหน้าที่ทางเอกสารถือเป็นแนวปฏิบัติที่ดีที่ทุกองค์กรควรนำไปปฏิบัติ

กรณีผู้ควบคุมต้องการประมวลผลข้อมูลส่วนบุคคลสำหรับวัตถุประสงค์ใหม่หรือแตกต่างไปจากวัตถุประสงค์เดิม ผู้ควบคุมจะกระทำได้ต่อเมื่อได้รับความยินยอมจากเจ้าของข้อมูลเสียก่อน ดังนั้น หลักการจำกัดวัตถุประสงค์มิได้ห้ามการประมวลผลนอกขอบวัตถุประสงค์ไว้อย่างเด็ดขาด เพียงแต่ผู้ควบคุมจะต้องขอความยินยอมจากเจ้าของข้อมูลสำหรับการประมวลผลนอกขอบวัตถุประสงค์นั้น ซึ่งการขยายข้อจำกัดวัตถุประสงค์ดังกล่าวผู้ควบคุมอาจไม่ต้องขอความยินยอมหากการประมวลผลข้อมูลส่วนบุคคลมีวัตถุประสงค์ที่ยอมรับได้ (Compatible Purpose) เช่น การประมวลผลข้อมูลส่วนบุคคลเพื่อประโยชน์สาธารณะ หรือเพื่อวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ

ในการพิจารณาว่าการประมวลผลข้อมูลส่วนบุคคลสำหรับวัตถุประสงค์ใหม่หรือแตกต่างไปจากวัตถุประสงค์เดิมเป็นวัตถุประสงค์ที่ยอมรับได้หรือไม่นั้น ให้คำนึงถึงความเชื่อมโยงใด ๆ ระหว่างวัตถุประสงค์เดิมและวัตถุประสงค์ใหม่ ประเภทของข้อมูลส่วนบุคคล เช่น

เป็นข้อมูลที่มีความอ่อนไหว (Sensitive) หรือไม่ หรือผลกระทบที่เกิดขึ้นอันเนื่องมาจากการประมวลผลตามวัตถุประสงค์ใหม่ ตลอดจนการปกป้องข้อมูลอย่างเหมาะสม เช่นการเข้ารหัส (Encryption) หรือการแฝงข้อมูล (Pseudonymisation) สำหรับตัวอย่างในการพิจารณาวัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคลว่าแตกต่างไปจากเดิมหรือไม่ เช่น กรณีคุณหมอเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับสุขภาพของคนไข้ให้กับภริยาของตนซึ่งทำธุรกิจท่องเที่ยว ต่อมาภริยานำข้อมูลดังกล่าวมาประมวลผลเพื่อจัดทำโปรแกรมท่องเที่ยงในเชิงบำบัดเสนอต่อคนไข้รายนั้น ตามตัวอย่างจะเห็นได้ว่าการประมวลผลข้อมูลสุขภาพเพื่อนำเสนอสถานที่ท่องเที่ยวที่เหมาะสมต่อการบำบัดหรือรักษาโรคภัยไข้เจ็บของบุคคลใด เป็นการประมวลผลข้อมูลส่วนบุคคลด้วยวัตถุประสงค์ใหม่ที่ไม่เชื่อมโยงใด ๆ กับวัตถุประสงค์เดิม และข้อมูลสุขภาพถือเป็นข้อมูลประเภทที่มีความอ่อนไหว การประมวลผลดังกล่าวย่อมเป็นการประมวลผลที่ยอมรับไม่ได้

การระบุวัตถุประสงค์ในการเก็บรวบรวบข้อมูลส่วนบุคคลนอกจากจะเป็นการจำกัดวัตถุประสงค์ในการประมวลผลแล้ว ยังทำให้เจ้าของข้อมูลสามารถประเมินความเสี่ยงผลกระทบที่อาจเกิดจากการให้สิทธิแก่ผู้ควบคุมมีอำนาจบางประการเหนือข้อมูลส่วนบุคคลของพวกเขา และแบ่งปันข้อมูลส่วนบุคคลให้ด้วยความเต็มใจ

2.3.4.3 หลักการลดจำนวนข้อมูล (Data Minimisation) บัญญัติไว้ในมาตรา 5 (1) (c) แห่ง GDPR ว่า “ข้อมูลส่วนบุคคลจะต้องเพียงพอ เกี่ยวข้อง และจำกัดเท่าที่จำเป็นต่อวัตถุประสงค์ของการประมวลผล”[67]

หลักการลดจำนวนข้อมูล เป็นการลดจำนวนการเก็บรวบรวมและเก็บรักษาข้อมูลส่วนบุคคลให้น้อยที่สุดแต่ให้เพียงพอต่อความจำเป็นตามวัตถุประสงค์ของการประมวลผล ดังนั้นการระบุวัตถุประสงค์ในการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลจึงเป็นปัจจัยสำคัญในการพิจารณาว่าจำนวนข้อมูลที่เก็บรักษาไว้เพียงพอ เกี่ยวข้อง หรือจำเป็นต่อการประมวลผลหรือไม่ และผู้เก็บรักษาข้อมูลจะต้องกำหนดระยะเวลาเพื่อตรวจสอบและลบข้อมูลส่วนบุคคลที่ไม่เกี่ยวข้อง หรือจำเป็นต่อวัตถุประสงค์ของการประมวลผลอีกต่อไป ทั้งไม่ควรเก็บรักษาข้อมูลส่วนบุคคลที่ไม่มีความเกี่ยวข้องด้วย เช่น กรณีที่บริษัททวงหนี้ทำการค้นหาและเก็บรวบรวมข้อมูลของบุคคลที่มีชื่อ

---

[67] GDPR Article 5 (1)(c) Personal data shall be: (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

เหมือนกับลูกหนี้ บริษัทควรเก็บข้อมูลให้น้อยที่สุดเท่าที่จำเป็น และลบข้อมูลส่วนเกินเสียโดยเก็บบันทึกไว้เพียงรายชื่อของบุคคลที่ไม่ใช่ลูกหนี้เพื่อป้องกันการติดต่อทวงถามหนี้กับบุคคลที่ไม่เกี่ยวข้อง อย่างไรก็ตามหลักการลดจำนวนข้อมูล ไม่ได้หมายความว่าผู้เก็บรักษาข้อมูลจะต้องทำการลดการเก็บรักษาข้อมูลเท่านั้น ในบางกรณีที่ข้อมูลที่เก็บรักษาไว้ไม่เพียงพอต่อวัตถุประสงค์ ก็อาจมีการเก็บรวบรวมข้อมูลเพิ่มเติมให้เพียงพอต่อวัตถุประสงค์ที่คาดหมายไว้ได้ เช่น สโมสรที่เพิ่มก่อตั้งซึ่งสมาชิกทุกคนรู้จักกันดี ข้อมูลพื้นฐานที่จะใช้ในการบริหารจัดการเกี่ยวกับกิจกรรมต่าง ๆ ของสโมสรมีเพียงชื่อ และที่อยู่อีเมล์ ต่อมาสโมสรเริ่มเป็นที่นิยมและมีสมาชิกเพิ่มขึ้นอย่างรวดเร็ว เช่นนี้ การเก็บรวบรวมข้อมูลสมาชิกเพิ่มเติมจึงมีความจำเป็นเพื่อให้สโมสรสามารถระบุตัวตนของสมาชิกได้อย่างถูกต้อง และทราบถึงสถานภาพการชำระค่าสมาชิกของสมาชิกผู้นั้น

นอกจากนี้ตามหลักการลดจำนวนข้อมูลยังก่อให้เกิดสิทธิแก่เจ้าของข้อมูลในอันที่จะแก้ไขข้อมูล (Right to rectification) ของตนที่ไม่สมบูรณ์ให้สมบูรณ์ได้เพื่อให้เพียงพอต่อการประมวลผล และมีสิทธิที่จะขอให้ลบ (Right to erasure) ข้อมูลส่วนบุคคลที่ไม่มีความจำเป็นต่อวัตถุประสงค์ของการประมวลผลซึ่งสิทธิดังกล่าวอาจเรียกว่าเป็น “สิทธิที่จะถูกลืม” (Right to be forgotten)

2.3.4.4. หลักความถูกต้องของข้อมูล (Accuracy) บัญญัติไว้ในมาตรา 5 (1) (d) แห่ง GDPR ว่า “ข้อมูลส่วนบุคคลจะต้องมีความถูกต้อง และเก็บรักษาข้อมูลให้เป็นปัจจุบัน โดยข้อมูลที่ไม่ถูกต้องจะต้องถูกลบ หรือถูกแก้ไขโดยไม่ชักช้า”[68] เมื่อพิจารณา GDPR แล้วไม่ปรากฏคำนิยามของ “ความถูกต้องของข้อมูล” (Accurate) แต่กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหราชอาณาจักรได้นิยามคำว่า “ความไม่ถูกต้องของข้อมูล” (Inaccurate) ไว้ตามพระราชบัญญัติคุ้มครองข้อมูล ค.ศ. 2018 ว่าหมายความถึง ความไม่ถูกต้อง หรือการทำให้เข้าใจผิดในข้อเท็จจริงใด

---

[68] GDPR Article 5 (1)(d) “1. Personal data shall be: (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.”

หลักความถูกต้องของข้อมูลเป็นหลักสำคัญในการบันทึกและเก็บรักษาบันทึกข้อมูลที่มีรายละเอียดเกี่ยวกับข้อเท็จจริง หรือรายละเอียดใด ๆ ของบุคคล รวมถึงการเก็บบันทึกความผิดพลาดของข้อมูลนั้นด้วย (Records of Mistakes) แต่การบันทึกข้อมูลที่ผิดพลาดผู้บันทึกข้องต้องแสดงข้อมูลที่ถูกต้องให้ปรากฏด้วย เพื่อป้องกันมิให้เกิดความเข้าใจผิดในรายละเอียด ทั้งยังเป็นประโยชน์ต่อบุคคลผู้เป็นเจ้าของข้อมูลและบุคคลอื่น ๆ ด้วย เช่น ข้อมูลการวินิจฉัยโรคที่ผิดพลาดเป็นข้อมูลที่จำเป็นต้องบันทึกและเก็บรักษาไว้เพื่อประโยชน์ในการรักษาโรคให้แก่ผู้ป่วยที่มีอาการในลักษณะเดียวกันโดยการบันทึกต้องแสดงรายละเอียดให้ปรากฏถึงความผิดพลาดที่เกิดขึ้นและวิธีการที่วินิจฉัยโรคที่ถูกต้องอย่างชัดเจน

ในทางปฏิบัติการบันทึกและเก็บรักษาข้อมูลตามหลักความถูกต้องของข้อมูล ผู้บันทึกควรระบุสถานะและแหล่งที่มาของข้อมูล รายละเอียดการตรวจสอบหรือรับรองความถูกต้องของข้อมูล ตลอดจนมีหน้าที่ในการปรับปรุงข้อมูลให้เป็นปัจจุบันอยู่เสมอ ซึ่งการระบุสถานะของข้อมูลทำให้ผู้เก็บรักษาบันทึกข้อมูลไม่จำเป็นต้องปรับปรุงข้อมูลให้เป็นปัจจุบัน และทำให้ข้อมูลมีความถูกต้องอยู่เสมอแม้ข้อมูลนั้นจะไม่เป็นปัจจุบันก็ตาม เช่น การบันทึกข้อมูลภูมิลำเนาของบุคคลที่ย้ายภูมิลำเนาไปแล้ว โดยระบุสถานะว่าเป็นภูมิลำเนาในปัจจุบันย่อมทำให้ข้อมูลนั้นไม่มีความถูกต้อง การระบุสถานะของบันทึกข้อมูลใหม่ว่าสถานที่นั้นเคยเป็นภูมิลำเนาที่บุคคลนั้นอาศัยอยู่ก็เพียงพอที่จะทำให้ข้อมูลนั้นมีความถูกต้องอยู่เสมอ

สำหรับการแสดงแหล่งที่มาของข้อมูลใช้กับการบันทึกข้อมูลที่ได้รับมาจากบุคคลที่ไม่ใช่เจ้าของข้อมูลนั้น หรือไม่อาจยืนยันความถูกต้องของข้อมูลที่ได้รับมาได้ ซึ่งข้อมูลประเภทนี้จำเป็นที่จะมีการตรวจสอบ หรือรับรองความถูกต้องของข้อมูล เช่น ข้อมูลเกี่ยวกับประสบการณ์ทำงานที่ระบุในใบสมัครงานตำแหน่งพนักงานขับรถบรรทุก เป็นข้อมูลที่ไม่อาจยืนยันความถูกต้องของข้อมูลได้จำเป็นที่นายจ้างจะต้องตรวจสอบเพื่อยืนยันข้อมูลนั้นไม่ว่าจะโดยการสัมภาษณ์ หรือทดสอบผู้สมัคร แต่ถ้าข้อมูลที่ระบุไม่จำเป็นต่อตำแหน่งงานเช่นข้อมูลที่ผู้สมัครระบุว่าเคยทำงานในห้างสรรพสินค้า เป็นข้อมูลที่ไม่จำเป็นสำหรับตำแหน่งพนักงานขับรถบรรทุก ผู้รับสมัครก็ไม่จำเป็นต้องตรวจสอบความถูกต้องของข้อมูลนั้น หรือข้อมูลที่ได้รับมาจากบุคคลที่น่าเชื่อถือหรือเป็นบุคคลที่มีชื่อเสียง เบื้องต้นอาจสันนิษฐานไว้ก่อนว่าข้อมูลนั้นมีความน่าเชื่อถือ แต่ถ้าการใช้ข้อมูลนั้นอาจก่อให้เกิดผลกระทบร้ายแรง หรือมีเหตุอันควรสงสัยถึงความถูกต้องของข้อมูลนั้น ผู้บันทึกข้อมูลจำเป็นต้องทำการตรวจสอบความถูกต้องของข้อมูลที่ได้รับมาอีกครั้งหนึ่ง (Double-check) เช่น บริษัทที่กำลังจะปิดกิจการแนะนำพนักงานบริษัทของตนให้แก่บริษัทอื่น ถ้า

ผู้บริหารของทั้งสองบริษัทรู้จักมักคุ้นกันดี คำแนะนำดังกล่าวถือเป็นข้อมูลที่มีค่าเสมือนเป็นการรับรองประสบการณ์ทำงานของพนักงานไปในตัว แต่ถ้าตำแหน่งที่ต้องการจำเป็นต้องใช้ทักษะหรือคุณสมบัติเฉพาะ บริษัทที่รับพนักงานดังกล่าวก็จำเป็นที่จะต้องตรวจสอบตามสมควร

ส่วนการปรับปรุงข้อมูลเป็นขั้นตอนหนึ่งที่ทำให้บันทึกข้อมูลยังคงมีความถูกต้องอยู่เสมอ ทั้งนี้ขึ้นอยู่กับวัตถุประสงค์ในการใช้ข้อมูลนั้นด้วย ถ้าการบันทึกข้อมูลมีวัตถุประสงค์เพื่อทราบข้อเท็จจริงที่เป็นปัจจุบันอยู่เสมอ ผู้เก็บบันทึกข้อมูลก็จำเป็นต้องตรวจสอบและปรับปรุงบันทึกข้อมูลอยู่เสมอเมื่อพบความเปลี่ยนแปลงของข้อมูลนั้น เช่น บันทึกข้อมูลที่แสดงอัตราเงินเดือนของลูกจ้างควรได้รับการปรับปรุงทันทีเมื่อมีการขึ้นเงินเดือนให้แก่ลูกจ้าง แต่ถ้าวัตถุประสงค์ของการใช้ข้อมูลไม่จำเป็นต้องใช้บันทึกข้อมูลที่แสดงข้อเท็จจริงที่เป็นปัจจุบันอยู่เสมอก็ไม่มีความจำเป็นที่จะต้องทำการตรวจสอบและปรับปรุงบันทึกข้อมูลนั้น เช่น การใช้บันทึกข้อมูลที่มีวัตถุประสงค์เพื่อแสดงข้อเท็จจริงทางด้านประวัติศาสตร์ หรือข้อเท็จจริงในเชิงสถิติ

นอกจากนี้เพื่อให้บันทึกข้อมูลมีความถูกต้องมากยิ่งขึ้น บุคคลใด ๆ ยังมีสิทธิร้องขอให้แก้ไขข้อมูลส่วนบุคคลที่ไม่ถูกต้องให้มีความถูกต้องได้โดยคัดค้านถึงความถูกต้องของข้อมูลนั้น และผู้เก็บบันทึกข้อมูลต้องพิจารณาคำคัดค้านความถูกต้องด้วยความระมัดระวัง

2.3.4.5 หลักการจำกัดระยะเวลาในการเก็บรักษาข้อมูล (Storage Limitation) บัญญัติไว้ในมาตรา 5 (1) (e) แห่ง GDPR ว่า “ข้อมูลส่วนบุคคลจะต้องเก็บรักษาไว้ไม่นานเกินกว่าความจำเป็นเพื่อบรรลุวัตถุประสงค์สำหรับการประมวลผลข้อมูลส่วนบุคคล เว้นแต่เป็นการประมวลผลข้อมูลส่วนบุคคลมีวัตถุประสงค์สำคัญเพื่อประโยชน์สาธารณะ เพื่อบรรลุวัตถุประสงค์ในการวิจัยทางวิทยาศาสตร์หรือทางประวัติศาสตร์ หรือวัตถุประสงค์ในเชิงสถิติ ตามที่บัญญัติไว้ในมาตรา 89 (1) ว่าด้วยเรื่องการดำเนินมาตรการทางเทคนิค และการจัดระเบียบองค์กรที่เหมาะสม เพื่อปกป้องสิทธิและเสรีภาพของเจ้าของข้อมูล”[69] เนื่องจาก GDPR มิได้กำหนดระยะเวลาในการเก็บ

---

[69] GDPR Article 5(1)(e) Personal data shall be: (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal

รักษาข้อมูลไว้ เพื่อให้การเก็บรักษาข้อมูลเป็นไปตามหลักการจำกัดระยะเวลาในการเก็บรักษาข้อมูล ผู้เก็บรักษาข้อมูลจะต้องกำหนดระยะเวลาในการเก็บรักษาข้อมูลนั้น ซึ่งระยะเวลาในการเก็บรักษาข้อมูลอาจขึ้นอยู่กับวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล เช่น การกำหนดระยะเวลาเก็บรักษาภาพจากกล้องวงจรปิดที่บันทึกหน้าบุคคลผู้มาติดต่อทำธุรกรรมทางการเงินกับธนาคาร อาจกำหนดระยะเวลาตามความจำเป็นเพื่อประโยชน์ในการตรวจสอบความผิดปกติของการทำธุรกรรมทางการเงิน หรือในกรณีสถานบันเทิงอาจกำหนดระยะเวลาเก็บรักษาภาพกล้องวงจรปิดในระยะเวลาสั้น ๆ เนื่องเหตุการณ์ที่น่าสงสัยในสถานบันเทิงมักปรากฏขึ้นอย่างรวดเร็ว สถานบันเทิงจึงไม่มีความจำเป็นต้องเก็บรักษาบันทึกภาพกล้องวงจรปิดไว้เป็นระยะเวลานาน ดังนั้น เมื่อบรรลุวัตถุประสงค์ของการเก็บรักษาบันทึก หรือการประมวลผลแล้วผู้เก็บรักษาข้อมูลควรลบ หรือทำลายข้อมูลนั้นเสีย

การดำเนินการลบหรือทำลายข้อมูลที่ไม่มีความจำเป็นต่อวัตถุประสงค์ของการประมวลผลมีความสอดคล้องกับหลักการลดจำนวนข้อมูล และลดความเสี่ยงที่จะเกิดความผิดพลาดจากการใช้ข้อมูลที่ไม่เป็นปัจจุบันอันเป็นการปฏิบัติตามหลักความถูกต้องของข้อมูลอีกด้วย นอกจากนี้การเก็บข้อมูลไว้นานเกินความจำเป็นยังเพิ่มค่าใช้จ่ายในการจัดเก็บและค่าใช้จ่ายในการวางมาตรการรักษาความปลอดภัยให้แก่ข้อมูลด้วย

2.3.4.6 หลักความซื่อสัตย์และการรักษาความลับ (Integrity and Confidentiality) บัญญัติไว้ในมาตรา 5 (1) (f) แห่ง GDPR ว่า “การประมวลผลข้อมูลส่วนบุคคลจะต้องมีการจัดการรักษาความปลอดภัยให้แก่ข้อมูลส่วนบุคคลที่เหมาะสม รวมถึงการใช้มาตรการทางเทคนิค หรือการจัดระเบียบองค์กรเพื่อป้องกันการประมวลผลโดยไม่ได้รับอนุญาต หรือไม่ชอบด้วยกฎหมาย และป้องกันข้อมูลสูญหาย ถูกทำลาย หรือถูกทำให้เสียหายโดยไม่ตั้งใจ”[70]

---

data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

[70] GDPR Article 5(1)(f) Personal data shall be: (f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful

ข้อมูลที่องค์กรได้รับมานั้นจะต้องทำการเก็บรักษาไว้อย่างปลอดภัย และในส่วนของผู้ควบคุมจะต้องมีหน้าที่ในการดำเนินการตามขั้นตอนที่เหมาะสม เพื่อให้มั่นใจในความน่าเชื่อถือของพนักงานทุกคนที่มีสิทธิ์เข้าถึงข้อมูลส่วนบุคคล ในกรณีที่มีบุคคลที่สามนำข้อมูลไปใช้ในการประมวลผล องค์กรต้องมั่นใจได้ว่ามีการทำสัญญากับผู้ประมวลผลข้อมูลนั้น ๆ โดยจะต้องมีมาตรการรักษาความปลอดภัยที่เหมาะสม

2.3.4.7 หลักความรับผิดชอบ(Accountability) บัญญัติไว้ในมาตรา 5 (2) แห่ง GDPR ว่า “ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่และภาระการพิสูจน์ถึงการปฏิบัติตามหลักการคุ้มครองข้อมูลที่บัญญัติไว้ในวรรคหนึ่ง”[71] หลักความรับผิดชอบเป็นหลักที่กำหนดภาระให้แก่ผู้ควบคุม 2 ประการคือ ภาระหน้าที่(Responsible) ในการปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคลตามที่ GDPR บัญญัติไว้ และภาระการพิสูจน์(Demonstrate) ว่าได้มีการปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคลแล้ว

ภาระหน้าที่และภาระการพิสูจน์การปฏิบัติตามกฎหมายไม่เพียงแต่จะทำให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพ แต่ยังเป็นการแสดงถึงการเคารพต่อสิทธิส่วนบุคคล ดังนั้น เพื่อให้การปฏิบัติตามภาระหน้าที่และภาระการพิสูจน์บรรลุผลแห่งหลักความรับผิดชอบจำเป็นที่จะต้องจัดให้มีมาตรการทางเทคนิคและการจัดระเบียบองค์กรที่เหมาะสม ซึ่งมาตรการดังกล่าวได้แก่ การวางนโยบายและสร้างมาตรฐานการคุ้มครองข้อมูล เก็บรักษาบันทึกกิจกรรมการประมวลผล กำหนดมาตรการรักษาความปลอดภัยที่เหมาะสม บันทึกและรายงานเหตุการละเมิดข้อมูลส่วนบุคคล ทำสัญญาเป็นลายลักษณ์อักษรในกรณีที่สั่งให้บุคคลภายนอกดำเนินการประมวลผลข้อมูลส่วนบุคคล ทำการประเมินผลกระทบต่อการคุ้มครองข้อมูลเพื่อใช้ข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงที่อาจกระทบต่อประโยชน์ของบุคคล แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล เป็นต้น ทั้งจะต้องจัดให้มีการทบทวนและปรับปรุงมาตรการต่าง ๆ ให้มีความเหมาะสมต่อสถานการณ์ปัจจุบันอยู่เสมอ

---

processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

[71] GDPR Article 5(2) The controller shall be responsible for, be able to demonstrate compliance with, paragraph 1.

หลักความรับผิดชอบส่วนใหญ่จะเป็นการกำหนดหน้าที่ทางเอกสารที่จะต้องมีการจัดทำบันทึกกิจกรรมการประมวลผล บันทึกวัตถุประสงค์ของการประมวลผล บันทึกการแบ่งปันข้อมูล(Data Sharing) ระยะเวลาการเก็บรักษาบันทึก(Retention)

2.4 แนวความคิดและหลักการของบันทึก

จากการศึกษาถึงหลักการคุ้มครองข้อมูลส่วนบุคคลตามกรอบขององค์การระหว่างประเทศพบหลักการคุ้มครองของแต่ละองค์กรมีความคล้ายคลึงกัน เช่น การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะกระทำได้ ต่อเมื่อมีการขอความยินยอม, มีความจำเป็นเพื่อให้บรรลุวัตถุประสงค์ตามปกติของสัญญา หรือเป็นการปฏิบัติตามกฎหมาย ซึ่งอาจเรียกได้ว่าเป็นฐานของกฎหมาย (Lawful Basis) ที่ทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เป็นไปโดยชอบด้วยกฎหมาย และจะต้องเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็นภายใต้กรอบระยะเวลาที่เหมาะสม นอกจากนั้นผู้เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะต้องจัดทำบันทึกเกี่ยวกับกิจกรรมต่าง ๆ ที่เกิดขึ้นกับข้อมูลส่วนบุคคลไว้เป็นหลักฐานเพื่อใช้พิสูจน์หรือแสดงต่อเจ้าหน้าที่ที่รัฐตั้งขึ้นมาเพื่อตรวจสอบ

ในหัวข้อนี้ผู้วิจัยมีวัตถุประสงค์เพื่อศึกษาถึงการจัดทำบันทึก ซึ่งเป็นส่วนสำคัญที่ทำให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพ เนื่องจากกระบวนการภายหลังผ่านขั้นตอนการขอความยินยอมจากเจ้าของข้อมูลแล้ว หากไม่มีการจัดทำบันทึกเจ้าของข้อมูลจะไม่สามารถตรวจสอบการใช้ หรือเปิดเผยข้อมูลของตนได้เลย ดังนั้นจึงมีความจำเป็นที่จะต้องศึกษาเกี่ยวกับแนวความคิดและหลักการของบันทึก ประกอบกับหลักการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง เพื่อให้ทราบถึงลักษณะของบันทึกที่สามารถใช้เป็นหลักฐานในการตรวจสอบกิจกรรมต่าง ๆ ที่เกิดขึ้นกับข้อมูลส่วนบุคคลได้ ตลอดจนศึกษาถึงหน้าที่และข้อยกเว้นในการจัดทำบันทึกเพื่อวิเคราะห์ผลกระทบอันเกิดจากการบังคับใช้กฎหมายต่อไป

2.4.1 แนวความคิดเกี่ยวกับการบันทึก

แนวความคิดเกี่ยวกับการบันทึกอาจสะท้อนผ่านบทนิยาม ซึ่งบันทึก (Records) นั้นคือข้อมูลที่จะเป็นหลักฐาน (Evidence) ของกิจกรรมต่าง ๆ ที่ได้เกิดขึ้นแล้ว เพื่อใช้เป็นประโยชน์ในการตรวจสอบ (Audit) และสอบสวน (Investigate) ในภายหลัง เช่น การสั่งซื้อสินค้าก็จะมีข้อมีที่

เกี่ยวข้องเช่น เอกสารการสั่งซื้อ (Purchase Order), เอกสาร TOR, ข้อมูลการเปรียบเทียบราคาหรืออีเมล์การต่อรองราคา เป็นต้น หรือการชำระเงินก็จะมีใบเสร็จรับเงิน, ใบแจ้งหนี้หรือข้อมูลที่เกี่ยวข้อง สิ่งที่สำคัญคือข้อมูลที่ถูกกำหนด (Declare) ให้เป็น “ข้อมูลบันทึก” จะต้องไม่มีการเปลี่ยนแปลงอีกต่อไป และต้องมีการจัดเป็นระยะเวลาค่อนข้างนาน เนื่องจากข้อมูลเหล่านี้จะเป็นข้อมูลที่ใช้สำหรับการตรวจสอบในภายหลัง[72]

บันทึกเป็นหลักฐานของการติดต่อสื่อสาร การทำกิจกรรมขององค์กร สะท้อนกระบวนการทำงานขององค์กรหรือบุคคล เป็นหลักฐานการปฏิบัติงานขององค์กร และเป็นแหล่งข้อมูลที่เชื่อถือได้เพราะบันทึกมีลักษณะเป็นเอกสารที่ประกอบด้วยองค์ประกอบดังนี้[73]

2.4.1.1 เนื้อหา (Content) ต้องมีเรื่องราว ข้อเท็จจริง ข้อมูลหรือสารสนเทศที่ปรากฏบนเอกสารนั้น

2.4.1.2 บริบท (Context) ต้องมีส่วนประกอบแวดล้อมที่แสดงถึงเรื่องราวความเป็นมาของเอกสารเป็นส่วนที่แสดงให้รู้เรื่องราวเกี่ยวกับการจัดทำ การติดต่อสื่อสาร การดูแลรักษาและใช้เอกสารนั้น ๆ เป็นสิ่งแวดล้อมที่สัมพันธ์ตั้งแต่ผู้ที่เกี่ยวข้องในการรับ-ส่ง และใช้เอกสารนั้น ส่วนที่เป็นข้อความโต้ตอบที่ปรากฏบนเอกสารนั้นที่จะทำให้ทราบว่าเอกสารนั้นมีการดำเนินการอย่างไร และเกี่ยวข้องกับผู้ใดบ้าง รวมถึงสิ่งอื่น ๆ ที่บันทึกบนเอกสารนั้นด้วย

2.4.1.3 โครงสร้างของเอกสาร (Structure) ต้องมีรูปแบบโครงสร้างของเนื้อหาที่ชัดเจน ซึ่งส่วนประกอบของเอกสารแต่ละฉบับจะมีทั้งส่วนประกอบที่แสดงให้เห็นได้ด้วยตา เช่น วัสดุในการจัดทำเอกสาร อักขระหรือตัวอักษร ภาษา เครื่องหมายที่แสดงให้ปรากฏบนเอกสาร ส่วนที่ระบุผู้เกี่ยวข้องในการจัดทาและใช้เอกสาร ตราประทับ และส่วนของข้อความที่ผู้รับผิดชอบหรือผู้

---

[72] จาก *การจัดการบันทึก(Record management)* (น.49), โดย ไพโรจน์ ต้นศิริอนุสรณ์, 2558. สืบค้นจาก http://www.techconsbiz.com/img/file/BPM_Dec_2015.pdf

[73] จาก *การจัดการเอกสารโดยใช้หลักการจัดเอกสารแบบวิเคราะห์หน้าที่ กรณีศึกษา: บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร ตลิ่งชัน*, โดย พิสมัย ระพีพัฒน์ชัย, 2560 วิทยานิพนธ์ปริญญามหาบัณฑิต มหาวิทยาลัยศิลปากร.

ที่เกี่ยวข้องบันทึกเป็นข้อความไว้บนเอกสารนั้น ๆ และส่วนประกอบที่ต้องมีการอ่านจึงจะบอกได้ เช่น วิธีการเสนอเนื้อหา ลีลาในการเขียน สานวนภาษา

2.4.1.4 ความจริงแท้ของเอกสาร (Authenticity) ต้องสามารถพิสูจน์ได้ว่าเอกสารเป็นต้นฉบับไม่ใช่เอกสารที่ถูกคัดลอก ปลอมแปลงขึ้น โดยต้องมีการระบุได้ถึงเจตนา ผู้ที่มีอำนาจในการจัดทำเอกสารนั้น และเอกสารจะต้องสามารถตรวจสอบได้และมีการปกป้องการปลอมแปลงเอกสารเพื่อเป็นการยืนยันและสร้างความมั่นใจในความจริงแท้ของเอกสาร

2.4.1.5 ความสมบูรณ์ (Integrity) ต้องมีความสมบูรณ์ ไม่ขาดหาย หรือไม่ถูกเปลี่ยนแปลงแก้ไขในส่วนใดส่วนหนึ่งของเอกสาร หากมีการเปลี่ยนแปลงแก้ไข การเพิ่ม การลบจะต้องทำโดยผู้ที่มีอำนาจหรือผู้ที่รับผิดชอบเอกสารนั้น

2.4.1.6 ความน่าเชื่อถือ (Reliability) ต้องมีเนื้อหาที่แสดงถึงการดำเนินงานและกิจกรรมที่ถูกต้อง ชัดเจน ครบถ้วน และเป็นข้อเท็จจริงที่พิสูจน์ได้ สามารถนำไปใช้อ้างอิงในการดำเนินงานและกิจกรรมต่าง ๆ ได้

2.4.1.7 การใช้งาน (Usability) ต้องสามารถเรียกใช้งานได้ตลอดเวลาที่ต้องการ ดังนั้นเอกสารจะต้องจัดเก็บในที่ที่สามารถระบุที่จัดเก็บได้ สามารถค้นหา นำมาใช้งานได้อยู่ตลอดเวลา

2.4.2 หลักการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวกับการบันทึก

จากการศึกษาแนวความคิดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่มีหลักการห้ามมิให้บุคคลหนึ่งบุคคลใดนำข้อมูลส่วนบุคคลของผู้อื่นไปประมวลผลโดยไม่ได้รับอนุญาต หรือห้ามผู้ที่ได้รับอนุญาตให้ดำเนินการประมวลผลข้อมูลส่วนบุคคลดำเนินการที่อาจมีผลกระทบต่อสิทธิหรือเสรีภาพของเจ้าของข้อมูล ซึ่งหลักการดังกล่าวอาจเพียงพอในแง่ของทฤษฎี แต่ในทางปฏิบัติเพื่อให้เกิดการคุ้มครองข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพ จำเป็นต้องมีการตรวจสอบถึงการปฏิบัติตามหลักการ ดังนั้น การวางมาตรการเพื่อตรวจสอบถึงการปฏิบัติหน้าที่จึงเป็นส่วนสำคัญที่จะทำให้

มาตรการต่าง ๆ ที่กำหนดไว้สำหรับคุ้มครองข้อมูลส่วนบุคคลมีผลใช้บังคับได้อย่างมีประสิทธิภาพ[74]

บันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล(Records of Processing Activities) ถือเป็นมาตรการหนึ่งที่ใช้ควบคุม หรือตรวจสอบกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ซึ่งบันทึกจะเป็นหลักฐานที่แสดงให้เห็นถึงการปฏิบัติตามบทบัญญัติแห่งกฎหมาย อันจะส่งผลให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพมากขึ้น มาตรการดังกล่าวได้รับการยอมรับโดยนำไปบัญญัติไว้ในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ซึ่งปรากฏในส่วนของหลักการและเหตุผลข้อที่ 82 แห่ง GDPR ว่า “เพื่อที่จะพิสูจน์ถึงการปฏิบัติตามกฎหมายฉบับนี้ ผู้ควบคุมหรือผู้ประมวลผลข้อมูลมีหน้าที่จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผล และต้องให้ความร่วมมือกับหน่วยงานที่มีอำนาจกำกับดูแลให้สามารถตรวจสอบบันทึกดังกล่าวได้เมื่อมีการร้องขอ นอกจากนี้บันทึกยังทำหน้าที่ติดตามการดำเนินกิจกรรมการประมวลผลทั้งหลายด้วย”[75]

ข้อมูลส่วนบุคคลเป็นสิทธิอย่างหนึ่งในสิทธิความเป็นอยู่ส่วนตัว ด้วยการดำเนินชีวิตในปัจจุบัน ไม่ว่าจะเป็นการทำธุรกรรมทางการเงิน การดำเนินกิจกรรมต่าง ๆ ทางอินเตอร์เน็ต เช่น การซื้อหรือขายของออนไลน์ การจองตั๋วหรือที่พักในการท่องเที่ยว ย่อมต้องใช้ข้อมูลส่วนบุคคลเพื่อแสดงตัวตนและดำเนินกิจกรรมต่าง ๆ ต่อไป ซึ่งการให้ข้อมูลส่วนบุคคลแก่ผู้ประกอบธุรกิจต่าง ๆ แม้จะมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลคุ้มครองการประมวลผลข้อมูลเหล่านั้นแล้วก็ตาม แต่เจ้าของข้อมูลไม่อาจทราบได้เลยว่าข้อมูลส่วนบุคคลของตนถูกนำไปประมวลผลนอกวัตถุประสงค์หรือไม่ ดังนั้นการจัดทำและเก็บรักษาบันทึกกิจกรรมการประมวลผลจึงเป็นหลักฐานสำคัญที่จะ

---

[74] From *The Processing Records* (p.6), by Wolfgang, B. & Susanne, D., 2017, Copyright 2017 by Wolfgang, B. and Susanne, D. Retrieved form https://www.bitkom.org/sites/default/files/file/import/180529-LF-Verarbeitungsverzeichnis-ENG-online-final.pdf

[75] GDPR Whereas: (82) In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.

พิสูจน์ว่าข้อมูลส่วนบุคคลได้รับความคุ้มครองตามกฎหมาย และเพื่อที่จะสนับสนุนการตรวจสอบของเจ้าหน้าที่คุ้มครองข้อมูลและหน่วยงานที่มีอำนาจกำกับดูแลถึงการปฏิบัติตามกฎหมายของผู้ควบคุม และผู้ประมวลผลข้อมูล ดังนั้นการจัดทำและเก็บรักษาบันทึกกิจกรรมการประมวลผลจึงอยู่ภายใต้หลักการพื้นฐานดังต่อไปนี้

2.4.2.1 หลักความโปร่งใส (Transparency)

หลักความโปร่งใส เป็นหลักการพื้นฐานที่เน้นเรื่องของการประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการด้วยความโปร่งใสโดยผู้ควบคุม หรือผู้ประมวลผลข้อมูลจะต้องแจ้งชื่อและการติดต่อกับผู้ควบคุมหรือผู้ประมวลผลข้อมูล ตลอดจนวิธีดำเนินการประมวลผลให้ปรากฏอย่างชัดเจน เพื่อประโยชน์แก่เจ้าของข้อมูลส่วนบุคคลในการเข้าถึงผู้ควบคุมหรือผู้ประมวลผลข้อมูลในกรณีที่ต้องการใช้สิทธิตรวจสอบบันทึกกิจกรรมการประมวลผล ตลอดจนการใช้สิทธิร้องขอให้แก้ไข ลบ หรือทำลายข้อมูลส่วนบุคคลนั้น

2.4.2.2 หลักการจำกัดวัตถุประสงค์ (Purpose Limitation)

หลักความโปร่งใส เป็นหลักการพื้นฐานที่เน้นเรื่องของการประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการด้วยความโปร่งใสโดยผู้ควบคุม หรือผู้ประมวลผลข้อมูลจะต้องแจ้งชื่อและการติดต่อกับผู้ควบคุมหรือผู้ประมวลผลข้อมูล ตลอดจนวิธีดำเนินการประมวลผลให้ปรากฏอย่างชัดเจน เพื่อประโยชน์แก่เจ้าของข้อมูลส่วนบุคคลในการเข้าถึงผู้ควบคุมหรือผู้ประมวลผลข้อมูลในกรณีที่ต้องการใช้สิทธิตรวจสอบบันทึกกิจกรรมการประมวลผล ตลอดจนการใช้สิทธิร้องขอให้แก้ไข ลบ หรือทำลายข้อมูลส่วนบุคคลนั้น

2.4.2.3 หลักความรับผิดชอบ (Accountability)

หลักความรับผิดชอบกำหนดให้การจัดทำและบันทึกกิจกรรมการประมวลผลเป็นมาตรการทางเทคนิคและการจัดระเบียบองค์กรมาตรการหนึ่ง[76] ซึ่งกำหนดให้องค์กรใด ๆ ไม่ว่าจะมีฐานะเป็นผู้ควบคุม หรือผู้ประมวลผลข้อมูล มีหน้าที่จัดทำและเก็บรักษาบันทึก

[76] จาก Information Commissioner's Office, *อ้างแล้วเชิงอรรถที่ 64* (น.153).

กิจกรรมการประมวลผลต่าง ๆ ที่องค์กรได้ดำเนินการประมวลผลข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษร

2.4.3 ลักษณะของบันทึก

สำหรับลักษณะของบันทึกตาม GDPR ได้บัญญัติไว้ในมาตรา 30 ซึ่งมีหลักการและรายละเอียดเกี่ยวกับการจัดทำและเก็บรักษาบันทึกรายการไว้ดังต่อไปนี้

1) ผู้ควบคุมแต่ละคนรวมถึงตัวแทนของผู้ควบคุมมีหน้าที่ต้องเก็บรักษาบันทึกกิจกรรมการประมวลผลอันประกอบด้วยรายละเอียดดังต่อไปนี้[77]

1.1) ชื่อและรายละเอียดการติดต่อของผู้ควบคุมและให้รวมถึงผู้ควบคุมร่วม ตัวแทนของผู้ควบคุม และเจ้าหน้าที่คุ้มครองข้อมูลด้วย[78]

1.2) วัตถุประสงค์ของการประมวลผล[79]

1.3) คำอธิบายประเภทของเจ้าของข้อมูลและข้อมูลส่วนบุคคล[80]

1.4) ประเภทของผู้รับข้อมูลหรืออาจได้รับข้อมูลรวมถึงผู้รับข้อมูลที่อยู่ในประเทศนอกสหภาพยุโรปหรือองค์กรระหว่างประเทศ[81]

---

[77]GDPR Article 30(1) Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information.

[78] GDPR Article 30(1(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer.

[79]GDPR Article 30 (1)(b) the purposes of the processing.

[80]GDPR Article 30(1)(c) a description of the categories of data subjects and of the categories of personal data.

1.5) การป้องกันที่เหมาะสมในการโอนข้อมูลส่วนบุคคลไปยังประเทศนอกสหภาพยุโรปหรือองค์กรระหว่างประเทศรวมถึงการโอนข้อมูลตามอนุสองของมาตรา 49 วรรคหนึ่ง[82]

1.6) ระยะเวลาสำหรับทำลายข้อมูลแต่ละประเภท[83]

1.7) คำอธิบายเกี่ยวกับมาตรการทางเทคนิคและการรักษาความมั่นคงปลอดภัยตามมาตรา 32 วรรคหนึ่ง[84]

2) ผู้ประมวลผลข้อมูลแต่ละคนรวมถึงตัวแทนของผู้ประมวลผลข้อมูลมีหน้าที่ต้องเก็บรักษาบันทึกกิจกรรมการประมวลผลทุกประเภทซึ่งดำเนินการตามคำสั่งของผู้ควบคุมอันประกอบไปด้วยรายละเอียดดังต่อไปนี้[85]

2.1) ชื่อและรายละเอียดการติดต่อของผู้ประมวลผลข้อมูล และผู้ควบคุมแต่ละคนซึ่งผู้ประมวลผลข้อมูลกระทำตามคำสั่ง และให้รวมถึงตัวแทนของผู้ควบคุมหรือผู้ประมวลผลข้อมูลและเจ้าหน้าที่คุ้มครองข้อมูลด้วย[86]

---

[81] GDPR Article 30 (1)(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations.

[82] GDPR Article 30 (1)(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards.

[83] GDPR Article 5 (1)(f) where possible, the envisaged time limits for erasure of the different categories of data.

[84] GDPR Article 30 (1)(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

[85] GDPR Article 30(2) Each processor and where applicable the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing.

2.2) ประเภทของการประมวลผลที่ดำเนินการตามคำสั่งของผู้ควบคุมแต่ละคน[87]

2.3) การป้องกันที่เหมาะสมในการโอนข้อมูลส่วนบุคคลไปยังประเทศนอกสหภาพยุโปร หรือองค์กรระหว่างประเทศรวมถึงการโอนข้อมูลตามอนุสองของมาตรา 49 วรรคหนึ่ง[88]

2.4) คำอธิบายเกี่ยวกับมาตรการทางเทคนิคและการรักษาความมั่นคงปลอดภัยตามมาตรา 32 วรรคหนึ่ง[89]

3) การบันทึกข้อมูลตามวรรคหนึ่ง และวรรคสอง ให้ทำเป็นลายลักษณ์อักษณ์หรือจัดให้อยู่ในรูปแบบอิเล็กทรอนิกส์[90]

4) ผู้ควบคุมหรือผู้ประมวลผลข้อมูล และรวมถึงตัวแทนของผู้ควบคุมหรือผู้ประมวลผลข้อมูลจะต้องทำบันทึกที่สามารถแสดงต่อหน่วยงานที่มีอำนาจกำหนดดูแลได้เมื่อมีการร้องขอ[91]

---

[86] GDPR Article 30 (2)(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer.

[87] GDPR Article 30 (2) (b) the categories of processing carried out on behalf of each controller.

[88] GDPR Article 30 (2)(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards.

[89] GDPR Article 30 (2) (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

[90] GDPR Article 30 3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

5) หน้าที่ตามที่บัญญัติไว้ในวรรคหนึ่งและวรรคสองไม่ใช้บังคับแก่วิสาหกิจขนาดกลางและขนาดย่อม หรือองค์กรที่มีพนักงานน้อยกว่า 250 คน เว้นแต่มีการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่ประมวลผลข้อมูลส่วนบุคคลเป็นครั้งคราว หรือเป็นการประมวลผลข้อมูลส่วนบุคคลชนิดพิเศษตามมาตรา 9 (1) หรือเป็นข้อมูลส่วนบุคคลที่เกี่ยวกับประวัติอาชญากรรม ตามมาตรา 10[92]

ตารางที่ 2.1 รูปแบบการบันทึกรายการกิจกรรมการประมวลผล (Records of Processing Activities) ที่เกี่ยวกับรายละเอียดของผู้ควบคุมมีดังนี้

ชื่อ	Localdirect Limited
ผู้ติดต่อ	Stuart Frank
ตำแหน่ง	กรรมการผู้จัดการ
เมือง	Penrith
ประเทศ	United Kingdom
เบอร์โทรศัพท์	0845 838 2019
อีเมล	stuart@wishloop.com
URL	http://wishloop.com

ที่มา: Stuart, 2018, น. 1

[91] GDPR Article 30 4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

[92] GDPR Article 30 5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

ตารางที่ 2.2 รูปแบบการบันทึกรายการกิจกรรมการประมวลผลที่เกี่ยวกับการลงทะเบียนลูกค้า เช่น ผ่านทางเว็บแบบฟอร์ม

เปลี่ยนแปลงครั้งล่าสุดเมื่อวันที่	2018-5-16
คำอธิบายเกี่ยวกับกิจกรรมการประมวลผล	
การพัฒนาแผนกที่รับผิดชอบ	Stuart Frank, stuart@wishloop.com
วัตถุประสงค์ของกิจกรรมการประมวลผล	การประมวลผลข้อมูลเพื่อวัตถุประสงค์ในการลงทะเบียนผู้ใช้กับบริการซอฟต์แวร์ของเราในฐานะผู้ทดสอบสามคนหรือลูกค้าที่จ่าย เราใช้เว็บฟอร์มเพื่อลงทะเบียนผู้ใช้ของเราระบบซอฟต์แวร์ เราใช้ข้อมูลผู้ใช้นี้ในระบบภายใน (ตัวอย่างเช่นการติดตามการซื้อและประวัติบัญชี) และแบ่งปันข้อมูลด้วยบุคคลที่สามที่อนุญาตให้มีการส่งมอบการฝึกอบรม บทแนะนำซอฟต์แวร์และการติดตามการตลาด
ฐานของกฎหมายของกิจกรรมการประมวลผล	ความยินยอม ความจำเป็นตามสัญญา
ประเภทเจ้าของข้อมูลในกิจกรรมการประมวลผล	บุคคลที่สนใจ ลูกค้า
ประเภทข้อมูลในการประมวลผล	ชื่อ ผู้ติดต่อ
กิจกรรม	ที่อยู่ ที่อยู่อีเมล เบอร์โทรศัพท์ ประวัติการสั่งซื้อ ประวัติการใช้สื่อออนไลน์

ที่มา: Stuart, 2018, น. 11-12

ตารางที่ 2.3 รูปแบบการบันทึกรายการกิจกรรมการประมวลผลที่เกี่ยวกับการใช้ข้อมูลลูกค้าเพื่อการตลาด

เปลี่ยนแปลงครั้งล่าสุดเมื่อวันที่ (Last Changed On)	2018-5-16
คำอธิบายเกี่ยวกับกิจกรรมการประมวลผล	
แผนกที่รับผิดชอบ	การตลาด Stuart Frank, stuart@wishloop.com
วัตถุประสงค์ของกิจกรรมการประมวลผล	การประมวลผลข้อมูลและการแบ่งประเภทผู้ใช้ยังใช้สำหรับการปรับปรุงกลุ่มเป้าหมายและผู้ใช้ผลิตภัณฑ์และบริการใหม่ ,ข่าวอุตสาหกรรม เหตุการณ์และข้อเสนอ เราใช้ระบบการสื่อสารภายในระหว่างกันและกิจกรรมสำหรับอัพเดทกลุ่มเป้าหมายและผู้ใช้ผลิตภัณฑ์ใหม่และบริการข่าวอุตสาหกรรม เหตุการณ์และข้อเสนอ ในกรณีที่มีการนำเสนอทางอีเมลเราอาจมีความสัมพันธ์กับพันธมิตรกับเจ้าของผลิตภัณฑ์ / บริการและอาจได้รับรางวัลสำหรับรายได้ที่เราแนะนำ เราจะแนะนำผลิตภัณฑ์ บริการที่เราได้ตรวจสอบอย่างรอบคอบเท่านั้น เราอาจใช้โฆษณาที่มีค่าใช้จ่ายเพื่อสนับสนุนการส่งเสริมภายในหรือภายนอก
ฐานกฎหมายของกิจกรรมการประมวลผล	ฐานความยินยอม ความจำเป็นตามสัญญา
ประเภทเจ้าของข้อมูลในกิจกรรมการประมวลผล	บุคคลที่สนใจ ลูกค้า

ที่มา: Stuart, 2018, น. 17-19

2.4.4 หน้าที่และข้อยกเว้นในการจัดทำบันทึก

ใน GDPR มาตรา 30 ได้มีการกำหนดยกเว้นหน้าที่ในการจัดทำบันทึกโดยจะไม่ใช้บังคับกับกิจการหรือองค์กรที่มีจำนวนการจ้างงานน้อยกว่า 250 คน เว้นแต่มีการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่ประมวลผลข้อมูลส่วนบุคคลเป็นครั้งคราว หรือเป็นการประมวลผลข้อมูลส่วนบุคคลชนิดพิเศษตามมาตรา 9 (1) หรือเป็นข้อมูลส่วนบุคคลที่เกี่ยวกับประวัติอาชญากรรม ตามมาตรา 10[93]

2.4.4.1 วิสาหกิจขนาดกลางและขนาดย่อม

ในเรื่องของข้อยกเว้นตาม GDPR มาตรา 30 ที่วิสาหกิจขนาดกลางและขนาดย่อมได้รับยกเว้นไม่ต้องจัดทำบันทึกกิจกรรมการประมวลผลนั้น ปรากฏคำปรารภ(Recital) ของ GDPR ข้อที่ 13 ซึ่งอ้างถึงข้อ 2 ของภาคผนวกของคำแนะนำของคณะกรรมการแห่งประชาคมยุโรป (Commission of the European Community)เกี่ยวกับคำนิยามของกิจการขนาดย่อม (Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises) เพื่อให้เป็นมาตราฐานของประชาคมยุโรป ดังนี้

1) ประเภทของวิสาหกิจขนาดกลางและขนาดย่อม (SMEs) ประกอบไปด้วยวิสาหกิจที่มีพนักงานลูกจ้างน้อยกว่า 250 คน และมีผลประกอบการประจำปีไม่เกิน เกิน 50 ล้านยูโรและหรืองบดุลประจำปีรวมกันไม่เกิน 43 ล้านยูโร[94]

---

[93] GDPR Article 30 5. “The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.”

[94] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises Article2 1.The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which

2) ในกลุ่ม SME องค์กรขนาดเล็กนั้นถูกกำหนดให้เป็นองค์กรที่มีพนักงานน้อยกว่า 50 คนและผลประกอบการประจำปีและ หรืองบดุลรวมประจำปีไม่เกิน 10 ล้านยูโร[95]

3) ในหมวด SME นั้นองค์กรขนาดย่อมถูกกำหนดให้เป็นองค์กรที่มีพนักงานน้อยกว่า 10 คนและผลประกอบการประจำปีและ หรืองบดุลรวมประจำปีไม่เกิน 2 ล้านยูโร[96]

2.4.4.2 ความเสี่ยงที่มีผลต่อสิทธิและเสรีภาพของเจ้าของข้อมูล

จากคำปรารภ (Recital) ของ GDPR ที่ 75[97] ที่เกี่ยวกับความเสี่ยงต่อเสรีภาพของเจ้าของข้อมูล คือความเสี่ยงต่อสิทธิและเสรีภาพของบุคคล เป็นผลมาจากการประมวลผลข้อมูล

---

have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million.

[95] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises Article2 2.Within the SME category, a small enterprise is defined as an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million.

[96] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises Article2 3.Within the SME category, a microenterprise is defined as an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million.

[97] Recital of GDPR (75) “The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their

ส่วนบุคคล โดยเฉพาะการใช้ข้อมูลส่วนบุคคลที่อาจทำให้มีผลเป็นการเลือกปฏิบัติ ทำให้เสี่ยงต่อการถูกขโมยข้อมูล หรือนำข้อมูลส่วนบุคคลไปหลอกลวงบุคคลอื่น ทำให้บุคคลอื่นเสียหายต่อชื่อเสียง ถูกเปิดเผยความลับที่ควรได้รับการคุ้มครอง มีการแปลงข้อมูลแฝงโดยไม่ได้รับอนุญาต ตลอดจนทำให้เกิดความเสียเปรียบทางสังคมหรือเศรษฐกิจ จนทำให้เจ้าของข้อมูลอาจจำกัดสิทธิเสรีภาพ หรือถูกขัดขวางมิให้เข้าถึงข้อมูลของตนอันเป็นข้อมูลเกี่ยวกับเชื้อชาติ หรือชาติกำเนิด (ethnic origin) การแสดงความเห็นทางการเมือง ศาสนา ปรัชญาความเชื่อ ความเป็นสมาชิกสหภาพแรงงาน ข้อมูลเกี่ยวกับพันธุกรรม สุขภาพ ประสบการณ์ทางเพศ(Sex Life) ตลอดจนประวัติอาชญากรรม หรือเกี่ยวกับมาตรการความปลอดภัยของบุคคล ซึ่งจะถูกนำมาประเมินผล เพื่อวิเคราะห์ หรือคาดการณ์แนวโน้มเกี่ยวกับประสิทธิภาพในการทำงาน สถานการณ์ทางเศรษฐกิจ สุขภาพ ความชอบหรือความสนใจ ความน่าเชื่อถือ หรือพฤติกรรม ตำแหน่งที่อยู่ หรือ การเคลื่อนไหว เพื่อที่จะสร้างหรือใช้แฟ้มข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลในกลุ่มที่เปราะบาง โดยเฉพาะเด็กหรือการประมวลผลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลจำนวนมากและมีผลต่อบุคคลจำนวนมากซึ่งเป็นเจ้าของข้อมูล

2.4.4.3 กิจการที่ไม่ใช่การประมวลผลข้อมูลส่วนบุคคลเป็นครั้งคราว

จากที่ได้กล่าวมาแล้วในหัวข้อที่เกี่ยวกับข้อยกเว้นไม่ต้องจัดทำบันทึกรายการ เพื่อให้เกิดความเข้าใจเกี่ยวกับความหมายของกิจการที่ประมวลผลข้อมูลส่วนบุคคลเป็นครั้งคราว จึงขอยกตัวอย่างการประมวลผลที่ไม่เป็นครั้งคราว โดยมีตัวอย่างดังนี้

---

personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

บริษัทประกันภัยที่มีพนักงาน 100 คนมีการประมวลผลข้อมูลส่วนบุคคลเป็นประจำที่เกี่ยวกับการขายและทรัพยากรบุคคล แม้ว่าบริษัทจะมีพนักงานน้อยกว่า250คนก็ตามแต่บริษัทยังมีหน้าที่ต้องบันทึกกิจกรรมการประมวลผล(Processing Activities) เพราะบริษัทไม่ได้ประมวลผลที่เป็นครั้งคราว อย่างไรก็ตามในกรณีที่บริษัทมีการสำรวจความพึงพอใจของพนักงานภายในบริษัทโดยไม่ได้ทำกิจกรรมการประมวลผลดังกล่าวบ่อยครั้งมากนักกรณีแบบนี้บริษัทก็ไม่จำต้องทำบันทึกกิจกรรมการประมวลผล[98]

2.4.4.4 ข้อมูลส่วนบุคคลชนิดพิเศษ

ตาม GDPR มาตรา 30 แม้ผู้ควบคุมเป็นวิสาหกิจขนาดกลางและขนาดย่อมหรือ เป็นองค์กรที่มีพนักงานน้อยกว่า 250 คนก็ตาม ถ้ามีการประมวลผลข้อมูลส่วนบุคคลชนิดพิเศษตามมาตรา 9(1) ผู้ควบคุมก็มีหน้าที่ต้องจัดทำบันทึกรายการ ซึ่งข้อมูลชนิดพิเศษตามมาตรา 9(1) มีรายละเอียดดังนี้

การประมวลผลข้อมูลส่วนบุคคลที่เปิดเผย เชื้อชาติหรือชาติพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนาหรือปรัชญา หรือ สมาชิกสหภาพแรงงานและการประมวลผลข้อมูลทางพันธุกรรม ข้อมูลไบโอเมตริกซ์ (Biometric) เพื่อวัตถุประสงค์ในการระบุตัวบุคคล ข้อมูลเกี่ยวกับสุขภาพหรือข้อมูลที่เกี่ยวข้องกับ ชีวิตทางเพศของบุคคลธรรมดาหรือรสนิยมทางเพศจะต้องห้าม[99]

---

[98] จาก *Who needs to document their processing activities?*, โดย Information Commissioner's Office, 2018. สืบค้นจาก https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/who-needs-to-document-their-processing-activities/

[99] GDPR Article 9 Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2.4.4.5 ข้อมูลส่วนบุคคลที่เกี่ยวกับประวัติอาชญากรรม

ข้อมูลส่วนบุคคลที่เกี่ยวกับประวัตอาชญากรรม ตาม GDPR มาตรา10 มีรายละเอียดดังต่อไปนี้

การประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องกับประวัติอาชญากรรมหรือมาตรการรักษาความปลอดภัยที่เกี่ยวข้องตามมาตรา 6 (1) จะดำเนินการภายใต้การควบคุมของเจ้าหน้าที่ผู้มีอำนาจหรือเมื่อการประมวลผลได้รับอนุญาตจากกฎหมายของสหภาพหรือรัฐสมาชิกสิทธิและเสรีภาพของเจ้าของข้อมูล การลงทะเบียนที่ครอบคลุมเกี่ยวกับความผิดทางอาญาใด ๆ จะถูกเก็บไว้ภายใต้การควบคุมของเจ้าหน้าที่ผู้มีอำนาจเท่านั้น[100]

จากการศึกษาถึงแนวความคิดและหลักการคุ้มครองข้อมูลส่วนบุคคล ลักษณะของผู้ควบคุมซึ่งมีหน้าที่จัดทำบันทึก ตลอดจนศึกษาถึงแนวความคิดและหลักการของบันทึกที่มีผลกระทบอันเกิดจากหน้าที่การจัดทำบันทึกจนต้องมีการยกเว้นหน้าที่ในบางกรณีแล้ว พบว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นกฎหมายที่มีความสำคัญอย่างมากสำหรับผู้ที่เป็นเจ้าของข้อมูลและผู้ควบคุมข้อมูลเพราะกฎหมายฉบับนี้มีวัตถุประสงค์เพื่อป้องกันการละเมิดสิทธิของเจ้าของข้อมูลและในขณะเดียวกันผู้ควบคุมข้อมูลซึ่งเป็นผู้ประกอบการต้องปฏิบัติตามกฎหมายอย่างเคร่งครัดและถูกต้องเพื่อให้การคุ้มครองสิทธิของเจ้าของข้อมูลสมดังเจตนารมณ์รมของกฎหมาย ซึ่งประเทศหลายประเทศให้ความสำคัญเกี่ยวกับข้อมูลส่วนบุคคลโดยมีการนำหลักการคุ้มรองตามกรอบองค์การระหว่างประเทศ เช่น หลักการคุ้มครองข้อมูลส่วนบุคคลของ UN หลักการคุ้มครองข้อมูลส่วนบุคคลของ OECD หลักการคุ้มครองข้อมูลส่วนบุคคลของ APEC และ หลักการคุ้มครองข้อมูลส่วนบุคคลของ EU มาเป็นแนวทางในการร่างกฎหมาย ซึ่งหลักการคุ้มครองของแต่ละองค์กรมีความคล้ายคลึงกัน เช่น การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะกระทำได้

---

[100]GDPR Article 10 “Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.”

ต่อเมื่อมีการขอความยินยอมก่อนหรือมีความจำเป็นเพื่อให้บรรลุวัตถุประสงค์ตามปกติของสัญญา หรือเป็นการปฏิบัติตามกฎหมาย ซึ่งอาจเรียกได้ว่าเป็นฐานของกฎหมาย (Lawful Basis) ที่ทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เป็นไปโดยชอบด้วยกฎหมาย และจะต้องเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็นภายใต้กรอบระยะเวลาที่เหมาะสม นอกจากนี้ผู้เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะต้องจัดทำบันทึกเกี่ยวกับกิจกรรมต่าง ๆ ที่เกิดขึ้นกับข้อมูลส่วนบุคคลไว้เป็นหลักฐานเพื่อใช้พิสูจน์หรือแสดงต่อเจ้าหน้าที่ที่รัฐตั้งขึ้นมาเพื่อตรวจสอบเมื่อเกิดปัญหาเกี่ยวกับข้อมูลดังกล่าวเช่น เกิดข้อมูลที่รั่วไหล หรือเกิดความผิดพลาดของข้อมูล แม้กฎหมายจะมีข้อยกเว้นให้กับผู้ควบคุมที่ไม่ต้องจัดทำบันทึกเอาไว้ก็ตามแต่วัตถุประสงค์ของข้อยกเว้นดังกล่าวก็เพื่อที่จะให้ผู้ควบคุมที่มีกิจการขนาดเล็กสามารถแข็งขันทางการค้ากับกิจการที่มีขนาดใหญ่ได้กฎหมายจึงมีการยกเว้นให้กับผู้ประกอบกิจการขนาดเล็กไม่ต้องจัดทำบันทึกรายการดังกล่าวแต่อย่างไรก็ดีก็ยังคงมีข้อยกเว้นอยู่บางประการตรงที่ว่าแม้ผู้ควบคุมจะเป็นกิจการขนาดเล็กแต่ถ้าเป็นการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลที่มีความเสี่ยงความเสี่ยงที่มีผลต่อสิทธิและเสรีภาพของเจ้าของข้อมูลหรือกิจการที่ไม่ใช่การประมวลผลข้อมูลส่วนบุคคลเป็นครั้งคราวหรือข้อมูลส่วนบุคคลชนิดพิเศษตามที่กฎหมายกำหนดไว้ผู้ควบคุมข้อมูลก็ยังมีหน้าที่ในการจัดทำบันทึกรายการโดยไม่ได้รับประโยชน์จากข้อยกเว้นดังกล่าวซึ่งในส่วนของบทถัดไปผู้วิจัยจะทำการศึกษากฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวกับการบันทึกรายการตามกฎหมายของประเทศไทยและต่างประเทศเพื่อเป็นการเพิ่มองค์ความรู้ของการศึกษาวิจัยฉบับนี้ให้สามารถปรับใช้กับสถานการณ์ของประเทศไทยได้อย่างเหมาะสม

บทที่ 3

กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวกับการบันทึกรายการตามกฎหมายของประเทศไทยและต่างประเทศ

เนื่องจากการคุ้มครองข้อมูลส่วนบุคคลยังเป็นองค์ความรู้ที่เพิ่งเริ่มต้นพัฒนาขึ้นในสังคมไทย ขณะที่ในต่างประเทศได้ผ่านประสบการณ์บังคับใช้กฎหมายและมาตรการต่าง ๆ เพื่อปกป้องคุ้มครองข้อมูลส่วนบุคคลมายาวนานกว่า[101] การศึกษามาตรการคุ้มครองข้อมูลส่วนบุคคลในประเทศที่มีพัฒนาการมาก่อน จะทำให้สามารถทำการวิเคราะห์ และสังเคราะห์ข้อเสนอแนะเพื่อปรับใช้กับสถานการณ์ของประเทศไทยได้อย่างเหมาะสม ดังนั้นในส่วนของบทนี้ ผู้วิจัยจึงได้ทำการศึกษากฎหมายที่เกี่ยวข้องกับหลักการคุ้มครองข้อมูลส่วนบุคคล และหลักการจัดทำบันทึกรายการ โดยจะทำการศึกษากฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย สหราชอาณาจักร สหรัฐอเมริกา และ สาธารณะรัฐสิงค์โปร์ โดยมีรายละเอียดดังต่อไปนี้

3.1 ประเทศไทย

ปัจจุบันประเทศไทยมีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (Personal Data Protection Act B.E.2562 หรือ PDPA) โดยมีการนำเอาหลักการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปที่เรียกว่า GDPR มาเป็นแม่แบบในการร่างกฎหมาย เพื่อให้เกิดความเข้าใจเกี่ยวกับหลักการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยมากยิ่งขึ้นจึงต้องศึกษาความเป็นมาและกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยว่ามีหลักในการคุ้มครองข้อมูลส่วนบุคคลเหมือนหรือแตกต่างจากประเทศอื่นอย่างไรบ้าง โดยจะทำการศึกษาหลักการคุ้มครองและหลักการจัดทำบันทึกรายการของประเทศไทยดังนี้

---

[101] จาก *การคุ้มครองข้อมูลส่วนบุคคล: ประสบการณ์เยอรมัน* (น.2), โดย นคร เสรีรักษ์, 2556. สืบค้นจาก http://www.oic.go.th/FILEROOM/CABOICFORM05/DRAWER02/ GENERAL /DATA0001/00001907.PDF

3.1.1 หลักการคุ้มครองข้อมูลส่วนบุคคล

ประเทศไทยให้ความสำคัญกับสิทธิในความเป็นอยู่ส่วนตัวอันเกี่ยวกับข้อมูลส่วนบุคคลในฐานะที่เป็นส่วนหนึ่งของสิทธิมนุษยชนโดยบัญญัติไว้ในรัฐธรรมนูญพุทธศักราช 2560 ในหมวด 3 สิทธิและเสรีภาพของปวงชนชาวไทยในมาตรา 32 กำหนดให้การนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่จะได้รับยกเว้นตามกฎหมาย[102] กล่าวคือเป็นการห้ามนำข้อมูลส่วนบุคคลไปใช้ประโยชน์โดยเด็ดขาด เว้นแต่มีกฎหมายบัญญัติไว้โดยเฉพาะยกเว้นให้นำข้อมูลส่วนบุคคลของบุคคลอื่นไปใช้ได้ ถือเป็นบทบัญญัติคุ้มครองสิทธิความเป็นส่วนตัว รวมถึงข้อมูลส่วนบุคคลมิให้ถูกละเมิดตลอดทั้งเพื่อกำกับและควบคุมรัฐในเรื่องการเปิดเผยข้อมูลของปัจเจกบุคคลต่อสาธารณะ[103] จากข้อยกเว้นดังกล่าวจึงทำให้ต้องมีการบัญญัติ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลขึ้นมาเพื่อให้เป็นไปตามที่รัฐธรรมนูญกำหนดเอาไว้ และสำหรับการเข้าถึงข้อมูลข่าวสารสาธารณะของรัฐมีการบัญญัติไว้ในรัฐธรรมนูญมาตรา 41(1) กำหนดให้บุคคลและชุมชนย่อมมีสิทธิได้รับทราบและเข้าถึงข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานรัฐตามที่กฎหมายบัญญัติ[104] กล่าวคือ เป็นการกำหนดสิทธิของบุคคลและชุมชนในการเข้าถึงข้อมูลหรือข่าวสารสาธารณะของรัฐและการเข้าถึงข้อมูลข่าวสารสาธารณะนั้นทำให้เกิดความโปร่งใสในการบริหารงานของรัฐและง่ายต่อการตรวจสอบ โดยมีการมุ่งเน้นการคุ้มครองในส่วนที่เกี่ยวกับข้อมูลสาธารณะที่ประชาชนมีสิทธิเข้าถึงได้ซึ่งแตกต่างจาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลที่มุ่งเน้นการให้ความคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูลเป็นหลัก โดยรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ได้แยกสิทธิต่าง ๆ ดังกล่าวให้มีความเหมาะสม

---

[102] จาก รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 มาตรา 32 “บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ”

[103] จาก สำนักงานเลขาธิการสภาผู้แทนราษฎร,.*อ้างแล้วเชิงอรรถที่ 34* (น.47).

[104] จาก รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 มาตรา 41(1) บุคคลและชุมชนย่อมีสิทธิ “(1) ได้รับทราบและเข้าถึงข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐตามที่กฎหมายบัญญัติ…”

ชัดเจนมากยิ่งขึ้น เพื่อประโยชน์ในการบัญญัติกฎหมายลำดับรอง[105] นอกจากนี้สิทธิในการรับรู้ข่าวสารของประชาชนมีการบัญญัติไว้ใน พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ.2540 ซึ่งหลักการในรัฐธรรมนูญและในพระราชบัญญัติข้อมูลข่าวสารของทางราชการถือการเปิดเผยเป็นหลักและความลับหรือการปกปิดเป็นข้อยกเว้น[106]

แต่อย่างไรก็ดีสิทธิรับรู้ข้อมูลข่าวสารสาธารณะตามรัฐธรรมนูญมาตรา 41(1) และสิทธิการเข้าถึงข้อมูลข่าวสารของราชการตาม พระราชบัญญัติข้อมูลข่าวสารของทางราชการฯ นั้นมีข้อแตกต่างกันบางประการคือ รัฐธรรมนูญมุ่งคุ้มครองสิทธิรับรู้ข้อมูลข่าวสารสาธารณะ ส่วนพระราชบัญญัติข้อมูลข่าวสารของทางราชการขยายความคุ้มครองรวมไปถึงข้อมูลข่าวสารในความครอบครองหรือในความดูแลของหน่วยงานรัฐโดยไม่จำกัดว่าข้อมูลข่าวสารนั้นจะเป็นข้อมูลข่าวสารสาธารณะหรือไม่[107]

ในยุคเริ่มแรกของการให้ความคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย ประเทศไทยมุ่งเน้นไปที่การควบคุมข้อมูลที่อยู่ในความครอบครองของรัฐ เพราะเป็นที่ทราบดีว่าหน่วยงานของรัฐมีอำนาจเข้าถึงข้อมูลข่าวสารได้อย่างกว้างขวาง โดยกฎหมายฉบับแรกที่ออกมาเพื่อควบคุมข้อมูลที่อยู่ในความครอบครองของรัฐ คือ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มีหลักการสำคัญอยู่สองประการ คือ หลักการแรกการรับรองสิทธิของประชาชนในการเข้าถึงข้อมูลข่าวสาร(Access to Information)ที่อยู่ในความครอบครองของหน่วยงานของรัฐโดยถือว่าข้อมูลส่วนใหญ่ต้องสามารถเปิดเผยต่อสาธารณะโดยมีข้อยกเว้นเป็นส่วนน้อยเท่านั้นที่หน่วยงานของรัฐอาจมีคำสั่งมิให้เปิดเผย เช่น ข้อมูลข่าวสารของทางราชการที่อาจก่อให้เกิดความเสียหายต่อสถาบันพระมหากษัตริย์ ข้อมูลซึ่งการเปิดเผยจะเกิดความเสียหายต่อความมั่นคงของประเทศ ความสัมพันธ์ระหว่างประเทศ เมื่อกฎหมายรับรองสิทธิของประชาชนในการเข้าถึงข้อมูลข่าวสารที่อยู่ในครอบครองของหน่วยงานของรัฐเอาไว้อย่างชัดเจนแล้วดังนั้นหน่วยงานของรัฐจึงมีหน้าที่ที่ต้องจัดทำและให้บริการข้อมูลข่าวสารที่อยู่ในความครอบครองแก่สาธารณะ[108] สำหรับหลักการที่สองคือการคุ้มครองความเป็นส่วนตัวในข้อมูลส่วนบุคคลของประชาชนหากหน่วยงานของรัฐจะเปิดเผย

---

[105] จาก สำนักงานเลขาธิการสภาผู้แทนราษฎร, *อ้างแล้วเชิงอรรถที่ 34* (น.60).

[106] จาก นคร เสรีรักษ์, *อ้างแล้วเชิงอรรถที่ 32* (น.113).

[107] จาก นคร เสรีรักษ์, *อ้างแล้วเชิงอรรถที่ 32* (น.115).

[108] จาก นคร เสรีรักษ์, *อ้างแล้วเชิงอรรถที่ 32* (น.109-110).

ข้อมูลส่วนบุคคลที่หน่วยงานของตนเก็บรักษาอยู่ ไม่ว่าจะเป็นการเปิดเผยต่อหน่วยงานราชการอื่น ๆ หรือต่อบุคคลอื่น ๆ จะต้องได้รับความยินยอมจากเจ้าของข้อมูล เว้นแต่ กรณีที่กฎหมายยกเว้นให้ อย่างไรก็ตามยังคงปรากฏให้เห็นอยู่ทั่วไปว่าข้อมูลส่วนบุคคลของประชาชนที่หน่วยงานของรัฐมีหน้าที่ต้องควบคุมดูแลและคุ้มครองอย่างดีนั้นถูกเปิดเผยและนำไปใช้ประโยชน์กันอยู่บ่อยครั้งโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลซึ่ง ปัญหาการล่วงละเมิดข้อมูลส่วนบุคคลเกิดขึ้นเป็นจำนวนมากโดยเฉพาะการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ เปิดเผย หรือเผยแพร่จนทำให้เกิดความเสียหาย การบังคับใช้ พระราชบัญญัติข้อมูลข่าวสารของราชการนั้นไม่เพียงพอเนื่องจากพระราชบัญญัติข้อมูลข่าวสารของทางราชการใช้บังคับเฉพาะในหน่วยงานของรัฐเท่านั้น ไม่ครอบคลุมถึงข้อมูลส่วนบุคคลที่อยู่ในภาคเอกชนที่มีปริมาณข้อมูลที่จัดเก็บไม่น้อยกว่าข้อมูลในภาครัฐ เช่น ข้อมูลในธนาคารพาณิชย์ ข้อมูลในโรงพยาบาลเอกชน ข้อมูลพนักงานลูกจ้างในบริษัทและหน่วยงานองค์กรในภาคเอกชนต่าง ๆ ข้อมูลของลูกค้า ข้อมูลของสมาชิก กิจกรรมทางธุรกิจ ข้อมูลของผู้สมัครสมาชิกบัตรเครดิต บัตรเดบิต และบัตรสมาชิกต่าง ๆ เช่น สมาชิกร้านอาหาร สมาชิกโรงแรม สมาชิกสถานที่ออกกำลังกาย[109]

ดังนั้นจะเห็นได้ว่าการคุ้มครองข้อมูลส่วนบุคคลภายใต้พระราชบัญญัติข้อมูลข่าวสารของทางราชการไม่คุ้มครองถึงระบบการจัดเก็บและการใช้ข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานภาคเอกชน[110]

นอกจากนี้ยังให้ความคุ้มครองข้อมูลส่วนบุคคลไว้ในกฎหมายเฉพาะฉบับอื่นอีกมากมาย เช่น พระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 ฯลฯ จนกระทั่งมีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act B.E.2562 หรือ PDPA) เมื่อวันที่27 พฤษภาคม พ.ศ. 2562 เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแรกของประเทศไทย

---

[109] จาก *การคุ้มครองข้อมูลส่วนบุคคลข้อเสนอสำหรับประเทศไทย* (น. 23-25), โดย นคร เสรีรักษ์, 2558, กรุงเทพฯ: พี.เพรส. ลิขสิทธิ์ 2558 โดย นคร เสรีรักษ์.

[110] จาก นคร เสรีรักษ์ *อ้างแล้วเชิงอรรถที่ 32* (น.253).

ในการร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลนอกจากจะมีวัตถุประสงค์เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไปแล้ว ยังมีวัตถุประสงค์เพื่อให้ได้รับการยอมรับจากสหภาพยุโรปและป้องกันปัญหาทางการค้าที่เกิดจากการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ดังนั้นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยจึงได้รับอิทธิพลทางความคิดในการให้ความคุ้มครองข้อมูลส่วนบุคคลมาจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ซึ่งจะเห็นได้จากบทบัญญัติต่าง ๆ ของ PDPA ที่มีหลักการคล้าย ๆ กับ GDPR จนอาจกล่าวได้ว่ากฎหมายคุ้มครองข้อมูลของไทยร่างขึ้นโดยมี GDPR เป็นกฎหมายแม่แบบ (Model Laws) ในเบื้องต้นเพื่อเป็นการขจัดปัญหาในเรื่องของบทบัญญัติเกี่ยวกับข้อมูลส่วนบุคคลที่มีผลบังคับใช้อยู่ในกฎหมายอื่น ๆ PDPA จึงกำหนดให้กฎหมายใดที่มีบทบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลไว้โดยเฉพาะ ยังคงต้องบังคับตาม PDPA ในเรื่องที่เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และเกี่ยวกับสิทธิของเจ้าของข้อมูล รวมทั้งบทกำหนดโทษที่เกี่ยวข้องไม่ว่าจะซ้ำกับบทบัญญัติแห่งกฎหมายว่าด้วยการนั้นหรือไม่ก็ตาม และถ้ากฎหมายนั้นมีบทบัญญัติให้อำนาจแก่เจ้าหน้าที่ออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลได้ แต่ไม่เพียงพอเท่ากับอำนาจของคณะกรรมการผู้เชี่ยวชาญตาม PDPA และเจ้าหน้าที่ผู้มีอำนาจตามกฎหมายอื่นร้องขอต่อคณะกรรมการผู้เชี่ยวชาญหรือเจ้าของข้อมูลผู้เสียหายยื่นคำร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ ก็ให้นำบทบัญญัติเกี่ยวกับการร้องเรียน บทบัญญัติที่ให้อำนาจแก่คณะกรรมการผู้เชี่ยวชาญออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูล และบทบัญญัติเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่รวมทั้งบทกำหนดโทษที่เกี่ยวข้องตามที่บัญญัติไว้ใน PDPA มาใช้บังคับ[111]

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นับเป็นกฎหมายฉบับแรกของประเทศไทยที่ให้ความคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป และมีผลใช้บังคับในทุกภาคส่วนไม่ว่าจะเป็นภาครัฐ หรือภาคเอกชน ถึงกระนั้นก็ยังมีบทบัญญัติยกเว้นไม่ใช้บังคับแก่การเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อกิจกรรมในครอบครัวของบุคคลนั้น (Household Activities) หรือการดำเนินการของหน่วยงานรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ (National Security) หรือการดำเนินกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นประโยชน์สาธารณะ หรือการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ

[111] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 3

หรือการพิจารณาพิพากษาคดีของศาล หรือการดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต[112]

สำหรับการคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีหลักการที่สำคัญดังต่อไปนี้

1) หลักการจำกัดวัตถุประสงค์ (The Purpose Limitation Principle) กำหนดให้ผู้ควบคุมต้องทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลไว้ก่อนหรือในขณะที่เก็บรวบรวม[113] ตลอดจนบุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคลมาจากการเปิดเผยของผู้ควบคุมจะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมในการขอรับข้อมูลส่วนบุคคลนั้น[114] โดยเฉพาะอย่างยิ่งในการขอความยินยอมจากเจ้าของข้อมูล ผู้ควบคุมต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลด้วยภาษาที่อ่านง่าย และไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลเข้าใจผิดในวัตถุประสงค์[115]

2) หลักคุณภาพและความได้สัดส่วนของข้อมูล (The Data Quality and Proportionality Principle) ในเรื่องคุณภาพของข้อมูลนั้นได้กำหนดมาตรฐานไว้ในมาตรา 35 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้บัญญัติไว้ว่า “ผู้ควบคุมข้อมูลส่วนต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้องเป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด” ตามบทบัญญัติดังกล่าวมีลักษณะคล้ายกับหลักความถูกต้องของข้อมูล (Accuracy) ของ GDPR ที่กำหนดให้ข้อมูลส่วนบุคคลจะต้องมีความถูกต้อง และเก็บรักษาข้อมูลให้เป็นปัจจุบัน หากปรากฏข้อมูลที่ไม่ถูกต้องจะต้องทำการลบหรือแก้ไขข้อมูลนั้นโดยไม่ชักช้า

สำหรับหลักความได้สัดส่วนของข้อมูลเป็นเรื่องการเก็บรวบรวมข้อมูลส่วนบุคคลโดยคำนึงถึงฐานประโยชน์อันชอบด้วยกฎหมาย (Legitimate Interest) และสิทธิของเจ้าของ

---

[112] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 4

[113] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 21

[114] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 27 วรรคสอง

[115] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 วรรคสาม

ข้อมูลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กล่าวคือการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลจะกระทำมิได้ เว้นแต่เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ เพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูล เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลก่อนเข้าทำสัญญานั้นหรือเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุม หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุม เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุม เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูล ตลอดจนเป็นการปฏิบัติตามกฎหมายของผู้ควบคุม[116]

3) หลักการเก็บรักษาข้อมูล (Data Retention Principle) บัญญัติไว้ในมาตรา 37(3) กำหนดให้ผู้ควบคุมมีหน้าที่จัดมาตรการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล ในกรณีที่พ้นกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล หรือเมื่อไม่มีความจำเป็นต้องเก็บรวบรวมข้อมูลส่วนบุคคลตามวัตถุประสงค์อีกต่อไป หรือเมื่อเจ้าของข้อมูลร้องขอให้ทำลายข้อมูลหรือถอนความยินยอม อย่างไรก็ตาม ผู้ควบคุมไม่จำเป็นต้องลบข้อมูลส่วนบุคคลและยังคงมีสิทธิเก็บรักษาข้อมูลส่วนบุคคลนั้นต่อไปได้เพื่อวัตถุประสงค์ดังต่อไปนี้

3.1) เพื่อการใช้เสรีภาพในการแสดงความคิดเห็น

3.2) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ เพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสม เพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูล

3.3) เพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุม หรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุม เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูล

---

[116] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24

3.4) เพื่อการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพ หรือวิชาชีพ หรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลกับผู้ประกอบวิชาชีพทางการแพทย์

3.5) เพื่อการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับประโยชน์สาธารณด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยาเวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

3.6 การใช้เพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

4) หลักการรักษาความมั่นคงปลอดภัยและการรักษาความลับ (The Security And Confidentiality) เป็นหลักการที่กำหนดให้ทั้งผู้ควบคุมและผู้ประมวลผลข้อมูลต้องจัดให้มีมาตรฐานการรักษาความมั่นคงปลอดภัยแก่การประมวลผลข้อมูลส่วนบุคคล ซึ่งตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคล พ.ศ. 2562 มาตรา 37 (1) กำหนดให้ผู้ควบคุมมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็น หรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด สำหรับผู้ประมวลผลข้อมูลก็มีหน้าที่ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมตามที่บัญญัติไว้ในมาตรา 40 (2) ซึ่งมีหลักการเช่นเดียวกับที่บัญญัติไว้ในมาตรา 37 (1)

ในกรณีที่มีการละเมิดข้อมูลส่วนบุคคล มาตรา 37(4) กำหนดให้ผู้ควบคุมจะต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้องมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่สามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า ทั้งนี้การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด สำหรับผู้ประมวลผลข้อมูลมีหน้าที่เพียงแจ้งให้ผู้ควบคุมทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นตามที่กำหนดไว้ในมาตรา 40 (2)

การไม่ปฏิบัติตามหลักการรักษาความมั่นคงปลอดภัยและการรักษาความลับย่อมเป็นการกระทำความผิดซึ่งมีโทษทั้งทางปกครองและอาญา โดยโทษปรับทางปกครองสูงถึง 300,000 บาท[117] ส่วนโทษทางอาญากำหนดให้ผู้ล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งได้นำไปเปิดเผยแก่ผู้อื่นต้องระวางโทษจำคุกสูงสุดถึงหกเดือน หรือปรับสูงถึง 500,000 บาท หรือทั้งจำทั้งปรับ[118]

5) หลักความโปร่งใส (The Transparency Principle) ปรากฏตามมาตรา 23 และมาตรา 25 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นหลักการที่กำหนดให้การเก็บรวบรวมข้อมูลส่วนบุคคลไม่ว่าจะเป็นการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลนั้นโดยตรงหรือไม่ก็ตาม ผู้ควบคุมจะต้องแจ้งให้เจ้าของข้อมูลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดต่าง ๆ เว้นแต่เจ้าของข้อมูลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว ซึ่งรายละเอียดที่จะต้องแจ้งนั้นมาตรา 23 กำหนดไว้ดังต่อไปนี้

5.1) วัตถุประสงค์ของการเก็บรวบรวมเพื่อการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยซึ่งรวมถึงวัตถุประสงค์ที่ให้อำนาจในการเก็บรวบรวมได้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล

---

[117] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 83 และมาตรา 86

[118] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 80

5.2) แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญาหรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล

5.3) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม

5.4) ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

5.5) ข้อมูลเกี่ยวกับผู้ควบคุม สถานที่ติดต่อ และวิธีการติดต่อในกรณีที่มีตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย

5.6) สิทธิต่าง ๆ ของเจ้าของข้อมูลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

สำหรับมาตรา 25 เป็นการห้ามมิให้ผู้ควบคุมทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลโดยตรง เว้นแต่เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอม หรือมีการแจ้งถึงวัตถุประสงค์ใหม่และรายละเอียดการในการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลทราบโดยไม่ชักช้า แต่ต้องไม่เกิน 30 วันนับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูล เว้นแต่กรณีที่นำข้อมูลส่วนบุคคลไปใช้เพื่อการติดต่อกับเจ้าของข้อมูลต้องแจ้งในการติดต่อครั้งแรก และกรณีที่จะนำข้อมูลส่วนบุคคลไปเปิดเผย ต้องแจ้งก่อนที่จะนำข้อมูลส่วนบุคคลไปเปิดเผยเป็นครั้งแรก อย่างไรก็ตามผู้ควบคุมไม่จำต้องแจ้งให้เจ้าของข้อมูลทราบถึงรายละเอียดหากเป็นกรณีที่เจ้าของข้อมูลทราบวัตถุประสงค์ใหม่หรือรายละเอียดนั้นอยู่แล้ว หรือผู้ควบคุมพิสูจน์ได้ว่าการแจ้งวัตถุประสงค์ใหม่หรือรายละเอียดดังกล่าวไม่สามารถทำได้หรือจะเป็นอุปสรรคต่อการใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ในกรณีนี้ผู้ควบคุมต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิ

เสรีภาพ และประโยชน์ของเจ้าของข้อมูล หรือการใช้หรือการเปิดเผยข้อมูลส่วนบุคคลต้องกระทำโดยเร่งด่วนตามที่กฎหมายกำหนด ซึ่งได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูล หรือเมื่อผู้ควบคุมเป็นผู้ซึ่งล่วงรู้หรือได้มาซึ่งข้อมูลส่วนบุคคลจากเจ้าหน้าที่หรือจากการประกอบอาชีพและต้องรักษาวัตถุประสงค์ใหม่หรือรายละเอียดบางประการไว้เป็นความลับตาม

การไม่ปฏิบัติตามมาตรา 23 หรือมาตรา 25 อาจได้รับโทษทางปกครอง ซึ่งกำหนดโทษปรับไว้สูงถึง 1,000,000 บาท[119]

3.1.2 หลักการจัดทำและการบันทึกรายการ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดหน้าที่ให้ผู้ควบคุมซึ่งเป็นผู้ประกอบการที่ทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จะต้องบันทึกรายการแสดงรายละเอียดของกิจกรรมต่าง ๆ ที่ได้กระทำต่อข้อมูลส่วนบุคคลตามที่มาตรา 39 กำหนดเอาไว้เป็นหลักฐาน เพื่อให้เจ้าของข้อมูลหรือคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้ ซึ่งการบันทึกรายการจะสามมารถตรวจสอบถึงการปฏิบัติหน้าที่ตามกฎหมายของผู้ควบคุม โดยบันทึกจะมีรายละเอียดดังต่อไปนี้[120]

1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูล

---

[119] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 82

[120] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 39 วรรคแรก

6) การใช้หรือเปิดเผยข้อมูลตามมาตรา 27 วรรคสาม กล่าวคือ ผู้ควบคุมมีหน้าที่จะต้องบันทึกรายการในการใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 27 ที่ได้รับยกเว้นไม่ต้องขอความยินยอมจากเจ้าของข้อมูลตามมาตรา 24หรือมาตรา26ซึ่งรายการที่ได้รับยกเว้น มีรายการดังต่อไปนี้

6.1) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์ หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือเกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตราการปกป้องที่เหมาสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูล ทั้งนี้ตามที่คณะกรรมการประกาศกำหนด[121]

6.2) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล[122]

6.3) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลเป็นคู่สัญญา หรือ เพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลก่อนเข้าทำสัญญานั้น[123]

6.4) เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุม หรือปฏิบัติหน้าที่ในการใช้อานาจรัฐที่ได้มอบให้แก่ผู้ควบคุม[124]

6.5) เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุม เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูล[125]

6.6) เป็นการปฏิบัติตามกฎหมายของผู้ควบคุม[126]

---

[121] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(1)

[122] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(2)

[123] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(3)

[124] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(4)

[125] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(5)

6.7) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล ซึ่งเจ้าของข้อมูลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม[127]

6.8) เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคมหรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรนั้น[128]

6.9) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูล[129]

6.10) เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย[130]

6.11) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ[131] (ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลกับผู้ประกอบวิชาชีพทางการแพทย์ (ข) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่อ อันตรายหรือ โรคระบาดที่อาจ

---

[126] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(6)

[127] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26(1)

[128] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26(2)

[129] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26(3)

[130] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26(4)

[131] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26(5)

ติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ (ค) การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองงทางสังคมซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจาเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุมหรือเจ้าของข้อมูล โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูล (ง) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่นทั้งนี้ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลตามที่คณะกรรมการประกาศกำหนด (จ) ประโยชน์สาธารณะที่สำคัญ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูล

7) การปฏิเสธคำขอหรือการคัดค้านของเจ้าของข้อมูล ตามมาตรา 30 วรรคสาม มาตรา 31วรรคสาม มาตรา 32วรรคสาม และ มาตรา 36วรรคแรก ผู้ควบคุมมีหน้าที่ต้องบันทึกรายการปฏิเสธคำขอหรือคำคัดค้านของเจ้าของข้อมูลในกรณีดังต่อไปนี้

7.1) ในกรณีที่เจ้าของข้อมูลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนที่อยู่ในความรับผิดชอบของผู้ควบคุมหรือขอให้เปิดเผยการได้มาของข้อมูลส่วนบุคคลที่เจ้าของข้อมูลไม่ได้ให้ความยินยอม หากที่ผู้ควบคุมปฏิเสธคำขอของเจ้าของข้อมูล ผู้ควบคุมมีหน้าที่ต้องทำการบันทึกรายการพร้อมด้วยเหตุผลเอาไว้ด้วย แต่อย่างไรก็ตามการที่ผู้ควบคุมจะปฏิเสธคำขอของเจ้าของข้อมูลได้เฉพาะในกรณีที่เป็นการปฏิเสธตามกฎหมายหรือตามคำสั่งศาลและการขอรับสำเนาข้อมูลส่วนบุคคลนั้นจะส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น[132]

7.2) ในกรณีที่ผู้ควบคุมปฏิเสธคำขอของเจ้าของข้อมูลที่ขอรับข้อมูลส่วนบุคคลของตนจากผู้ควบข้อมูลที่คุมควบคุมข้อมูลได้ทำให้ข้อมูลส่วนบุคคลนั้นอยู่ในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติและ

[132] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 30 วรรคสาม

สามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ หรือ ขอให้ผู้ควบคุมส่งหรือโอนข้อมูลส่วนบุคคลในรูปแบบดังกล่าวไปยังผู้ควบคุมอื่นเมื่อสามารถทำได้โดยวิธีอัตโนมัติ หรือขอรับข้อมูลส่วนบุคคลที่ผู้ควบคุมส่งหรือโอนข้อมูลในรูปแบบดังกล่าวไปยังผู้ควบคุมอื่นโดยตรง ทั้งนี้ผู้ควบคุมจะต้องทำการบันทึกการปฏิเสธคำขอพร้อมด้วยเหตุผลดังกล่าวเอาไว้ในรายการด้วย[133]

7.3) ในกรณีที่เจ้าของข้อมูลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนในกรณีต่อไปนี้

7.3.1) กรณีที่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24(4) หรือ (5) เว้นแต่ผู้ควบคุมพิสูจน์ได้ว่า การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น ผู้ควบคุมได้แสดงให้เห็นถึงเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า หรือการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นไปเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย ถ้าผู้ควบคุมปฏิเสธการคัดค้าน ผู้ควบคุมมีหน้าที่ต้องบันทึกรายการบันทึกการปฏิเสธการคัดค้านพร้อมด้วยเหตุผลเอาไว้ด้วย[134]

7.4) ในกรณีที่ผู้ควบคุมปฏิเสธการคัดค้านของเจ้าของข้อมูลที่มีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ถ้าผู้ควบคุมพิสูจน์ได้ว่า เป็นการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลเมื่อ แสดงให้เห็นถึงเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า หรือ เป็นการเก็บรวบรวมใช้หรือเปิดเผยเป็นไปเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามสิทธิเรียกร้องตามกฎหมายหรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย[135]

8) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 37(1) ผู้ควบคุมมีหน้าที่ต้องบันทึกรายการคำอธิบายที่เกี่ยวกับการจัดการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือ เปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

---

[133] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 31วรรคสาม

[134] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 32 วรรคสาม

[135] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 36 วรรคแรก

รูปแบบของการบันทึกรายการ[136] บันทึกรายการจะต้องจัดทำเป็นลายลักษณ์อักษร โดยจะอยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์ก็ได้

ผู้ควบคุมที่อาจได้รับยกเว้นไม่ต้องทำบันทึกรายการ ผู้ควบคุมที่มีกิจการขนาดเล็กอาจได้รับยกเว้นไม่ต้องจัดทำบันทึกตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด อย่างไรก็ดี ผู้ควบคุมที่เป็นกิจการขนาดเล็กจะมีหน้าที่ในการบันทึกกิจกรรมต่อเมื่อเป็นการดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระต่อสิทธิและเสรีภาพของเจ้าของข้อมูลหรือไม่ใช่กิจการที่เก็บรวบรวมใช้หรือเปิดเผยเป็นการเป็นครั้งคราว หรือมีการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นการดำเนินการเกี่ยวกับข้อมูลอ่อนไหว[137]

3.2 สหราชอาณาจักร

เนื่องจากสหราชอาณาจักรยังอยู่ในสมาชิกของสหภาพยุโรปจึงต้องบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป(GDPR) แต่สหราชอาณาจักรกำลังจะออกจากการเป็นสมาชิกของสหภาพยุโรป จึงต้องมีการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลขึ้นมาที่มีชื่อว่า พระราชบัญญัติคุ้มครองข้อมูล ค.ศ. 2018 (Data Protection Act 2018 หรือ DPA) โดยมีการนำเอาหลักการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปเป็นแม่แบบในการร่างกฎหมาย จึงน่าศึกษาว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักรมีหลักการคุ้มครองข้อมูลส่วนบุคคลอย่างไร โดยจะศึกษา เกี่ยวกับหลักการคุ้มครองและหลักการจัดทำบันทึกรายการ โดยมีรายละเอียดดังนี้

3.2.1 หลักการคุ้มครองข้อมูลส่วนบุคคล

การให้ความคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักรสืบเนื่องจากการเข้าเป็นสมาชิกสภายุโรป (The Council of Europe) จำเป็นต้องอนุวัติกฎหมายภายในให้เป็นไปตามอนุสัญญาว่าด้วยการคุ้มครองบุคคลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลโดยอัตโนมัติ

---

[136] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 39 วรรคแรก

[137] จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 39วรรคสาม

(Convention For The Protection of Individuals With Regard to Automatic Processing of Personal Data) จนกระทั่งได้ตราพระราชบัญญัติคุ้มครองข้อมูล ค.ศ. 1984 (Data Protection Act 1984)

เมื่อสหราชอาณาจักรได้เข้าเป็นสมาชิกของสหภาพยุโรป (European Union หรือ EU) ซึ่งมีการวางแนวทางในการให้ความคุ้มครองข้อมูลส่วนบุคคลไว้เช่นเดียวกับสภายุโรปแต่มีมาตรฐานที่สูงกว่าตามคำสั่งฉบับที่ 95/46/EC (Directive 95/46/EC) ว่าด้วยการคุ้มครองบุคคลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลและเสรีภาพในการเคลื่อนไหวของข้อมูล (The Protection of Individuals With Regard to The Processing of Personal Data And on The Free Movement of Such Data) สหราชอาณาจักรจึงได้ออกพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 1998 เพื่ออนุวัติให้เป็นไปตามคำสั่งดังกล่าว และเพื่อยกระดับมาตรฐานในการให้ความคุ้มครองข้อมูลส่วนบุคคล ต่อมาเมื่อมีการแก้ไข Directive 95/46/EC เป็น Regulation (EU) 2016/679 ว่าด้วยการคุ้มครองบุคคลในเรื่องการประมวลผลข้อมูลส่วนบุคคลและและว่าด้วยการไหลเวียนของข้อมูล (the protection of natural persons with regard to the processing of personal data and on the free movement of such data) หรือเรียกว่า กฎหมายว่าด้วยการคุ้มครองข้อมูลทั่วไป (General Data Protection Regulation หรือ GDPR) ซึ่งประกาศใน Official Journal of the European Union เมื่อวันที่ 27 เมษายน ค.ศ. 2016 สหราชอาณาจักรจึงได้ปรับปรุงกฎหมายคุ้มครองข้อมูลอีกครั้งหนึ่งจนตราออกมาเป็นพระราชบัญญัติคุ้มครองข้อมูล ค.ศ. 2018 (Data Protection Act 2018 หรือ DPA) ทั้งนี้เพื่อรองรับหากเมื่อไหร่ก็ตามที่สหราชอาณาจักรออกจากการเป็นสมาชิกภาพแห่งสหภาพยุโรป (Brexit) โดยไม่มีข้อตกลง (No-deal) DPA ก็จะมีผลใช้บังคับ แต่ในขณะที่สหราชอาณาจักรยังไม่ได้ออกจากการเป็นสมาชิกภาพแห่งสหภาพยุโรปสหราชอาณาจักรยังคงอยู่ภายใต้บังคับแห่ง GDPR ดังนั้นการให้ความคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักรจึงมีลักษณะพิเศษอาจแบ่งได้เป็น 2 ช่วงเวลา คือช่วงเวลาที่อยู่ภายใต้บังคับแห่ง GDPR และช่วงเวลาที่ต้องบังคับตาม DPA สำหรับการคุ้มครองข้อมูลส่วนบุคคลภายใต้บังคับแห่ง GDPR ได้กล่าวไว้แล้วในบทก่อน ในหัวข้อนี้จึงเป็นการศึกษาการให้ความคุ้มครองข้อมูลส่วนบุคคลตาม DPA ของสหราชอาณาจักรอันมีสาระสำคัญดังต่อไปนี้

3.2.1.1 นิยามความหมายของ “ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลข่าวสารใด ๆ อันระบุหรือสามารถระบุเกี่ยวกับชีวิตความเป็นอยู่ของบุคคลได้[138] ในกรณีที่สามารถระบุเกี่ยวกับชีวิตความเป็นอยู่ของบุคคลได้ หมายถึง ชีวิตความเป็นอยู่ของบุคคลที่สามารถระบุได้ไม่ว่าโดยทางตรงหรือทางอ้อม โดยเฉพาะอย่างยิ่งการอ้างอิงถึงการระบุตัวตน เช่น ชื่อ เลขบัตรประจำตัวประชาชน ข้อมูลตำแหน่งที่อยู่ หรือการระบุตัวตนออนไลน์ หรือการระบุลักษณะเฉพาะของบุคคลอย่างหนึ่งอย่างใดที่ประกอบไปด้วยลักษณะเฉพาะทางกายภาพ สรีรวิทยา พันธุกรรม สภาพจิตใจ สภาพเศรษฐกิจ สภาพวัฒนธรรมหรือสังคม[139]

3.2.1.2 หลักการพื้นฐานที่สำคัญในการคุ้มครองข้อมูลส่วนบุคคลอาจจำแนกได้ 6 ประการดังต่อไปนี้[140]

ประการแรก เป็นหลักที่กำหนดให้การประมวลผลข้อมูลส่วนบุคคลต้องกระทำโดยชอบด้วยกฎหมาย เป็นธรรม และมีความโปร่งใส เป็นหลักปฏิบัติที่ให้ผู้ควบคุมดำเนินการประมวลผลข้อมูลส่วนบุคคลได้เท่าวัตถุประสงค์ที่ได้แจ้งให้เจ้าของข้อมูลทราบ ซึ่งการแจ้งนั้นต้องมีรายละเอียดและเหตุผลการนำข้อมูลส่วนบุคคลไปใช้อย่างชัดเจน และได้รับความยินยอมจากเจ้าของข้อมูลอย่างชัดแจ้ง

ประการที่สอง เป็นหลักการที่กำหนดให้ระบุวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลให้ชัดแจ้ง และไม่ประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ไม่อาจยอมรับได้สำหรับวัตถุประสงค์ที่ได้ระบุไว้นั้น

---

[138] Data Protection Act 2018 Section 3 (2) “Personal data means any information relating to any information relating to an identified or identifiable living individual (subject to subsection (14) (c)).”

[139] Data Protection Act 2018 Section 3 (2) “identifiable living individual” means a living individual who can be identified, directly or indirectly, in particular by reference to (a) an identifier such as a name, an identification number, location data or an online identifier, or (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.”

[140] Data Protection Act 2018 Art. 86 to 91.

ประการที่สาม เป็นหลักการที่กำหนดการเก็บรวบรวมข้อมูลส่วนบุคคล จะต้องเก็บรวบรวมอย่างเพียงพอ เกี่ยวข้อง และไม่มากจนเกินไปจากวัตถุประสงค์ของการประมวลผลที่ได้ระบุไว้

ประการที่สี่ เป็นหลักการที่กำหนดให้การประมวลผลข้อมูลส่วนบุคคล จะต้องมีความถูกต้อง และเก็บรักษาข้อมูลให้เป็นปัจจุบันอยู่เสมอ

ประการที่ห้า เป็นหลักการที่กำหนดการเก็บรักษาข้อมูลส่วนบุคคล จะต้องไม่เก็บรักษาไว้นานเกินความจำเป็นสำหรับวัตถุประสงค์ของการประมวลผล

ประการที่หก เป็นหลักการที่กำหนดให้การประมวลผลข้อมูลส่วนบุคคล ต้องมีมาตรการรักษาความปลอดภัยที่เหมาะสมเพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นจากการประมวลผลข้อมูลส่วนบุคคลโดยผู้ที่ไม่มีอำนาจเข้าถึง ทำลาย ทำให้สูญหาย ใช้ แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลนั้น

3.2.2 หลักการจัดทำและการบันทึกรายการ

หลักการบันทึกรายการประมวลผลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักรได้บัญญัติไว้ในมาตรา 61[141] ซึ่งมีสาระสำคัญดังต่อไปนี้

1) ผู้ควบคุมแต่ละรายมีหน้าที่ต้องเก็บรักษาบันทึกประเภทของกิจกรรมการประมวลผลทั้งหมด[142]

2) บันทึกของผู้ควบคุมต้องประกอบไปด้วยรายละเอียดดังต่อไปนี้[143]

---

[141] Data Protection Act2018 Section 61 Records of processing activities

[142] Data Protection Act2018 Section 61(1) Each controller must maintain a record of all categories of processing activities for which the controller is responsible.

[143] Data Protection Act2018 Section 61(2) The controller's record must contain the following information.

2.1) ชื่อและรายละเอียดการติดต่อของผู้ควบคุม[144]

2.2) ชื่อและรายละเอียดการติดต่อของผู้ควบคุมร่วมถ้าหากมี[145]

2.3) ชื่อและรายละเอียดการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูล[146]

2.4) วัตถุประสงค์ของการประมวลผล[147]

2.5) ประเภทของผู้รับข้อมูลส่วนบุคคล (recipient) หรือผู้ที่จะได้รับข้อมูลส่วนบุคคล รวมถึงผู้รับข้อมูลที่อยู่ในประเทศที่สามหรือองค์กรระหว่างประเทศด้วย[148]

2.6) คำอธิบายประเภทของเจ้าของข้อมูล และประเภทของข้อมูลส่วนบุคคล[149]

2.7) รายละเอียดการใช้โปรไฟล์ลิ่ง (Profiling)[150]

---

[144] Data Protection Act2018 Section 61(2)(a) the name and contact details of the controller.

[145] Data Protection Act2018 Section 61(2)(b) where applicable, the name and contact details of the joint controller."

[146] Data Protection Act2018 Section 61(2)(c) where applicable, the name and contact details of the data protection officer.

[147] Data Protection Act2018 Section 61(2)(d) the purposes of the processing.

[148] Data Protection Act2018 Section 61(2)(e) the categories of recipients to whom personal data has been or will be disclosed including recipients in third countries or international organisations.

[149] Data Protection Act2018 Section 61(2)(f) and(i) a description of the categories of data subject, and,(ii) personal data.

[150] Data Protection Act2018 Section 61(2) (g) where applicable, details of the use of profiling.

2.8) ประเภทของการโอนข้อมูลส่วนบุคคลไปยังประเทศที่สามหรือองค์กรระหว่างประเทศ[151]

2.9) ฐานของกฎหมายที่ใช้ในการประมวลผลรวมถึงที่ใช้การโอนข้อมูลส่วนบุคคล[152]

2.10) กำหนดระยะเวลาเพื่อทำลายข้อมูลส่วนบุคคลในแต่ละประเภท[153]

2.11) คำอธิบายทั่วไปถึงมาตรการทางเทคนิคและการรักษาความปลอดภัยขององค์กร[154]

3) ผู้ควบคุมและผู้ประมวลผลข้อมูลต้องทำการเก็บรักษาบันทึกไว้ในลักษณะที่หน่วยงานที่มีอำนาจสามารถตรวจสอบได้เมื่อร้องขอ[155]

สำหรับการไม่จัดทำหรือเก็บรักษาบันทึกการประมวลผลพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักรกำหนดโทษปรับไว้ในอัตราที่เรียกว่า อัตราสูงสุดขั้นมาตรฐาน (Standard Maximum Amount) ซึ่งมีโทษปรับจำนวนสิบล้านยูโร หรือร้อยละสองของรายได้จากผลประกอบการทั่วโลกในรอบบัญชีของปีล่าสุด แล้วแต่ว่าจำนวนใดจะสูงกว่ากัน[156]

---

[151] Data Protection Act2018 Section 61(2)(h) where applicable, the categories of transfers of personal data to a third country or an international organization.

[152] Data Protection Act2018 Section 61(2)(i) an indication of the legal basis for the processing operations, including transfers, for which the personal data is intended.

[153] Data Protection Act2018 Section 61(2)(j) where possible, the envisaged time limits for erasure of the different categories of personal data.

[154] Data Protection Act2018 Section 61(2)(k) where possible, a general description of the technical and organisational security measures referred to in section 66.

[155] Data Protection Act2018 Section 61(3) Each processor must maintain a record of all categories of processing activities carried out on behalf of a controller.

[156] Data Protection Act 2018 Article 157 (2)(b) and (6).

3.3 ประเทศสหรัฐอเมริกา

เนื่องจากปัจจุบันประเทศสหรัฐอเมริกายังไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป กล่าวคือ สหรัฐอเมริกาจะมีการตรารัฐบัญญัติก็ต่อเมื่อเกิดปัญหาการป้องกันความลับหรือความเป็นอยู่ส่วนตัวของประชาชนที่ถูกละเมิดอันมีลักษณะเป็นการวิ่งไล่แก้ปัญหา สหรัฐอเมริกาจึงเป็นประเทศที่น่าศึกษาเพราะการที่สหรัฐอเมริกาไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปนั้นสหรัฐอเมริกามีวิธีการในการคุ้มครองข้อมูลส่วนบุคคลในรูปแบบใด โดยจะศึกษากฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลและการจัดทำและบันทึกรายการ ซึ่งมีรายละเอียดดังนี้

3.3.1 หลักการคุ้มครองข้อมูลส่วนบุคคล

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหรัฐอเมริกาเป็นกฎหมายเฉพาะเรื่องที่เรียกว่า Sectoral หรือ *ad hoc* ซึ่งต่างจากกฎหมายของกลุ่มประเทศสหภาพยุโรปที่มีกฎหมายแม่บทครอบคลุมหรือวางกฎเกณฑ์ในเรื่องของการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปไว้ สำหรับสหรัฐอเมริกาจะมีการตรารัฐบัญญัติก็ต่อเมื่อเกิดปัญหาการป้องกันความลับหรือความเป็นอยู่ส่วนตัวของประชาชนถูกละเมิด ดังนั้น การออกกฎหมายคุ้มครองส่วนบุคคลของประเทศอเมริกาจึงมีลักษณะเป็นการวิ่งไล่แก้ไขปัญหาที่เกิดขึ้นมากกว่าที่จะวางหลักเกณฑ์ทั่วไปเพื่อป้องกันปัญหา เช่น ในเหตุการณ์ที่นักแสดงหญิงของสหรัฐอเมริกาชื่อว่า Rebecca Shaeffer ได้ถูกฆาตกรรมที่บ้านของเธอ เมื่อปี ค.ศ. 1989 โดยคนร้ายสืบหาข้อมูลที่อยู่จากใบขับขี่ที่ได้มาจากกรมขนส่งทางบกแห่งแคลิฟอร์เนีย (The California Department of Motor Vehicles) สภาคองเกรส (Congress) จึงได้ตรากฎหมาย The Drivers Privacy Protection Act ขึ้นมาเพื่อคุ้มครองความเป็นส่วนตัว หรือกรณีที่ผู้พิพากษานามว่า Robert Bork ถูกผู้สื่อข่าวเผยแพร่ข้อมูลการเช่าวิดีโอเทปที่มีรายการเกี่ยวกับหนังโป๊หรือภาพลามกอนาจาร ทำให้มีการวิพากษ์วิจารณ์ถึงความประพฤติของผู้พิพากษาท่านนี้ เป็นเหตุให้ไม่ได้รับการคัดเลือกเป็นผู้พิพากษาศาลสูง หลังจากนั้นสภาคองเกรสได้มีการตรา The Video Privacy Protection Act การตรากฎหมายเช่นนี้อาจมีที่มาจากปรัชญาหรือที่มาทางประวัติศาสตร์การสร้างชาติของประเทศสหรัฐอเมริกาที่พยายามมิให้เจ้าหน้าที่ของรัฐลิดรอนสิทธิเสรีภาพของประชาชน ในขณะเดียวกัน ประชาชนก็มีสิทธิเสรีภาพที่จะดำเนินธุรกิจแบบทุนนิยมอันเป็นปรัชญาที่ชาวอเมริกันยึดถือมาเป็นเวลานาน โดยทั่วไปแล้วประเทศสหรัฐอเมริกาไม่มีกฎหมายให้ประชาชนต้องให้ความยินยอมในเรื่องของการประมวลผลข้อมูล หรือการจัดทำการตลาดและการ

ขายข้อมูลส่วนบุคคลให้กับบุคคลที่สาม จะเห็นได้ว่า ประเทศสหรัฐอเมริกาให้ความสำคัญเกี่ยวกับสิทธิเสรีภาพในการเข้าถึงความเป็นส่วนตัว โดยปล่อยให้เป็นนโยบายของเอกชนที่จะกำกับควบคุมดูแลกันเอง (Self-regulations) แล้วเจ้าหน้าที่ของรัฐจะควบคุมอีกทีหนึ่ง อย่างไรก็ตามเจ้าของข้อมูลที่ถูกละเมิดมีสิทธิดำเนินคดีทางศาลได้อย่างเต็มที่โดยศาลสามารถกำหนดค่าเสียหายในเชิงลงโทษ (Punitive Damages) แก่ผู้กระทำละเมิดได้[157]

เมื่อพิจารณารัฐธรรมนูญของประเทศสหรัฐอเมริกา ไม่ปรากฏบทบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลหรือความเป็นอยู่ส่วนตัวอย่างแจ้งชัด แต่ศาลสูงสุด (Supreme Court) ได้วินิจฉัยคุ้มครองสิทธิความเป็นอยู่ของประชาชนไว้ในคดี Whalen *v.* Roe ว่า การที่กฎหมายของมลรัฐนิวยอร์คกำหนดว่า ในกรณีที่มีการจ่ายยาที่อยู่ในบัญชียาเสพติดให้โทษประเภทที่ 2 แพทย์จะต้องส่งสำเนารายงานชื่อของแพทย์ที่สั่งจ่ายยา ร้านที่ขายยา ตัวยาและปริมาณที่จ่าย ตลอดจนชื่อ ที่อยู่และอายุของผู้ป่วย แก่รัฐเพื่อการประมวลผลของคอมพิวเตอร์ และเก็บรักษาไว้เป็นเวลา 5 ปี เป็นการละเมิดความเป็นอยู่ส่วนตัวของคนไข้[158]

อย่างไรก็ตามแม้ประเทศสหรัฐอเมริกายังไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลออกมาใช้บังคับเป็นการทั่วไปแต่ประเทศสหรัฐอเมริกายังมีกฎหมายเฉพาะซึ่งมีบทบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแทรกอยู่ด้วยโดยมีกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลดังต่อไปนี้

3.3.1.1 กฎหมายคุ้มครองความเป็นส่วนตัว Privacy Act 1974

เนื่องจากรัฐธรรมนูญของประเทศสหรัฐอเมริกามีบทบัญญัติคุ้มครองความเป็นส่วนตัวของประชาชน โดยเฉพาะอย่างยิ่ง Fourth Amendment ได้รับรองว่าบุคคลมีสิทธิที่จะ

---

[157] จาก *สรุปผลการศึกษาวิจัย โครงการจัดทำความเห็นทางวิชาการเกี่ยวกับการเปิดเผยข้อมูลข่าวสารของราชการและการปฏิบัติตามคำวินิจฉัยและผลกระทบจากคำวินิจฉัยของคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสาร* (น. 61), โดย สหธน รัตนไพจิตร, 2547, กรุงเทพฯ: โรงพิมพ์มหาวิทยาลัยธรรมศาสตร์.

[158] From *U.S. Supreme Court Whalen v. Roe, 429 U.S. 589 (1977)*, 1997. Retrieved from https://supreme.justia.com/cases/federal/us/429/589/

ได้รับความปลอดภัยในร่างกาย เคหสถาน เอกสาร และทรัพย์สินจากการค้น ยึดและจับกุมโดยปราศจากเหตุอันสมควร ซึ่งเคหสถานและทรัพย์สินของบุคคลที่ได้รับความคุ้มครองนั้นรวมไปถึงการสนทนาทางโทรศัพท์ด้วย ในขณะที่การเก็บรวบรวมข้อมูล ใช้ และเปิดเผยส่วนบุคคลโดยองค์กรของรัฐบาลกลับไม่มีข้อจากัด รัฐบาลได้รวบรวมข้อมูลของประชาชนจานวนมากมายทั้งข้อมูลทั่วไปและข้อมูลที่มีความอ่อนไหว เช่น ภาษีรายได้ ประกันสังคม หรือข้อมูลที่ได้จากการสำรวจเพื่อทำวิจัย เป็นต้น ซึ่งหากรัฐบาลมีข้อมูลเกี่ยวกับประชาชนมากเท่าไรก็ย่อมก่อให้เกิดผลเสียต่อประชาชนผู้เป็นเจ้าของข้อมูลมากขึ้นเท่านั้น โดยเฉพาะอย่างยิ่งเทคโนโลยีทางคอมพิวเตอร์ที่ถูกนำมาใช้เพื่อการเก็บรวบรวมและเปิดเผยข้อมูลส่วนบุคคลย่อมทำให้กระทำได้ง่ายขึ้น[159]

Privacy Act 1974 เป็นกฎหมายในระดับสหพันธรัฐมิใช่ระดับมลรัฐกล่าวอีกนัยหนึ่งกฎหมายฉบับนี้ใช้กับรัฐบาลกลาง หรือFederal Government ทำให้แต่ละมลรัฐในอเมริกามีอำนาจอิสระที่จะตราหรือไม่ตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือไม่ก็ได้ ซึ่ง Privacy Act 1974 เป็นกฎหมายที่ใช้กับรัฐเท่านั้น กล่าวคือ กฎหมายฉบับนี้คุ้มครองข้อมูลประชาชนที่ถูกจัดเก็บและรักษาโดยหน่วยงานต่าง ๆ ของรัฐเท่านั้น ไม่ใช่ถูกจัดเก็บโดยภาคเอกชน กฎหมายฉบับนี้มุ่งคุ้มครองการบันทึกข้อมูล (Record) ซึ่งหมายถึงรายการใด ๆ การสะสม หรือ การจัดกลุ่มของข้อมูลเกี่ยวกับบุคคลซึ่งจัดเก็บรักษาโดยหน่วยงานของรัฐ ไม่รวมถึงข้อมูลที่จัดเก็บโดยเอกชนไม่ว่าจะเป็นข้อมูลเกี่ยวกับการศึกษา การทำธุรกรรมต่าง ๆ ประวัติทางการแพทย์ ข้อมูลทางอาชญากรรม การจ้างงาน ฯลฯ โดยข้อมูลต่อไปนี้ได้บรรจุรายการต่อไปนี้ คือ ชื่อ หมายเลขที่สามารถระบุตัวบุคคลได้ สัญลักษณ์ หรือ สิ่งอื่นใดที่สามารถบ่งชี้ตัวบุคคลได้เช่น ลายนิ้วมือ เสียงหรือภาพ ซึ่งโดยหลักแล้วการเปิดบันทึกข้อมูลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลเป็นลายลักษณ์อักษรก่อน อย่างไรก็ตามก็มีการกำหนดข้อยกเว้นบางกรณี เช่น 1) เพื่อใช้งานปรกติประจำวัน หรือ 2)เปิดเผยต่อ The Bureau of the Census เพื่อวางแผนเกี่ยวกับการสำรวจประชากรหรือกิจกรรมที่เกี่ยวข้องเป็นต้น[160]

---

[159] จาก ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็กทรอนิกส์ (น.58-59), โดย อธิพร สิทธิธีรรัตน์, 2558 วิทยานิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์.

[160] จาก สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, *อ้างแล้วเชิงอรรถที่38* (น.12).

บุคคลที่จะได้รับความคุ้มครองตาม Privacy Act ได้แก่ บุคคลซึ่งมีสัญชาติอเมริกัน หรือบุคคลซึ่งมีภูมิลำเนาถาวรถูกต้องตามกฎหมายในประเทศสหรัฐอเมริกา บุคคลอื่นใดนอกจากนี้ไม่สามารถอ้างความคุ้มครองตามพระราชบัญญัติฉบับนี้ได้[161]

ตาม Privacy Act 1974 ได้กำหนดหน้าที่ของหน่วยงานรัฐในการควบคุมดูแลข้อมูลข่าวสารส่วนบุคคลในความครอบครอง และสิทธิของเจ้าของข้อมูลไว้ดังนี้[162]

1) หน้าที่รักษาข้อมูลด้วยความถูกต้องและเลือกจัดเก็บเฉพาะข้อมูลที่เกี่ยวข้องเท่านั้น

2) แจ้งแก่เจ้าของข้อมูลให้ทราบเกี่ยวกับวัตถุประสงค์หลักของการจัดเก็บและข้อมูลที่จะนำไปใช้การนำข้อมูลไปใช้ในงานปรกติทั่วไป (Routine Uses)

3) หากมีการเผยแพร่ต่อบุคคลจะต้องมีการตรวจสอบว่าข้อมูลนั้นมีความถูกต้องสมบูรณ์และเกี่ยวข้องกับวัตถุประสงค์ของหน่วยงานที่จัดเก็บหรือไม่

4) หน่วยงานต้องออก (Rules of Conduct) บังคับใช้แก่บุคคลที่เกี่ยวข้องในการออกแบบ การพัฒนา การจัดการ การเก็บรักษาเกี่ยวกับระบบการบันทึกข้อมูล อีกทั้งยังต้องตักเตือนให้บุคคลเหล่านี้เคารพกฎดังกล่าวและจะได้รับโทษหากไม่ได้ปฏิบัติตาม

5) หน่วยงานจะต้องกำหนดมาตรการทางบริหารทางเทคนิคและทางกายภาพที่เหมาะสมเพื่อเป็นหลักประกันด้านความปลอดภัยและความลับของการบันทึกข้อมูลและป้องกันการคุกคามหรือ ภยันตรายใด ๆซึ่งจะก่อให้เกิดผลร้ายแก่ข้อมูลส่วนบุคคลได้

3.3.1.2 กฎหมายคุ้มครองความเป็นส่วนตัวของเด็กออนไลน์ Children's Online Privacy Protection Act of 1998[163]

---

[161] จาก อธิพร สิทธิธีรรัตน์, *อ้างแล้วเชิงอรรถที่ 159* (น. 59).

[162] จาก สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, *อ้างแล้วเชิงอรรถที่38* (น.14-15).

กฎหมาย Children's Online Privacy Protection Act of 1998หรือ COPPA ตราขึ้นในปี ค.ศ. 1998 เพื่อแก้ไขปัญหาความเป็นส่วนตัวของเด็กออนไลน์ให้ทันกับยุคของเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็วซึ่งนำไปใช้กับผู้ประกอบการเชิงพาณิชย์ที่เก็บรวบรวมประมวลผลหรือเปิดเผยข้อมูลส่วนตัวของเด็กที่มีอายุต่ำกว่าสิบสามปี โดยจะต้องได้รับการตรวจสอบหรือยินยอมจากผู้ปกครองก่อนจัดเก็บรวบรวมประมวลผลหรือปิดเผยข้อมูลส่วนตัวเด็ก โดยกำหนดให้ผู้ดำเนินการเว็บไซต์เชิงพาณิชย์และบริการออนไลน์มีหน้าที่ต้องติดประกาศนโยบายในการขอข้อมูลส่วนบุคคล (Privacy Policies) บนเว็บไซต์อย่างชัดเจน หากเว็บไซต์มีการขอข้อมูลจากเด็กจะต้องมีการแจ้ง การขออนุญาตพ่อแม่หรือผู้ปกครองของเด็กก่อนที่จะมีการจัดเก็บประมวลหรือเปิดเผยข้อมูลของเด็ก และพ่อแม่หรือผู้ปกครองของเด็กมีสิทธิเข้าไปตรวจสอบแก้ไข หรือลบล้างข้อมูลเด็กที่มีการจัดเก็บประมวลผลได้ตลอดเวลา ทั้งมีสิทธิดาเนินการเพื่อป้องกันการขอข้อมูลเพิ่มเติม การนำไปใช้ หรือการนำไปเปิดเผย และผู้ประกอบการไม่มีสิทธิที่จะนำข้อมูลที่เก็บรวมรวมไปเปิดเผยต่อบุคคลที่สาม แต่มีหน้าที่ดูแล รักษาข้อมูลให้ถูกต้อง ปลอดภัย และเป็นความลับอยู่เสมอ

กฎหมายฉบับนี้ ได้นิยามคำว่า ข้อมูลส่วนบุคคล หมายถึง ข้อมูลที่ถูกเก็บทางออนไลน์ใด ๆ ที่สามารถบ่งชี้ตัวบุคคลนั้นได้ซึ่งรวมถึงชื่อและนามสกุลที่อยู่อาศัยรหัสของ Email เบอร์โทรศัพท์ หมายเลขบัตรประกันสังคม รวมทั้งข้อมูลเกี่ยวกับเด็กหรือบิดามารดาของเด็กซึ่งทางเครือข่ายข้อมูลทางอินเตอร์เน็ต

ผู้ควบคุมตามกฎหมายนี้ คือ ผู้ประกอบการเครือข่ายอินเตอร์เน็ตที่มีวัตถุประสงค์ทางการค้าหรือธุรกิจออนไลน์ซึ่งมีหน้าที่ดังนี้

1) หน้าที่ต้องแจ้งให้ทราบ ผู้ประกอบการเครือข่ายบนอินเตอร์เน็ตมีหน้าที่ต้องแจ้งให้คณะกรรมาธิการทราบว่าข้อมูลใดบ้างที่ถูกจัดเก็บและจะใช้ข้อมูลนั้นอย่างไร

---

[163] จาก มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของเด็กบนเครือข่ายอินเทอร์เน็ต (น.52-53), โดย พนิดา พูลสวัสดิ์, 2556 วิทยานิพนธ์มหาบัณฑิต สถาบันบัณฑิตพัฒนบริหารศาสตร์.

2) หน้าที่ต้องรับความยินยอมจากบิดามารดา ในกรณีของการจัดเก็บการใช้ และ การเปิดเผยข้อมูลของเด็กนั้น ผู้ประกอบการเครือข่ายบนอินเตอร์เน็ตจะต้องได้รับความเห็นชอบที่พิสูจน์ได้จากบิดามารดาของเด็ก (Verifiable Parental Consent) เสียก่อน

3)หน้าที่ที่จะห้ามมิให้เด็กมีส่วนร่วมกับ เกมส์ การวิงรางวัล หรือกิจกรรมอื่นใดที่สามารถเปิดเผยข้อมูลของเด็กมากกว่าที่ควรจำเป็นสำหรับการมีส่วนร่วมในกิจกรรมดังกล่าว

4) หน้าที่ให้มีขั้นตอนที่เหมาะสมที่จะปกป้องความลับ ความปลอดภัย และความน่าเชื่อถือของข้อมูล (Integrity)

5) หน้าที่จะต้องจัดหา (Self-regulation)

สิทธิของเจ้าของข้อมูล เนื่องจากเจ้าของข้อมูลตามกฎหมายนี้คือเด็กอายุต่ำกว่า 13ปี บิดามารดาของเด็กนั้นจึงเป็นผู้มีอำนาจดำเนินการแทนเด็กซึ่งมีสิทธิดังนี้

1) สิทธิที่จะปฏิเสธมิให้ผู้ประกอบการเครือข่ายบนอินเตอร์เน็ตได้ ใช้ หรือ เก็บรักษาข้อมูลที่มีลักษณะเรียกคืนได้ (Retrievable Form) อีกต่อไป รวมทั้งแหล่งที่รวม (collection)ของข้อมูลส่วนบุคคลที่จะใช้ในอนาคตด้วยซึ่งสิทธิที่ว่านี้บิดามารดาจะใช้เมื่อใดก็ได้

2) สิทธิที่จะได้รับข้อมูลที่เก็บจากเด็ก สำหรับองค์กรที่ทำหน้าที่ควบคุมและบังคับการให้เป็นไปตามกฎหมายฉบับนี้ คือ The Federal Trade Commission และ Attomey General มีอำนาจหน้าที่โดยแบ่งออกเป็นสองระดับ คือระดับfederalนั้นเป็นอำนาจของ Federal Trade Commission ซึ่ง Federal Trade Commission มีอำนาจออกระเบียบข้อบังคับและจะต้องหาแรงจูงใจที่จะให้ผู้ประกอบการเครือข่ายบนอินเตอร์เน็ตปฏิบัติตาม Self-regulation ที่ออกโดยผู้แทนฝ่ายการตลาดของผู้ประกอบการเครือข่ายบนอินเตอร์เน็ตหรือOnline industries ผู้ละเมิดจะถูกปรับเป็นเงินมากกว่า11,000 $ต่อการละเมิดหนึ่งครั้ง สำหรับในส่วนในระดับของมลรัฐนั้น Attorney General จะดำเนินคดีฟ้องศาลต่อ District Court เพื่อที่ศาลจะบังคับให้ผู้กระทำละเมิดปฏิบัติตาม Self-regulation และใช้ค่าสินไหมทดแทนด้วย

3.3.1.3 ร่างกฎหมายสิทธิความเป็นส่วนตัวของผู้บริโภค Consumer Privacy Bill of Right 2015[164]

ร่างกฎหมาย Consumer Privacy Bill of Right ถูกเสนอครั้งแรกในปี ค.ศ. 2012 และได้ถูกนำเสนอใหม่อีกครั้งหนึ่งในวันที่ 27 กุมภาพันธ์ ค.ศ. 2015 ซึ่ง Consumer Privacy Bill of Right นี้จะเป็นกฎหมายควบคู่ไปกันกับ Data Security and Breach Notification Act of 2015 ที่มีบทบัญญัติกำหนดให้องค์กรต้องเปิดเผยเมื่อมีการละเมิดข้อมูลส่วนบุคคลในทันทีเพื่อบรรเทาความเสียหายที่จะเกิดขึ้น โดย Consumer Privacy Bill of Right มีบทบัญญัติควบคุมการเก็บรวบรวมและการเปิดเผยข้อมูลของผู้บริโภค ให้สิทธิแก่ผู้บริโภคในการควบคุมข้อมูลส่วนบุคคลของตนเอง ในขณะเดียวกันก็กำหนดหน้าที่และความรับผิดชอบแก่บริษัทหรือผู้ค้าซึ่งเป็นผู้เก็บรวบรวมข้อมูลส่วนบุคคลให้มีความชัดเจน ภายใต้ Consumer Bill of Right ข้อมูลส่วนบุคคล หมายถึง ข้อมูลใด ๆ รวมถึงกลุ่มของข้อมูลซึ่งเชื่อมโยงไปยังบุคคลใดบุคคลหนึ่ง และรวมถึงข้อมูลเกี่ยวกับคอมพิวเตอร์หรืออุปกรณ์ในลักษณะอื่น หลักการสำคัญของกฎหมายฉบับดังกล่าวประกอบด้วยหลัก 7 ประการ กล่าวคือ

1) หลักการควบคุมข้อมูลส่วนบุคคลของเจ้าของข้อมูล ผู้บริโภคซึ่งเป็นเจ้าของข้อมูลสามารถใช้สิทธิในการควบคุมข้อมูลของตนซึ่งบริษัทได้เก็บรวบรวมจากผู้บริโภค บริษัทต้องมีการควบคุมที่เหมาะสมต่อข้อมูลส่วนบุคคลที่ผู้บริโภคแบ่งปันแก่บุคคลอื่นและมีการควบคุมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยบริษัทต้องจัดเตรียมวิธีการให้ผู้บริโภคสามารถเข้าถึงข้อมูลส่วนบุคคลของตนเองได้โดยง่าย และต้องมีการแจ้งผู้บริโภคถึงวิธีการที่เข้าถึงและสามารถใช้สิทธิได้ง่ายเพื่อการเพิกถอนหรือจากัดความยินยอม

2) หลักความโปร่งใส กำหนดให้บริษัทจะต้องจัดให้มีการแจ้งอย่างชัดเจนถึงข้อมูลที่ทำการเก็บรวบรวม เหตุผลที่ทำการเก็บรวบรวม การนำข้อมูลส่วนบุคคลไปใช้ เวลาที่จะทำลายข้อมูลนั้นหรือทำให้ข้อมูลนั้นไม่สามารถเชื่อมโยงไปยังผู้บริโภคผู้เป็นเจ้าของข้อมูลได้ และบริษัทเปิดเผยหรือจะเปิดเผยข้อมูลนั้นแก่บุคคลอื่นหรือไม่พร้อมด้วยวัตถุประสงค์ในการเปิดเผยข้อมูลส่วนบุคคล

---

[164] จาก อธิพร สิทธิธีรรัตน์, *อ้างแล้วเชิงอรรถที่ 152* (น.65-67).

3) หลักเคารพต่อบริบท เว้นแต่กฎหมายจะบัญญัติไว้เป็นอย่างอื่น บริษัทจะต้องจำกัดการใช้งานและการเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ที่สอดคล้องกับทั้งความสัมพันธ์ที่บริษัทมีต่อผู้บริโภคและบริบทที่ผู้บริโภคยินยอมเปิดเผยข้อมูลส่วนบุคคลแก่บริษัท หากภายหลังการเก็บรวบรวมข้อมูลส่วนบุคคล บริษัทต้องการใช้หรือเปิดเผยข้อมูลส่วนบุคคลในลักษณะที่ขัดกับบริบทที่ข้อมูลนั้นถูกเก็บรวบรวม บริษัทต้องจัดให้มีมาตรการเกี่ยวกับความโปร่งและให้สิทธิแก่ผู้บริโภคในการตัดสินใจ บริษัทต้องปฏิบัติหน้าที่ภายใต้หลักการนี้โดยคำนึงถึงอายุและวิสัยของบุคคลนั้น ซึ่งเด็กและวัยรุ่นอาจได้รับความคุ้มครองมากขึ้น

4) หลักความปลอดภัย บริษัทจะต้องประเมินความเสี่ยงในความเป็นส่วนตัวและความปลอดภัยของแนวปฏิบัติเกี่ยวกับข้อมูลส่วนบุคคลของตน และคงไว้ซึ่งการป้องกันที่เหมาะสมเพื่อที่จะควบคุมความเสี่ยง เช่น การสูญหาย การเข้าถึงโดยไม่ได้รับอนุญาต การใช้ การทำลาย หรือการเปลี่ยนแปลง หรือการเปิดเผยที่ไม่ถูกต้อง

5) หลักการเข้าถึงและความถูกต้อง บริษัทต้องใช้มาตรการที่เหมาะสมเพื่อคงไว้ซึ่งความถูกต้องของข้อมูลส่วนบุคคล บริษัทต้องให้สิทธิแก่ผู้บริโภคในการเข้าถึงข้อมูลส่วนบุคคลของผู้บริโภคที่บริษัทได้เก็บหรือรักษาไว้ และมีวิธีการที่เหมาะสมเพื่อให้แก้ไขข้อมูลที่ผิดพลาดหรือขอให้ลบข้อมูลหรือใช้สิทธิในการจำกัดการใช้ข้อมูลส่วนบุคคลของผู้บริโภค

6) หลักคำนึงถึงการเก็บรวบรวม บริษัทต้องเก็บรวบรวมข้อมูลส่วนบุคคลได้เพียงเท่าที่จำเป็นเพื่อบรรลุวัตถุประสงค์ตามที่ระบุไว้ในหลักเคารพต่อบริบท บริษัทต้องทำลายหรือทำให้ข้อมูลส่วนบุคคลนั้นไม่สามารถสืบกลับไปยังผู้เป็นเจ้าของข้อมูลได้เมื่อข้อมูลนั้นไม่จำเป็นอีกต่อไป เว้นแต่มีกฎหมายกำหนดไว้เป็นอย่างอื่น

7) หลักความเชื่อถือได้ บริษัทมีหน้าที่ต้องปฏิบัติตามหลักการที่ 1 – 6 ทั้งให้พนักงานปฏิบัติตามหลักการดังกล่าวด้วย โดยต้องจัดอบรมพนักงานตามที่เหมาะสมเพื่อให้สามารถปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคลดังกล่าวได้ และหากบริษัทได้เปิดเผยข้อมูลส่วนบุคคลแก่บุคคลอื่น บริษัทต้องดาเนินการเพื่อให้มั่นใจว่าผู้รับข้อมูลส่วนบุคคลนั้นได้ปฏิบัติตามหลักการทั้งหมดที่กล่าวมาได้ เว้นแต่มีกฎหมายบัญญัติไว้เป็นอย่างอื่น

หลักการทั้งหมดของ Consumer Privacy Bill of Right ดังที่กล่าวมา มีความสอดคล้องกับหลักการของ OECD และหลักการของ APEC นอกจากนี้ Consumer Privacy Bill of Right ยังเปิดโอกาสให้บริษัทสามารถกำหนดแนวปฏิบัติของตนเองได้ทั้งนี้แนวปฏิบัติดังกล่าวต้องได้รับความเห็นชอบจาก FTC ด้วย

3.3.1.4 พระราชบัญญัติคุ้มครองความเป็นส่วนตัวของผู้บริโภคแคลิฟอร์เนีย (California Consumer Privacy Act หรือ CCPA)

เป็นกฎหมายที่คุ้มครองความเป็นส่วนตัวของผู้บริโภคที่อาศัยอยู่ในแคลิฟอร์เนีย และเป็นการควบคุมผู้ประกอบธุรกิจในแคลิฟอร์เนียที่ทำการเก็บรวบรวมและขายข้อมูลส่วนบุคคลของผู้บริโภคโดยตรงหรือผ่านบุคคลที่สาม ซึ่งกฎหมายฉบับนี้จะใช้บังคับกับผู้ประกอบธุรกิจที่มีรายได้อย่างน้อย 25 ดอลลาร์ต่อปี หรือ มีการรับซื้อ ขาย แบ่งปันข้อมูลของผู้บริโภคหรือครัวเรือนเพื่อวัตถุประสงค์ทางการค้าอย่างน้อย50,000 ราย หรือ รับรายได้จากการขายข้อมูลของผู้บริโภคมากกว่ากึ่งหนึ่งของรายได้ต่อปี[165] มีการกำหนดให้ผู้ประกอบธุรกิจที่เก็บรวบรวมข้อมูลส่วนบุคคลจะต้องแจ้งให้ผู้บริโภคทราบถึงประเภทของข้อมูลส่วนบุคคลที่จะเก็บรวบรวมและวัตถุประสงค์ของการใช้ข้อมูล ซึ่งผู้ประกอบธุรกิจจะต้องไม่รวบรวมข้อมูลส่วนบุคคลเพิ่มเติมหรือใช้ข้อมูลเพื่อวัตถุประสงค์เพิ่มเติมโดยที่ไม่ได้แจ้งให้กับผู้บริโภคทราบ[166] กฎหมายฉบับนี้ช่วยให้สิทธิแก่ผู้บริโภคสามารถควบคุมข้อมูลของตนที่บริษัทได้ทำการเก็บรวบรวมได้มากขึ้น มีการให้สิทธิแก่ผู้บริโภคในดังนี้

---

[165] From *California Consumer Privacy Act Guide* (น .3), 2019. Retrieved from https://www.skadden.com/-/media/files/publications/2019/03/cybersecurity_california_privacy .pdf

[166] TITLE 1.81.5. California Consumer Privacy Act of 2018

1798.100.(b) **"**A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section."

1) สิทธิในการลบข้อมูลส่วนบุคคลของผู้บริโภค (Right to Require Deletion of Consumer Personal Information) กำหนดสิทธิของผู้บริโภคในการขอให้ผู้ประกอบธุรกิจลบข้อมูลส่วนบุคคลใด ๆ ที่ผู้ประกอบธุรกิจที่ได้รวบรวมจากผู้บริโภค และกำหนดให้ผู้ประกอบธุรกิจต้องเปิดเผยสิทธินี้แก่ผู้บริโภคทราบ หากผู้ประกอบธุรกิจได้รับคำขอดังกล่าวจากผู้บริโภคแล้ว ผู้ประกอบธุรกิจนั้นจะต้องลบข้อมูลส่วนบุคคลของผู้บริโภคออกจากบันทึกและสั่งให้ผู้ให้บริการต่าง ๆ ลบข้อมูลของผู้บริโภคออกจากบันทึก แต่อย่างไรก็ดีผู้ประกอบธุรกิจอาจปฏิเสธคำขอของผู้บริโภคได้ หากแสดงให้เห็นว่าข้อมูลมีความจำเป็นที่ต้องรักษาข้อมูลส่วนบุคคลดังกล่าวเพื่อการ ทำธุรกรรมที่มีการเก็บรวบรวมข้อมูลส่วนบุคคล จัดหาสินค้า หรือ บริการที่ผู้บริโภคร้องขอ หรือ เพื่อคาดเดาตามเหตุอันสมควรภายในบริบทด้านความสัมพันธ์ทางธุรกิจที่กำลังดำเนินอยู่อย่างต่อเนื่องกับผู้บริโภค หรือ เพื่อทำสัญญาระหว่างธุรกิจกับผู้บริโภค เพื่อการตรวจสอบเหตุการณ์ความปลอดภัย ป้องกันกิจกรรมที่เป็นอันตราย การหลอกลวง การฉ้อโกง หรือการกระทำที่ผิดกฎหมาย หรือดำเนินคดีแก่ผู้ที่รับผิดชอบในการกระทำดังกล่าว เพื่อการแก้ไขข้อบกพร่องเพื่อระบุและแก้ไขข้อผิดพลาดที่ทำให้การปฏิบัติตามเจตนารมณ์ที่มีอยู่มีอุปสรรค เพื่อการใช้สิทธิในการพูดรับประกันสิทธิของผู้บริโภครายอื่นในการใช้สิทธิเสรีภาพการพูด หรือ ใช้สิทธิอื่น ๆตามที่กฎหมายได้กำหนดเอาไว้ เพื่อการปฏิบัติตามกฎหมายว่าด้วยความเป็นส่วนตัวด้านการสื่อสารอิเล็กทรอนิกส์ของรัฐแคลิฟอร์เนีย เพื่อการมีส่วนร่วมทางวิทยาศาสตร์ ประวัติศาสตร์ หรือ การวิจัยประโยชน์สาธารณะ ในสถาณการณ์ที่จำกัด เพื่อการเปิดให้ใช้งานเพียงภายในที่สอดคล้องกับความคาดหวังของผู้บริโภคที่ตั้งอยู่บนความสัมพันธ์ของผู้ภริโภคกับผู้ประกอบธุรกิจ เพื่อการปฏิบัติตามข้อผูกพันทางกฎหมาย และเพื่อการใช้ข้อมูลส่วนบุคคลของผู้บริโภคโดยชอบด้วยกฎหมายซึ่งเข้ากันได้กับบริบทที่ผู้บริโภคให้ข้อมูล

หากผู้ประกอบธุรกิจปฏิเสธคำขอของผู้บริโภคภายใต้ CCPA จะต้องแจ้งให้ผู้บริโภคทราบถึงเหตุผลที่ไม่ดำเนินการใด ๆ และผู้บริโภคมีสิทธิใด ๆ ที่จะอุทธรณ์คำตัดสินของผู้ประกอบธุรกิจ[167]

2) สิทธิในการยกเลิกการขายข้อมูลส่วนบุคคล (Right to Opt- Out of the Sale of Personal Information) โดยอนุญาตให้ผู้บริโภคยกเลิกการขายข้อมูลส่วนบุคคลของตนได้และห้ามไม่ให้ผู้ประกอบธุรกิจขอให้ผู้บริโภคเปลี่ยนการตัดสินใจเป็นระยะเวลาอย่างน้อย 12

[167] จาก California Consumer Privacy Act Guide, *อ้างแล้วเชิงอรรถที่ 165* (น.9).

เดือน นอกจากนี้ในกรณีที่ผู้บริโภคเป็นผู้ที่มีอายุระหว่าง 13 ถึง 16 ปี ผู้ประกอบธุรกิจจะต้องได้รับอนุญาตจากผู้บริโภคที่มีอายุระหว่าง 13 ถึง 16ปี และได้รับความยินยอมจากผู้ปกครองของผู้เยาว์ที่อายุน้อยกว่า 13 ปีก่อนการขายข้อมูลส่วนบุคคล[168]

3) สิทธิในการบริการที่เท่าเทียมและไม่เลือกปฏิบัติ (Right to Equal Service and Non-Discrimination) กล่าวคือ CCPA ไม่อนุญาต ให้ผู้ประกอบธุรกิจทำการเลือกปฏิบัติต่อผู้บริโภคที่ใช้สิทธิใด ๆ ที่กำหนดไว้ในกฎหมาย เช่น ผู้ประกอบธุรกิจจะต้องไม่ทำการปฏิเสธสินค้า หรือ การให้บริการแก่ผู้บริโภค หรือ เรียกเก็บราคา หรือ อัตราสำหรับสินค้าหรือบริการ รวมถึงการใช้ส่วนลดหรือผลประโยชน์อื่น ๆของผู้บริโภคที่แตกต่างกัน เป็นต้น[169]

4) สิทธิในการเข้าถึงข้อมูลของผู้บริโภค (Consumers' Right to Access) ผู้บริโภคมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของตนที่ผู้ประกอบธุรกิจได้รวบรวมไว้ เมื่อผู้ประกอบธุรกิจได้รับคำขอจากผู้บริโภคที่สามารถตรวจสอบได้ ผู้ประกอบธุรกิจจะต้องให้รายการต่าง ๆ แก่ผู้บริโภค ได้แก่ ข้อมูลส่วนบุคคลที่ทำการรวบรวม หมวดหมู่ของข้อมูลผู้บริโภคที่รวบรวม แหล่งที่มาของข้อมูลส่วนบุคคลที่ทำการรวบรวม วัตถุประสงค์ทางธุรกิจหรือเชิงพาณิชย์เพื่อรวบรวมหรือเพื่อขายข้อมูล และ หมวดหมู่ของบุคคลที่สามที่ผู้ประกอบธุรกิจได้แบ่งปันข้อมูล

โดย CCPAได้มีคำนิยามที่เกี่ยวกับข้อมูลส่วนบุคคลเอาไว้ดังนี้

1798.140.(1) "ข้อมูลส่วนบุคคล" หมายถึง ข้อมูลที่มีความเกี่ยวข้องกับผู้บริโภคไม่ว่าจะเป็นทางตรงหรือทางอ้อมรวมถึงครัวเรือน แต่ไม่จำกัดเฉพาะสิ่งต่อไปนี้ หากเป็นการระบุตัวตน มีการเกี่ยวข้อง มีการอธิบาย ถือว่าอาจมีการเชื่อมโยง หรืออาจมีการเชื่อมโยงอย่างสมเหตุสมผลทั้งโดยทางตรงและทางอ้อมกับผู้อยู่อาศัยหรือครัวเรือน[170]

---

[168] จาก California Consumer Privacy Act Guide, *อ้างแล้วเชิงอรรถที่ 165* (น.10).

[169] จาก California Consumer Privacy Act Guide, *อ้างแล้วเชิงอรรถที่ 165* (น.11).

[170] TITLE 1.81.5. California Consumer Privacy Act of 2018

1798.140.(1) "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not

1798.140.(2) “ข้อมูลส่วนบุคคล” ไม่รวมถึงข้อมูลที่เปิดเผยต่อสาธารณะ เพื่อจุดประสงค์ของวรรคนี้ “การเปิดเผยต่อสาธารณชน” หมายถึงข้อมูลที่จัดทำบันทึกโดยชอบด้วยกฎหมายของรัฐบาลกลางรัฐหรือท้องถิ่น “การเผยแพร่ต่อสาธารณชน”ไม่ได้หมายความถึง ข้อมูลไบโอเมตริกซ์(biometric) เกี่ยวกับผู้บริโภคที่ทำการเก็บรวบรวมโดยผู้ประกอบธุรกิจที่ปราศจากความรู้ของผู้บริโภค[171]

1798.140.(3) “ข้อมูลส่วนบุคคล” ไม่รวมถึงข้อมูลผู้บริโภคที่ไม่ปรากฏ หรือรวบรวมข้อมูลผู้บริโภคไว้[172]

1798.140. (q) “การประมวลผล” หมายถึง การดำเนินการหรือชุดการดำเนินการใด ๆ ที่ดำเนินการกับข้อมูลส่วนบุคคลหรือชุดข้อมูลส่วนบุคคลไม่ว่าจะด้วยวิธีอัตโนมัติหรือไม่ก็ตาม[173]

3.3.2 หลักการจัดทำและการบันทึกรายการ

จากการศึกษาหลักการจัดทำและเก็บรักษาบันทึกรายการ ทำให้ทราบว่าหลักการดังกล่าวอยู่ภายใต้หลักการพื้นฐานของหลักความโปร่งใส และหลักความรับผิดชอบ อย่างไรก็ดี

---

limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household.”

[171] TITLE 1.81.5. California Consumer Privacy Act of 2018

1798.140.(2) “Personal information” does not include publicly available information. For purposes of this paragraph, “publicly available” means information that is lawfully made available from federal, state, or local government records. “Publicly available” does not mean biometric information collected by a business about a consumer without the consumer’s knowledge.”

[172] TITLE 1.81.5. California Consumer Privacy Act of 2018

1798.140. (o) (3) “Personal information” does not include consumer information that is deidentified or aggregate consumer information.”

[173] 1798.140. (q) “Processing means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means.”

ประเทศสหรัฐอเมริกาแม้ไม่มีกฎหมายกลางสำหรับคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป แต่มีการให้ความคุ้มครองข้อมูลส่วนบุคคลอยู่ในกฎหมายเฉพาะเรื่อง การคุ้มครองข้อมูลส่วนบุคคลเฉพาะเรื่องจึงคำนึงถึงเฉพาะหลักการของกฎหมายในเรื่องนั้น ๆ ไม่จำต้องคำนึงถึงหลักการพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคล แต่เมื่อศึกษากฎหมายในระดับสหพันรัฐและมลรัฐแล้วพบกฎหมายที่เกี่ยวข้องกับหลักการจัดทำและบันทึกรายการดังต่อไปนี้

1) กฎหมายคุ้มครองความเป็นส่วนตัว The Privacy Act 1974 เป็นกฎหมายในระดับสหพันรัฐ ซึ่งกฎหมายฉบับนี้มุ่งคุ้มครองการบันทึกข้อมูล (Record) ที่ทำการจัดเก็บรักษาโดยหน่วยงานของรัฐ ไม่รวมถึงข้อมูลที่จัดเก็บโดยเอกชน มีการกำหนดหลักเกณฑ์เกี่ยวกับการรักษาการเก็บรวบรวม การใช้ หรือการเผยแพร่ข้อมูลส่วนบุคคล ซึ่งนำมาบังคับใช้แก่หน่วยงานของรัฐ คือ หน่วยงานด้านการบริหาร หน่วยงานทางทหาร รัฐวิสาหกิจ บริษัทที่รัฐบาลมีอำนาจในควบคุม หน่วยงานของรัฐที่มีหน้าที่ดูแลระบบบันทึกต้องยินยอมให้เจ้าของข้อมูลเข้าถึงข้อมูลของตน โดยเจ้าของข้อมูลสามารถตรวจสอบความถูกต้องและขอสำเนาข้อมูลส่วนบุคคลของตนได้หากพบว่าข้อมูลไม่ถูกต้องสามารถที่จะขอแก้ไขข้อมูลได้ เมื่อมีคำขอแก้ไขข้อมูลแล้วหน่วยงานของรัฐจะต้องพิจารณาและตอบรับคำร้องขอของเจ้าของข้อมูลภายใน 10 วันทำการ หากหน่วยงานของรัฐปฏิเสธคำขอหน่วยงานของรัฐต้องแจ้งเหตุผลในการปฏิเสธและแจ้งหน่วยงานที่เจ้าของข้อมูลสามารถอุทธรณ์คำสั่งได้[174]

แต่กฎหมายฉบับนี้ไม่ได้ระบุเอาไว้โดยตรงว่ารายละเอียดของรายการที่ผู้ควบคุมต้องทำบันทึกนั้นมีอะไรบ้าง เพียงแต่บอกว่าหากหน่วยงานของรัฐเปิดเผยข้อมูลส่วนบุคคลแล้วหน่วยงานของรัฐมีหน้าที่ต้องทำรายงานข้อมูลเกี่ยวกับวันเวลา บุคคลที่ได้รับการเปิดเผยข้อมูล ข้อมูลเกี่ยวกับการติดต่อ หรือ องค์กรที่ได้รับข้อมูลส่วนบุคคลนั้นโดยต้องเก็บรายงานดังกล่าวเป็นเวลา 5 ปี หรือ ตลอดอายุของบันทึกระยะเวลาใดจะยาวให้ถือระยะเวลานั้น ซึ่งหากเจ้าของข้อมูลร้องขอหน่วยงานของรัฐต้องเปิดเผยรายงานนี้แก่เจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นการเปิดเผยเพื่อการบังคับตามกฎหมาย[175] และกฎหมายคุ้มครองความเป็นส่วนตัว The Privacy Act 1974 มีการบัญญัติความหมายของการบันทึกเอาไว้ได้ดังนี้

---

[174] จาก อธิพร สิทธิธีรรัตน์, *อ้างแล้วเชิงอรรถที่ 152* (น.60).

[175] จาก อธิพร สิทธิธีรรัตน์, *อ้างแล้วเชิงอรรถที่ 152* (น.60).

U.S.C.§ 552a.(a)(4) “บันทึก” หมายถึง รายการใด ๆ ที่ทำการรวบรวมหรือการจัดกลุ่มของข้อมูลเกี่ยวกับบุคคลที่ถูกเก็บรักษาโดยหน่วยงานของรัฐ ทั้งนี้ให้รวมไปถึง, การศึกษา การทำธุรกรรมทางการเงิน ประวัติทางการแพทย์ ประวัติอาชญากรรม หรือ การจ้างงานและที่มีชื่อ หรือ หมายเลขประชาชน สัญลักษณ์ หรือ การระบุอื่นใดที่สามารถระบุถึงตัวบุคคลนั้นได้ เช่นลายพิมพ์นิ้วมือหรือลายพิมพ์พิมพ์เสียงหรือภาพถ่าย[176]

5 U.S.C.§ 552a.(a)(5) คำว่า "ระบบของบันทึก" หมายถึง กลุ่มของบันทึกใด ๆ ที่อยู่ภายใต้การควบคุมของหน่วยงานของรัฐ ที่ข้อมูลนั้นถูกเรียกคืนด้วยชื่อของบุคคลหรือเลขบัตรประชาชนหรือสิ่งอื่นใดที่ระบุถึงตัวบุคคลนั้น[177]

5 U.S.C.§ 552a.(a)(6) คำว่า “บันทึกสถิติ” หมายถึง การบันทึกในระบบบันทึกที่เก็บรักษาไว้เพื่อการวิจัยทางสถิติหรือเพื่อวัตถุประสงค์ในการทำรายงานเท่านั้นและการบันทึกสถิติหรือรายงานต่าง ๆ ทั้งนี้บันทึกดังกล่าวจะไม่นำมาใช้ประกอบในการตัดสินใจที่เกี่ยวกับลักษณะของบุคคลไม่ว่าทั้งหมดหรือบางส่วน เว้นแต่ตามที่บัญญัติไว้ในมาตรา 8 ของลักษณะที่ 13 นี้[178]

---

[176] The Privacy Act of 1974 5 U.S.C.§ 552a.(a) (4)the term record means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

[177]The Privacy Act of 1974 5 U.S.C.§ 552a.(a)(5) the term “system of records” means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

[178] The Privacy Act of 1974 5 U.S.C.§ 552a.(a)(6) the term statistical record means a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of Title 13.

นอกจากนี้ สำนักงาน Office of Management and Budget (OMB) ซึ่งเป็นหน่วยงานที่มีหน้าที่สำคัญเกี่ยวกับการอธิบายแนวทางและข้อปฏิบัติของหน่วยงานราชการเกี่ยวกับการบังคับใช้บทบัญญัติของ Privacy Act ก็ได้วางแนวทางเอาไว้ว่า “บันทึกข้อมูลส่วนบุคคล”นั้นหมายถึง การบันทึกข้อมูลข่าวสารใด ๆเกี่ยวกับบุคคล ซึ่งประกอบด้วยลักษณะเฉพาะอันสามารถแสดงถึงบุคคลใดบุคคลหนึ่งได้ ซึ่งสอดคล้องกับกฎเกณฑ์ที่ศาลเขตอำนาจ D.C. (D.C. Circuit) ได้กำหนดเอาไว้ว่า บันทึกข้อมูลส่วนบุคคลจะต้องประกอบไปด้วยชื่อของบุคคลนั้น หรือลักษณะเฉพาะประการอื่นและศาลอุทธรณ์เขตอำนาจที่3 (Third Circuit) ได้ตัดสินไว้ในคดี Quinn *v.* Stone (3d Cir. 1992) ซึ่งสอดคล้องกับแนวทางของสำนักงาน Office of Management and Budget (OMB) ว่า บันทึกข้อมูลส่วนบุคคลประกอบด้วยข้อมูลข่าวสารใด ๆเกี่ยวกับบุคคลซึ่งเกี่ยวโยงกับลักษณะของบุคคล และไม่จำกัดว่าข้อมูลข่าวสารนั้นจะต้องแสดงโดยตรงถึงบุคลิกลักษณะ (Characteristic) หรือคุณสมบัติ (Quality) ของบุคคล ดังนั้น ที่อยู่ซึ่งไม่เป็นปัจจุบันที่ได้ลงไว้ในบัญชีรายชื่อและสมุดบันทึกเวลาทำงาน เป็นบันทึกข้อมูลส่วนบุคคลซึ่งอยู่ในบังคับของ Privacy Act[179]

ในคดี Henk *v.* United States Dep’t of Commerce (D.D.C. Aug. 19, 1994) ศาลได้วินิจฉัยทำนองเดียวกันว่ารายชื่อของผู้เขียนบทวิจารณ์หนังสือ (reviewer) ซึ่งอนุญาตให้บทความของผู้เสนบทความลงพิมพ์ได้เป็นบันทึกข้อมูลส่วนบุคคลของผู้เสนอบทความ[180]

ในคดี Reuber *v.* United States (D.C.Cir.1987) ศาลวินิจฉัยว่าหนังสือกล่าวโทษ (letter reprimanding) ส่งไปยังหน่วยงานราชการและถูกเปิดเผย เป็นบันทึกข้อมูลส่วนบุคคล (record) เนื่องจากมีการแสดงอย่างชัดเจนถึงชื่อและที่อยู่ของผู้กล่าวโทษ หรือในคดี Robinson *v.*United States Dep’t of Educ. (E.D. Pa. Jan. 20 ,1988) หนังสืออธิบายถึงคำร้องทุกข์ในทางปกครอง ไม่ใช่บันทึกข้อมูลส่วนบุคคล เนื่องจากไม่ได้มีการกล่าวอ้างถึง ชื่อ ของผู้ร้องทุกข์[181]

---

[179] จาก สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, *อ้างแล้วเชิงอรรถที่ 38* (น.13-14).

[180] จาก สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, *อ้างแล้วเชิงอรรถที่ 38* (น.14).

[181] จาก สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, *อ้างแล้วเชิงอรรถที่ 38* (น.13).

จากความหมายของ “บันทึกข้อมูลส่วนบุคคล” ที่กล่าวมา จะเห็นได้ว่ามีขอบเขตค่อนข้างกว้างขวาง แต่อย่างไรก็ตามในแนวทางปฏิบัติของอีกหลายๆศาล จะตีความจำกัดขอบเขตของคำว่า “Record” ให้แคบลง ยกตัวอย่างเช่น ในคดี Tobey *v.* NLRB (D.C. Cir. 1994) ศาลได้กล่าวว่า “ข้อเท็จจริงอันเป็นข้อมูลข่าวสารซึ่งระบุชื่อของบุคคลใด ไม่ได้หมายความว่าข้อมูลข่างสารนั้นจะเป็นเรื่องเกี่ยวกับบุคคลนั้นเสมอไป กล่าวคือ Privacy Act คุ้มครองเฉพาะข้อมูลข่าวสารซึ่งบรรยายอย่างแท้จริง (Actually Describes) ถึงบุคคลนั้นในทางใดทางหนึ่ง ดังนั้น พนักงานของ NLRB จึงสามารถใช้ข้อมูลจากระบบคอมพิวเตอร์ในการรวบรวมกับข้อมูลอื่น ๆเพื่อที่จะเขียนข้อสรุป เกี่ยวกับลักษณะการปฏิบัติงานของพนักงานผู้เป็นโจทก์ได้ หรือในคดี Blair *v.* United States Forest Serv (D.Alaska Sept. 24, 1985) ศาลวินิจฉัยว่าแผนดำเนินงานฉบับสมบูรณ์ซึ่งจัดทำโดยโจทก์ไม่ใช่บันทึกข้อมูลส่วนบุคคลของโจทก์เนื่องจากไม่ได้มีการแสดงให้เห็นถึงสิ่งใดเกี่ยวกับธุรกิจส่วนตัวของโจทก์หรือในคดี Ingerman *v.* IRS (D.N.J. Apr.3 ,1991) ซึ่งศาลได้ตีความคำว่าบันทึกข้อมูลส่วนบุคคล (record) ค่อนข้างแคบว่า หมายเลขประกันสังคม (Social Security Number) จะต้องระบุชื่อ หมายเลขประจำตัว หรือ ลักษณะบ่งชี้เฉพาะอย่างอื่นจึงจะเป็นการบันทึกข้อมูลส่วนบุคคล “Record” ซึ่งอยู่ในบังคับของPrivacy Act เป็นต้น[182]

2) พระราชบัญญัติคุ้มครองความเป็นส่วนตัวของผู้บริโภคแคลิฟอร์เนีย (California Consumer Privacy Act หรือ CCPA) เป็นกฎหมายในระดับมลรัฐ ที่ให้ความคุ้มครองเกี่ยวกับข้อมูลส่วนบุคคลที่ก้าวหน้าที่สุดของประเทศสหรัฐอเมริกา ประกาศใช้ในปี 2561 และมีผลบังคับใช้ในวันที่ 1 มกราคม 2563 โดยกฎหมายฉบับนี้เป็นหลักประกันสิทธิความเป็นอยู่ส่วนตัวฉบับใหม่ของผู้บริโภคในแคลิฟอร์เนีย แต่ยังคงให้ความคุ้มครองที่จำกัดเฉพาะการเก็บรวบรวมและการขายข้อมูลของผู้บริโภคเท่านั้น[183] ไม่มีการบัญญัติถึงรายละเอียดของรายการที่ผู้ควบคุมซึ่งเป็นผู้ประกอบธุรกิจหรือผู้ให้บริการต้องทำการบันทึกเอาไว้ ดังนั้นการที่ผู้ประกอบธุรกิจหรือผู้ให้บริการดำเนินกิจกรรมต่าง ๆ เช่นการใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลของลูกค้าโดยไม่ได้จัดทำและเก็บรักษาบันทึกกิจกรรมในการใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น ย่อมไม่มีความผิดตาม CCPA

---

[182]จาก สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, *อ้างแล้วเชิงอรรถที่ 38* (น.14).

[183]From *California Consumer Privacy Act (CCPA),* 2019. Retrieved https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf

อย่างไรก็ตามข้อกำหนดในส่วนที่ให้ผู้ประกอบธุรกิจหรือผู้ให้บริการต้องจัดให้มีขั้นตอนในการร้องขอเพื่อการใช้สิทธิของผู้บริโภคที่เกี่ยวกับการขอยกเลิกความยินยอม (Opt-out) การใช้สิทธิเข้าถึงข้อมูลส่วนบุคคล หรือการใช้สิทธิขอให้ลบข้อมูลส่วนบุคคล ได้มีการเสนอแนะให้ร่างเป็นกฎระเบียบโดยให้ผู้ประกอบธุรกิจหรือผู้ให้บริการควรจัดเก็บรักษาบันทึกคำร้องขอดังกล่าวและการปฏิบัติตามคำร้องไว้เป็นเวลาอย่างน้อย 24 เดือน เพื่อที่จะเป็นหลักฐานในการตรวจสอบถึงการปฏิบัติตามกฎหมาย[184]

3.4 ประเทศสาธารณรัฐสิงคโปร์

ประเทศสาธารณรัฐสิงคโปร์ หรือเรียกสั้น ๆ ว่าสิงคโปร์ มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลไว้โดยเฉพาะคือ พระราชบัญญัติความคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2012 (Personal Data Protection Act 2012) ซึ่งตราขึ้นเพื่อกำกับดูแลองค์กรต่าง ๆ ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล และเพื่อก่อตั้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Commission) โดยคำนึงถึงสิทธิของบุคคลในการปกป้องข้อมูลของตน และความจำเป็นในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลตามวัตถุประสงค์ที่วิญญูชน(Reasonable Persons) พึงพิจารณาว่าเหมาะสม โดยจะศึกษาหลักการคุ้มครองและการจัดทำและบันทึกรายการดังนี้

3.4.1 หลักการคุ้มครองข้อมูลส่วนบุคคล

มาตรา 4 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2012 ได้กำหนดขอบเขตของกฎหมายซึ่งมีการกล่าวถึงกฎเกณฑ์ทั่วไปเกี่ยวกับการคุ้มครอง การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลจะไม่บังคับใช้กับบุคคลทั่วไปที่กระทำไปตามความสามารถเฉพาะบุคคลนั้น ไม่ได้เป็นไปในนามขององค์กร รวมถึงลูกจ้างขององค์กร ตัวแทนขององค์กร และไม่บังคับใช้กับองค์กรที่ตั้งขึ้นมาเพื่อวัตถุประสงค์ของการใช้กฎหมายนี้ และไม่บังคับใช้กับข้อมูลส่วนบุคคลที่ถูกเก็บไว้อย่างน้อย 100 ปี หรือกับผู้ที่เสียชีวิตแล้ว ยกเว้นหลักการเกี่ยวกับการเปิดเผยข้อมูลจะบังคับใช้กับผู้

[184]จาก California Consumer Privacy Act (CCPA), *อ้างแล้วเชิงอรรถที่ 183.*

ที่เสียชีวิตแล้ว 10 ปี หรือต่ำกว่านั้น ทั้งยังไม่บังคับใช้กับข้อมูลติดต่อเชิงธุรกิจเว้นแต่จะมีจะมีการระบุไว้อย่างชัดแจ้ง[185]

กฎหมายคุ้มครองข้อมูลส่วนบุคคลให้คำนิยามของ ข้อมูลส่วนบุคคล(Personal Data) หมายถึง ข้อมูลไม่ว่าจริงหรือเท็จเกี่ยวกับบุคคลซึ่งสามารถระบุได้จากข้อมูลนั้น หรือจากข้อมูลและข่าวสารอื่นใดซึ่งเอกชนเข้าถึงหรืออาจเข้าถึงได้[186]

การประมวลผล(Processing) หมายถึง วิธีดำเนินการตามขั้นตอนอย่างหนึ่งอย่างใดที่เกี่ยวข้องกับข้อมูลส่วนบุคคล และรวมถึงการบันทึก การครอบครอง การจัดระเบียบองค์กร การดัดแปลงหรือเปลี่ยนแปลง การแก้ไข การรวบรวม การโอน การลบหรือทำลายข้อมูลส่วนบุคคล[187]

ผู้ควบคุม อยู่ในรูปแบบขององค์กรซึ่งมีบทนิยามว่า องค์กร(Organization) หมายความรวมถึงบุคคลใด ๆ บริษัท สมาคม หรือแผนกบุคคลขององค์กรหรือหน่วยงานไม่ว่าจะมีรูปแบบหรือ

---

[185] จาก สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, *อ้างแล้วเชิงอรรถที่ 17* (น.56).

[186] Personal Data Protection Act 2012 Section 2 personal data" means data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the organization has or is likely to have access.

[187] Personal Data Protection Act 2012 Section 2 processing", in relation to personal data, means the carrying out of any operation or set of operation in relation to the personal data, and includes any of the following:

(a)recording;

(b)holding;

(c)organization, adaptation or alteration;

(d)retrieval;

(e)combination;

(f)transmission;

(g)erasure or destruction.

เป็นที่ยอมรับตามกฎหมายของสิงคโปร์หรือไม่ หรือไม่ว่าจะเป็นผู้อยู่อาศัยหรือมีสำนักงานหรือสถานประกอบธุรกิจในสิงคโปร์หรือไม่[188]

สำหรับหลักการสำคัญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเนื่องจากวิจัยฉบับนี้ให้ความสำคัญกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปที่ถือเป็นกฎหมายฉบับที่มีความก้าวหน้าในการให้ความคุ้มคราองแก่ข้อมูลส่วนบุคคลมากที่สุดฉบับหนึ่งเมื่อนำหลักการพื้นฐานตาม GDPR มาเปรียบเทียบกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสิงคโปร์แล้วปรากฏว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์มีหลักการพื้นฐานสำคัญทางกฎหมายที่มีลักษณะคล้ายคลึงกัน ดังต่อไปนี้

1) หลักการจำกัดวัตถุประสงค์ (Limitation of Purpose)[189] เป็นหลักที่จำกัดสิทธิขององค์กรในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลให้อยู่ภายใต้กรอบวัตถุประสงค์ที่วิญญูชน (Reasonable Person) พึงคาดหมายได้ โดยกำหนดให้องค์กรแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลนั้น

ในกรณีที่องค์กรเก็บรวบรวมข้อมูลส่วนบุคคลมาจากองค์กรอื่นโดยปราศจากความยินยอม องค์กรที่เก็บรวบรวมต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นให้เจ้าของข้อมูลทราบก่อนหรือในขณะทำการเก็บรวบรวม และวัตถุประสงค์ของการเก็บรวบรวมขององค์กรอื่นจะต้องอนุญาตให้เปิดเผยข้อมูลนั้นได้ด้วย

2) หลักความถูกต้องของข้อมูลส่วนบุคคล (Correction of Personal Data)[190] เป็นหลักการที่กำหนดให้องค์กรซึ่งเก็บรวบรวมข้อมูลส่วนบุคคลไว้และมีแนวโน้มที่จะใช้ข้อมูลส่วน

---

[188] Personal Data Protection Act 2012, Section 2“organisation” includes any individual, company, association or body of persons, corporate or unincorporated, whether or not (a)formed or recognized under the law of Singapore; or (b) resident, or having an office or a place of business, in Singapore;

[189] Personal Data Protection Act 2012 Section 18 to 20

[190] Personal Data Protection Act 2012 Section 22, 23

บุคคลในลักษณะที่อาจกระทบต่อบุคคลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลนั้น หรือมีแนวโน้มว่าองค์กรจะเปิดเผยข้อมูลส่วนบุคคลต่อองค์กรอื่น องค์กรนั้นจะต้องดำเนินการให้ข้อมูลส่วนบุคคลมีความถูกต้องและสมบูรณ์อยู่เสมอ ตามหลักความถูกต้องของข้อมูลส่วนบุคคลยังให้สิทธิแก่เจ้าของข้อมูลที่จะเรียกร้องให้องค์กรแก้ไขความผิดพลาดเกี่ยวกับข้อมูลส่วนบุคคลที่อยู่ในความครอบครองหรือภายใต้การควบคุมดูแลอีกด้วย

3) หลักการจำกัดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล (Retention of Personal Data)[191] เป็นหลักที่เรียกร้องให้องค์กรต้องหยุดการเก็บข้อมูลหรือนำข้อมูลนั้นออกเมื่อวัตถุประสงค์ของการเก็บข้อมูลนั้นไม่มีอยู่ต่อไป หรือการเก็บข้อมูลนั้นไม่จำเป็นอีกต่อไปสำหรับวัตถุประสงค์ทางธุรกิจหรือตามกฎหมาย

4) หลักความปลอดภัยของข้อมูลส่วนบุคคล (Protection of Personal Data)[192] เป็นหลักที่กำหนดให้องค์กรต้องให้ความคุ้มครองแก่ข้อมูลส่วนบุคคลที่อยู่ในความครอบครองหรือการควบคุมโดยจัดทำมาตรการรักษาความปลอดภัยที่เหมาะสมเพื่อป้องกันการเข้าถึง เก็บรวบรวม ใช้ เปิดเผย ทำสำเนา แก้ไขเปลี่ยนแปลง หรือทำลายข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

5) หลักความรับผิดชอบ (Accountability) เป็นหลักการที่มีวัตถุประสงค์เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลเกิดแนวทางปฏิบัติอย่างเป็นรูปธรรม มาตรา 11 จึงกำหนดให้แต่ละองค์กรจะต้องรับผิดชอบต่อข้อมูลส่วนบุคคลซึ่งอยู่ในความครอบครองหรือภายใต้การกำกับดูแลและต้องแต่งตั้งบุคคลหรือคณะบุคคลขึ้นมาทำหน้าที่ตรวจสอบการปฏิบัติตามกฎหมายฉบับนี้ อย่างไรก็ตามการแต่งตั้งบุคคลดังกล่าวไม่ทำให้องค์กรหมดความรับผิดชอบที่มีต่อข้อมูลส่วนบุคคลซึ่งตนได้ตรอบครองหรือกำกับดูแล

นอกจากนี้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2012 ได้กำหนดหลักการห้ามโทร (Do-Not-Call : DNC) ไว้ด้วย ซึ่งถือเป็นหลักการที่แตกต่างจากกรอบการคุ้มครองข้อมูลส่วนบุคคลฉบับอื่น ๆ โดยหลักการนี้จะห้ามการส่งข้อความทางการตลาดให้แก่บุคคลทั่วไปที่ได้

---

[191] Personal Data Protection Act 2012 Section 25

[192] Personal Data Protection Act 2012 Section 24

ลงทะเบียนไว้ไม่ว่าจะเป็นข้อความเสียง ข้อความตัวอักษร หรือโทรสาร เว้นแต่ได้รับความยินยอมที่ชัดแจ้งและไม่คลุมเครือจากบุคคลนั้น[193]

3.4.2 หลักการจัดทำและการบันทึกรายการ

หลักการจัดทำและเก็บรักษาข้อมูลเป็นหลักที่เกี่ยวข้องกับหน้าที่ทางเอกสาร (Document) ซึ่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2012 นิยามคำว่า “เอกสาร” หมายความรวมถึงข้อมูลข่าวสารที่ถูกบันทึกไว้ไม่ว่าอยู่ในรูปแบบใด[194]

โดยองค์กรต้องเก็บรักษาบันทึกความเคลื่อนไหวของข้อมูลส่วนบุคคลไม่ว่าจะเป็นการใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นไว้อย่างน้อย 12 เดือน ทั้งนี้เพื่อรองรับสิทธิของเจ้าของข้อมูลหากมีการร้องขอเข้าถึงข้อมูลนั้น[195]

อย่างไรก็ตามการจัดทำและเก็บรักษาข้อมูลของบันทึกกิจกรรมการประมวลผลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสิงคโปร์ไม่ได้บัญญัติรายละเอียดไว้โดยตรง กฎหมายเพียงแต่กำหนดให้องค์กรซึ่งเปรียบเสมือนเป็นผู้ควบคุม หรือผู้ประมวลผลข้อมูล ทำเอกสารเป็นบันทึกในกรณีที่นำข้อมูลส่วนบุคคลที่อยู่ในความครอบครองหรือกำกับดูแลไปใช้ หรือเปิดเผยเท่านั้น เช่น มาตรา 50(4) [196] องค์กรต้องเก็บรักษาบันทึกที่เกี่ยวข้องกับการสอบสวน เป็น

---

[193] จาก การโอนข้อมูลส่วนบุคคลระหว่างประเทศ (น.164), โดย ณัชพงษ์ สำราญ, *วารสารนิติศาสตร์มหาวิทยาลัยนเรศวร, ปีที่11,* ฉบับที่1, 2561.

[194] Personal Data Protection Act 2012, Section 2 “document” includes information recorded in any form;

[195]From A guide to GDPR for companies in Singapore, by CMS Cameron McKenna Naborro Olswang LLP, 2017, Copyright 2017 by CMS Cameron McKenna Naborro Olswang LLP. Retrieved from https://cms.law/en/Media/Affiliates/Singapore/ Images/Publications /GDPR-guide-for-Singapore-companies

[196]Personal Data Protection Act 2012, Section 50 (4) “An organisation shall retain records relating to an investigation under this section for one year after the conclusion of the investigation or any longer period specified in writing by the Commission.”

ระยะเวลาหนึ่งปีหลังจากการสรุปผลการสอบสวนหรือระยะเวลาที่ยาวนานกว่าตามที่คณะกรรมการกำหนดเป็นลายลักษณ์อักษร

จากการศึกษากฎหมายที่เกี่ยวข้องกับหลักการคุ้มครองข้อมูลส่วนบุคคล และหลักการจัดทำบันทึกรายการ ของประเทศไทย สหราชอาณาจักร สหรัฐอเมริกา และ สาธารณะรัฐสิงค์โปร์ทำให้ผู้วิจัยพบว่าประเทศสหรัฐอเมริกาเป็นประเทศเดียวที่ยังไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป ซึ่งต่างจากกฎหมายของประเทศอื่น ๆ ที่มีกฎหมายแม่บทครอบคลุมหรือวางกฎเกณฑ์ในเรื่องของการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปไว้ นอกจากนี้ในแต่ละประเทศมีหลักการคุ้มครองข้อมูลส่วนบุคคลที่แตกต่างกันออกไปแต่มีสิ่งหนึ่งที่มีลักษณะคล้าย ๆกันก็คือก่อนทำการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลนั้น จะต้องมีการขอความยินยอมจากเจ้าของข้อมูลก่อนเสมอ ในส่วนของหน้าที่ในการจัดทำบันทึกรายการจากการศึกษาในบทที่2และบทที่3ซึ่งเป็นบทที่คาบเกี่ยวกันแล้วนั้นพบว่า หน้าที่ในการจัดทำบันทึกรายจะพบในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป มาตรา30 สหราชอาณาจักรมาตรา 61 และ ของไทยมาตรา 39 สำหรับในส่วนข้อยกเว้นที่ผู้ควบคุมไม่ต้องจัดทำบันทึกนั้นจะพบในกฎหมายของสหภาพยุโรปมาตรา 30(5) และของไทยตามมาตรา 39วรรคสาม เพื่อให้เกิดความเข้าใจมากยิ่งขึ้นจึงอาจสรุปได้จากตารางดังต่อไปนี้

ตารางที่ 3.1 ตารางเปรียบเทียบหน้าที่ของผู้ควบคุมที่ต้องจัดทำบันทึกรายการของประเทศไทยและต่างประเทศ

ประเทศที่ศึกษา	หน้าที่ในการจัดทำบันทึก	ข้อยกเว้นที่ไม่ต้องจัดทำบันทึก
สหภาพยุโรป GDPR	✓	✓
ไทย	✓	✓
สหราชอาณาจักร	✓	×
สหรัฐอเมริกา	×	×
สาธารณรัฐสิงค์โปร์	×	×

ตารางที่ 3.2 ตารางเปรียบเทียบรายการที่ผู้ควบคุมข้อมูลมีหน้าที่ต้องจัดทำบันทึกของประเทศไทยและต่างประเทศ

สหภาพยุโรป GDPR	สหราชอาณาจักร	ไทย
มาตรา 30(1)(a)	มาตรา 61(2)(1)	มาตรา 39(3)

ตารางที่ 3.2 ตารางเปรียบเทียบรายการที่ผู้ควบคุมข้อมูลมีหน้าที่ต้องจัดทำบันทึกของประเทศไทยและต่างประเทศ(ต่อ)

สหภาพยุโรป GDPR	สหราชอาณาจักร	ไทย
ชื่อและรายละเอียดการติดต่อของผู้ควบคุมข้อมูล	ชื่อและรายละเอียดการติดต่อของผู้ควบคุมข้อมูล	ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

ตารางที่ 3.3 ตารางเปรียบเทียบหลักเกณฑ์การยกเว้นที่ผู้ควบคุมข้อมูลไม่ต้องจัดทำบันทึกรายการของประเทศไทยและต่างประเทศ

สหภาพยุโรป	สหราชอาณาจักร	ไทย
มาตรา 30(5)	×	มาตรา 39วรรคสาม
ยกเว้นให้กับวิสาหกิจขนาดกลางและขนาดย่อม หรือองค์กรที่มีพนักงานน้อยกว่า 250 คน	×	อาจได้รับยกเว้นธุรกิจขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด

แม้กฎหมายจะมีการยกเว้นหน้าที่ให้กับผู้ควบคุมข้อมูลที่มีกิจการขนาดเล็กให้ไม่ต้องจัดทำบันทึกรายการเอาไว้แล้วดังที่ปรากฏในตารางที่ 3.3 ก็ตาม แต่หากเข้ากรณีใดกรณีหนึ่งที่กฎหมายกำหนดเอาไว้ผู้ควบคุมข้อมูลแม้จะเป็นกิจการขนาดเล็กก็ยังมีหน้าที่ต้องจัดทำบันทึกรายการอยู่ซึ่งข้อยกเว้นดังกล่าวจะพบในGDPRมาตรา 30และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทยมาตรา 39วรรคสามซึ่งมีการบัญญัติกฎหมายเอาไว้ในลักษณะที่เหมือนกันจะเห็นได้จากตารางดังต่อไปนี้

ตารางที่ 3.4 ตารางเปรียบเทียบความแตกต่างของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของ สหภาพยุโรป (GDPR) และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

GDPRมาตรา 30	มาตรา	ไทยมาตรา39วรรคสาม	มาตรา
1.เป็นการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูล	GDPR Recital 75	1.เป็นการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูล	×

ตารางที่ 3.4 ตารางเปรียบเทียบความแตกต่างของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของ สหภาพยุโรป (GDPR) และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (ต่อ)

GDPRมาตรา 30	มาตรา	ไทยมาตรา39วรรคสาม	มาตรา
2.มิใช่กิจการที่ประมวลผลที่เป็นครั้งคราว	GDPR Recital 75	2.มิใช่กิจการที่เก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว	×
3.การเก็บรวบรวมใช้หรือเปิดเผยข้อมูลตามมาตรา 26	✓	3.เป็นการประมวลผลข้อมูลส่วนบุคคลชนิดพิเศษตามมาตรา 9 (1) หรือเป็นข้อมูลส่วนบุคคลที่เกี่ยวกับประวัติอาชญากรรม ตามมาตรา 10	✓

บทที่ 4

วิเคราะห์ปัญหาเกี่ยวกับการจัดทำบันทึกตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

เนื่องมาจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญ หรือความเสียหายให้แก่เจ้าของข้อมูล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวมประเทศไทยจึงได้ตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยอาศัยอำนาจรัฐธรรมนูญพุทธศักราช2560 มาตรา 32 เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไปขึ้น

สำหรับวิจัยฉบับนี้จะทำการวิเคราะห์มาตรการตรวจสอบถึงการปฏิบัติตามวิธีการที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้ ในกรณีที่บุคคลใดกระทำการใด ๆ ต่อข้อมูลส่วนบุคคลโดยชอบด้วยกฎหมาย ไม่ว่าจะเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ให้มีหน้าที่ต้องจัดทำบันทึกรายการต่าง ๆ ตามที่กฎหมายกำหนด ซึ่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้บัญญัติไว้ในมาตรา 39 ให้ผู้ที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล หรือที่เรียกว่า “ผู้ควบคุม”ซึ่งเป็นผู้ประกอบกิจการ มีหน้าที่ต้องจัดทำบันทึกรายการ แต่จากการศึกษารายละเอียดของรายการต่าง ๆ ตามมาตรา 39 แล้วพบว่า รายละเอียดของรายการที่กฎหมายกำหนดไว้ให้ผู้ควบคุมที่เป็นผู้ประกอบกิจการต้องจัดทำบันทึกนั้น บางรายการมีรายละเอียดที่ซับซ้อน หรือไม่มีความจำเป็นต้องใช้เพื่อให้เจ้าของข้อมูลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตรวจสอบ นอกจากนี้ เมื่อศึกษาต่อมาในส่วนที่ยกเว้นให้ผู้ควบคุมไม่ต้องจัดทำบันทึก ตามมาตรา 39 วรรคสาม พบว่า หลักเกณฑ์อันเป็นเงื่อนไขที่จะทำให้ผู้ควบคุมได้รับประโยชน์จากการไม่ต้องจัดทำบันทึกนั้นไม่มีความชัดเจนจนไม่อาจทราบได้อย่างแน่ชัดว่ากรณีใดบ้างที่ผู้ควบคุมจะได้รับการยกเว้นให้ไม่ต้องจัดทำบันทึกรายการ ดังนั้น เพื่อให้ผู้ควบคุมที่เป็นผู้ประกอบกิจการจัดทำบันทึกเฉพาะรายละเอียดของรายการเท่าที่จำเป็น และเพื่อให้หลักเกณฑ์ที่จะยกเว้นหน้าที่การจัดทำบันทึกมีความชัดเจน ผู้วิจัยจึงได้แบ่งหัวข้อสำหรับการวิจัยออกเป็น การวิเคราะห์รายละเอียดที่จำเป็นต่อบันทึกรายการ และการวิเคราะห์หลักเกณฑ์ที่ใช้ยกเว้นหน้าที่จัดทำบันทึกรายการ โดยการศึกษาหลักเกณฑ์ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพ

ยุโรป ประเทศสหราชอาณาจักร ประเทศสหรัฐอเมริกา และประเทศสาธารณรัฐสิงคโปร์ ประกอบการวิจัย ซึ่งมีรายละเอียดดังต่อไปนี้

4.1 วิเคราะห์รายละเอียดที่จำเป็นต่อบันทึกรายการ

ในการกระทำใด ๆ ต่อข้อมูลส่วนบุคคล ไม่ว่าจะเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยหลักการกฎหมายกำหนดให้ต้องขอความยินยอม พร้อมทั้งแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลให้แก่เจ้าของข้อมูลทราบเสียก่อนดำเนินการใด ๆ ต่อไปตามวัตถุประสงค์ที่ได้แจ้งไว้ การกระทำต่อข้อมูลส่วนบุคคลนั้นถึงจะเป็นไปโดยชอบด้วยกฎหมาย ทั้งนี้เพื่อเป็นการแสดงความเคารพต่อสิทธิของบุคคลที่เป็นเจ้าของข้อมูลนั้น หากบุคคลใดฝ่าฝืนไม่ปฏิบัติตามที่กฎหมายจักต้องรับโทษทั้งทางแพ่ง ทางอาญา หรือทางปกครอง แล้วแต่กรณี อย่างไรก็ตามเพื่อให้การคุ้มครองสิทธิของเจ้าของข้อมูลมีประสิทธิภาพ การวางกลไก หรือมาตการในการตรวจสอบว่าผู้เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้มีการปฏิบัติตามที่กฎหมายกำหนดไว้ครบถ้วนแล้วจึงเป็นเรื่องที่สำคัญเทียบเท่ากับการบัญญัติกฎหมายเพื่อลงโทษผู้ละเมิดต่อสิทธิในข้อมูลส่วนบุคคล กลไกหรือมาตรการหนึ่งที่ใช้ในการตรวจสอบถึงการปฏิบัติตามกฎหมายก็คือการจัดทำบันทึก โดยการวางรูปแบบให้บันทึกมีรายละเอียดเท่าที่จำเป็นเพื่อให้เจ้าของข้อมูลและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบบันทึกดังกล่าวได้ แต่จากการศึกษารายละเอียดต่าง ๆ ของบันทึกที่บัญญัติไว้ตามมาตรา 39 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลแล้ว พบว่ามีรายละเอียดตามมาตรา 39(3) ที่ระบุให้บันทึก “ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล” มีรายละเอียดไม่มีความชัดเจน

เนื่องจากกฎหมายบัญญัติว่า ข้อมูลเกี่ยวกับผู้ควบคุม หากตีความจากตัวบทแล้วคำว่า “ข้อมูลที่เกี่ยวกับผู้ควบคุม” มีความหมายว่าต้องการข้อมูลทุกอย่างที่เกี่ยวกับผู้ควบคุม ย่อมมิได้หมายถึงชื่อ ที่อยู่ ของผู้ควบคุมเพียงอย่างเดียวซึ่งอาจเป็นข้อมูลที่มากกว่าชื่อและรายละเอียดในการติดต่อของผู้ควบคุมซึ่งไม่มีความจำเป็นสำหรับการบันทึกเช่น ข้อมูลเกี่ยวกับเลขบัญชีธนาคารของผู้ควบคุม จำนวนลูกจ้างของผู้ควบคุม ผลประกอบการก็นับว่าเป็นข้อมูลที่เกี่ยวกับผู้ควบคุมเช่นเดียวกัน แม้ข้อมูลบางอย่างจะเป็นข้อมูลที่ผู้ควบคุมซึ่งเป็นผู้ประกอบกิจการจะต้องเปิดเผยอยู่แล้ว แต่ก็ถือเป็นรายละเอียดที่ไม่มีความจำเป็นจะต้องบันทึกไว้ในรายการเพื่อให้เจ้าของข้อมูล หรือ

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตรวจสอบ เมื่อศึกษาจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปหรือ GDPR มาตรา 30(1)(a) และ สหราชอาณาจักรมาตรา 61(2)(1) พบว่ากฎหมายบัญญัติให้บันทึกรายละเอียดของผู้ควบคุมเพียงที่เป็น ชื่อ สถานที่ติดต่อ ของผู้ควบคุมเท่านั้น ย่อมเห็นเจตนารมณ์ได้ว่าเมื่อเจ้าของข้อมูลขอตรวจสอบบันทึกก็จะสามารถทราบว่าผู้ใดเป็นผู้ควบคุม และสามารถติดต่อผู้ควบคุมได้ เพื่อให้เจ้าของข้อมูลได้ดำเนินการใช้สิทธิตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้ต่อไป

จะเห็นได้ว่า กฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยมีความแตกต่างจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป และของสหราชอาณาจักรที่ได้มีการบัญญัติรายการที่เกี่ยวกับผู้ควบคุมเอาไว้โดยชัดเจน การที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยมาตรา 39(3) บัญญัติให้บันทึกข้อมูลเกี่ยวกับผู้ควบคุม ทำให้เกิดปัญหาในการตีความว่าผู้ควบคุมจะต้องให้รายละเอียดทั้งหมดของผู้ควบคุม หรือให้ข้อมูลใดก็ได้ที่เกี่ยวกับผู้ควบคุม ทั้งที่วัตถุประสงค์ในการจัดทำบันทึกก็เพื่อใช้ในการตรวจสอบ การบันทึกข้อมูลเกี่ยวกับผู้ควบคุมจึงควรเป็นข้อมูลที่ทำให้เจ้าของข้อมูลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถทราบถึงชื่อ ที่อยู่ หรือวิธีการติดต่อผู้ควบคุมเพื่อดำเนินการตรวจสอบรายละเอียดอื่น ๆ หรือเพื่อการใช้สิทธิตามกฎหมายต่อไป ดังนั้น ผู้วิจัยเห็นว่าควรแก้ไขมาตรา 39(3) ให้มีความชัดเจน โดยให้ผู้ควบคุมบันทึกรายละเอียดเพียงเท่าที่จำเป็นที่สามารถใช้ติดต่อกับผู้ควบคุมได้ซึ่งได้แก่ ที่อยู่ เบอร์โทรศัพท์ อีเมล เท่านั้น

4.2 วิเคราะห์หลักเกณฑ์ที่ใช้ยกเว้นหน้าที่จัดทำบันทึกรายการ

จากการศึกษามาแล้วในเรื่องการจัดทำบันทึก ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 39 โดยหลักการแล้วผู้ประกอบกิจการทุกรายที่เป็นผู้ควบคุมต้องจัดทำบันทึกรายการต่าง ๆตามมาตรา39 ที่มีรายละเอียดตามที่กฎหมายกำหนดไว้ สำหรับในทางปฏิบัติพบว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลมีรายละเอียดที่ซับซ้อน และเข้าใจยากทำให้ผู้ประกอบกิจการต้องจ้างผู้เชี่ยวชาญทั้งทางด้านวิศวกรและทางด้านกฎหมายเพื่อให้คำปรึกษาในการวางระบบก่อให้เกิดภาระค่าใช้จ่ายที่ค่อนข้างสูง ก่อให้เกิดปัญหาความเลื่อมล้ำกันระหว่างกิจการขนาดเล็กและกิจการขนาดใหญ่ในเรื่องของต้นทุนในการประกอบธุรกิจ โดยกิจการขนาดเล็กที่มีต้นทุนต่ำอาจไม่สามารถจ้างผู้เชี่ยวชาญเพื่อจัดการข้อมูลให้เป็นระบบได้ แม้กิจการขนาดเล็กจะสามารถจัดการข้อมูล

ให้เป็นระบบได้ด้วยตัวเองก็ตาม แต่ก็ต้องรับมือกับความเสี่ยงที่ระบบอาจเกิดความผิดพลาดและต้องถือว่ากิจการนั้นไม่ได้ปฏิบัติตามหลักเกณฑ์ที่กฎหมายกำหนดจนถูกปรับ ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลก็ได้กำหนดอัตราโทษปรับไว้ค่อนข้างสูงอาจทำให้กิจการขนาดเล็กที่ต้องโทษปรับต้องปิดกิจการสร้างผลกระทบต่อเศรษฐกิจอย่างกว้างขวาง ดังนั้นมาตรา 39 วรรคสาม แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงบัญญัติยกเว้นหน้าที่การจัดทำบันทึกให้แก่ผู้ควบคุมซึ่งเป็นกิจการขนาดเล็ก เพื่อบรรเทาผลกระทบที่อาจเกิดขึ้นกับระบบเศรษฐกิจ และเพื่อให้กิจการขนาดเล็กมีโอกาสในการแข่งขันทางการค้ากับกิจการขนาดใหญ่มากขึ้น

อย่างไรก็ตาม เมื่อได้ศึกษารายละเอียดของข้อยกเว้นหน้าที่ในการจัดทำบันทึกแล้ว ผู้วิจัยพบว่าเงื่อนไขที่ผู้ประกอบกิจการจะได้รับประโยชน์จากข้อยกเว้นมีความไม่ชัดเจนจนถึงขนาดที่ผู้ประกอบกิจการไม่อาจรับความเสี่ยงในการถือประโยชน์จากข้อยกเว้นได้ โดยมีรายละเอียดดังนี้

4.2.1 ปัญหาความไม่ชัดเจนเกี่ยวกับข้อยกเว้นการจัดทำบันทึก

ตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 39 วรรคสาม บัญญัติว่า “ความใน (1) (2) (3) (4) (5) (6) และ (8) อาจยกเว้นมิให้นำมาใช้บังคับกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด...”

เมื่อพิจารณาความใน (1) (2) (3) (4) (5) (6) และ (8) แล้ว เป็นเรื่องที่ผู้ควบคุมจะต้องบันทึกรายการที่มีรายละเอียดเกี่ยวกับ ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย ตลอดจนบันทึกการใช้หรือเปิดเผยข้อมูลส่วนบุคคลประเภทที่กฎหมายอนุญาตให้การเก็บรวบรวมข้อมูลส่วนบุคคลได้โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูล ซึ่งรายละเอียดของบันทึกรายการทั้งหลายเหล่านี้ มาตรา39วรรคสาม บัญญัติว่า “...อาจยกเว้นมิให้นำมาใช้บังคับกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด...” ซึ่งคำว่าอาจทำให้เกิดความยืดหยุ่นและไม่ชัดเจนก่อให้เกิดปัญหาว่ากรณีใดที่ผู้ประกอบธรกิจที่มีกิจการขนาดเล็กจะได้รับการยกเว้นโดยไม่ต้องจัดทำบันทึกรายการหรือในกรณีที่ผู้ประกอบกิจการการขนาดเล็กไม่ต้องจัดทำบันทึกรายการ จะถือว่าเป็นการยกเว้นการ

จัดทำบันทึกทุกรายการทั้งหมดหรือบางส่วน จึงเป็นกรณีที่หลักเกณฑ์ของกฎหมายไม่มีความชัดเจน ทำให้ผู้ประกอบกิจการที่จะถือเอาประโยชน์จากข้อยกเว้นเกิดปัญหาในการตีความ ในขณะที่วัตถุประสงค์ของการยกเว้นหน้าที่ในการจัดทำบันทึกนั้นก็เพื่อช่วยเหลือกิจการขนาดเล็กให้ไม่ต้องแบกรับภาระค่าใช้จ่ายที่จะต้องจ้างวิศวกรเพื่อวางระบบข้อมูลและนักกฎหมายเพื่อให้คำปรึกษาและวางแนวปฏิบัติให้เป็นไปตามที่กฎหมายกำหนด ให้กิจการขนาดเล็กซึ่งมักมีทุนในการประกอบกิจการจำกัดสามารถค้าขายแข่งขันกับกิจการขนาดใหญ่ได้ ปัญหาดังกล่าวจึงเป็นความเสี่ยงที่ทำให้ผู้ประกอบกิจการขนาดเล็กไม่อาจถือเอาประโยชน์จากข้อยกเว้นเพื่อให้ตนไม่ต้องจัดทำบันทึกรายการได้ และเพื่อหลีกเลี่ยงความเสี่ยงก็จำเป็นที่จะต้องจัดทำบันทึกรายการตามที่กฎหมายกำหนด

เมื่อได้ศึกษากฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป หรือ GDPR ซึ่งเป็นกฎหมายที่ถือว่าเป็นแม่แบบของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย พบว่าแนวความคิดที่ยกเว้นหน้าที่ในการจัดทำบันทึกรายการตามมาตรา 39 วรรคสาม แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น มีหลักการเดียวกันกับมาตรา 30(5) แห่ง GDPR ซึ่งเรียกการจัดทำบันทึกรายการเป็น “การจัดทำบันทึกกิจกรรมการประมวลผล” (Records of processing activities) โดยมาตรา 30(5) บัญญัติว่า “หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 30(1) ที่ผู้ควบคุมมีหน้าที่ต้องเก็บรักษาบันทึกกิจกรรมการประมวลผล จะไม่บังคับใช้แก่กิจการหรือองค์กรที่มีจำนวนการจ้างงานน้อยกว่า 250 คน เว้นแต่การประมวลผลนั้นจะทำให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพแก่เจ้าของข้อมูล การประมวลผลนั้นไม่ได้เกิดขึ้นเป็นครั้งคราว หรือเป็นการประมวลผลข้อมูลชนิดพิเศษตามมาตรา 9(1) หรือข้อมูลส่วนบุคคลที่เกี่ยวข้องกับประวัติอาชญากรรมตามมาตรา 10”[197]

จะเห็นได้ว่าข้อยกเว้นตามมาตรา 30(5) แห่ง GDPR กำหนดกิจการหรือองค์กรที่ได้รับยกเว้นหน้าที่การจัดทำบันทึกกิจกรรมการประมวลผลไว้อย่างชัดเจนโดยใช้จำนวนการจ้างงานเป็นเกณฑ์ในการพิจารณากิจการที่ควรได้รับประโยชน์ให้ไม่ต้องจัดทำบันทึก ถ้ากิจการใดมีจำนวนการ

---

[197] GDPR Article 30 (5) The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

จ้างงานน้อยกว่า 250 คน กิจการนั้นย่อมได้รับการยกเว้นให้ไม่ต้องจัดทำบันทึกกิจกรรมการประมวลผล ทั้งปรากฏในคำปรารภ (Recital) ของ GDPR ข้อที่ 13 ว่า “เพื่อให้การคุ้มครองบุคคลสอดคล้องกันทั่วทั้งสหภาพยุโรป และป้องกันมิให้ความแตกต่างกันของกฎหมายไปขัดขวางเสรีภาพในการเคลื่อนไหวข้อมูลส่วนบุคคล จึงมีความจำเป็นที่จะต้องกำหนดความรับผิดเกี่ยวกับการเก็บรักษาบันทึกเป็นการเฉพาะแก่กิจการขนาดย่อมและองค์กรที่มีจำนวนการจ้างงานไม่เกิน 250 คน” ซึ่งคำปรารภดังกล่าวได้อ้างถึงข้อ 2 ในส่วนของภาคผนวกตามประกาศของคณะกรรมการแห่งประชาคมยุโรป (Commission of the European Community) เกี่ยวกับคำนิยามของกิจการขนาดย่อม (Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises) ซึ่งระบุว่า “จำนวนพนักงานและรายได้ต่อปีในการพิจารณาประเภทกิจการนั้น ถ้าเป็นกิจการขนาดย่อม ขนาดเล็ก และขนาดกลาง (SMEs) ซึ่งประกอบด้วยพนักงานไม่เกิน 250 คน และมีรายได้ต่อปีไม่เกิน 50 ล้านยูโร และหรือมีงบดุลประจำปีรวมไม่เกิน 43 ล้านยูโร ถ้าเป็น SMEs ประเภทกิจการขนาดเล็กกำหนดจำนวนพนักงานไม่เกิน 50 คน และมีรายได้ต่อปี และหรืองบดุลประจำปีรวมไม่เกิน 10 ล้านยูโร ถ้าเป็น SMEs ขนาดย่อมกำหนดจำนวนพนักงานไม่เกิน 10 คน และมีรายได้ประจำปี และหรืองบดุลประจำปีรวมไม่เกิน 2 ล้านยูโร”[198]

ในขณะที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดเกณฑ์ของกิจการที่จะได้รับยกเว้นไม่ต้องจัดทำบันทึกโดยใช้เกณฑ์ของ “กิจการขนาดเล็ก” ตามที่

---

[198] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (2003/361/EC)

Article 2

1. The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 milion, and/or an annual balance sheet total not exceeding EUR 43 million

2. Within the SME category, a small enterprise is defined as an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million.

3. Within the SME category, a microenterprise is defined as an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total dose not exceed EUR 2 million.

คณะกรรมการประกาศกำหนด จึงมีประเด็นที่ควรต้องวิเคราะห์ถึงความเหมาะสมของเกณฑ์ที่จะนำมาเป็นเงื่อนไขของกิจการขนาดเล็ก เมื่อศึกษาต่อไปพบว่าประเทศไทยมีกฎกระทรวงกำหนดลักษณะของวิสาหกิจขนากลางและขนาดย่อม พ.ศ. 2562 อันเป็นกฎหมายที่กำหนดขนาดของกิจการเช่นเดียวกับสหภาพยุโรป โดยในข้อ 2 กำหนดให้วิสาหกิจขนาดย่อม ได้แก่กิจการที่ผลิตสินค้าที่มีจำนวนการจ้างงานไม่เกินห้าสิบคนหรือมีรายได้ต่อปีไม่เกินหนึ่งร้อยล้านบาท หรือกิจการที่ให้บริการ กิจการค้าส่ง หรือกิจการค้าปลีก ที่มีจำนวนการจ้างงานไม่เกินสามสิบคนหรือมีรายได้ต่อปีไม่เกินห้าสิบล้านบาท และในข้อ 3 กำหนดให้วิสาหกิจขนาดกลาง ได้แก่กิจการที่ผลิตสินค้าที่มีจำนวนการจ้างงานเกินกว่าห้าสิบคนแต่ไม่เกินสองร้อยคนหรือมีรายได้ต่อปีเกินกว่าหนึ่งร้อยล้านบาทแต่ไม่เกินห้าร้อยล้านบาท หรือกิจการให้บริการ กิจการค้าส่ง หรือกิจการค้าปลีก ที่มีจำนวนการจ้างงานเกินกว่าสามสิบคนแต่ไม่เกินหนึ่งร้อยคนหรือมีรายได้ต่อปีเกินกว่าห้าสิบล้านบาทแต่ไม่เกินสามร้อยล้านบาท

เมื่อพิจารณาคำว่า “กิจการขนาดเล็ก” ตามมาตรา 39 วรรคสามแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กับกฎกระทรวงกำหนดลักษณะของวิสาหกิจขนาดกลางและขนาดย่อม พ.ศ. 2562 แล้ว กิจการขนาดเล็กอาจเทียบได้กับวิสาหกิจขนาดย่อมที่มีจำนวนการจ้างงานไม่เกินห้าสิบคนหรือมีรายได้ต่อปีไม่เกินหนึ่งร้อยล้านบาท แต่เมื่อพิจารณาประกอบกับข้อยกเว้นในมาตรา 30(5) แห่ง GDPR ที่กำหนดจำนวนการจ้างงานไม่เกิน 250 คน คำว่า “กิจการขนาดเล็ก” อาจเทียบได้วิสาหกิจขนานกลาง ตามข้อ 3 แห่งกฎกระทรวงฯ ซึ่งมีจำนวนการจ้างงานเกินกว่าห้าสิบคนแต่ไม่เกินสองร้อยคนหรือมีรายได้ต่อปีเกินกว่าหนึ่งร้อยล้านบาทแต่ไม่เกินห้าร้อยล้านบาท ดังนั้นจึงเป็นข้อที่น่าพิจารณาว่าหากคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนดลักษณะของกิจการขนาดเล็กโดยใช้เกณฑ์ของวิสาหกิจขนาดย่อม จะทำให้กิจการจากทางสหภาพยุโรปที่มีการจ้างงานไม่เกิน 250 คน เมื่อเข้ามาประกอบกิจการในประเทศไทยจะไม่ได้รับยกเว้นหน้าที่การจัดทำบันทึกรายการ แม้หน้าที่ในการจัดทำบันทึกรายการจะเป็นหน้าที่หนึ่งที่ผู้ประกอบกิจการพึงกระทำเพื่อให้เกิดการตรวจสอบถึงการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล แต่จากวัตถุประสงค์ของข้อยกเว้นการจัดทำบันทึกรายการที่ได้กล่าวไปแล้วว่า เพื่อให้กิจการขนาดเล็กสามารถค้าขายแข่งขันกับกิจการขนาดใหญ่ได้ ไม่ต้องแบกรับภาระค่าใช้จ่ายในการจัดทำระบบเพื่อจัดทำบันทึกรายการโดยเฉพาะเพื่อไม่ให้เป็นการเสียเปรียบเมื่อต้องแข่งขันทางการค้ากับผู้ประกอบกิจการจากสหภาพยุโรป ผู้วิจัยเห็นว่าควรที่จะใช้เกณฑ์ของวิสาหกิจขนาดกลางซึ่งกำหนดจำนวนการจ้างงานเกินกว่าห้าสิบคนแต่ไม่เกินสองร้อยคน มาเป็นเกณฑ์ในการพิจารณาคำว่า “กิจการขนาดเล็ก”

และเนื่องจากข้อยกเว้นดังกล่าวเป็นการยกเว้นให้ผู้ประกอบกิจการไม่ต้องจัดทำบันทึกรายการข้อมูลต่าง ๆ จึงควรยึดถือหลักเกณฑ์เฉพาะจำนวนของลูกจ้าง ไม่ควรพิจารณาถึงหลักเกณฑ์ของรายได้ต่อปีของกิจการเพราะรายได้ต่อปีของกิจการไม่ได้เป็นการวัดจำนวนปริมาณของข้อมูลและขนาดของกิจการควรขึ้นอยู่กับปริมาณข้อมูลที่กิจการนั้นจะได้รับเป็นหลัก เนื่องจากในการจ้างงานผู้ประกอบกิจการจำเป็นจะต้องเก็บข้อมูลส่วนบุคคลของลูกจ้างเช่น ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ บัญชีธนาคาร บุคคลอื่นที่สามารถติดต่อได้ ฯลฯ อย่างไรก็ตาม หลักเกณฑ์ที่กำหนดขนาดของกิจการที่จะได้รับยกเว้นหน้าที่ในการจัดทำบันทึกนั้น ปัจจุบันยังไม่มีประกาศของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงเป็นที่น่าสนใจว่าประกาศของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่จะออกมานั้นใช้หลักเกณฑ์ใดในการพิจารณาลักษณะของกิจการขนาดเล็ก

ข้อพิจารณาต่อมาเมื่อทราบถึงลักษณะของกิจการขนาดเล็กแล้ว กิจการนั้นก็ควรที่จะได้รับยกเว้นหน้าที่ในการจัดทำบันทึก แต่การที่กฎหมายของไทยบัญญัติว่า “ความใน (1) (2) (3) (4) (5) (6) และ (8) อาจยกเว้น...” ทั้งในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ฉบับแปลเป็นภาษาอังกฤษที่มีการรับรองแล้วนั้นบัญญัติว่า “The provision in (1),(2),(3),(4),(5),(6) and (8) may not apply…” ทำให้ไม่อาจสรุปได้ว่าเมื่อกิจการนั้นเป็นกิจการขนาดเล็กแล้วจะได้รับการยกเว้นให้ไม่ต้องจัดทำบันทึก เมื่อเปรียบเทียบกับ GDPR มาตรา 30(5) ซึ่งใช้คำว่า “shall not apply…” ซึ่งชัดเจนว่าหน้าที่ในการจัดทำบันทึกกิจกรรมการประมวลผล จะต้องไม่บังคับ ดังนั้นจึงเกิดปัญหาว่าเมื่อกิจการนั้นเป็นกิจการขนาดเล็กแล้วกรณีใดจะได้ประรับโยชน์ให้ไม่ต้องจัดทำบันทึก ถ้ากิจการนั้นถือเอาประโยชน์ไม่จัดทำบันทึกรายการก็จะเกิดความเสี่ยงที่จะได้รับโทษตามกฎหมายในอัตราโทษที่สูงถึง 1 ล้านบาท เพื่อหลีกเลี่ยงความเสี่ยงทำให้ผู้ประกอบกิจการเลือกที่จะไม่รับประโยชน์จากข้อยกเว้นนี้ และวัตถุประสงค์ของกฎหมายที่จะลดภาระให้แก่ผู้ประกอบกิจการที่มีกิจการขนาดเล็กก็จะคลาดเคลื่อนไป ผู้วิจัยเห็นว่าควรแก้ไขในส่วนของข้อยกเว้นตามมาตรา 39วรรคสามนี้ให้มีความชัดเจนขึ้น โดยเอาคำว่า “อาจ” ออกเป็น “ความใน (1) (2) (3) (4) (5) (6) และ (8) ยกเว้นมิให้นำมาใช้บังคับกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก...” จึงจะทำให้ผู้ประกอบกิจการได้รับประโยชน์จากข้อยกเว้นของกฎหมาย และมีความสามารถแข่งขันทางการค้ากับผู้ประกอบกิจการขนาดใหญ่ได้อย่างแท้จริง

4.2.2 ปัญหาความไม่ชัดเจนเกี่ยวกับข้อยกเว้นของข้อยกเว้น

ตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 39 วรรคสาม บัญญัติว่า .... “เว้นแต่มีการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล หรือ มิใช่กิจการที่เก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือ มีการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26” ซึ่งเป็นข้อยกเว้นของข้อยกเว้น กล่าวคือ แม้ผู้ควบคุมจะมีกิจการขนาดเล็กก็ตามถ้าเป็นการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของข้อมูล หรือ เป็นกิจการที่ที่เก็บรวบรวมใช้หรือเปิดเผยข้อมูลที่ไม่เป็นครั้งคราว หรือ เปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

ผู้ควบคุมก็ยังมีหน้าที่ต้องจัดทำบันทึกรายการตามมาตรา 39 เมื่อทำการพิจารณาจากข้อยกเว้นของข้อยกเว้นดังกล่าวแล้วก่อให้เกิดปัญหาว่าอะไรคือความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของข้อมูล และ การเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว เพราะกฎหมายไม่ได้กำหนดหลักเกณฑ์ที่เกี่ยวกับความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของข้อมูลและการเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราวเอาไว้ ทำให้เกิดช่องว่างของว่างของกฎหมายที่ไม่ชัดเจนส่งผลให้เกิดการตีความที่แตกต่างกันออกไปและผู้ประกอบกิจการไม่สามารถเข้าใจได้ว่าอะไรคือความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของข้อมูลและอะไรคือการเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราวเพราะไม่มีหลักเกณฑ์กำหนดเอา อาจทำให้ผู้ประกอบการปฏิบัติได้ไม่ถูกต้องส่งผลทำให้มีการละเมิดสิทธิของเจ้าของข้อมูลที่ไม่เป็นไปตามเจตนารมณ์ของกฎหมายคุ้มครองข้อมูลส่วนบุคคล

เมื่อได้ศึกษากฎหมายคุ้มครองของสหภาพยุโรป หรือ GDPR มาตรา 30 ซึ่งมีหลักการยกเว้นของข้อยกเว้นเช่นเดียวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แต่ GDPR มีการบัญญัติเอาไว้ชัดเจนเลยว่า “เว้นแต่มีการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่ประมวลผลข้อมูลส่วนบุคคลเป็นครั้งคราวหรือเป็นการประมวลผลข้อมูลส่วนบุคคลชนิดพิเศษตามมาตรา 9 (1) หรือเป็นข้อมูลส่วนบุคคลที่เกี่ยวกับประวัติอาชญากรรม ตามมาตรา 10” โดย GDPR มีการบัญญัติในส่วนของข้อยกเว้นของข้อยกเว้นที่เกี่ยวกับความเสี่ยงที่มีผลกระทบต่อสิทธิเสรีภาพของเจ้าของ

ข้อมูลเอาไว้ซึ่งมีหลักเกณฑ์ของคำปรารภ (Recital) ที่ 75 ว่า ความเสี่ยงต่อสิทธิเสรีภาพของของเจ้าของข้อมูล คือ ความเสี่ยงต่อสิทธิและเสรีภาพของบุคคลอันเป็นผลมาจากการประมวลผลข้อมูลส่วนบุคคลโดยเฉพาะการใช้ข้อมูลที่อาจเป็นผลเป็นการเลือกปฏิบัติทำให้เสี่ยงต่อการถูกขโมยข้อมูลหรือนำข้อมูลไปหลอกลวงผู้อื่นทำให้บุคคลอื่นเสียหายต่อชื่อเสียง ถูกเปิดเผยความลับที่ควรได้รับการคุ้มครอง มีการแปลงข้อมูลแฝงโดยไม่ได้รับอนุญาต ตลอดจนทำให้เกิดความเสียเปรียบทางสังคมหรือเศรษฐกิจ จนทำให้เจ้าของข้อมูลอาจจำกัดสิทธิเสรีภาพ หรือถูกขัดขวางมิให้เข้าถึงข้อมูลของตนอันเป็นข้อมูลเกี่ยวกับเชื้อชาติ หรือชาติกำเนิด (Ethnic Origin) การแสดงความเห็นทางการเมือง ศาสนา ปรัชญาความเชื่อ ความเป็นสมาชิกสหภาพแรงงาน ข้อมูลเกี่ยวกับพันธุกรรม สุขภาพ ประสบการณ์ทางเพศ (Sex Life) ตลอดจนประวัติอาชญากรรม หรือเกี่ยวกับมาตรการความปลอดภัยของบุคคล ซึ่งจะถูกนำมาประเมินผล เพื่อวิเคราะห์ หรือคาดการณ์แนวโน้มเกี่ยวกับประสิทธิภาพในการทำงาน สถานการณ์ทางเศรษฐกิจ สุขภาพ ความชอบหรือความสนใจ ความน่าเชื่อถือ หรือพฤติกรรม ตำแหน่งที่อยู่ หรือ การเคลื่อนไหว เพื่อที่จะสร้างหรือใช้แฟ้มข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลในกลุ่มที่เปราะบาง โดยเฉพาะเด็กหรือการประมวลผลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลจำนวนมากและมีผลต่อบุคคลจำนวนมากซึ่งเป็นเจ้าของข้อมูล

จะเห็นได้ว่าความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของข้อมูลตาม GDPR มีการบัญญัติเอาไว้ชัดเจนไม่ทำให้เกิดช่องว่างของกฎหมายที่จะเกิดการตีความได้หลายรูปแบบเป็นการสร้างหลักเกณฑ์และแนวทางให้กับผู้ควบคุมที่เป็นผู้ประกอบการได้ว่าอะไรคือความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของข้อมูลหากผู้ควบคุมได้ทำการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลที่เป็นความเสี่ยงกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลตามที่กฎหมายบัญญัติไว้ผู้ควบคุมก็มีหน้าที่ในการจัดทำบันทึกดังกล่าว ผู้วิจัยเห็นว่าควรมีการเพิ่มบทบัญญัติคำนิยามที่เกี่ยวกับความเสี่ยงที่ต่อสิทธิเสรีภาพของเจ้าของข้อมูลตามแบบอย่างของ GDPR เอาไว้ใน มาตรา 6 แห่งพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลโดยบัญญัติว่า “ความเสี่ยงต่อสิทธิเสรีภาพของของเจ้าของข้อมูล คือ ความเสี่ยงต่อสิทธิและเสรีภาพของบุคคลอันเป็นผลมาจากการประมวลผลข้อมูลส่วนบุคคลโดยเฉพาะการใช้ข้อมูลที่อาจเป็นผลเป็นการเลือกปฏิบัติทำให้เสี่ยงต่อการถูกขโมยข้อมูลหรือนำข้อมูลไปหลอกลวงผู้อื่นทำให้บุคคลอื่นเสียหายต่อชื่อเสียง ถูกเปิดเผยความลับที่ควรได้รับการคุ้มครอง มีการแปลงข้อมูลแฝงโดยไม่ได้รับอนุญาต ตลอดจนทำให้เกิดความเสียเปรียบทางสังคมหรือเศรษฐกิจ จนทำให้เจ้าของข้อมูลอาจจำกัดสิทธิเสรีภาพ หรือถูกขัดขวางมิให้เข้าถึงข้อมูลของตนอันเป็นข้อมูลเกี่ยวกับเชื้อชาติ หรือชาติกำเนิด (Ethnic Origin) การแสดงความเห็นทางการเมือง ศาสนา ปรัชญาความเชื่อ ความเป็นสมาชิกสหภาพแรงงาน ข้อมูลเกี่ยวกับพันธุกรรม สุขภาพ ประสบการณ์ทางเพศ (Sex Life) ตลอดจนประวัติ

อาชญากรรม หรือเกี่ยวกับมาตรการความปลอดภัยของบุคคล ซึ่งจะถูกนำมาประเมินผล เพื่อวิเคราะห์ หรือคาดการณ์แนวโน้มเกี่ยวกับประสิทธิภาพในการทำงาน สถานการณ์ทางเศรษฐกิจ สุขภาพ ความชอบหรือความสนใจ ความน่าเชื่อถือ หรือพฤติกรรม ตำแหน่งที่อยู่ หรือ การเคลื่อนไหว เพื่อที่จะสร้างหรือใช้แฟ้มข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลในกลุ่มที่เปราะบาง โดยเฉพาะเด็กหรือการประมวลผลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลจำนวนมากและมีผลต่อบุคคลจำนวนมากซึ่งเป็นเจ้าของข้อมูล" จึงจะทำให้กฎหมายเกิดความชัดเจนยิ่งขึ้น

นอกจากนี้ GDPR มาตรา 30 ใช้คำว่า "มิใช่กิจการที่ประมวลผลข้อมูลส่วนบุคคลเป็นครั้งคราว" แต่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ใช้คำว่า "มิใช่กิจการที่เก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว" ซึ่งหลักเกณฑ์ดังกล่าวยังไม่มีกำหนดไว้ทั้งของไทยและของGDPRว่ากิจการที่มีลักษณะเป็นครั้งคราวมีลักษณะเป็นอย่างไร แต่อย่างไรก็ดี GDPR มาตรา 30 มีการบัญญัติข้อยกเว้นของข้อยกเว้นในลักษณะที่กว้างกว่า พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กล่าวคือ GDPR ใช้คำว่า "มิใช่กิจการที่เป็นการประมวลผล..." แต่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ใช้คำว่า "มิใช่กิจการที่เก็บ รวบรวม ใช้ หรือ เปิดเผย..." ซึ่งคำว่าการประมวลผลตาม GDPR มาตรา 4(2) หมายถึง การดำเนินการใด ๆ ซึ่งประกอบไปด้วยข้อมูลส่วนบุคคลหรือชุดของข้อมูลส่วนบุคคลไม่ว่าจะดำเนินการอัตโนมัติหรือไม่ก็ตาม การดำเนินการดังกล่าวได้แก่ การเก็บรวบรวม การบันทึก การจัดระเบียบ การวางโครงสร้าง การปรับเปลี่ยน หรือการแก้ไข การเผยแพร่ หรือ วิธีอื่น ๆ ที่ทำให้สามารถนำไปใช้งานได้ การจัดวางหรือการจัดกลุ่มข้อมูลการจำกัดสิทธิ ตลอดจนการลบ หรือ ทำลายข้อมูลส่วนบุคคล

จะเห็นได้ว่า จากคำนิยามของคำว่าประมวลผลข้อมูล ตาม GDPR เป็นคำจำกัดความที่กว้างกว่าการเก็บรวบรวมใช้ เปิดเผย ของไทย ซึ่งจะต้องมาดูกันต่อไปว่าหลักเกณฑ์นี้จะมีลักษณะเป็นอย่างไร แต่อย่างไรก็ตามลักษณะของการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่เป็นครั้งคราว เช่น การเก็บข้อมูลส่วนบุคคลที่เกี่ยวกับความชอบความพึงพอใจของพนักงานภายในบริษัทเพื่อทำการปรับปรุงบริษัทโดยไม่ได้ทำกิจกรรมการประมวลผลบ่อยครั้งมากนักในกรณีแบบนี้บริษัทก็ไม่จำต้องทำบันทึกรายการดังกล่าว

บทที่ 5

บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

ด้วยการพัฒนาของเทคโนโลยีในโลกยุคดิจิทัลที่รวดเร็วและมีแนวโน้มที่จะพัฒนาขึ้นเรื่อย ๆ ส่งผลให้การติดต่อสื่อสารและการเผยแพร่ข้อมูลสามารถเคลื่อนย้ายและเชื่อมโยงกันได้อย่างสะดวกรวดเร็ว ที่ไม่จำกัดสถานที่อีกต่อไปเป็นทั้งโอกาสและภัยคุกคามทำให้เกิดปัญหาในการละเมิดสิทธิความเป็นอยู่ส่วนตัวของข้อมูลส่วนบุคคลมากยิ่งขึ้นโดยเฉพาะการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่ได้รับอนุญาตจากเจ้าของข้อมูลเป็นการละเมิดสิทธิของเจ้าของข้อมูล ผู้ควบคุมจึงมีหน้าที่ในการขอความยินยอมเมื่อทำการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคล อย่างไรก็ดีขั้นตอนในการขอความยินยอมเป็นเพียงหลักการคุ้มครองข้อมูลส่วนบุคคลประการหนึ่งเท่านั้น ผู้ประกอบกิจการในฐานะที่เป็นผู้ควบคุมยังมีหน้าที่รับผิดชอบจัดมาตรการต่าง ๆ ให้เป็นไปตามหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลประการอื่นอีก นอกจากนี้หน้าที่ในการจัดทำบันทึกรายการเป็นมาตรการหนึ่งที่ถือเป็นความรับผิดชอบของผู้ประกอบกิจการซึ่งเป็นผู้ควบคุม และจัดเป็นภารกิจภายใต้หลักความรับผิดชอบ (Accountability) อันเป็นหลักการคุ้มครองข้อมูลส่วนบุคคลที่สำคัญที่ผู้ควบคุมข้อมูลจะต้องปฏิบัติตาม เพื่อทำให้เกิดความโปร่งใสในการดำเนินหน้าที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพราะการบันทึกรายการข้อมูลจะทำให้เห็นภาพรวมได้ว่าผู้ควบคุมเอาข้อมูลไปใช้ทำอะไรบ้างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เป็นกฎหมายที่มีวัตถุประสงค์เพื่อคุ้มครองการละเมิดสิทธิของเจ้าของข้อมูล แม้ประเทศไทยจะมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลตามที่ได้ศึกษามาแล้วในบทข้างต้นก็ตาม แต่กฎหมายฉบับนี้ยังมีข้อบกพร่องอยู่บางประการกล่าวคือมีการบัญญัติที่ไม่ชัดเจนอาจทำให้ผู้ที่ต้องปฏิบัติตามซึ่งก็คือผู้ประกอบกิจการที่เป็นผู้ควบคุมข้อมูลเกิดความสับสนส่งผลให้ในทางปฏิบัติอาจปฏิบัติได้ไม่ถูกต้องเท่าที่ควรเสี่ยงที่จะถูกค่าปรับที่สูงถึง1ล้านบาทและส่งผลให้เจตนารมณ์ของกฎหมายไม่บรรลุวัตถุประสงค์ในการป้องกันการละเมิดสิทธิของเจ้าของข้อมูลได้

เมื่อศึกษากฎหมายต่างประเทศที่เกี่ยวกับการคุ้มครองครองข้อมูลส่วนบุคคลแล้วพบว่ามีกฎหมายของสหภาพยุโรป ที่เรียกว่า General Data Protection Regulation หรือGDPR เป็นกฎหมาย

คุ้มครองข้อมูลส่วนบุคคลที่เป็นแม่แบบให้กับหลาย ๆ ประเทศ นอกจากนี้ยังมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักรที่เรียกว่าพระราชบัญญัติคุ้มครองข้อมูล ค.ศ. 2018 (Data Protection Act 2018 หรือ DPA) และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณะรัฐสิงค์โปร์ที่มีชื่อว่าพระราชบัญญัติความคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2012 (Personal Data Protection Act 2012) สำหรับสหรัฐอเมริกาก็ยังไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลบัญญัติเอาไว้เป็นการทั่วไป การออกกฎหมายคุ้มครองส่วนบุคคลของประเทศสหรัฐอเมริกาจึงมีลักษณะเป็นการวิ่งไล่แก้ไขปัญหาที่เกิดขึ้นมากกว่าที่จะวางหลักเกณฑ์ทั่วไปเพื่อป้องกันปัญหา ซึ่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทยได้มีการนำหลักการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป หรือ GDPR มาเป็นแม่แบบในการออกกฎหมายฉบับนี้ โดยมีการกำหนดหน้าที่ของผู้ควบคุมเอาไว้ในมาตรา 39 เป็นหน้าที่ที่สำคัญของผู้ควบคุมข้อมูลที่ต้องทำการบันทึกรายการต่าง ๆ ที่ทำการเก็บรวบรวม ใช้ หรือ เปิดเผย เพื่อให้เจ้าของข้อมูลและคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้

จากการศึกษากฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยและต่างประเทศ พบว่าในเรื่องของรายละเอียดของรายการที่ผู้ควบคุมมีหน้าที่ต้องจัดทำบันทึกนั้นมีบัญญัติไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทยมาตรา 39 กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป GDPR มาตรา 30 และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร มาตรา 61 เท่านั้น สำหรับสหรัฐอเมริกา และ สิงค์โปร์ไม่มีการบัญญัติถึงรายการที่ผู้ควบคุมต้องทำจัดทำบันทึกเอาไว้ มีเพียงหลักการคุ้มครองข้อมูลส่วนบุคคลนั้น

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทยมีรายละเอียดบางประการที่ไม่มีความจำเป็นให้ผู้ควบคุมต้องจัดทำบันทึกเนื่องจากไม่เป็นประโยชน์ต่อการตรวจสอบของเจ้าของข้อมูลหรือสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือบางรายการไม่มีความชัดเจนเป็นการบัญญัติในลักษณะที่กว้างเกินไป ทำให้ผู้ควบคุมข้อมูลอาจจัดทำบันทึกผิดพลาดได้ กล่าวคือรายการตามมาตรา 39(3) กฎหมายมีวัตถุประสงค์ให้ผู้ควบคุมที่เป็นผู้ประกอบกิจการต้องจัดทำบันทึกรายการดังกล่าวก็เพื่อที่จะให้เจ้าของข้อมูลทราบว่าผู้ควบคุมข้อมูลคือใครหากเกิดข้อมูลพลาดเกี่ยวกับข้อมูลส่วนบุคคลเจ้าของข้อมูลสามารถติดต่อผู้ควบคุมข้อมูลได้อย่างไร เมื่อพิจารณามาตรา 39 (3)บัญญัติว่า “ข้อมูลที่เกี่ยวกับผู้ควบคุมข้อมูล” หากตีความจากตัวบทแล้วมีความหมายว่าต้องการข้อมูลทุกอย่างที่เกี่ยวกับผู้ควบคุมข้อมูล ซึ่งอาจเป็นข้อมูลที่มากกว่าชื่อและรายละเอียดในการติดต่อของผู้ควบคุมข้อมูลซึ่งเป็นข้อมูลที่ไม่มีความจำเป็นสำหรับการบันทึกเพราะ เช่น ข้อมูล

เกี่ยวกับเลขบัญชีธนาคารของผู้ควบคุมข้อมูล จำนวนลูกจ้างของผู้ควบคุมข้อมูล ผลประกอบการก็นับว่าเป็นข้อมูลที่เกี่ยวกับผู้ควบคุมเช่นเดียวกัน แม้ข้อมูลบางอย่างจะเป็นข้อมูลที่ผู้ประกอบธุรกิจจะต้องเปิดเผยอยู่แล้ว แต่ก็ถือเป็นรายละเอียดที่ไม่มีความจำเป็นจะต้องบันทึกไว้ในรายการเพื่อให้เจ้าของข้อมูล หรือเจ้าหน้าที่ที่มีอำนาจตามกฎหมายคุ้มครองข้อมูลตรวจสอบ เมื่อศึกษาจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป(GDPR) มาตรา 30(1)(a) และ สหราชอาณาจักรมาตรา 61(2)(1) พบว่ากฎหมายบัญญัติให้บันทึกรายละเอียดของผู้ควบคุมเพียง ชื่อ และสถานที่ติดต่อ ของผู้ควบคุมเท่านั้น ย่อมเห็นเจตนารมณ์ได้ว่าเมื่อเจ้าของข้อมูลขอตรวจสอบบันทึกก็จะสามารถทราบว่าผู้ใดเป็นผู้ควบคุมข้อมูล และสามารถติดต่อผู้ควบคุมข้อมูลได้ เพื่อให้เจ้าของข้อมูลได้ดำเนินการใช้สิทธิตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้ต่อไป จะเห็นได้ว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทยมีความแตกต่างจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป GDPRและของสหราชอาณาจักรที่ได้มีการบัญญัติรายการที่เกี่ยวกับผู้ควบคุมข้อมูลเอาไว้โดยชัดเจน ในความเห็นของผู้วิจัยการที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทยบัญญัติเอาไว้กว้างและไม่ชัดเจนเช่นนี้ส่งผลในทางปฏิบัติกล่าวคือในทางปฏิบัติอาจปฏิบัติไม่ได้อย่างแท้จริงเพราะผู้ควบคุมข้อมูลไม่เข้าใจว่ารายการข้อมูลที่เกี่ยวกับผู้ควบคุมข้อมูลนั้น มีอะไรบ้างทำได้ไม่ถูกต้องครบถ้วนอาจส่งผลให้ถูกค่าปรับที่ค่อนข้างสูงจึงควรแก้ไขบทบัญญัติมาตรา 39(3)ให้ชัดเจนตามแบบอย่างของ GDPR และ สหราชอาณาจักร โดยบัญญัติว่า เอาไว้ในมาตรา39(3)ให้ระบุเฉพาะชื่อและรายละเอียดในการติดต่อกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งได้แก่ ที่อยู่ เบอร์โทรศัพท์ อีเมล เท่านั้น

ในส่วนของหลักเกณฑ์ที่ใช้ยกเว้นหน้าที่ของผู้ควบคุมที่ไม่ต้องจัดทำบันทึกรายการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. มาตรา 39วรรคสาม กฎหมายมีวัตถุประสงค์เพื่อลดภาระค่าใช้จ่ายให้กับธุรกิจขนาดเล็กเพื่อไม่ให้เสียเปรียบในทางการค้ากับธุรกิจขนาดใหญ่กล่าวคือกิจการขนาดเล็กที่มีต้นทุนต่ำอาจไม่สามารถจ้างผู้เชี่ยวชาญเพื่อจัดการข้อมูลให้เป็นระบบได้ แม้กิจการขนาดเล็กจะสามารถจัดการข้อมูลให้เป็นระบบได้ด้วยตัวเองก็ตาม แต่ก็ต้องรับมือกับความเสี่ยงที่ระบบอาจเกิดความผิดพลาดและต้องถือว่ากิจการนั้นไม่ได้ปฏิบัติตามหลักเกณฑ์ที่กฎหมายกำหนดจนถูกปรับ ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลก็ได้กำหนดอัตราโทษปรับไว้ค่อนข้างสูงอาจทำให้กิจการขนาดเล็กที่ต้องโทษปรับต้องปิดกิจการสร้างผลกระทบต่อเศรษฐกิจอย่างกว้างขวาง เมื่อศึกษาบทบัญญัติในส่วนของข้อยกเว้นพบใน พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทยและกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป(GDPR)เท่านั้น สำหรับสหราชอาณาจักร สหรัฐอเมริกา และสิงค์โปร์ ไม่มีการบัญญัติถึงข้อยกเว้นที่ผู้ควบคุมไม่ต้องบันทึกรายการเอาไว้ เมื่อ

ทำการวิเคราะห์หลักเกณฑ์ที่ใช้ยกเว้นหน้าที่จัดทำบันทึกรายการของไทยตามมาตรา 39วรรคสาม เปรียบเทียบกับ GDPRมาตรา 30(5) แล้วพบว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทย มีการบัญญัติข้อยกเว้นเอาไว้ไม่ชัดเจน กล่าวคือมาตรา 39วรรคสาม บัญญัติว่า “ความใน (1) (2) (3) (4) (5) (6) และ (8) อาจยกเว้นมิให้นำมาใช้บังคับกับผู้ควบคุมข้อมูลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด เว้นแต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล หรือ มิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26” ซึ่งคำว่า “อาจ” ทำให้เกิดความยืดหยุ่นและไม่ชัดเจนก่อให้เกิดปัญหาว่ากรณีใดที่ผู้ประกอบธุรกิจที่มีกิจการขนาดเล็กจะได้รับการยกเว้นโดยไม่ต้องจัดทำบันทึกรายการ หรือในกรณีที่ผู้ประกอบกิจการการขนาดเล็กไม่ต้องจัดทำบันทึกรายการ จะถือว่าเป็นการยกเว้นการจัดทำบันทึกทุกรายการทั้งหมดหรือบางส่วน จึงเป็นกรณีที่หลักเกณฑ์ของกฎหมายไม่มีความชัดเจน ทำให้ผู้ประกอบกิจการที่จะถือเอาประโยชน์จากข้อยกเว้นเกิดปัญหาในการตีความ นอกจากนี้ไม่ได้มีการบัญญัติถึงความหมายของความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลคืออะไร แต่ GDPR มาตรา 30(5) บัญญัติว่า “หน้าที่ได้รับยกเว้นนั้นจะไม่ใช้บังคับแก่วิสาหกิจขนาดกลางและขนาดย่อม หรือองค์กรที่มีพนักงานน้อยกว่า 250 คน เว้นแต่มีการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่ประมวลผลข้อมูลส่วนบุคคลเป็นครั้งคราว หรือเป็นการประมวลผลข้อมูลส่วนบุคคลชนิดพิเศษตามมาตรา 9 (1) หรือเป็นข้อมูลส่วนบุคคลที่เกี่ยวกับประวัติอาชญากรรม ตามมาตรา 10” จะเห็นได้ว่า GDPRมีการบัญญัติข้อยกเว้นเอาไว้อย่างชัดเจนว่าหน้าที่ได้รับยกเว้นนั้นจะไม่บังคับใช้กับใครบ้างและมีการบัญญัติในส่วนความหมายของความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลเอาไว้อย่างชัดเจนในGDPR Recital ข้อที่75 ความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูล หมายความว่าความเสี่ยงต่อสิทธิและเสรีภาพของบุคคล เป็นผลมาจากการประมวลผลข้อมูลส่วนบุคคล โดยเฉพาะการใช้ข้อมูลส่วนบุคคลที่อาจทำให้มีผลเป็นการเลือกปฏิบัติ ทำให้เสี่ยงต่อการถูกขโมยข้อมูล หรือนำข้อมูลส่วนบุคคลไปหลอกลวงบุคคลอื่น ทำให้บุคคลอื่นเสียหายต่อชื่อเสียง ถูกเปิดเผยความลับที่ควรได้รับการคุ้มครอง มีการแปลงข้อมูลแฝงโดยไม่ได้รับอนุญาต ตลอดจนทำให้เกิดความเสียเปรียบทางสังคมหรือเศรษฐกิจ จนทำให้เจ้าของข้อมูลอาจจำกัดสิทธิเสรีภาพ หรือถูกขัดขวางมิให้เข้าถึงข้อมูลของตนอันเป็นข้อมูลเกี่ยวกับเชื้อชาติ หรือชาติกำเนิด (Ethnic Origin) การแสดงความเห็นทางการเมือง ศาสนา ปรัชญาความเชื่อ ความเป็นสมาชิกสหภาพแรงงาน ข้อมูลเกี่ยวกับพันธุกรรม สุขภาพ ประสบการณ์ทางเพศ (Sex Life) ตลอดจนประวัติอาชญากรรม หรือเกี่ยวกับมาตรการความ

ปลอดภัยของบุคคล ซึ่งจะถูกนำมาประเมินผล เพื่อวิเคราะห์ หรือคาดกาณณ์แนวโน้มเกี่ยวกับประสิทธิภาพในการทำงาน สถานการณ์ทางเศรษฐกิจ สุขภาพ ความชอบหรือความสนใจ ความน่าเชื่อถือ หรือพฤติกรรม ตำแหน่งที่อยู่ หรือ การเคลื่อนไหว เพื่อที่จะสร้างหรือใช้แฟ้มข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลในกลุ่มที่เปราะบาง โดยเฉพาะเด็กหรือการประมวลผลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลจำนวนมากและมีผลต่อบุคคลจำนวนมากซึ่งเป็นเจ้าของข้อมูล

จะเห็นได้ว่าของไทย ใช้คำว่าอาจได้รับยกเว้น และ ไม่ได้กำหนดเอาไว้ว่าเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลคืออะไร นอกจากนี้กิจการขนาดเล็กที่ได้รับยกเว้นตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนดนั้นปัจจุบันก็ยังไม่มีประกาศดังกล่าวออกมา เพื่อให้ผู้ควบคุมข้อมูลที่เป็นผู้ประกอบกิจการได้รับประโยชน์จากข้อยกเว้นของกฎหมายดังกล่าวและเพื่อให้กฎหมายคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพและสามารถคุ้มครองสิทธิของเจ้าของข้อมูลได้ตรงตามเจตนารมณ์ของกฎหมายจึงควรแก้ไขบทบัญญัติมาตรา 39 ให้มีความชัดเจน

5.2 ข้อเสนอแนะ

เนื่องจากประเทศไทยได้ประกาศกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปเป็นฉบับแรกคือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และมีผลบังคับใช้ทั้งฉบับในวันที่ 27 พฤษภาคม 2563 ซึ่งในการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลนั้น ประเทศไทยได้นำกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป หรือ GDPR มาเป็นแม่แบบ ทำให้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยคล้ายกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลอยู่พอสมควร ในแง่หนึ่งเป็นการแสดงว่าประเทศเราให้ความสำคัญกับการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวในเรื่องข้อมูลส่วนบุคคล จึงนำกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปที่ถือว่าเป็นกฎหมายที่พัฒนาในเรื่องการให้ความคุ้มครองข้อมูลส่วนบุคคลที่มีความก้าวหน้ามากที่สุดมาเป็นแบบอย่าง แต่ในอีกแง่หนึ่งขณะที่ประชากรส่วนใหญ่ของประเทศไทยยังมีความตระหนักรู้ในเรื่องของการเคารพต่อสิทธิส่วนบุคคลที่ค่อนข้างจำกัด เมื่อกฎหมายคุ้มครองข้อมูลส่วนบุคคลมีผลบังคับใช้ ก็ย่อมสร้างผลกระทบต่อผู้ที่เกี่ยวข้องจำนวนมาก ดังนั้น แม้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยจะนำกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปมาเป็นแม่แบบก็ตาม แต่ก็ไม่ได้นำมาปรับใช้ทั้งฉบับ โดยมีการบัญญัติให้เข้ากับบริบทของประเทศไทยให้มากที่สุด อย่างไรก็ตามในประเด็นที่กฎหมายกำหนดหน้าที่ให้ผู้ควบคุมต้องจัดทำบันทึก รวมทั้งข้อยกเว้นที่ผู้ควบคุมไม่ต้องจัดทำบันทึกนั้น มีการปรับบริบทของกฎหมายให้แตกต่างออกไปจาก GDPR จนทำให้บาง

หลักเกณฑ์กำหนดภาระให้แก่ผู้ประกอบกิจการมากเกินความจำเป็น และบางหลักเกณฑ์ยังต้องรอประกาศของคณะกรรมการคุ้มครองข้อมูล ซึ่งผู้วิจัยขอเสนอแนะและให้ข้อสังเกตดังต่อไปนี้

1) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 39(3) ซึ่งบัญญัติให้ผู้ควบคุมต้องจัดทำบันทึกรายการที่มีรายละเอียดของข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลนั้น เป็นรายการที่มีรายละเอียดเกินความจำเป็นต่อการตรวจสอบ ทั้งข้อมูลบางอย่างเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลอาจเป็นข้อมูลที่ผู้ประกอบกิจการต้องการเก็บเป็นความลับ ทั้ง ๆ ที่รายละเอียดที่จำเป็นของผู้ควบคุมมีเพียงแค่ชื่อ และวิธีติดต่อกับผู้ควบคุมเพื่อการใช้สิทธิอื่น ๆ ต่อไปเท่านั้น จึงควรนำหลักเกณฑ์ตาม GDPR มาตรา 30 (1) มาปรับใช้ โดยแก้ไขมาตรา 39(3) ให้ระบุเฉพาะชื่อและรายละเอียดในการติดต่อกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งได้แก่ ที่อยู่ เบอร์โทรศัพท์ อีเมลเท่านั้น

2) ประเด็นที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 39 วรรคสามบัญญัติว่า “...อาจยกเว้นมิให้นำมาใช้บังคับกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก” ก่อให้เกิดปัญหาว่ากรณีใดที่ผู้ประกอบธุรกิจที่มีกิจการขนาดเล็กจะได้รับการยกเว้นโดยไม่ต้องจัดทำบันทึกรายการ หรือในกรณีที่ผู้ประกอบกิจการการขนาดเล็กไม่ต้องจัดทำบันทึกรายการ จะถือว่าเป็นการยกเว้นการจัดทำบันทึกทุกรายการ หรือได้รับยกเว้นไม่ต้องจัดทำบันทึกเฉพาะบางรายการ จึงเป็นกรณีที่หลักเกณฑ์ของกฎหมายไม่มีความชัดเจน ผู้วิจัยขอเสนอแนะว่าควรแก้ไขพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยตัดคำว่า “อาจ” ออกไปเสียก็จะทำให้หลักเกณฑ์ของข้อยกเว้นมีความชัดเจนมากขึ้น

3) ประเด็นที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 39 วรรคสามยกเว้นหน้าที่การจัดทำบันทึกรายการให้แก่ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก โดยหลักเกณฑ์ของกิจการขนาดเล็กจะเป็นไปตามที่คณะกรรมการประกาศกำหนด แม้ปัจจุบัน (เดือนพฤษภาคม 2563) จะยังไม่มีการประกาศหลักเกณฑ์ดังกล่าวก็ตาม แต่ผู้วิจัยมีข้อสังเกตเกี่ยวกับหลักเกณฑ์ของกิจการขนาดเล็กว่าควรใช้หลักเกณฑ์ตาม GDPR มาตรา 30(5) ที่ใช้เกณฑ์ของจำนวนการจ้างงานมาเป็นหลักเกณฑ์ในการพิจารณาขนาดของกิจการที่ควรได้รับการยกเว้นมากกว่าการใช้หลักเกณฑ์รายได้ของกิจการมาพิจารณาเพราะเกณฑ์ของรายได้ไม่ได้บ่งบอกถึงปริมาณในการเก็บข้อมูลส่วนบุคคล เนื่องจากการจ้างงานเกี่ยวข้องกับการเก็บรวบรวมข้อมูลส่วนบุคคล เช่น นายจ้างจะต้องเก็บข้อมูล ชื่อ ที่อยู่ เบอร์ติดต่อ และข้อมูลส่วนตัวอื่น ๆ ของลูกจ้าง ถ้ากิจการใดมีข้อมูลของลูกจ้างจำนวนมากก็จำเป็นต้องจัดทำบันทึกที่มีรายการที่กำหนดไว้ตามมาตรา 39(1) ถึง(8) ดังนั้น

หลักเกณฑ์สำหรับกิจการขนาดเล็กจึงควรใช้จำนวนของการจ้างงานมาเป็นเกณฑ์ในการพิจารณาความเหมาะสมของกิจการที่จะได้รับยกเว้นให้ไม่ต้องจัดทำบันทึก

4) ประเด็นที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 39 วรรคสาม ในส่วนข้อยกเว้นของข้อยกเว้นที่บัญญัติว่า “เป็นการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูล” ผู้วิจัยขอเสนอแนะว่าควรเพิ่มบทบัญญัติในส่วนนิยามความหมายของความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลตามแบบอย่างของ (GDPR)โดยปรับตามบริบทของสังคมไทยเพื่อให้เกิดแนวทางที่ชัดเจน โดยบัญญัติเอาไว้ในบทนิยามมาตรา 6 ของพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 โดยบัญญัติว่า “ความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูล” หมายความว่าความเสี่ยงต่อสิทธิและเสรีภาพของบุคคล เป็นผลมาจากการประมวลผลข้อมูลส่วนบุคคล โดยเฉพาะการใช้ข้อมูลส่วนบุคคลที่อาจทำให้มีผลเป็นการเลือกปฏิบัติ ทำให้เสี่ยงต่อการถูกขโมยข้อมูล หรือนำข้อมูลส่วนบุคคลไปหลอกลวงบุคคลอื่น ทำให้บุคคลอื่นเสียหายต่อชื่อเสียง ถูกเปิดเผยความลับที่ควรได้รับการคุ้มครอง มีการแปลงข้อมูลแฝงโดยไม่ได้รับอนุญาต ตลอดจนทำให้เกิดความเสียเปรียบทางสังคมหรือเศรษฐกิจ จนทำให้เจ้าของข้อมูลอาจจำกัดสิทธิเสรีภาพ หรือถูกขัดขวางมิให้เข้าถึงข้อมูลของตนอันเป็นข้อมูลเกี่ยวกับเชื้อชาติ หรือชาติกำเนิด (Ethnic Origin) การแสดงความเห็นทางการเมือง ศาสนา ปรัชญาความเชื่อ ความเป็นสมาชิกสหภาพแรงงาน ข้อมูลเกี่ยวกับพันธุกรรม สุขภาพ ประสบการณ์ทางเพศ (Sex Life) ตลอดจนประวัติอาชญากรรม หรือเกี่ยวกับมาตรการความปลอดภัยของบุคคล ซึ่งจะถูกนำมาประเมินผล เพื่อวิเคราะห์ หรือคาดกาณณ์แนวโน้มเกี่ยวกับประสิทธิภาพในการทำงาน สถานการณ์ทางเศรษฐกิจ สุขภาพ ความชอบหรือความสนใจ ความน่าเชื่อถือ หรือพฤติกรรม ตำแหน่งที่อยู่ หรือ การเคลื่อนไหว เพื่อที่จะสร้างหรือใช้แฟ้มข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลในกลุ่มที่เปราะบาง โดยเฉพาะเด็กหรือการประมวลผลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลจำนวนมากและมีผลต่อบุคคลจำนวนมากซึ่งเป็นเจ้าของข้อมูล

บรรณานุกรม

ไพโรจน์ ต้นศิริอนุสรณ์. (2558). *การจัดการบันทึก (Record management)*. สืบค้นจาก http://www.techconsbiz.com/img/file/BPM_Dec_2015.pdf

กระทรวงการต่างประเทศ กรมยุโรป. (2563). *สหภาพยุโรป/กรอบความร่วมมือพหุภาคี: สหภาพยุโรป(The European Union-EU)*. สืบค้นจาก http://www.mfa.go.th/europetouch/th/other/8331/89715-สหภาพยุโรป-(The-European-Union---EU).html

กุลพล พลวัน. (2547). *สิทธิมนุษยชนในสังคมโลก*. กรุงเทพฯ: สำนักพิมพ์นิติธรรม.

ณัชพงษ์ สำราญ. (2561). การโอนข้อมูลส่วนบุคคลระหว่างประเทศ. *วารสารนิติศาสตร์มหาวิทยาลัยนเรศวร*, 11(1), 155-175.

นคร เสรีรักษ์. (2556). *การคุ้มครองข้อมูลส่วนบุคคล: ประสบการณ์เยอรมัน*. สืบค้นจาก http://www.oic.go.th/FILEROOM/CABOICFORM05/DRAWER02/GENERAL/DATA0001/00001907.PDF

นคร เสรีรักษ์. (2557). *ความเป็นส่วนตัว ความคิด ความรู้ ความจริงและพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย*. กรุงเทพฯ: พี.เพรส.

นคร เสรีรักษ์. (2558). *การคุ้มครองข้อมูลส่วนบุคคลข้อเสนอสำหรับประเทศไทย*. กรุงเทพฯ: พี.เพรส.

ปิยะบุตร บุญอร่ามเรือง, ปิติ เอี่ยมจำรูญลาภ, ชวิน อุ่นภัทร และฐิติรัตน์ ทิพย์สัมฤทธิ์กุล. (2561). *Thailand data protection guideline 1.0*. กรุงเทพฯ: จุฬาลงกรณ์มหาวิทยาลัย.

ปิยะพร วงศ์เบี้ยสัจจ์. (2552). *การเปิดเผยข้อมูลส่วนบุคคลโดยธนาคารพาณิชย์กับมาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคล* (Master's thesis). สืบค้นจาก โครงการเครือข่ายห้องสมุดในประเทศไทย (ThaiLIS).

พนิดา พูลสวัสดิ์. (2556). *มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของเด็กบนเครือข่ายอินเทอร์เน็ต* (Master's thesis). สืบค้นจาก โครงการเครือข่ายห้องสมุดในประเทศไทย (ThaiLIS).

พิสมัย ระพีพัฒน์ชัย. (2560). *การจัดการเอกสารโดยใช้หลักการจัดเอกสารแบบวิเคราะห์หน้าที่ กรณีศึกษา: บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร ตลิ่งชัน* (Master's thesis). สืบค้นจากโครงการเครือข่ายห้องสมุดในประเทศไทย (ThaiLIS).

ราชกิจจานุเบกษา. (2560). *รัฐธรรมนูญแห่งราชอาณาจักรไทย*. เล่ม 134 ตอนที่ 40 ก หน้า 1 ประกาศใช้ 6 เมษายน 2560

บรรณานุกรม (ต่อ)

ราชกิจจานุเบกษา. (2562). *พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562*. เล่ม 136 ตอนที่ 69 ก หน้า 52 ประกาศใช้ 27 พฤษภาคม 2562.

ศิริกุล ภู่พันธ์. (2548). *ข้อความคิดว่าด้วยข้อมูลข่าวสารส่วนบุคคล* (Master's thesis). สืบค้นจาก โครงการเครือข่ายห้องสมุดในประเทศไทย (ThaiLIS).

สหธน รัตนไพจิตร. (2547). *สรุปผลการศึกษาวิจัย โครงการจัดทำความเห็นทางวิชาการเกี่ยวกับการเปิดเผยข้อมูลข่าวสารของราชการและการปฏิบัติตามคำวินิจฉัยและผลกระทบจากคำวินิจฉัยของคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสาร*. กรุงเทพฯ: โรงพิมพ์มหาวิทยาลัยธรรมศาสตร์.

สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์. (2557). *รายงานผลการดำเนินการโครงการพัฒนามาตรการในการดำเนินการ การพิจารณาความเหมาะสม ความเป็นไปได้ เพื่อจัดนำแนวทาง ขั้นตอนและวิธีการในการเข้าร่วมหรือทำความตกลงตามกรอบว่าด้วยการคุ้มครองความเป็นส่วนตัวของ APEC*. สืบค้นจาก http://www.oic.go.th/ web2017 /iwebform_viewer.asp?i=21111%2E14129605112112151111211

สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์. (2558). *รายงานฉบับสมบูรณ์โครงการศึกษาและพัฒนาแนวทางการคุ้มครองข้อมูลส่วนบุคคลภายใต้ประชาคมอาเซียน*. สืบค้นจาก http://www.oic.go.th/FILEWEB/ CABIWEBSITE/DRAWER01/GENERAL/ DATA0007/00007559.PDF

สำนักงานเลขาธิการสภาผู้แทนราษฎร. (2556). *เอกสารประกอบการพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.... อ.พ.6/2556 สมัยสามัญทั่วไป*. สืบค้นจาก http://www. parliament.go.th/library

สำนักงานเลขาธิการสภาผู้แทนราษฎร. (2562). *ความมุ่งหมายและคำอธิบายประกอบรายมาตราของรัฐธรรมนูญแห่งราชอาณาจักร พุทธศักราช 2560*. สืบค้นจาก https://www.parliament. go.th/ ewtcommittee/ewt/draftconstitution2/download/article/article_201910 21103453.pdf.

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. (2557). *การคุ้มครองข้อมูลส่วนบุคคล (Data Privacy)*. สืบค้นจาก http://www.etcommission.go.th/article-dp-topic-dp.html

บรรณานุกรม (ต่อ)

สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ. (2558). *รายงานการศึกษาวิจัยฉบับสมบูรณ์ เรื่อง ปัญหาและมาตรการทางกฎหมายในการรับรองและคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว.* กรุงเทพฯ: ดอกเบี้ย.

หนุนธุรกิจปรับตัวรับ พรบ.คุ้มครองข้อมูลส่วนบุคคล. (2562, 21 พฤษภาคม). *ฐานเศรษฐกิจ.* สืบค้นจาก https://www.thansettakij.com/content/401625

อธิพร สิทธิธีรรัตน์. (2558). *ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็กทรอนิกส์* (Master's thesis). สืบค้นจาก โครงการเครือข่ายห้องสมุดในประเทศไทย (ThaiLIS).

Aleksandra. (2018). *63 Fascinating google search statistics*. Retrieved from https://seotribunal.com/blog/google-stats-and-facts/

California Consumer Privacy Act Guide. (2019). Retrieved 3 December, 2562, from https://www.skadden.com/-/media/files/publications/2019/03/cybersecurity_california_privacy.pdf

CMS Cameron McKenna Nabarro Olswang LLP. (2017). A guide to GDPR for companies in Singapore. Retrieved from https://cms.law/en/Media/Affiliates/Singapore/Images/Publications /GDPR-guide-for-Singapore-companies

Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. (2003). *Official Journal of the European Union, 46*(124), 36-41. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2003:124:FULL&from=EN

David, P. (2017). *The world's most valuable resource is no longer oil, but data.* Retrieved from https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

European Union Agency for Fundamental Rights and Council of Europe. (2018). *Handbook on European data protection law*. Luxembourg: Office of the European Union.

General Data Protection Regulation. (2016). *Official Journal of the European Union*, *59*(119), 1-88. Retrieved from http:// https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL

IM2Market. (2558). *ข้อมูลหมายถึงหัวใจหลักของการทำงาน*. สืบค้นจาก https://www.im2market.com/2015/11/14/2031

บรรณานุกรม (ต่อ)

Information Commissioner's Office. (2018a). *Guide to the General Data Protection Regulation (GDPR).* Retrieved from https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

Information Commissioner's Office. (2018b). *Who needs to document their processing activities?*. Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/who-needs-to-document-their-processing-activities/

Juan, D. R. (2017). *Top 10 Companies and Brands Owned by Google as of 2017*. Retrieved from https://learn.stashinvest.com/companies-brands-owned-google, 25

Judgment of European Court retrieved system. (2003). Case 101/01. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1590535498929&uri=CELEX:62001CJ0101

Judgment of European Court retrieved system. (2014a). Case 131/12. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1590535376164&uri=CELEX:62012CJ0131

Judgment of European Court retrieved system. (2014b). Case 212/13. Retrieved from https://eur-lex. europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62013CJ0212&from=EN

Judgment of European Court retrieved system. (2017). Case 398/15. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1590534459389&uri=CELEX:62015CJ0398

Modify. (2556). *ประวัติ Google (กูเกิล) ความเป็นมามีมาอย่างไร*. สืบค้นจาก https://www.modify.in.th/1772

Organisation for Economic Co-operation and Development. (2013). *The OECD Privacy Framework*. Retrieved from https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Samuel, F. (2019). *Data is not the new oil*. Retrieved from https://towardsdatascience.com /data-is-not-the-new-oil-bdb31f61bc2d

บรรณานุกรม (ต่อ)

Stuart, F. (2018). *Records of Processing Activities*. Retrieved from https://wishloop.com/wishloop-data-protection-activities.pdf

U.S. Supreme Court Whalen v. Roe, 429 U.S. 589 (1977). (1997). Retrieved from *https://supreme.justia.com/cases/federal/us/429/589/*

Wolfgang, B. & Susanne, D. (2017). *The Processing Records.* Retrieved from https://www.bitkom.org/sites/default/files/file/import/180529-LF-Verarbeitungsverzeichnis-ENG-online-final.pdf

ประวัติผู้วิจัย

ชื่อ	ณฐพร วิริยะลัพภะ
วัน เดือน ปีเกิด	18 ตุลาคม 2535
สถานที่เกิด	จังหวัดจันทบุรี ประเทศไทย
ประวัติการศึกษา	มหาวิทยาลัยรังสิต ปริญญานิติศาสตรบัณฑิต, 2558 มหาวิทยาลัยรังสิต ปริญญานิติศาสตรมหาบัณฑิต, 2563
ที่อยู่ปัจจุบัน	4/117 หมู่9 ตำบลท่าช้าง อำเภอเมือง จังหวัดจันทบุรี 22000