ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลประเภทข้อมูลชีวภาพ

นางสาวแสงระวี วิปุลาคม

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต
วิชาเอกกฎหมายธุรกิจ สาขาวิชานิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช
พ.ศ. 2563

Legal Problems Regarding Personal Data Protection for Biometrics

Miss Sangravee Vipulakom

A Thesis Submitted in Partial Fulfillment of the Requirements for
the Degree of Master of Laws in Business Law
School of Law
Sukhothai Thammathirat Open University
2020

หัวข้อวิทยานิพนธ์ ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลประเภทข้อมูลชีวภาพ
ชื่อและนามสกุล นางสาวแสงระวี วิปุลาคม
วิชาเอก กฎหมายธุรกิจ
สาขาวิชา นิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช
อาจารย์ที่ปรึกษา 1. ศาสตราจารย์ ดร.สราวุธ ปิติยาศักดิ์
2. ผู้ช่วยศาสตราจารย์ ดร.วราภรณ์ วนาพิทักษ์

วิทยานิพนธ์นี้ ได้รับความเห็นชอบให้เป็นส่วนหนึ่งของการศึกษา
ตามหลักสูตรระดับปริญญาโท เมื่อวันที่ 29 มีนาคม 2564

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(อาจารย์เธียรชัย ณ นคร)

..... กรรมการ
(ศาสตราจารย์ ดร.สราวุธ ปิติยาศักดิ์)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.วราภรณ์ วนาพิทักษ์)

..... ประธานกรรมการบัณฑิตศึกษา
(รองศาสตราจารย์ ดร.สมพร พุทธาพิทักษ์ผล)

ชื่อวิทยานิพนธ์ ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลประเภทข้อมูลชีวภาพ
ผู้วิจัย นางสาวแสงระวี วิปุลาคม **รหัสนักศึกษา** 2614000137
ปริญญา นิติศาสตรมหาบัณฑิต **วิชาเอก** กฎหมายธุรกิจ
อาจารย์ที่ปรึกษา (1) ศาสตราจารย์ ดร.สราวุธ ปิติยาศักดิ์ (2) ผู้ช่วยศาสตราจารย์ ดร.วราภรณ์ วนาพิทักษ์
ปีการศึกษา 2563

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อ (1) ศึกษาแนวคิดเกี่ยวกับข้อมูลส่วนบุคคล ข้อมูลชีวภาพ และลักษณะทั่วไปของเทคโนโลยีเกี่ยวกับการใช้ข้อมูลชีวภาพ (2) ศึกษามุมมองที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลสำหรับข้อมูลชีวภาพตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร (DPA) และกฎหมายคุ้มครองข้อมูลชีวภาพของรัฐอิลลินอยส์ ประเทศสหรัฐอเมริกา (BIPA) (3) วิเคราะห์พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เปรียบเทียบกับส่วนที่เกี่ยวข้องกับข้อมูลชีวภาพตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร (DPA) และกฎหมายคุ้มครองข้อมูลชีวภาพของรัฐอิลลินอยส์ ประเทศสหรัฐอเมริกา (BIPA) และ (4) เสนอแนวทางในการปรับปรุงกฎหมายคุ้มครองข้อมูลชีวภาพ

งานวิจัยเรื่องนี้เป็นการวิจัยทางกฎหมายโดยการวิจัยเชิงคุณภาพ ด้วยการวิจัยทางเอกสาร จากตัวบทกฎหมาย หนังสือ ตำรา บทความและเอกสารที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลประเภทชีวภาพ ทั้งภาษาไทยและภาษาต่างประเทศจากแหล่งต่าง ๆ ไม่ว่าจะเป็นห้องสมุด หรือจากเว็บไซต์ต่าง ๆ ในเครือข่ายอินเตอร์เน็ต

ผลการศึกษาพบว่า (1) โดยรวมกฎหมายคุ้มครองข้อมูลชีวภาพของไทยสอดคล้องกับแนวคิดเกี่ยวกับข้อมูลส่วนบุคคล และแนวคิดเกี่ยวกับข้อมูลชีวภาพในการให้ความคุ้มครองเจ้าของข้อมูลส่วนบุคคล หากแต่สามารถปรับปรุงเพื่อให้มีความคุ้มครองข้อมูลชีวภาพที่เหมาะสมมากขึ้นได้ (2) กฎหมายคุ้มครองข้อมูลส่วนบุคคล GDPR ของสหภาพยุโรป และ BPA ของสหราชอาณาจักรนั้นสอดคล้องกันและให้ความคุ้มครองข้อมูลชีวภาพในลักษณะเดียวกัน ทางด้านกฎหมายคุ้มครองข้อมูลชีวภาพ BIPA ของรัฐอิลลินอยส์ให้ความคุ้มครองข้อมูลชีวภาพโดยเฉพาะ อีกทั้งยังมีการให้คำจำกัดความที่ชัดเจน หากแต่มิได้มีการกำหนดแนวทางในการรักษาความปลอดภัยไว้ สำหรับรัฐอิลลินอยส์ และสหราชอาณาจักรนั้นศาลได้มีคำพิพากษาให้การฟ้องคดีสามารถกระทำได้โดยมิต้องเกิดความเสียหายอันสามารถกำหนดมูลค่าได้ (3) กฎหมายคุ้มครองข้อมูลชีวภาพของไทยสอดคล้องกับกฎหมายคุ้มครองข้อมูลชีวภาพของสหภาพยุโรป และของสหราชอาณาจักร หากแต่มิได้มีการกำหนดแนวทางในการรักษาความปลอดภัยอย่างพอเพียงเพื่อคุ้มครองข้อมูลชีวภาพ และไม่มีการประเมินผลกระทบและความจำเป็นในการเก็บข้อมูลก่อนการประมวลผลข้อมูลชีวภาพ (4) สำหรับแนวทางในการปรับปรุงกฎหมายคุ้มครองข้อมูลชีวภาพของไทย ควรมีการปรับเปลี่ยนคำจำกัดของคำว่า “ข้อมูลชีวภาพ” ให้มีความเหมาะสม อีกทั้งปรับเปลี่ยนการรักษาความปลอดภัยสำหรับข้อมูลชีวภาพให้มีการคุ้มครองข้อมูลชีวภาพโดยยึดหลักมาตรฐานสากลในการรักษาความปลอดภัย และมีการประเมินผลกระทบและความจำเป็นในการเก็บข้อมูลก่อนการประมวลผลข้อมูลชีวภาพ สำหรับการร้องเรียนการละเมิดข้อมูลชีวภาพเจ้าของข้อมูลส่วนบุคคลไม่จำเป็นต้องได้รับความเสียหายหรือความเดือดร้อนอันสามารถกำหนดมูลค่าได้จึงจะสามารถร้องเรียนได้ การลงโทษสำหรับการละเมิดข้อมูลส่วนบุคคลประเภทชีวภาพควรกำหนดอัตราโทษทางปกครองโดยกำหนดจำนวนค่าปรับต่อผู้เสียหายหนึ่งราย เพื่อเป็นการป้องปรามให้ผู้ควบคุมข้อมูลส่วนบุคคลกำหนดให้มีมาตรการการรักษาความปลอดภัยข้อมูลชีวภาพที่เหมาะสม

คำสำคัญ การคุ้มครองข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลชีวภาพ ฐานการประมวลผล การรักษาความปลอดภัยข้อมูลชีวภาพ

Thesis title: Legal Problems Regarding Personal Data Protection for Biometrics
Researcher: Miss Sangravee Vipulakom **ID:** 2614000137
Degree: Master of Laws **Major:** Business Laws
Thesis advisor: (1) Dr. Saravuth Pitiyasak, Professor (2) Dr.Varaporn Vanaphituk, Assistant Professor
Academic year: 2020

Abstract

The objectives of this thesis are to (1) study concepts relating to personal data, biometrics data, and general characteristics of biometric technology; (2) study perspectives in relations to data privacy laws on biometrics from EU's Data Protection Regulation (GDPR), UK's Data Protection Act, Illinois Biometrics Information Protection Act (3) analyze Thailand's Personal Data Protection Act 2019 and make comparisons with EU's Data Protection Regulation (GDPR), UK's Data Protection Act (DPA), and Illinois Biometrics Information Protection Act (BIPA); and (4) propose ways to improve Personal Data Protection Act 2019.

This is a qualitative legal research based on information on personal biometrics data protection collected from various sources; such as laws, books, and journal articles in both Thai and English from libraries, and websites.

The results of the study are (1) overall Thai Personal Data Protection Act is in line with the concepts of personal data and biometrics data in terms of providing protection for data subjects. However, the act can be improved to provide more suitable protections ; (2) European Union's GDPR and United Kingdom's DPA are in line and provide the same level of protection for biometrics data, while Illinois's BIPA provide protection exclusively for biometrics data with clear definition but did not provide guidance for biometrics data security. Furthermore, courts in Illinois and United Kingdom have adjudicated that lawsuits can be filed even without actual and/or financial damages; (3) While PDPA's protection for biometrics data are in line with GDPR and DPA, the guideline for biometrics data protection has not been determined. Also, it does not require impact assessment and the justifications prior to the use of biometrics data; (4) for the improvement of Personal Data Protection law, the definition of the word "Biometrics" should be adjusted accordingly. The security of biometrics should be based on international standard, and impact assessment and the justifications for using biometrics should always be done prior to the decision to use biometrics technology. Data subjects should be able to file complaints or lawsuits on biometrics violations without having to proof actual or financial damages. Penalties for violations relating to biometrics under Personal Data Protection Act 2019 should be set per data subject instead of per violation. This will be a deterrence to data controller and encourage them to put in place proper security measures.

Keywords: Personal Data Protection, Biometrics Data, Lawful Basis, Biometrics Security

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้เนื่องด้วยผู้มีพระคุณหลายท่านได้กรุณาให้โอกาส ให้คำปรึกษา ชี้แนะแนวทาง รวมทั้งให้ความช่วยเหลือและสนับสนุนในด้านต่าง ๆ แก่ผู้วิจัยในการจัดทำวิทยานิพนธ์

ผู้วิจัยขอกราบขอบพระคุณ ศาสตราจารย์ ดร.สราวุธ ปิติยาศักดิ์ ที่ได้ให้ความกรุณาสละเวลาอันมีค่ารับเป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ พร้อมทั้งสละเวลามาให้ความรู้ คำแนะนำ ตลอดจนแนวทางอันเป็นประโยชน์ต่อการศึกษาค้นคว้าในการทำวิทยานิพนธ์นี้จนสำเร็จลุล่วงด้วยดี

ผู้วิจัยขอกราบขอบพระคุณ อาจารย์เธียรชัย ณ นคร ประธานกรรมการสอบวิทยานิพนธ์ ศาสตราจารย์ ดร.สราวุธ ปิติยาศักดิ์ และ ผู้ช่วยศาสตราจารย์ ดร.วราภรณ์ วนาพิทักษ์ กรรมการสอบวิทยานิพนธ์ ซึ่งได้กรุณาสละเวลาอันมีค่ายิ่งในการเป็นคณะกรรมการสอบวิทยานิพนธ์ รวมถึงให้คำแนะนำ ชี้แนะแนวทาง ตลอดจนให้ข้อคิดและข้อสังเกตอันเป็นประโยชน์อย่างยิ่งในการจัดทำวิทยานิพนธ์ฉบับนี้

ขอขอบพระคุณคุณพ่อประเสริฐ วิปุลาคม ผู้เป็นแรงบันดาลใจให้ผู้วิจัยได้ศึกษาเล่าเรียนเพิ่มเติมในสาขาวิชานิติศาสตร์ และผู้ช่วยศาสตราจารย์ ดร.ธีรเดช มโนลีหกุล ผู้ชักชวนให้ผู้วิจัยเข้าร่วมศึกษาในระดับปริญญาโท สาขาวิชานิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช ขอขอบคุณคุณนวพร วิปุลาคม และครอบครัววิปุลาคมที่มอบความรัก การสนับสนุนในทุกด้าน และเป็นกำลังใจในการศึกษาเล่าเรียน ขอบคุณคุณธนาภา กังสกุลนิติสำหรับความช่วยเหลือในด้านต่าง ๆ ในระหว่างการศึกษาเล่าเรียน ทุกท่านล้วนเป็นแรงสำคัญที่ทำให้ผู้วิจัยไม่ย่อท้อต่ออุปสรรคจนทำให้วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปด้วยดี

หากวิทยานิพนธ์ฉบับนี้สามารถก่อให้เกิดประโยชน์ไม่ว่าในทางศึกษาหรือทางอื่นใด ผู้วิจัยขอมอบความดีทั้งหมดให้แก่ครูบาอาจารย์ทุกท่านที่ได้ประสิทธิ์ประสาทวิชาความรู้แก่ผู้วิจัย รวมทั้งผู้แต่งตำรา ผู้เขียนบทความซึ่งผู้วิจัยใช้เป็นข้อมูลในการทำวิทยานิพนธ์ฉบับนี้ทุกท่าน และขอมอบความกตัญญูกตเวทิตาคุณแด่บิดา มารดา และผู้มีพระคุณของผู้วิจัยดังที่กล่าวมาทุกท่าน แต่หากวิทยานิพนธ์ฉบับนี้มีข้อผิดพลาดหรือข้อบกพร่องประการใด ผู้วิจัยกราบขออภัย และขอน้อมรับไว้แต่เพียงผู้เดียว

นางสาวแสงระวี วิปุลาคม
มีนาคม 2564

สารบัญ

สารบัญตาราง

สารบัญภาพ

บทที่ 1
บทนำ

1. ความเป็นมาและความสำคัญของปัญหา

ในสมัยก่อนการซื้อขายสินค้าและบริการผู้ซื้อจะต้องเดินทางไปร้านค้าด้วยตนเอง โดยลักษณะของร้านค้าในอดีตนั้นมีหน้าร้าน (Brick and Mortar) ที่ลูกค้าสามารถเลือกชมสินค้าได้ ซึ่งการซื้อขายอาจมีการเก็บข้อมูลส่วนตัวของลูกค้า หรือที่เรียกว่าข้อมูลส่วนบุคคล โดยมีการเก็บข้อมูลเฉพาะที่ต้องใช้ในการติดต่อกับลูกค้า หรือข้อมูลที่เกี่ยวข้องกับการซื้อสินค้าเป็นครั้ง ๆ เท่านั้น เช่น ชื่อ ที่อยู่ หรือ หมายเลขโทรศัพท์ เป็นต้น ส่วนวิธีการเก็บข้อมูลขึ้นอยู่กับระบบของผู้ขายแต่ละราย ซึ่งอาจเก็บในรูปแบบของกระดาษ หรือเก็บในระบบคอมพิวเตอร์ แต่ไม่มีการเก็บข้อมูลแบบออนไลน์ และไม่มีการเก็บข้อมูลเกินกว่าที่จำเป็น

เมื่อโลกเปลี่ยนไปเข้าสู่ยุคอินเตอร์เน็ต วิธีการซื้อขายได้เปลี่ยนจากการซื้อขายแบบผ่านหน้าร้านมาเป็นแบบออนไลน์มากขึ้น โดยผู้ซื้อไม่จำเป็นต้องเดินทางไปถึงหน้าร้านเพื่อเลือกซื้อสินค้าอีกต่อไป การซื้อขายสามารถทำได้โดยผู้ซื้อและผู้ขายไม่ต้องพบหน้ากันเลย ผู้ซื้อสามารถเลือกสินค้าได้จากรายการสินค้าที่ผู้ขายได้ทำการประกาศขายบนอินเตอร์เน็ตได้อย่างสะดวกสบาย การใช้อินเตอร์เน็ตไม่ได้จำกัดอยู่เพียงแค่การซื้อขายสินค้าและบริการเท่านั้น หากอินเตอร์เน็ตยังสามารถใช้ในการทำธุรกรรมอื่น ๆ ได้อีกมากมาย เช่น การโอนเงิน การชำระค่าน้ำ ค่าไฟฟ้า ค่าโทรศัพท์ และการชำระภาษี เป็นต้น นอกจากนี้อินเตอร์เน็ตยังสามารถนำไปใช้ในเชิงสันทนาการผ่านการใช้เครือข่ายสังคมออนไลน์ (Social Network) เช่น Facebook หรือ Instagram อีกด้วย ในสมัยอินเตอร์เน็ตนี้การเก็บข้อมูลส่วนบุคคลได้เปลี่ยนไปเป็นการเก็บข้อมูลแบบออนไลน์ เมื่อผู้ใช้บริการต้องการใช้บริการออนไลน์ผู้ใช้บริการต้องสร้างบัญชีผู้ใช้ หรือ user account สำหรับใช้ในการเข้าสู่ระบบ หรือ ล็อกอิน โดยใส่ข้อมูลส่วนบุคคลของผู้ที่ต้องการใช้บริการ เช่น เลขบัตรประจำตัวประชาชน ชื่อ นามสกุล ที่อยู่ วันเดือนปีเกิด หมายเลขโทรศัพท์ และอีเมล เป็นต้น ซึ่งการสร้างบัญชีผู้ใช้นี้ทำให้ผู้ใช้บริการต้องให้ข้อมูลส่วนบุคคลกับทางผู้ประกอบการมากขึ้นกว่าในอดีต นอกจากผู้ประกอบการจะสามารถเก็บข้อมูลลูกค้าได้มากกว่าในอดีตแล้ว ความก้าวหน้าของเทคโนโลยียังทำให้ผู้ประกอบการสามารถเก็บข้อมูลอื่น ๆ ของลูกค้า ผ่านทางช่องทางต่าง ๆ ได้อย่างง่ายดาย ทั้งที่ลูกค้าให้ความยินยอม และไม่ได้ให้ความยินยอม เช่น การเก็บข้อมูลการเข้าใช้เว็บไซต์ ข้อมูลพฤติกรรมการบริโภค และหมายเลขประจำคอมพิวเตอร์ (Internet Protocol Address หรือ IP Address) เป็นต้น

ในปัจจุบันผู้ประกอบการมีข้อมูลส่วนบุคคลจำนวนมากมายอยู่ในครอบครอง และผู้ประกอบการหลายรายได้นำข้อมูลเหล่านี้ไปใช้เพื่อแสวงหาผลประโยชน์ โดยอาจนำข้อมูลไปใช้เพื่อวัตถุประสงค์ภายในองค์กร เช่น การเสนอโฆษณาเฉพาะบุคคล (personalized advertising) ของ Google, Facebook หรือ Amazon นอกจากนี้ผู้ประกอบการบางรายอาจนำข้อมูลเหล่านี้ไปให้ หรือขายให้กับผู้อื่นอีกด้วย

เป็นที่ยอมรับกันโดยทั่วไปว่าข้อมูลเหล่านี้คือสิ่งที่มีค่ามากสำหรับการประกอบธุรกิจในปัจจุบัน และผู้ประกอบการรายใหญ่ ๆ มักมีข้อมูลส่วนบุคคลอยู่ในครอบครองเป็นจำนวนมาก ซึ่งในสมัยของเศรษฐกิจดิจิทัลนั้น ข้อมูลคืออำนาจทางธุรกิจ เนื่องจากข้อมูลเหล่านั้นสามารถนำไปสร้างผลประโยชน์ในทางการค้า เพื่อเพิ่มส่วนแบ่งการตลาด ยอดขาย หรือผลกำไรให้กับองค์กรได้ ดังที่มีการกล่าวว่า “Data is the new oil”หรือ ข้อมูลนั้นมีค่าเหมือนดั่งน้ำมัน

อย่างไรก็ตามในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลอาจเกิดการล่วงละเมิดความเป็นส่วนตัว (privacy) ของเจ้าของข้อมูลได้ ถึงแม้ว่าเว็บไซต์ต่าง ๆ อาจมีการขอความยินยอมจากเจ้าของข้อมูลก่อนทำการเก็บข้อมูล แต่ผู้ใช้อินเตอร์เน็ตนั้นมักจะไม่ค่อยอ่านข้อตกลง และเงื่อนไขในการให้ความยินยอม ซึ่งส่งผลให้การให้ความยินยอมเป็นไปโดยไม่มีความเข้าใจอย่างถ่องแท้ถึงขอบเขต และเงื่อนไขของความยินยอมนั้น ๆ นอกจากนี้บางเว็บไซต์อาจใช้วิธีขอความยินยอมโดยปริยาย (implied consent) โดยถือว่าการเข้าสู่เว็บไซต์นั้น ๆ คือการให้ความยินยอม และเมื่อได้รับความยินยอมผู้ได้รับความยินยอมย่อมสามารถนำข้อมูลส่วนบุคคลไปใช้ได้ตามวัตถุประสงค์ที่ระบุไว้ตามที่ได้รับความยินยอมจากเจ้าของข้อมูล

อาจกล่าวได้ว่าข้อมูลส่วนบุคคลนั้นมีความสำคัญอย่างยิ่งยวด การคุ้มครองข้อมูลส่วนบุคคลนั้นไม่เพียงแต่เป็นการคุ้มครองข้อมูล แต่ยังเป็นการคุ้มครองสิทธิพื้นฐานในความเป็นส่วนตัวของบุคคลนั้น ๆ ดังนั้นการคุ้มครองข้อมูลส่วนบุคคลจึงเป็นการป้องกันไม่ให้เกิดการละเมิดสิทธิพื้นฐานในความเป็นส่วนตัว อันอาจก่อให้เกิดความเสียหายให้กับผู้ถูกละเมิดได้หลายทาง ตั้งแต่การไม่ยอมรับเข้าทำงาน หรือการถูกไล่ออกจากงาน ไปจนถึงความเสียหายทางการเงิน หรือแม้กระทั่งชีวิต ดังนั้นนานาประเทศจึงให้ความสำคัญกับการคุ้มครองการประมวลผลข้อมูลส่วนบุคคล และมีการตรากฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล เช่น ประเทศแคนาดาได้มีการประกาศใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลสำหรับองค์กรเอกชนในปี พ.ศ. 2543 เรียกว่า กฎหมายคุ้มครองข้อมูลส่วนบุคคลและเอกสารอิเล็กทรอนิกส์ (Personal Information and Electronic Documents Act 2000 หรือ PIPEDA) สำหรับประเทศฟิลิปปินส์ได้มีการประกาศใช้ Data Privacy Act 2012 ในปี พ.ศ. 2555 และในปีเดียวกันประเทศสิงคโปร์ได้ประกาศใช้ Personal Data Protection Act 2012 สำหรับสหภาพยุโรป (European Union หรือ EU) ได้ประกาศใช้มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประชาชน หรือ General Data Protection Regulation (GDPR) ในปี พ.ศ. 2559 ซึ่งมีผลบังคับใช้เมื่อวันที่ 25 พฤษภาคม พ.ศ. 2561 เป็นต้น สำหรับประเทศไทยนั้นก็ได้มีการประกาศใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล คือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

เมื่อมาถึงยุคดิจิทัล (Digital Age) ความก้าวหน้าทางเทคโนโลยีได้ทำให้พฤติกรรมของมนุษย์เปลี่ยนไปจากเดิม มีการใช้อุปกรณ์เคลื่อนที่ (Mobile Devices) เช่น โทรศัพท์มือถือแบบสมาร์ทโฟน (smart phone) หรือ แท็บเล็ต (tablet) ในการทำธุรกรรม และใช้เพื่อเข้าร่วมกลุ่มสังคมออนไลน์ และกิจกรรมอื่น ๆ อีกมากมาย เมื่อผสมผสานกับการเพิ่มขึ้นของประเภทของอุปกรณ์ที่สามารถต่อเชื่อมกับอินเตอร์เน็ตได้ หรือ Internet of Things (IoT) ทำให้โอกาสที่จะมีการรั่วไหลของข้อมูลเพิ่มมากขึ้น เปิดโอกาสให้ที่ผู้ไม่หวังดีเจาะระบบได้ง่ายขึ้น ผู้เจาะระบบ หรือแฮกเกอร์ (hacker) ที่ไม่หวังดีสามารถล้วงเอาข้อมูลส่วนบุคคล และรหัสผ่านไป ซึ่งสามารถสร้างความเสียหายให้กับ

เจ้าของข้อมูล และกิจการต่าง ๆ ได้อย่างมาก ดังนั้นจึงมีแนวคิดในการนำข้อมูลอัตลักษณ์บุคคล หรือข้อมูลชีวภาพ (biometric) มาใช้ในการยืนยันตัวตน เพื่อเป็นการยกระดับการรักษาความปลอดภัยของข้อมูล เนื่องจากมีความเชื่อว่าข้อมูลชีวภาพนั้นไม่สามารถลอกเลียนได้

นอกเหนือจากการใช้ชีวภาพในการยืนยันตัวตน (authentication) เพื่อการเข้าใช้งานในระบบต่าง ๆ แล้ว ยังมีการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลชีวภาพกันอย่างแพร่หลาย เช่น การรักษาความปลอดภัยของสนามบินต่าง ๆ การสแกนลายนิ้วมือแทนการตอกบัตรลงเวลาเข้า-ออกของพนักงาน หรือ การใช้ Face ID ของ Apple เพื่อเข้าใช้งานโทรศัพท์ เป็นต้น สำหรับธุรกิจธนาคารได้เริ่มมีการเปลี่ยนมาใช้ชีวภาพในการยืนยันตัวตนมากขึ้น มีการให้บริการลูกค้าสำหรับการเปิดบัญชีธนาคารผ่านโทรศัพท์มือถือ หรือ แท็บเล็ตได้ โดยการถ่ายรูปเซลฟี (selfie) เช่น ธนาคาร First National Bank ในประเทศแอฟริกาใต้เริ่มให้บริการนี้สำหรับผู้ประกอบการขนาดกลางและขนาดย่อม (SME) เมื่อเดือนพฤษภาคม พ.ศ. 2561[1] และธนาคารไทยพาณิชย์ได้เปิดตัวบริการเปิดบัญชีโดยไม่ต้องมาธนาคาร หรือ EASY E-KYC ในเดือนกรกฎาคม พ.ศ. 2561[2] เป็นต้น ส่วนนครดูไบ ในประเทศสหรัฐอาหรับเอมิเรตส์ได้มีการใช้เทคโนโลยีจดจำใบหน้า (Facial Recognition) ในรถบัสโดยสาร เพื่อสังเกตอากัปกิริยาของพนักงานขับรถ หากพบว่าขณะขับรถพนักงานขับรถใช้โทรศัพท์มือถือ หรือแสดงความอ่อนล้า หรือไม่อยู่ในสภาพที่ควบคุมรถได้ ระบบจะส่งสัญญาณเตือน ซึ่งระบบนี้สามารถใช้ในการป้องกันการเกิดอุบัติเหตุได้เป็นอย่างดี[3]

ข้อมูลชีวภาพนั้น ถือเป็นข้อมูลที่มีความสำคัญ และเป็นข้อมูลที่มีลักษณะพิเศษกว่าข้อมูลส่วนบุคคลอื่น ๆ อย่างเช่น ชื่อ ที่อยู่ หมายเลขโทรศัพท์ อีเมลหรือ แม้กระทั่งรหัสผ่าน (password) ซึ่งหากมีการรั่วไหลหรือเอาข้อมูลเหล่านี้ไปใช้ในทางมิชอบ เจ้าของข้อมูลย่อมสามารถทำการเปลี่ยนแปลงข้อมูลนั้นได้อย่างง่ายดาย แต่ข้อมูลชีวภาพนั้นเป็นข้อมูลที่ติดตัวเจ้าของข้อมูลตลอดชีวิต และไม่สามารถทำการเปลี่ยนแปลงได้ แม้บางอย่าง เช่น หน้าตา หรือ ลายนิ้วมือ อาจเกิดการเปลี่ยนแปลงได้ แต่ไม่ใช่เรื่องง่ายที่จะทำการเปลี่ยนแปลง และข้อมูลชีวภาพบางอย่างไม่สามารถเปลี่ยนแปลงได้และจะคงอยู่กับเจ้าของข้อมูลไปตลอดชีวิต ดังนั้นการรั่วไหล การนำข้อมูลไปใช้ในทางมิชอบ หรือการขโมยข้อมูลชีวภาพนั้นอาจทำให้เกิดความเสียหายที่อาจไม่สามารถระงับ หรือแก้ไขได้ ดังนั้นการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลชีวภาพจึงควรมีการควบคุมด้วยความเข้มงวดในระดับที่สูงกว่าข้อมูลส่วนบุคคลอื่น ๆ

ในการประมวลผลข้อมูลชีวภาพนั้น จะมีการเก็บตัวอย่าง (collect sample) จากเจ้าของข้อมูล หลังจากนั้นระบบจะทำการแปลงตัวอย่างนั้นเป็นแม่แบบ (template) และเก็บแม่แบบนั้นไว้เพื่อนำไปใช้ในการเปรียบเทียบ (matching) ต่อไป การนำข้อมูลชีวภาพมาใช้ในการยืนยันตัวตนนั้นมาจากความเชื่อว่าการนำข้อมูลชีวภาพมาใช้นั้นมีความปลอดภัยสูงเนื่องจากไม่สามารถลอกเลียน

---

[1] Moloi, S. (2018). Opening a new bank account as easy as taking a selfie. iAfrikan. สืบค้นจาก https://www.iafrikan.com/2018/05/18/open-a-new-bank/

[2] “SCB EASY” เดินหน้าพัฒนาเทคโนโลยีเจาะกลุ่มลูกค้าใหม่ เปิดตัว “EASY E-KYC” ธนาคารแรกที่ให้บริการเปิดบัญชีลูกค้าใหม่โดยไม่ต้องมาธนาคาร. (2561). สืบค้นจาก https://www.scb.co.th/th/about-us/news/jul-2561/nws-easy-e-kyc.html

[3] Dunham, A. (2016). Dubai buses get safer thanks to facial recognition technology. สืบค้นจาก https://www.timeoutdubai.com/aroundtown/news/74054-dubai-buses-get-safer-thanks-to-facial-recognition-technology

ได้ และการนำแม่แบบที่เก็บไว้ไปสร้างข้อมูลชีวภาพ (biometric reconstruction) นั้นยังไม่สามารถทำได้ในปัจจุบัน แต่ด้วยความก้าวหน้าทางเทคโนโลยีที่มีมากขึ้นทุกวัน ทำให้ไม่มีใครสามารถรับรองได้ว่าเทคโนโลยีจะไม่สามารถพัฒนาไปถึงจุดที่สามารถลอกเลียนแบบข้อมูลชีวภาพได้ นอกจากนี้ยังมีผลการรายงานทางวิชาการที่ศึกษาการนำแม่แบบไปสร้างข้อมูลชีวภาพที่บ่งชี้ว่าการนำแม่แบบลายนิ้วมือไปสร้างข้อมูลลายนิ้วมือขึ้นมาใหม่นั้นสามารถทำได้[4]

จุดอ่อนที่สำคัญของเทคโนโลยีชีวภาพนั้นคือการปลอมเป็นเจ้าของข้อมูล (spoofing) ซึ่งการปลอมเป็นเจ้าของข้อมูลสำหรับข้อมูลชีวภาพบางชนิดนั้นไม่ยากอย่างที่คิด รูปถ่ายของเราสามารถหาได้ทั่วไปจากอินเตอร์เน็ต ส่วนลายนิ้วมือของเราสามารถหาได้จากสิ่งของที่เราสัมผัส เช่น แก้วน้ำ ราวบันได หรือปุ่มลิฟต์ เป็นต้น ทั้งนี้กลุ่ม Chaos Computer Club ได้ทำการปลอมลายนิ้วมือเพื่อปลดล็อคไอโฟนได้ภายใน 2 วันหลังจากการเปิดตัวของไอโฟน 5s ในปี 2013 และภายในปีเดียวกันสามารถปลดล็อคไอโฟนได้โดยใช้ปริ้นเตอร์ 3 มิติพิมพ์ลายนิ้วมือปลอมจากลายนิ้วมือที่ได้จากรูปถ่าย[5] นอกจากนี้เทคโนโลยี Deep Learning ยังทำให้สามารถนำข้อมูลแม่แบบที่ใช้ในการทำ Facial Recognition ไปสร้างเป็นใบหน้าได้อีกด้วย[6] และเมื่อเดือน มิถุนายน 2562 ได้มีการใช้เทคโนโลยี Deepfake ซึ่งเป็นการใช้ Artificial Intelligence และ Machine Learning เข้ามาทำงานร่วมกันเพื่อปลอมแปลงวิดีโอของบุคคลที่มีชื่อเสียง เช่น มาร์ก ซักเคอร์เบิร์ก และ ประธานาธิบดี โดนัลด์ ทรัมป์ เห็นได้ชัดว่าการใช้ข้อมูลชีวภาพนั้นมีความเสี่ยง

Gemalto ผู้ให้บริการระบบความคุ้มครองข้อมูล (Data Protection) ชั้นนำของโลก ได้เปิดเผยว่าภายในครึ่งปีแรกของ พ.ศ. 2561 มีจำนวนข้อมูลที่รั่วไหลไปมากกว่า 3.3 พันล้านรายการ รูปแบบของการโจมตีที่พบมากที่สุด (65%) คือการขโมยตัวตน (identity theft) ช่องทางการโจมตีที่พบมากที่สุด (56%) คือการบุกรุกจากบุคคลภายนอก (malicious outsider) หากสถิติที่สำคัญอย่างหนึ่งคือในบรรดาข้อมูลที่หลุดรั่วออกไปนั้น มีเพียง 3% เท่านั้นที่ได้มีการเข้ารหัสลับข้อมูล (encrypt) ไว้ ซึ่งการเข้ารหัสลับจะทำให้ผู้ที่ได้ข้อมูลไปไม่สามารถนำไปใช้งานต่อได้ หรือใช้ได้ด้วยความยากลำบากเนื่องจากจะต้องมีการถอดรหัส[7] นอกจากนั้นจากการสำรวจของ International Data Corporation (IDC) พบว่า ในยุคของ Digital Transformation การเปลี่ยนแปลงของสิ่งแวดล้อมทำให้มีการใช้ข้อมูลที่อ่อนไหวมากขึ้น และการเข้ารหัสลับข้อมูลอ่อนไหวเหล่านี้มีน้อยมาก อีกทั้งยังมีความคิดว่าการพัฒนาระบบป้องกันข้อมูลที่ดีนั้นมีอุปสรรค เนื่องจากความซับซ้อนของระบบข้อมูล[8]

---

[4] Bromba, M. (2006, 23/12/2006). On the reconstruction of biometric raw data from template data. สืบค้นจาก https://www.bromba.com/knowhow/temppriv.htm

[5] Smith, M., Mann, M., & Urbas, G. (2018). *Biometrics, Crime and Security*. New York: Routledge.p 9.

[6] Mai, G., Cao, K., Yuen, P. C., & Jain, A. K. (2018). On the Reconstruction of Face Images from Deep Face Templates. Retrieved from https://arxiv.org/pdf/1703.00832.pdf

[7] Gemalto. (2018). *Data Breaches Compromised 3.3 Billion Records in First Half of 2018*. Retrieved from https://www.gemalto.com/press/Pages/Data-Breaches-Compromised-3-3-Billion-Records-in-First-Half-of-2018.aspx

[8] International Data Corporation. (2019). *2019 Thales Data Threat Report – Global Edition*. Retrieved from https://www.thalesesecurity.com/2019/data-threat-report

เมื่อเดือนสิงหาคม 2562 ได้มีการค้นพบการรั่วไหลของข้อมูลลายนิ้วมือของคนกว่า 1 ล้านคน และข้อมูลใบหน้าจากระบบ Biostar 2 ซึ่งเป็นระบบรักษาความปลอดภัยแบบใช้ผ่านเว็ปไซต์ (Web-based) ของบริษัท Suprema โดย Biostar 2 ให้บริการด้านการรักษาความปลอดภัยโดยใช้ข้อมูลชีวภาพประเภทจดจำใบหน้า (facial recognition) และลายนิ้วมือ (fingerprint) เพื่อใช้ในการเข้าถึงพื้นที่ต้องห้าม (secured area access control) และการจัดการสิทธิและบทบาทผู้ใช้งาน (user permission management) ระบบ Biostar 2 นั้นได้ถูกนำไปใช้ในระบบ AEOS ซึ่งเป็นระบบการควบคุมการเข้า-ออก (access control system) ซึ่งมีผู้ใช้กว่า 5,700 องค์กร ใน 83 ประเทศ รวมถึงหน่วยงานรัฐบาล องค์กรขนาดใหญ่ ธนาคาร และ ตำรวจนครบาลของสหราชอาณาจักร (UK Metropolitan Police) การรั่วไหลในกรณีนี้พบว่าไม่ได้มีการป้องกันฐานข้อมูล อีกทั้งข้อมูลลายนิ้วมือและภาพถ่ายนั้น ไม่ได้มีการเปลี่ยนเป็นแม่แบบ รวมถึงไม่ได้มีการเข้ารหัสแต่อย่างใด[9]

เมื่อเดือนกรกฎาคม 2562 คณะกรรมการสมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA) ซึ่งเป็นองค์กรที่ไม่แสวงหากำไรของกลุ่มนักวิชาชีพด้านความมั่นคงปลอดภัยสารสนเทศในประเทศไทย ได้แสดงความคิดเห็นว่า การเก็บข้อมูลชีวภาพในหนังสือเดินทางของประเทศไทยนั้นเป็นการเก็บข้อมูลที่มากเกินความจำเป็น เนื่องจากเก็บทั้งภาพถ่าย และลายนิ้วมือทั้งสิบนิ้ว[10] ในขณะที่องค์กรธุรกิจหลายแห่งได้ใช้การสแกนลายนิ้วมือเพื่อบันทึกเวลาการทำงานของพนักงาน นอกจากนี้โรงเรียนหลายแห่งได้ใช้การสแกนลายนิ้วมือ หรือสแกนใบหน้าเพื่อควบคุมการเข้า-ออกของนักเรียนอีกด้วย

แม้ขณะนี้หลาย ๆ ประเทศทั่วโลกได้มีการประกาศใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล แต่อาจไม่ได้ให้ความสำคัญกับข้อมูลชีวภาพอย่างเพียงพอ หรืออาจไม่มีการระบุว่าข้อมูลชีวภาพนั้นเป็นข้อมูลส่วนบุคคลที่ควรมีการควบคุมดูแลอย่างเข้มงวดกว่าข้อมูลส่วนบุคคลอื่น ๆ และมิได้แยกกฎหมายคุ้มครองข้อมูลชีวภาพออกมาเป็นกฎหมายเฉพาะ ในขณะเดียวกันอีกหลายประเทศเริ่มตระหนักถึงความเสียหายที่อาจเกิดขึ้นได้จากการรั่วไหลของข้อมูลชีวภาพ และการนำข้อมูลชีวภาพไปใช้ในทางมิชอบ โดยประเทศสหรัฐอเมริกาได้ประกาศใช้กฎหมายควบคุมข้อมูลชีวภาพใน 7 รัฐ คือ อิลลินอยส์ เท็กซัส วอชิงตัน แคลิฟอร์เนีย ออริกอน นิวยอร์ก และอาร์คันซอ โดยรัฐอิลลินอยส์นั้นบัญญัติเป็นกฎหมายเฉพาะสำหรับข้อมูลส่วนบุคคลประเภทชีวภาพเรียกว่า Biometric Information Privacy Act ส่วนรัฐเท็กซัสนั้นได้บัญญัติกฎหมายควบคุมข้อมูลชีวภาพไว้เป็นส่วนหนึ่งของกฎหมายพาณิชย์ ภายใต้ Texas Business and Commerce Code ใน BUS & COM 503.001 Capture or Use of Biometric Identifier สำหรับรัฐวอชิงตันนั้นได้บัญญัติกฎหมายคุ้มครองข้อมูลชีวภาพไว้ภายใต้ Washington House Bill 1493 (2017) ทางด้านรัฐแคลิฟอร์เนียได้บัญญัติกฎหมายคุ้มครองข้อมูลชีวภาพไว้เป็นส่วนหนึ่งใน California Consumer Privacy Act (CCPA) ซึ่งมีผลบังคับใช้ไปเมื่อวันที่ 1 มกราคม พ.ศ. 2563 พร้อมกันกับกฎหมายคุ้มครองข้อมูลชีวภาพของรัฐออริกอนซึ่งทำการเพิ่มบทบัญญัติให้ Consumer Information Protection Act (OCIPA, ORS 646A-600, *et seq*.)

---

[9] vpnMentor. (2019). *Report: Data Breach in Biometric Security Platform Affecting Millions of Users*. Retrieved from https://www.vpnmentor.com/blog/report-biostar2-leak/

[10] สกู๊ปข่าวหน้า 1 นสพ.มติชนรายวัน 21 กันยายน 2562. (2562). เทคโนโลยีระบุตัวตน “ชีวมาตร” น่ากลัวหรือไม่. สืบค้นจาก https://www.matichon.co.th/news-monitor/news_1679649

คุ้มครองข้อมูลส่วนบุคคลชีวภาพ ทางด้านรัฐนิวยอร์กได้ประกาศใช้ Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) ในเดือนมีนาคม พ.ศ. 2563 ทางด้านรัฐอาร์คันซอได้ทำการขยายกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Personal Information Protection Act - PIPA) ให้ครอบคลุมไปถึงข้อมูลส่วนบุคคลชีวภาพในปี พ.ศ. 2562 และสำหรับ GDPR ของสหภาพยุโรปนั้นได้มีการให้ความสำคัญกับข้อมูลชีวภาพเป็นพิเศษ โดยจัดข้อมูลชีวภาพเป็นข้อมูลส่วนบุคคลพิเศษ (special categories of personal data) ซึ่งต้องมีการควบคุมการประมวลผลในระดับที่สูงกว่าข้อมูลส่วนบุคคลอื่น ๆ สำหรับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของประเทศไทยเองนั้นได้กำหนดให้ข้อมูลชีวภาพเป็นข้อมูลที่มีความอ่อนไหวสูงตามที่บัญญัติไว้ใน มาตรา 26 แต่มิได้มีการกำหนดมาตรการ แนวทาง หลักเกณฑ์ หรือข้อปฏิบัติในการคุ้มครองข้อมูลชีวภาพ หรือข้อมูลที่มีความอ่อนไหวสูงอื่น ๆ ที่ต่างไปจากข้อมูลส่วนบุคคลอื่น ๆ

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นได้มีการประกาศในราชกิจจานุเบกษาเมื่อวันที่ 27 พฤษภาคม พ.ศ. 2562 โดยให้มีผลบังคับใช้เพียงบางส่วนในวันที่ 28 พฤษภาคม พ.ศ. 2562 คือมีผลบังคับใช้เฉพาะ หมวด 1 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และหมวด 4 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล สำหรับ หมวด 2 การคุ้มครองข้อมูลส่วนบุคคล หมวด 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล หมวด 5 การร้องเรียน หมวด 6 ความรับผิดทางแพ่ง หมวด 7 บทกำหนดโทษ และความในมาตรา 95 และ มาตรา 96 นั้นให้มีผลบังคับใช้ 1 ปี หลังจากวันประกาศในราชกิจจานุเบกษา ทำให้หมวดและมาตราดังกล่าวจะมีผลบังคับใช้ในวันที่ 27 พฤษภาคม พ.ศ. 2563 นอกจากนี้ มาตรา 96 ของพระราชบัญญัติฉบับนี้กำหนดให้ดำเนินการออกระเบียบ และประกาศทั้งหมดให้แล้วเสร็จภายใน 1 ปีนับแต่วันที่พระราชบัญญัติฉบับนี้ใช้บังคับทั้งฉบับ ซึ่งหมายความว่ากฎหมายลำดับรอง และกฎระเบียบต่าง ๆ จะออกมาบังคับใช้อย่างครบถ้วนภายในวันที่ 27 พฤษภาคม พ.ศ. 2564

อย่างไรก็ดี ในปัจจุบันแม้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลจะมีผลบังคับใช้แล้วก็ตาม หากการประกาศใช้พระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563 นั้นมีผลให้หน่วยงาน และกิจการ 22 กิจการมิได้อยู่ภายใต้บังคับของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลจนกว่าจะสิ้นสุดการบังคับใช้พระราชกฤษฎีกาฉบับดังกล่าวในวันที่ 31 พฤษภาคม พ.ศ. 2564

ขณะนี้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลอยู่ในขั้นตอนของการร่างกฎหมายลำดับรอง จึงเป็นที่น่ากังวลว่าข้อมูลชีวภาพเหล่านี้จะได้รับการคุ้มครองอย่างเหมาะสมหรือมีการกำหนดวิธีการรักษาความปลอดภัยที่ดีพอหรือไม่ ดังที่กล่าวมาแล้วว่าการรั่วไหลของข้อมูลชีวภาพนั้นสามารถก่อให้เกิดความเสียหายที่ไม่อาจระงับ หรือแก้ไขได้ จึงควรมีกฎเกณฑ์ในการเก็บรวบรวม ใช้ และเปิดเผยที่เข้มงวดกว่าข้อมูลส่วนบุคคลประเภทอื่น โดยอาจควบคุมการเก็บรวบรวมข้อมูลชีวภาพให้กระทำได้เท่าที่จำเป็น และต้องมีการศึกษาผลกระทบของการเก็บรวบรวมข้อมูลชีวภาพเสียก่อน รวมทั้งในขั้นตอนการขอความยินยอมควรมีการแจ้งให้ทราบถึงผลกระทบของการเก็บข้อมูลชีวภาพ นอกจากนี้กระบวนการในการร้องเรียน หรือฟ้องร้องการละเมิดข้อมูลชีวภาพนั้นควรมีความแตกต่างจากกระบวนการร้องเรียนสำหรับข้อมูลส่วนบุคคลอื่น ๆ โดยไม่ควรรอให้เกิดความเสียหายก่อนจึงจะ

อนุญาตให้ทำการร้องเรียน หรือฟ้องร้องตามกฎหมายได้ และอาจต้องพิจารณาความเหมาะสมของบทลงโทษสำหรับกรณีการกระทำผิดที่เกี่ยวกับข้อมูลชีวภาพให้มีความเหมาะสมอีกด้วย

ผู้วิจัยเห็นว่าการกำหนดกฎเกณฑ์ต่าง ๆ ที่เกี่ยวข้องกับข้อมูลชีวภาพนั้น ควรกระทำด้วยความระมัดระวัง และรอบคอบโดยมีการศึกษากฎหมายของต่างประเทศเพื่อหาแนวทางในการคุ้มครองข้อมูลส่วนบุคคลประเภทชีวภาพที่เหมาะสม จึงเห็นสมควรที่จะทำการวิจัยในเรื่องนี้ต่อไป

2. วัตถุประสงค์การวิจัย

2.1 ศึกษาแนวความคิดเกี่ยวกับข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลชีวภาพ และลักษณะทั่วไปของเทคโนโลยีเกี่ยวกับการใช้ข้อมูลชีวภาพ

2.2 ศึกษามุมมองที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล สำหรับข้อมูลประเภทชีวภาพตามกฎหมาย General Data Protection Regulation (GDPR) ของสหภาพยุโรป และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร และกฎหมายคุ้มครองข้อมูลชีวภาพของรัฐอิลลินอยส์ ประเทศสหรัฐอเมริกา

2.3 วิเคราะห์ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เปรียบเทียบกับส่วนที่เกี่ยวข้องกับข้อมูลชีวภาพตามกฎหมาย General Data Protection Regulation (GDPR) ของสหภาพยุโรป และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร และกฎหมายคุ้มครองข้อมูลชีวภาพของรัฐอิลลินอยส์ ประเทศสหรัฐอเมริกา

2.4 ศึกษาแนวทางในการปรับปรุงกฎหมายการคุ้มครองข้อมูลส่วนบุคคลประเภทชีวภาพ

3. สมมติฐานการวิจัย

เนื่องจากข้อมูลส่วนบุคคลประเภทชีวภาพนั้นถือเป็นข้อมูลประเภทพิเศษที่มีความอ่อนไหวสูง ความเสียหายที่อาจเกิดขึ้นจากการรั่วไหล และนำข้อมูลไปใช้ในทางที่ผิดนั้นไม่สามารถระงับได้ ดังนั้นกฎหมายจึงควรให้ความคุ้มครอง และการกำกับดูแลให้มากกว่าข้อมูลส่วนบุคคลประเภทอื่น

4. ขอบเขตของการวิจัย

การศึกษาวิจัยครั้งนี้ ผู้วิจัยมุ่งเน้นถึงปัญหาตามบทบัญญัติใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยทำการศึกษาเฉพาะการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลประเภทชีวภาพของภาคเอกชนเท่านั้น ทั้งนี้ผู้วิจัยจะดำเนินการศึกษาจาก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เปรียบเทียบกับกฎหมาย General Data Protection Regulation (GDPR) ของสหภาพยุโรป และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร (DPA) และกฎหมายคุ้มครองข้อมูลส่วนบุคคลชีวภาพของรัฐอิลลินอยส์ ประเทศสหรัฐอเมริกา (BIPA)

5. นิยามศัพท์เฉพาะ

5.1 ข้อมูลชีวภาพ (Biometric Data) หมายถึง ข้อมูลชีวมาตร หรือ ข้อมูลชีวมิติ หรือ ข้อมูลอัตลักษณ์ส่วนบุคคล หรือข้อมูลไบโอเมตริก ซึ่งคือคุณลักษณะหรือพฤติกรรมบางอย่าง ที่ถูกใช้ในการแยกแยะบุคคลด้วยวิธีการทางเทคโนโลยี ข้อมูลชีวภาพสามารถได้มาด้วยหลายวิธีการ เช่น จากลายนิ้วมือ ใบหน้า จอตา ม่านตา รูปทรงของฝ่ามือ เสียงพูด ลายมือเขียน เป็นต้น

5.2 ข้อมูลชีวภาพตั้งต้น (Biometric sample) หมายถึง ข้อมูลชีวภาพที่เกิดจากการรวบรวมลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลและนำมาแปลงให้อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์ โดยข้อมูลดังกล่าวเป็นข้อมูลตั้งต้นที่ยังไม่ถูกประมวลให้เป็นข้อมูลชีวภาพแม่แบบ เช่น ภาพใบหน้าที่ถูกถ่ายเพื่อนำไปใช้กับเทคโนโลยีการเปรียบเทียบใบหน้า หรือ ภาพลายนิ้วมือที่ถูกถ่ายเพื่อนำไปใช้กับเทคโนโลยีการเปรียบเทียบลายนิ้วมือ เป็นต้น

5.3 ข้อมูลชีวภาพแม่แบบ (Biometric template) หมายถึง ข้อมูลชีวภาพที่เป็นผลลัพธ์จากการประมวลผลข้อมูลชีวภาพตั้งต้นโดยผ่านกระบวนการใช้เทคนิคหรือเทคโนโลยี โดยถูกทำให้อยู่ในรูปแบบที่สามารถนำไปใช้เพื่อเปรียบเทียบข้อมูลชีวภาพของบุคคล เช่น พิกัดตำแหน่งของจุดสังเกตสำคัญต่าง ๆ บนใบหน้า

5.4 ข้อมูลส่วนบุคคลธรรมดา หมายถึง ข้อมูลส่วนบุคคลที่มิใช่ข้อมูลส่วนบุคคลที่มีความอ่อนไหว เช่น ชื่อ นามสกุล เป็นต้น

5.5 ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) หมายถึง ข้อมูลส่วนบุคคลที่เกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในลักษณะเดียวกัน

5.6 เจ้าของข้อมูลชีวภาพ หรือ เจ้าของข้อมูลส่วนบุคคลชีวภาพ หรือ เจ้าของข้อมูลส่วนบุคคลประเภทชีวภาพ หมายถึง ผู้ที่เป็นเจ้าของข้อมูลชีวภาพ เช่น เจ้าของลายนิ้วมือ เจ้าของจอตา หรือม่านตา เจ้าของข้อมูลในที่นี้มิได้หมายถึงผู้ที่มีข้อมูลส่วนบุคคลอยู่ในครอบครอง

5.7 เจ้าของข้อมูลส่วนบุคคล (Data Subject) หมายถึง ผู้ที่เป็นเจ้าของข้อมูลส่วนบุคคล ซึ่งเป็นข้อมูลที่ใช้ระบุตัวบุคคลได้ เช่น เจ้าของชื่อ ที่อยู่ หมายเลขโทรศัพท์ เจ้าของข้อมูลในที่นี้มิได้หมายถึงผู้ที่มีข้อมูลส่วนบุคคลอยู่ในครอบครอง

5.8 ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หมายถึง บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ทั้งนี้ผู้ควบคุมข้อมูลส่วนบุคคลมิใช่เจ้าของข้อมูลส่วนบุคคล

5.9 ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าว ต้องไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

6. ระเบียบวิธีวิจัย

การศึกษาค้นคว้าเรื่องนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) โดยการศึกษาและวิจัยเอกสาร (Documentary Research) จากกฎหมาย ตำรา บทความ และเอกสารที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลประเภทชีวภาพ ทั้งภาษาไทย และภาษาต่างประเทศจากแหล่งต่าง ๆ ไม่ว่าจะเป็นห้องสมุด หรือจากเว็บไซต์ต่าง ๆ ในเครือข่ายอินเตอร์เน็ต เพื่อหาแนวทางที่เหมาะสมในการปรับปรุงกฎหมายคุ้มครองข้อมูลส่วนบุคคลประเภทชีวภาพต่อไป

7. ประโยชน์ที่คาดว่าจะได้รับ

7.1 ได้ทราบแนวความคิดเกี่ยวกับข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลชีวภาพ และลักษณะทั่วไปของข้อมูลชีวภาพ

7.2 ได้ทราบมุมมองที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล สำหรับข้อมูลประเภทชีวภาพตามกฎหมาย General Data Protection Regulation (GDPR) ของสหภาพยุโรป และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร และกฎหมายคุ้มครองข้อมูลชีวภาพของรัฐอิลลินอยส์ ประเทศสหรัฐอเมริกา

7.3 เข้าใจความแตกต่างระหว่าง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 General Data Protection Regulation (GDPR) ของสหภาพยุโรป และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร และกฎหมายคุ้มครองข้อมูลชีวภาพของรัฐอิลลินอยส์ ประเทศสหรัฐอเมริกา ในส่วนที่เกี่ยวข้องกับข้อมูลชีวภาพตามกฎหมาย

7.4 นำเสนอแนวทางในการปรับปรุงกฎหมายการคุ้มครองข้อมูลส่วนบุคคลประเภทชีวภาพ

บทที่ 2
แนวคิดของการคุ้มครองข้อมูลส่วนบุคคล และลักษณะทั่วไปของข้อมูลชีวภาพ

ข้อมูลชีวภาพ หรือข้อมูลไบโอเมตริกเป็นข้อมูลส่วนบุคคลที่มีความสำคัญ และมีความอ่อนไหวมาก ในปัจจุบันการใช้ข้อมูลชีวภาพในประเทศไทยอาจยังไม่แพร่หลายเท่ากับในต่างประเทศ และประชาชนยังไม่ตระหนักถึงความรุนแรงของความเสียหายที่อาจเกิดขึ้นได้จากการรั่วไหลของข้อมูลชีวภาพ หรือการนำข้อมูลชีวภาพไปใช้ในทางมิชอบ เมื่อข้อมูลชีวภาพถือว่าเป็นข้อมูลส่วนบุคคลประเภทหนึ่ง ดังนั้นในการศึกษาแนวคิดและวิวัฒนาการของการคุ้มครองข้อมูลชีวภาพจึงควรเริ่มต้นจากการศึกษาแนวคิด และวิวัฒนาการของการคุ้มครองข้อมูลส่วนบุคคลเสียก่อน

1. แนวคิดของการคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัติประกอบรัฐธรรมนูญ ว่าด้วยคณะกรรมการสิทธิมนุษยชนแห่งชาติ พ.ศ. 2560 ได้ให้ความหมายของ “สิทธิมนุษยชน” ไว้ในมาตรา 4 ดังนี้ “สิทธิมนุษยชน หมายความว่า ศักดิ์ศรีความเป็นมนุษย์ สิทธิ เสรีภาพและความเสมอภาคของบุคคล บรรดาที่ได้รับการรับรองหรือคุ้มครองตามรัฐธรรมนูญ ตามกฎหมาย หรือตามหนังสือสัญญาที่ประเทศไทยเป็นภาคีและมีพันธกรณีที่จะต้องปฏิบัติตาม”

ข้อมูลส่วนบุคคลเป็นข้อมูลที่เกี่ยวข้องกับเจ้าของข้อมูลโดยตรง หรือสามารถใช้เชื่อมโยงไปยังเจ้าของข้อมูลได้ ข้อมูลส่วนบุคคลนั้นเป็นส่วนหนึ่งของสิทธิความเป็นส่วนตัว (Privacy) อันเป็นสิทธิขั้นพื้นฐานของบุคคล ซึ่งได้รับการรับรองในปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights) มาตรา 12 ดังนี้

> *“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.”*[11]
>
> *“บุคคลใดจะถูกแทรกแซงตามอำเภอใจในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย หรือการสื่อสาร หรือจะถูกลบหลู่เกียรติยศและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองของกฎหมายต่อการแทรกแซงสิทธิหรือการลบหลู่ดังกล่าวนั้น”*[12]

---

[11] ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน มาตรา 12.

[12] ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน แปลโดยกระทรวงการต่างประเทศ.

เมื่อความก้าวหน้าของเทคโนโลยีเจริญก้าวหน้าขึ้น การสืบค้น การแพร่กระจายของข้อมูลทำได้ง่าย และรวดเร็ว จึงมีแนวคิดที่จะพัฒนากฎหมายการคุ้มครองข้อมูลส่วนบุคคล เพื่อมิให้ผู้ใดนำข้อมูลส่วนบุคคลไปใช้ในทางมิชอบ อันจะสร้างความเสียหายไม่ว่าจะเป็นในด้านชื่อเสียง ทรัพย์สิน หรือความปลอดภัย ให้แก่ผู้เป็นเจ้าของข้อมูล

1.1 ความหมายของข้อมูลส่วนบุคคล

แต่ละประเทศได้ให้ความหมายของคำว่า “ข้อมูลส่วนบุคคล” ต่างกันออกไป โดยมาตรา 4 ของ GDPR ได้ให้ความหมายของข้อมูลส่วนบุคคลว่า เป็นข้อมูลที่เกี่ยวข้องกับบุคคลธรรมดาซึ่งใช้ระบุตัวตน (Identified) หรืออาจใช้ระบุตัวตน (Identifiable) บุคคลนั้นได้ ไม่ว่าโดยทางตรงหรือทางอ้อม ซึ่งนอกเหนือจาก ชื่อ นามสกุล หมายเลขบัตรประจำตัวประชาชนแล้ว ยังรวมไปถึง ข้อมูลตำแหน่งที่ตั้ง (Location Data) สิ่งระบุตัวบุคคลออนไลน์ (Online Identifier) และข้อมูลสรีรวิทยา พันธุกรรม จิตใจ เศรษฐกิจ วัฒนธรรม หรือ สังคมของบุคคลนั้นอีกด้วย[13]

The Data Protection Act 2018 (DPA) ซึ่งเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักรได้ให้ความหมายของข้อมูลส่วนบุคคลไว้ ว่าเป็นข้อมูลที่เกี่ยวกับบุคคลที่ยังมีชีวิตอยู่ที่ใช้ระบุตัวตนบุคคลได้ หรืออาจนำไปใช้เพื่อระบุตัวตนบุคคลได้[14]

องค์การเพื่อความร่วมมือและการพัฒนาทางเศรษฐกิจ (Organisation for Economic Co-operation and Development) ได้ให้ความหมายของคำว่า ข้อมูลส่วนบุคคล ว่า “เป็นข้อมูลที่เกี่ยวกับบุคคลที่ยังมีชีวิตอยู่ที่ใช้ระบุตัวตนบุคคลนั้นได้ หรืออาจนำไปใช้ระบุตัวตนบุคคลนั้นได้”[15]

สำหรับ Personal Data Protection Act 2010 (PDPA) ของประเทศมาเลเซียได้ให้ความหมายของข้อมูลส่วนบุคคลไว้ว่า เป็นข้อมูลใด ๆ ที่เกี่ยวข้องกับการทำธุรกรรมเชิงพาณิชย์ ซึ่งเกี่ยวข้องกับบุคคลธรรมดาไม่ว่าโดยตรง หรือโดยอ้อมที่สามารถใช้ระบุตัวตน (Identified) หรืออาจใช้ระบุตัวตน (Identifiable) ของบุคคลได้โดยข้อมูลนั้น ๆ หรือโดยข้อมูลอื่นใดที่อยู่ในครอบครองของผู้

---

[13] GDPR, 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.

[14] The Data Protection Act, Part I “Personal data” means any information relating to an identified or identifiable living individual (subject to subsection (14)(c)).

[15] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Part One – General Definitions. "personal data" means any information relating to an identified or identifiable individual (data subject).

ประมวลผลข้อมูล สำหรับข้อมูลอ่อนไหวนั้น PDPA ระบุให้จำกัดอยู่เพียงข้อมูลส่วนบุคคลที่เกี่ยวข้องกับสุขภาพ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา และประวัติอาชญากรรมเท่านั้น[16]

ประเทศสิงคโปร์ได้ให้คำจำกัดความของข้อมูลส่วนบุคคลไว้ใน Personal Data Protection Act 2012 ว่าเป็นข้อมูลที่ไม่ว่าจะจริงหรือไม่จริง สามารถนำไปใช้ระบุตัวตนของปัจเจกบุคคลได้จากข้อมูลนั้น หรือใช้ข้อมูลนั้นประกอบกับข้อมูลอื่นใดที่องค์กรนั้นมีอยู่หรือสามารถเข้าถึงได้[17]

สำหรับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ให้คำจำกัดความของข้อมูลส่วนบุคคลไว้ในมาตรา 6 ดังนี้ “ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ”

1.2 องค์ประกอบของข้อมูลส่วนบุคคล

องค์ประกอบของข้อมูลส่วนบุคคล มี 2 องค์ประกอบ ซึ่งหากไม่ครบองค์ประกอบทั้ง 2 นี้จะไม่ถือว่าเป็นข้อมูลส่วนบุคคล องค์ประกอบทั้ง 2 คือ

1) องค์ประกอบด้านเนื้อหา ซึ่งประกอบด้วย

(1) ข้อมูลข่าวสารที่เป็นสิ่งเฉพาะตัวบุคคล เช่น ชื่อ ที่อยู่ อาชีพ เป็นต้น

(2) ข้อมูลที่บ่งบอกให้รู้ตัวบุคคล เช่น รหัส หรือเลขประจำตัว ลักษณะทางกายภาพ อีเมล หรือ หมายเลขโทรศัพท์มือถือ เป็นต้น

(3) ข้อมูลที่เป็นความลับของบุคคล เช่น ประวัติทางการแพทย์ สุขภาพอนามัย ประวัติอาชญากรรม ข้อมูลทางการเงิน เป็นต้น

2) องค์ประกอบด้านรูปแบบ ซึ่งประกอบด้วย

(1) องค์กรที่เป็นผู้เก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล โดยหลักกฎหมายในอดีตถือว่าผู้ที่ทำหน้าที่จัดเก็บเป็นผู้มีกรรมสิทธิ์ในข้อมูล คือเป็นเจ้าของข้อมูลส่วนบุคคลนั้น แต่ภายหลังได้มีการวิวัฒนาการในเรื่องนี้และปัจจุบันถือว่าเจ้าของข้อมูลคือบุคคลธรรมดามิใช่องค์กรผู้จัดเก็บรวบรวมข้อมูล

---

[16] Personal Data Protection Act 2010. “personal data” means any information in respect of commercial transactions, which (a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose; (b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject; but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010;

[17] “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 organisation has or is likely to have access;

(2) วิธีการ หรือช่องทาง หรือสื่อที่ใช้ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ไม่ว่าจะเป็นในรูปของเอกสาร รายงาน แผนที่ ภาพถ่าย การบันทึกภาพหรือเสียง รวมถึงการบันทึกโดยเครื่องคอมพิวเตอร์[18]

1.3 ประเภทของข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลสามารถแบ่งออกได้เป็น 2 ประเภท คือ

1) ข้อมูลส่วนบุคคลทั่วไป (Non-sensitive data) เป็นข้อมูลที่เกี่ยวกับบุคคลที่สามารถใช้ระบุตัวตนของบุคคล เช่น ชื่อ นามสกุล ที่อยู่ หมายเลขโทรศัพท์ อายุ หรือข้อมูลใด ๆ ที่โดยสภาพแล้วเป็นข้อมูลที่สามารถเปิดเผยต่อสาธารณะได้ และสามารถนำมาประมวลผลเป็นข้อเท็จจริงเพื่อใช้ระบุตัวตนบุคคลได้

2) ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive data) เป็นข้อมูลที่เป็นเรื่องเฉพาะตัวบุคคล ที่อาจเป็นความลับ หรือเป็นข้อมูลที่เจ้าของข้อมูลไม่ประสงค์ให้เปิดเผย หรือหากเปิดเผยไปอาจเกิดผลกระทบต่อเจ้าของข้อมูล เช่น สถานะทางการเงิน ประวัติอาชญากรรม ประวัติสุขภาพ และข้อมูลชีวภาพ เป็นต้น

1.4 สิทธิความเป็นส่วนตัวกับข้อมูลส่วนบุคคล

เทคโนโลยี กับสิทธิส่วนบุคคลนั้นมีความสัมพันธ์ระหว่างกันอย่างไม่อาจปฏิเสธได้ โดยเมื่อมีการพัฒนาทางด้านเทคโนโลยี แนวความคิดของสิทธิความเป็นส่วนตัวก็จะพัฒนาตามควบคู่กันไป โดยเห็นได้ชัดจากการพัฒนาของสิทธิส่วนบุคคล 4 ประเภทมาเป็นสิทธิส่วนบุคคล 7 ประเภท

1.4.1 สิทธิส่วนบุคคล 4 ประเภท

ในช่วงกลางทศวรรษที่ 1990 โรเจอร์ คล้าก (Roger Clarke) ที่ปรึกษาด้านการจัดการข้อมูล และเทคโนโลยีสารสนเทศ ได้จัดประเภทของสิทธิความเป็นส่วนตัวออกเป็น 4 ประเภท ดังนี้

1) ความเป็นส่วนตัวของบุคคล (Privacy of the person) เป็นสิทธิความเป็นส่วนตัวที่เกี่ยวข้องกับร่างกายของบุคคลนั้น ๆ ที่สมควรได้รับความคุ้มครองมิให้ผู้อื่นมาล่วงละเมิดได้ ซึ่งนอกจากจะหมายความถึงการล่วงเกินทางร่างกายโดยทั่วไป เช่น การแตะเนื้อต้องตัวโดยไม่ได้รับความยินยอมแล้ว ยังหมายความรวมถึง การทรมานทางร่างกาย การบังคับให้ทำหมัน การให้เลือดโดยไม่ได้รับความยินยอม การบังคับให้ส่งตัวอย่างของเหลวในร่างกาย หรือเนื้อเยื่อ และการบังคับให้ส่งข้อมูลทางชีวภาพอีกด้วย

2) ความเป็นส่วนตัวด้านพฤติกรรมของบุคคล (Privacy of personal behaviour) หมายถึง การคุ้มครองสิ่งที่เกี่ยวข้องกับพฤติกรรมทั้งหมด ไม่ว่าจะเป็นการแสดงออกทางศาสนา พฤติกรรมทางเพศ การทำกิจกรรมทางการเมือง ซึ่งนอกเหนือจากพฤติกรรมแล้ว Clarke ยัง

---

[18] จันทจิรา เอี่ยมมยุรา. (2547). การคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย. วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, *34*(4), น. 637.

เห็นว่าบุคคลควรมีพื้นที่ (space) ที่จะใช้ทำกิจกรรมตามความเชื่อของตนเองในที่รโหฐานและมีสิทธิที่จะไม่ถูกจับตามองในพื้นที่สาธารณะ

3) ความเป็นส่วนตัวของข้อมูลส่วนบุคคล (Privacy of personal data) หมายถึงการคุ้มครองข้อมูลส่วนบุคคล

4) ความเป็นส่วนตัวของการสื่อสารของบุคคล (Privacy of personal communication) เป็นสิทธิที่เกี่ยวกับความเป็นส่วนตัวในการสื่อสารโดยปราศจากการดักฟัง หรือจับตามอง ไม่ว่าจะเป็นการสื่อสารทาง อีเมล โทรศัพท์ การพูดคุยในลักษณะเผชิญหน้า (face-to-face) หรือการพูดคุยแบบระยะไกล (Virtual Communication)[19]

นอกจากนี้ โรเจอร์ คล้าก ยังได้ให้ความเห็นว่า เนื่องจากการสื่อสารและระบบคอมพิวเตอร์มีความเกี่ยวเนื่องอย่างไม่สามารถแยกออกจากกันได้ ทำให้ความเป็นส่วนตัวของการสื่อสารของบุคคลและความเป็นส่วนตัวของข้อมูลส่วนบุคคลนั้นมีความสัมพันธ์กันอย่างใกล้ชิด และสามารถเรียกรวม ๆ ได้ว่า ความเป็นส่วนตัวทางข้อมูลสารสนเทศ (Information Privacy)[20]

1.4.2 สิทธิส่วนบุคคล 7 ประเภท

เทคโนโลยีสมัยใหม่ เช่น อากาศยานไร้คนขับ (Unmanned Aerial Vehicle) เทคโนโลยีวิเคราะห์การลำดับเบสยุคที่สอง (second-generation DNA) หรือ เทคโนโลยีเพื่อพัฒนาความสามารถของบุคลากร แม้กระทั่งเทคโนโลยีชีวภาพยุคที่สอง ล้วนแล้วแต่เป็นความก้าวหน้าทางเทคโนโลยีที่ทำให้เกิดประเด็นในด้านสิทธิส่วนบุคคล ซึ่งทำให้การแบ่งประเภทของสิทธิส่วนบุคคล 4 ประเภทตามที่โรเจอร์ คล้ากได้แบ่งไว้นั้นไม่สามารถครอบคลุมประเด็นต่าง ๆ ได้อย่างเพียงพออีกต่อไป ทำให้ต้องมีการเพิ่มประเภทของสิทธิส่วนบุคคล โดย Rachel Finn, David Wright และ Michael Friederwald ได้ทำการขยายประเภทของสิทธิส่วนบุคคลออกเป็น 7 ประเภท ดังนี้

1) ความเป็นส่วนตัวของบุคคล (Privacy of the person) ความเป็นส่วนตัวของบุคคลตามความหมายของ Finn, Wright และ Friederwald นั้น ได้ขยายความครอบคลุมไปถึงสิทธิความเป็นส่วนตัวในการทำงานของร่างกาย (bodily function) และ คุณลักษณะเฉพาะทางร่างกาย (เช่น รหัสพันธุกรรม และชีวภาพ)

2) ความเป็นส่วนตัวด้านพฤติกรรม และการกระทำ (Privacy of behaviour and action) นั้น นอกจากการคุ้มครองสิ่งที่เกี่ยวข้องกับพฤติกรรมแล้ว Rachel Finn, David Wright และ Michael Friederwald เห็นว่าควรมีการคุ้มครองสิทธิส่วนบุคคลในส่วนของการกระทำด้วย ไม่ว่าจะเป็นในที่รโหฐาน หรือในพื้นที่สาธารณะโดยมีความเป็นอิสระ ปราศจากการเฝ้าดู หรือควบคุม

---

[19] Clarke, R. (1997). *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*. In X. Consultancy (Ed.). Retrieved from http://www.rogerclarke.com/DV/Intro.html

[20] Clarke, R. (1997). *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*. In X. Consultancy (Ed.). Retrieved from http://www.rogerclarke.com/DV/Intro.html

ตราบที่ไม่เป็นการละเมิดสิทธิของผู้อื่น หรือทำให้ผู้อื่นเดือดร้อนรำคาญ เช่น การแต่งตัวด้วยเสื้อผ้าที่ตนเองเลือก หรือการนั่งหลับในรถไฟฟ้า เป็นต้น

3) ความเป็นส่วนตัวด้านการสื่อสาร (Privacy of communication) เป็นการคุ้มครองสิทธิที่เกี่ยวกับสื่อสารโดยปราศจากการดักฟัง หรือจับตามอง ไม่ว่าจะเป็นการสื่อสารทางอีเมล โทรศัพท์ การพูดคุยในลักษณะเผชิญหน้า (face-to-face) หรือการพูดคุยแบบระยะไกล (Virtual Communication)

4) ความเป็นส่วนตัวด้านข้อมูล และรูปถ่าย (Privacy of data and image) เป็นการขยายเพิ่มเติมจากความเป็นส่วนตัวของข้อมูลส่วนบุคคลของโรเจอร์ คล้าก โดยนอกจากข้อมูลส่วนตัวของบุคคลแล้ว รูปถ่ายของบุคคลนั้น ๆ ก็ควรได้รับการคุ้มครองด้วย

5) ความเป็นส่วนตัวด้านความคิดและความรู้สึก (Privacy of thoughts and feelings) เกิดจากผลกระทบของเทคโนโลยีสมัยใหม่ที่มีต่อความเป็นส่วนตัวของความคิดและความรู้สึก บุคคลย่อมมีสิทธิที่จะไม่เปิดเผยความรู้สึก หรือความคิดของตนให้กับผู้อื่น และมีสิทธิที่จะไม่ให้ผู้อื่นเปิดเผยความคิดและความรู้สึกของตน บุคคลควรมีอิสระที่จะมีความคิดเป็นของตนเอง แต่ในปัจจุบันความคิดและความรู้สึกของบุคคลอาจถูกละเมิดได้ เนื่องจากความก้าวหน้าทางวิทยาการปัญญา (Cognitive Science) ทำให้ความเป็นไปได้ของการนำข้อมูลสมอง (Neurodata) ไปใช้นั้นมีความเป็นไปได้มาก นอกจากนี้ยังมีความก้าวหน้าในการเชื่อมต่อสมองกับคอมพิวเตอร์ ซึ่งทำให้สามารถเก็บข้อมูลสมอง (Neurodata) จากสมองได้โดยตรง และนำไปวิเคราะห์ต่อไปได้[21] ความเป็นส่วนตัวด้านความคิดและความรู้สึกนั้นสามารถแยกออกจากความเป็นส่วนตัวด้านร่างกาย เช่นเดียวกับการแยกความคิด ความรู้สึก และการกระทำ สิ่งที่บุคคลหนึ่งคิดอาจจะไม่ใช่สิ่งที่บุคคลนั้นกระทำ และเช่นเดียวกันหลาย ๆ คนอาจกระทำการโดยมิได้ยั้งคิด

6) ความเป็นส่วนตัวด้านที่ตั้งและพื้นที่ (Privacy of location and space) หมายถึงบุคคลควรมีสิทธิที่จะเดินทางไปในที่สาธารณะ (public) หรือกึ่งสาธารณะ (semi-public) ได้โดยปราศจากการระบุตัวตน (identified) การติดตาม (tracked) หรือการตรวจสอบ (monitored) ซึ่งรวมถึงสิทธิที่จะอยู่อย่างสันโดษ หรือเป็นส่วนตัวในบ้าน ในรถยนต์ หรือในที่ทำงาน สิ่งเหล่านี้มีคุณค่าทางสังคม กล่าวคือเมื่อประชาชนมีอิสระที่จะเดินทางไปในที่ต่าง ๆ ได้โดยไม่ต้องกังวลว่าจะมีการระบุตัวตน การติดตาม หรือ การตรวจสอบ ประชาชนจะรู้สึกว่ามีความเป็นอิสระ ซึ่งเกี่ยวข้องโดยตรงกับความรู้สึกถึงความเป็นประชาธิปไตย ทั้งนี้ความเป็นส่วนตัวด้านที่ตั้งและพื้นที่นี้ไม่เหมือนกันกับความเป็นส่วนตัวด้านพฤติกรรม และการกระทำ เนื่องจากความเป็นส่วนตัวด้านพฤติกรรม และการกระทำนั้นเกี่ยวข้องกับการกระทำ ซึ่งไม่จำเป็นจะต้องเป็นการเดินทางเสมอไป

7) ความเป็นส่วนตัวด้านการสมาคม (Privacy of association) เป็นความเป็นส่วนตัวที่เกี่ยวกับสิทธิที่บุคคลจะสมาคมกับผู้ใดก็ได้ โดยปราศจากการตรวจสอบ ซึ่งเป็นสิทธิที่มี

---

[21] Hallinan, D., Schuetz, P., Friedewald, M., & Hert, P. d. (2012). Neurodata and Neuroprivacy: Data Protection Outdated? สืบค้นจาก https://www.researchgate.net/publication/265048889_Neurodata_and_Neuroprivacy_Data_Protection_Outdated

ความสัมพันธ์กับความเป็นประชาธิปไตย เนื่องจากเกี่ยวข้องกับเสรีภาพในการพูด หรือแสดงความคิดเห็นทางการเมือง และเสรีภาพในการยึดมั่นศรัทธา[22]

1.5 กรอบการคุ้มครองข้อมูลส่วนบุคคลของ OECD

เนื่องจากความก้าวหน้าทางเทคโนโลยีทำให้มีโอกาสที่บุคคลจะถูกละเมิดสิทธิความเป็นส่วนตัวได้มากขึ้น ข้อมูลส่วนบุคคลจึงควรได้รับการคุ้มครองเพื่อให้เจ้าของข้อมูลส่วนบุคคลเกิดความมั่นใจในการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยกรอบในการคุ้มครองข้อมูลที่นิยมนำมาใช้เป็นแนวทางในการดำเนินการในการคุ้มครองข้อมูลส่วนบุคคล คือ กรอบในการคุ้มครองข้อมูลส่วนบุคคลขององค์การเพื่อความร่วมมือและการพัฒนาทางเศรษฐกิจ (The Organization for Economic Cooperation and Development หรือ OECD) ในเรื่อง “ข้อแนะนำเกี่ยวกับแนวทางการคุ้มครองความเป็นส่วนตัวและการส่งผ่านข้อมูลส่วนบุคคลระหว่างประเทศ (Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data)” ซึ่งมีหลักเกณฑ์ 8 ประการ คือ

1.5.1 หลักข้อจำกัดในการเก็บรวบรวมข้อมูล (Collection Limitation Principle)

การจัดเก็บรวบรวมข้อมูลส่วนบุคคลต้องกระทำอย่างจำกัด เท่าที่จำเป็น โดยการเก็บรวบรวมนั้นต้องกระทำโดยวิธีที่ถูกต้องตามกฎหมายและต้องกระทำโดยที่เจ้าของข้อมูลรับรู้ รวมทั้งต้องได้รับความยินยอมจากเจ้าของข้อมูลอีกด้วย

1.5.2 หลักคุณภาพของข้อมูล (Data Quality Principle)

ข้อมูลส่วนบุคคลที่ทำการเก็บต้องมีความเกี่ยวข้องกับวัตถุประสงค์ในการเก็บรวบรวม ใช้ และเปิดเผย ทั้งนี้ข้อมูลที่เก็บต้องมีความถูกต้อง ครบถ้วน และเป็นปัจจุบัน

1.5.3 หลักการกำหนดวัตถุประสงค์ในการจัดเก็บ (Purpose Specification Principle)

วัตถุประสงค์ในการเก็บข้อมูลส่วนบุคคลนั้นจะต้องถูกระบุไว้อย่างชัดเจนก่อนที่จะทำการเก็บข้อมูลและการนำข้อมูลส่วนบุคคลไปใช้ในภายหลังจะถูกจำกัดให้ใช้ได้เฉพาะเพื่อให้กระทำการสำเร็จตามวัตถุประสงค์ที่ได้ระบุไว้ หรือเพื่อการอื่นที่ไม่เป็นการขัดแย้งกันกับวัตถุประสงค์ดังกล่าว ทั้งนี้ต้องมีการระบุวัตถุประสงค์การใช้ทุกครั้งที่มีการเปลี่ยนแปลง

1.5.4 หลักข้อจำกัดในการนำไปใช้ (Use Limitation Principle)

ข้อมูลส่วนบุคคลจะต้องไม่ถูกเปิดเผย ทำให้ใช้ได้ หรือนำไปใช้เพื่อการอื่นนอกจากวัตถุประสงค์ที่ได้ระบุไว้ ยกเว้น

1) ได้รับอนุญาตจากเจ้าของข้อมูล หรือ

---

[22] Friedewald, M., Finn, R., & Wright, D. (2013). Seven Types of Privacy. สืบค้นจาก https://www.researchgate.net/publication/258892458_Seven_Types_of_Privacy

2) โดยอาศัยอำนาจตามกฎหมาย

1.5.5 หลักการรักษาความมั่นคงปลอดภัยของข้อมูล (Security Safeguards Principle)

ต้องมีการรักษาความปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสม โดยมีการป้องกันความเสี่ยงจากการถูกโจรกรรม หรือการเข้าถึงโดยไม่ได้รับอนุญาต รวมทั้งการถูกทำลาย การใช้ การแก้ไข หรือการนำข้อมูลไปเปิดเผยโดยมิได้รับอนุญาต

1.5.6 หลักการเปิดเผยข้อมูล (Openness Principle)

ต้องมีนโยบายการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่มีความโปร่งใส โดยให้ผู้ที่เกี่ยวข้องทราบถึงกระบวนการที่เกี่ยวข้องกับการพัฒนา การปฏิบัติงาน และนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคล นอกจากนี้ยังต้องสามารถแสดงให้เห็นถึงการมีอยู่ และประเภทของข้อมูลส่วนบุคคล รวมถึงวัตถุประสงค์ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทั้งนี้ยังต้องเปิดเผยชื่อ และสถานที่ตั้งของผู้ควบคุมข้อมูลส่วนบุคคลอีกด้วย

1.5.7 หลักการมีส่วนร่วมของบุคคล (Individual Participation Principle)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะ

1) ได้รับการยืนยันจากผู้ควบคุมข้อมูลว่าผู้ควบคุมข้อมูลมีข้อมูลส่วนบุคคลของตนหรือไม่

2) ได้รับการติดต่อเกี่ยวกับข้อมูลส่วนบุคคลของตน

(1) ภายในระยะเวลาที่เหมาะสม

(2) โดยไม่มีค่าใช้จ่าย หรือมีค่าใช้จ่ายที่เหมาะสม ไม่มากเกินไป

(3) ด้วยวิธีการที่เหมาะสม

(4) ในรูปแบบที่สามารถเข้าใจได้โดยง่าย

3) ได้รับคำชี้แจงถึงเหตุผลในกรณีที่คำร้องของตนตาม ข้อ 1) และ 2) ถูกปฏิเสธ และสามารถโต้แย้งการปฏิเสธนั้นได้ และ

4) คัดค้านการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของตน และในกรณีที่การคัดค้านนั้นเป็นผลสำเร็จ ให้ลบ ปรับปรุงให้ถูกต้อง ทำให้สมบูรณ์ หรือให้แก้ไขเพิ่มเติมข้อมูลส่วนบุคคลของตน

1.5.8 หลักความรับผิดชอบ (Accountability Principle)

ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ความรับผิดชอบกระทำการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลให้เป็นไปตามหลักการทั้ง 8 ที่ได้กล่าวมาข้างต้น[23]

---

[23] The Organization for Economic Cooperation and Development. The OECD Privacy Framework, (2013).สืบค้นจาก http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

2. ลักษณะทั่วไปของข้อมูลชีวภาพ

องค์ประกอบที่ใช้ในการยืนยันตัวตนที่เป็นที่ยอมรับในระดับสากลมี 3 ประการ คือ 1) สิ่งที่คุณรู้ (what you know) เช่น รหัสผ่าน 2) สิ่งที่คุณมี (what you have) เช่น บัตรเอทีเอ็ม หรือบัตรประจำตัวพนักงาน และ 3) สิ่งที่คุณเป็น (what you are) เช่น ลายนิ้วมือ[24] ในปัจจุบันการใช้ระบบข้อมูลชีวภาพซึ่งเป็น “สิ่งที่คุณเป็น” เริ่มเป็นที่แพร่หลายมากขึ้น ส่วนหนึ่งเนื่องจากระบบข้อมูลชีวภาพสามารถใช้ยืนยันตัวตนได้โดยมีข้อดีเหนือจากวิธีการยืนยันตัวตนชนิดอื่น เช่น การยืนยันตัวตนโดยใช้ลายนิ้วมือเพื่อบันทึกเวลาทำงานของพนักงานบริษัท ทำให้พนักงานต้องทำการยืนยันตัวตนด้วยตนเอง ไม่สามารถทำการแทนกันได้ การใช้ระบบข้อมูลชีวภาพในการบันทึกเวลาทำงานจึงทำให้นายจ้างได้ข้อมูลที่ถูกต้องแม่นยำ

2.1 ความหมายของข้อมูลชีวภาพ

คำว่า “ชีวภาพ (Biometrics)” มีที่มาจากภาษากรีก โดย “bio” หรือ life หมายถึง ชีวิต และ “metrics” หมายถึง การวัด หรือมาตรวัด เมื่อรวมกันแล้ว “ชีวภาพ” หมายถึง การวัดสิ่งมีชีวิต หรือการวัดชีวภาพ

ข้อมูลชีวภาพ หมายถึง ข้อมูลอัตลักษณ์ส่วนบุคคล ซึ่งคือคุณลักษณะหรือพฤติกรรมบางอย่าง ที่ถูกใช้ในการแยกแยะบุคคลด้วยวิธีการทางชีวภาพ ข้อมูลชีวภาพสามารถได้มาจากหลายวิธี เช่น จากลายนิ้วมือ ใบหน้า จอตา ม่านตา รูปทรงของฝ่ามือ เสียงพูด ลายมือเขียน เป็นต้น

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งมีผลบังคับใช้ตั้งแต่วันที่ 28 พฤษภาคม พ.ศ. 2562 ได้ให้คำจำกัดความของ “ข้อมูลชีวภาพ" ไว้ใน มาตรา 26 วรรคสอง ดังนี้

> *“ข้อมูลชีวภาพตามวรรคหนึ่งให้หมายถึงข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือ ข้อมูลจำลองลายนิ้วมือ”*

อย่างไรก็ดี พจนานุกรม ฉบับราชบัณฑิตยสถาน พ.ศ. 2554 ได้นิยามคำว่า “ชีวภาพ” ไว้ว่า “ชีวภาพ (1) น. ความเป็นสิ่งมีชีวิต (2) ว. เกี่ยวกับสิ่งที่มีชีวิตและสิ่งที่สืบเนื่องมาจากสิ่งมีชีวิต เช่น วิทยาศาสตร์ชีวภาพ ปุ๋ยชีวภาพ

พจนานุกรมแปล ไทย-อังกฤษ NECTEC's Lexitron Dictionary ได้ให้ความหมาย “ชีวภาพ” ไว้ดังนี้ “Biological, เกี่ยวกับสิ่งที่มีชีวิต”

พจนานุกรม ฉบับราชบัณฑิตยสถาน ศัพท์วิทยาศาสตร์ (พิมพ์ครั้งที่ ๕ พ.ศ. ๒๕๔๖) ได้แปลคำว่า “ชีวมิติ”ว่า Biometrics

---

[24] Fadi Aloul, Syed Zahidi, & El-Hajj, W. (2009). *Two Factor Authentication Using Mobile Phones*. Paper presented at the The 7th IEEE/ACS International Conference on Computer Systems and Applications, AICCSA 2009, Rabat, Morocco.

พจนานุกรม ฉบับราชบัณฑิตยสถาน ศัพท์คอมพิวเตอร์และเทคโนโลยีสารสนเทศ (พิมพ์ครั้งที่ ๗ พ.ศ. ๒๕๔๙) ได้แปลคำว่า “ชีวมาตร” ว่า biometrics; biometry

นพ.สุธี ทุวิรัตน์ กรรมการสมาคมความมั่นคงปลอดภัยระบบสารสนเทศ ได้ให้คำจำกัดความของคำว่า “ชีวมาตร” ในงานสัมมนาเรื่อง "การเก็บข้อมูลชีวมาตรของหน่วยงานรัฐกับความเสี่ยงที่อาจมีการละเมิดสิทธิส่วนบุคคลและผลกระทบต่อความมั่นคงของประเทศ" ที่จัดโดยสมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA) ร่วมกับคณะนิติศาสตร์ มหาวิทยาลัยศรีปทุม ที่ห้องประชุมพัชรกิติยาภา อาคารเฉลิมพระบารมี 50 ปี ซอยศูนย์วิจัย เมื่อวันที่ 12 กรกฎาคม พ.ศ. 2562 ว่า “ชีวมาตร หรือ ไบโอเมตริก คือ ข้อมูลส่วนบุคคลที่เป็นเทคโนโลยีในการระบุตัวตน ได้แก่ 1. ภาพถ่าย 2. ลายนิ้วมือ และ 3. ม่านตา”[25]

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์ ได้ให้คำจำกัดความของคำว่า “ชีวมิติ” ไว้ดังนี้ “สิ่งที่ผู้ใช้บริการเป็น (something you are) คือ ข้อมูลทางชีวมิติ (biometric) ของผู้ใช้บริการ เช่น ลายนิ้วมือ ใบหน้า ม่านตา เสียง เป็นต้น”[26]

ประกาศธนาคารแห่งประเทศไทย ที่ สนส. 19/2562 เรื่อง หลักเกณฑ์การรู้จักลูกค้า (Know Your Customer: KYC) สำหรับการเปิดบัญชีเงินฝากของสถาบันการเงิน ได้ระบุว่า “สถาบันการเงิน อาจใช้เทคโนโลยีเปรียบเทียบข้อมูลชีวมิติของลูกค้า (Biometric Comparison) ในการยืนยันตัวตน เพื่อพิสูจน์ว่าเป็นลูกค้ารายนั้นจริง”[27]

ISO/IEC 2382-37:2017(en) Information technology - Vocabulary - Part 37: Biometrics ได้ให้คำจำกัดความของ ข้อมูลชีวภาพ (Biometric) ว่า “เป็นการรับรู้จดจำบุคคลด้วยวิธีการอัตโนมัติโดยใช้ลักษณะทางชีววิทยาและพฤติกรรมของบุคคลนั้น”[28]

หากพิจารณาแล้ว คำว่า “ข้อมูลชีวภาพ” “ข้อมูลชีวมาตร” และ “ข้อมูลชีวมิติ” นั้น หมายถึงข้อมูลไบโอเมตริก หรือ การนำลักษณะทางชีวภาพของบุคคลมาใช้ในการระบุตัวตน โดยรวมถึงข้อมูลเป็นที่เป็นลักษณะทางสรีรวิทยา (physiological characteristics) และลักษณะทางพฤติกรรม (behavioural characteristics) ซึ่งมิใช่เรื่องใหม่ แต่เป็นสิ่งที่มีมานานแล้ว โดยในอดีตมีการใช้การพิมพ์ลายนิ้วมือแทนการเซ็นชื่อ รวมถึงการใช้ลายนิ้วมือในการสืบสวนสอบสวนของตำรวจ

---

[25] สกู๊ปข่าวหน้า 1 นสพ.มติชนรายวัน 21 กันยายน 2562. (2562). เทคโนโลยีระบุตัวตน “ชีวมาตร” น่ากลัวหรือไม่. สืบค้นจาก https://www.matichon.co.th/news-monitor/news_1679649

[26] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2561). ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์ In: สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.

[27] ธนาคารแห่งประเทศไทย. ประกาศธนาคารแห่งประเทศไทย เรื่อง หลักเกณฑ์การรู้จักลูกค้า (Know Your Customer: KYC) สำหรับการเปิดบัญชีเงินฝากของสถาบันการเงิน, สนส. 19/2562 C.F.R. (2562).สืบค้นจาก http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/E/219/T_0008.PDF.

[28] Biometrics is “automated recognition of individuals based on their biological and behavioural characteristics”.

แม้กระทั่งโรงรับจำนำยังมีการพิมพ์ลายนิ้วมือของผู้มาใช้บริการ ซึ่งการนำข้อมูลมาใช้ในลักษณะนี้โดยส่วนใหญ่จะเป็นการเปรียบเทียบในลักษณะหนึ่งต่อหนึ่ง (one-to-one matching)[29]

การพัฒนาทางด้านเทคโนโลยีในช่วงทศวรรษที่ผ่านมาทำให้เกิดระบบคอมพิวเตอร์ที่สามารถทำการเปรียบเทียบข้อมูลชีวภาพแบบอัตโนมัติ (automate) และการเปรียบเทียบสามารถทำได้อย่างทันทีทันใด (real-time) โดยเฉพาะระบบการจดจำใบหน้า (facial recognition) และระบบจดจำลายนิ้วมือ (fingerprint recognition) เริ่มมีการใช้อย่างแพร่หลาย และเริ่มมีการนำข้อมูลชีวภาพมาใช้ในลักษณะหนึ่งต่อกลุ่ม (one-to-many matching) ซึ่งมักใช้ในการรักษาความปลอดภัยและการตรวจคนเข้าเมือง เป็นต้น

ข้อมูลชีวภาพถือเป็นข้อมูลที่มีความสำคัญ และเป็นข้อมูลที่มีลักษณะพิเศษกว่าข้อมูลส่วนบุคคลอื่น ๆ กล่าวคือ ข้อมูลส่วนบุคคลอื่น ๆ เช่น ชื่อ ที่อยู่ หมายเลขโทรศัพท์ อีเมลหรือแม้กระทั่งรหัสผ่าน (password) นั้น หากมีการรั่วไหลหรือเอาไปใช้ในทางมิชอบเจ้าของข้อมูลสามารถทำการเปลี่ยนแปลงข้อมูลนั้น ๆ ได้ แต่ข้อมูลชีวภาพเป็นข้อมูลที่ติดตัวเจ้าของข้อมูล และไม่สามารถทำการเปลี่ยนแปลงได้ การรั่วไหล การนำข้อมูลไปใช้ในทางมิชอบ หรือการขโมยข้อมูลชีวภาพนั้นอาจทำให้เกิดความเสียหายที่อาจไม่สามารถระงับ หรือแก้ไขได้

เนื่องจากความเสียหายที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลประเภทชีวภาพในกรณีของการรั่วไหล หรือนำข้อมูลไปใช้ในทางที่ผิดนั้นมีความรุนแรง ดังนั้นทุกฝ่ายควรตระหนักถึงความรุนแรงของความเสียหายที่อาจเกิดขึ้นได้จากการรั่วไหลของข้อมูลชีวภาพ การรั่วไหลหรือนำข้อมูลไปใช้ในทางที่ผิดจึงสามารถก่อให้เกิดความเสียหายได้อย่างไม่มีที่สิ้นสุด โดยที่เจ้าของข้อมูลไม่สามารถทำการระงับความเสียหายนั้นได้ จึงมีความจำเป็นอย่างยิ่งที่กฎหมายจะต้องบัญญัติบทลงโทษสำหรับการฝ่าฝืน หรือไม่ปฏิบัติตามบทบัญญัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในส่วนที่เกี่ยวข้องกับข้อมูลชีวภาพนั้นให้มีความรุนแรงเพียงพอที่จะทำให้ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นใช้ความระมัดระวังในการใช้ข้อมูลชีวภาพมากกว่าที่ใช้กับข้อมูลส่วนบุคคลอื่น ๆ

2.2 ประเภทของข้อมูลชีวภาพ

การแบ่งประเภทของข้อมูลชีวภาพสามารถแบ่งได้เป็น 2 ประเภท ดังนี้

1) ลักษณะทางสรีระ (Physiological Characteristics) หรือลักษณะทางชีวภาพ (Biological Characteristics) เช่น ลายนิ้วมือ โครงสร้างมือ ใบหน้า ดีเอ็นเอ ลักษณะของใบหู และม่านตา เป็นต้น ลักษณะทางสรีระนี้ในบางวรรณกรรมจะเรียกว่าข้อมูลชีวภาพยุคแรก (First Generation Biometric)

2) ลักษณะทางพฤติกรรม (Behavioural Characteristics) หรือ ลักษณะทางการกระทำ เช่น การจดจำรูปแบบเสียง (Voice Pattern Recognition) ท่าทางการเดิน ลายเซ็น

---

[29] Coseraru, R. (2017). Facial Recognition Systems and their Data Protection Risks Under the GDPR. (Master Thesis), Tilburg University, Retrieved from http://arno.uvt.nl/show.cgi?fid=143731 p 11.

และจังหวะการพิมพ์ (Keystroke Dynamics) เป็นต้น ลักษณะทางพฤติกรรมนี้ในบางวรรณกรรมจะเรียกว่าข้อมูลชีวภาพยุคที่สอง (Second Generation Biometric)[30]

2.3 คุณลักษณะของข้อมูลชีวภาพ

สำหรับการพิจารณาถึงความเหมาะสมของข้อมูลชีวภาพที่จะนำไปใช้ในระบบชีวภาพ (Biometric System) เพื่อการระบุตัวตน (identify) และการยืนยันตัวตน (authenticate หรือ verify) นั้นจะพิจารณาจากคุณลักษณะของข้อมูลชีวภาพ ดังต่อไปนี้

2.3.1 ความเป็นสากล (universal)

ข้อมูลชีวภาพที่จะนำมาใช้ในระบบข้อมูลชีวภาพนั้นต้องมีอยู่ในทุกคน ยกตัวอย่างเช่น ใบหน้า ซึ่งเป็นสิ่งที่ทุกคนมีและมนุษย์มีความสามารถในการรับรู้ (recognize) ใบหน้าของแต่ละคน จึงทำให้ใบหน้ามีคุณสมบัติที่เป็นสากล[31] นอกจากนี้ ม่านตา ลายนิ้วมือ และใบหูยังสามารถนับเป็นข้อมูลชีวภาพที่เป็นสากลได้ สำหรับรอยสัก รอยด่าง แผลเป็น อาจใช้ได้ดีสำหรับการยืนยันตัวตนในกรณีที่เกิดอุบัติเหตุร้ายแรง เช่น การยืนยันตัวตนผู้เสียชีวิตจากเหตุการณ์สึนามิ เมื่อปี พ.ศ. 2547 แต่ไม่เหมาะสมที่จะนำมาใช้เป็นข้อมูลชีวภาพเนื่องจากไม่ใช่สิ่งที่มีอยู่ในทุกคนจึงไม่มีความเป็นสากล

แม้ข้อมูลชีวภาพจะมีความเป็นสากลแต่อาจไม่ใช่สิ่งที่มนุษย์ทุกคนมี บางคนอาจสูญเสียดวงตา นิ้วมือ ลายนิ้วมือ หรือ ใบหู จากอุบัติเหตุหรือโรคภัยไข้เจ็บ และในบางชาติพันธุ์ข้อมูลชีวภาพบางอย่างอาจมีคุณสมบัติที่ด้อยกว่าชาติพันธุ์อื่น เช่น มีรายงานว่าคนเอเชียมีสันของลายนิ้วมือ (ridges) ไม่เด่นชัดเท่ากับคนชาติพันธุ์อื่น[32] ซึ่งหมายความว่าข้อมูลชีวภาพที่เลือกใช้นั้นจะใช้ไม่ได้กับบางคนหรือบางกลุ่ม ดังนั้นในการบัญญัติกฎหมาย หรือเกณฑ์กฎเกณฑ์ในการควบคุมข้อมูลชีวภาพจึงควรคำนึงถึงลักษณะเฉพาะ และข้อจำกัดต่าง ๆ ของข้อมูลชีวภาพ

2.3.2 ความเป็นเอกลักษณ์ (uniqueness หรือ distinctive)

ข้อมูลชีวภาพนั้นจะต้องเป็นเอกลักษณ์เฉพาะบุคคลจึงจะสามารถนำมาใช้ในการระบุตัวตนหรือยืนยันตัวตนได้ เช่น ใบหน้า หรือลายนิ้วมือของแต่ละคนมีความเป็นเอกลักษณ์และไม่ซ้ำกัน คุณลักษณะนี้ถือเป็นแก่นสำคัญของระบบข้อมูลชีวภาพ เนื่องจากระบบชีวภาพจะต้องสามารถใช้ข้อมูลในการแยกแยะบุคคลหนึ่งออกจากอีกบุคคลหนึ่ง เพื่อให้ทำการระบุตัวตนและ/หรือยืนยันตัวตนได้

---

[30] Smith, M., Mann, M., & Urbas, G. (2018). *Biometrics, Crime and Security*. New York: Routledge. p 2.

[31] Coseraru, R. (2017). Facial Recognition Systems and their Data Protection Risks Under the GDPR. (Master Thesis), Tilburg University, Retrieved from http://arno.uvt.nl/show.cgi?fid=143731. P 12.

[32] Kindt, E. J. (2013). *Privacy and Data Protection Issues of Biometrics Applications*. New York: Springer. p 20.

โดยทั่วไปแล้วลายนิ้วมือและม่านตาถือว่าเป็นข้อมูลชีวภาพที่มีความเป็นเอกลักษณ์ ซึ่งแม้แต่ฝาแฝดยังมีลายนิ้วมือและม่านตาที่ไม่เหมือนกัน นอกจากนี้ลายเซ็นยังถือเป็นข้อมูลชีวภาพที่มีความเป็นเอกลักษณ์อีกด้วย[33]

แม้ว่าความเป็นเอกลักษณ์จะเป็นสิ่งสำคัญที่ข้อมูลชีวภาพควรมี แต่ระบบข้อมูลชีวภาพจะไม่สามารถทำการยืนยันได้ว่าตัวอย่างข้อมูลชีวภาพที่เก็บมา หรือแม่แบบข้อมูลชีวภาพนั้นมีความเป็นเอกลักษณ์หรือไม่ ระบบสามารถทำได้เพียงยืนยันว่าตัวอย่าง หรือแม่แบบข้อมูลชีวภาพนั้นมาจากบุคคลคนเดียวกันหรือไม่เท่านั้น

2.3.3 ความเป็นถาวร (persistent หรือ permanent)

ข้อมูลชีวภาพจะต้องมีการคงอยู่อย่างถาวรและไม่เปลี่ยนแปลงตามกาลเวลา ดังนั้นลายนิ้วมือและม่านตาจึงนับได้ว่าเป็นข้อมูลชีวภาพที่มีความเป็นถาวรสูง เนื่องจากไม่มีการเปลี่ยนแปลงตราบชั่วชีวิตของเจ้าของข้อมูล นอกจากนี้เจ้าของข้อมูลไม่สามารถทำการเปลี่ยนแปลงได้ยกเว้นในกรณีของอุบัติเหตุหรือโรคภัยไข้เจ็บ สำหรับใบหน้านั้นจะมีการคงอยู่แต่ก็อาจมีการเปลี่ยนแปลงได้เนื่องจากการเพิ่มขึ้นหรือลดลงของน้ำหนักตัว การไว้หนวดเครา การทำศัลยกรรมหรืออุบัติเหตุ เป็นต้น ดังนั้นการใช้ใบหน้าในเทคโนโลยีชีวภาพนั้นอาจทำให้ต้องมีการลงทะเบียนใหม่ (re-enroll) เมื่อเกิดการเปลี่ยนแปลงของใบหน้า

ระดับของความเป็นถาวรของข้อมูลชีวภาพมีผลต่อระดับความปลอดภัยและความน่าเชื่อถือของระบบข้อมูลชีวภาพ ซึ่งทำให้มีผลกระทบต่อเนื่องไปยังการใช้งานและประสิทธิภาพของระบบอีกด้วย หากระดับความเป็นถาวรของข้อมูลต่ำจะทำให้อัตราการปฏิเสธที่ผิดพลาด (False Rejection) สูง การเพิ่มขึ้นของอัตราการปฏิเสธที่ผิดพลาดจะทำให้ต้องมีการเพิ่มขั้นตอนในการตรวจสอบซึ่งจะเพิ่มระยะเวลาในการตรวจสอบและอาจต้องมีการลงทะเบียนใหม่จึงมีผลกระทบต่อประสิทธิภาพของการทำงาน

2.4 หลักเกณฑ์การพิจารณาความเหมาะสมของข้อมูลชีวภาพ

ในการพิจารณาความเหมาะสมของข้อมูลชีวภาพที่จะนำมาใช้งานในระบบข้อมูลชีวภาพ นอกจากจะต้องพิจารณาคุณลักษณะของข้อมูลชีวภาพที่กล่าวมาแล้ว ยังต้องคำนึงถึงหลักเกณฑ์ที่เกี่ยวข้องกับการนำไปใช้อีก 4 ประการ ดังนี้

2.4.1 ความง่ายในการเก็บรวบรวมข้อมูล (collectability)

ข้อมูลชีวภาพที่นำมาใช้ควรง่ายต่อการเก็บรวบรวม เช่น การเก็บข้อมูลลายนิ้วมือนั้นสามารถทำได้โดยง่ายเพียงมีกล้องถ่ายรูปหรือเครื่องสแกนลายนิ้วมือ การเก็บภาพ

---

[33] Kindt, E. J. (2013). *Privacy and Data Protection Issues of Biometrics Applications*. New York: Springer. p 22.

ใบหน้าก็สามารถทำได้โดยง่ายโดยการถ่ายภาพเช่นกัน ส่วนการเก็บข้อมูลรูปแบบของเส้นเลือดดำจะกระทำได้ยากกว่า

2.4.2 การยอมรับ (Acceptability)

ข้อมูลชีวภาพที่เหมาะกับการนำมาใช้ในระบบข้อมูลชีวภาพควรเป็นที่ยอมรับเป็นที่แพร่หลายว่าสามารถนำไปใช้เพื่อการยืนยันตัวตนหรือระบุตัวตนได้ เช่น การเก็บลายนิ้วมือ การจดจำใบหน้า เป็นต้น

2.4.3 การหลอกลวง (Circumvention)

ระบบข้อมูลชีวภาพที่ดีต้องมีความทนทานต่อการหลอกลวง กล่าวคือระบบจะถูกหลอกโดยการปลอมข้อมูลชีวภาพได้ยาก เช่น ระบบที่มีการตรวจจับความมีชีวิต (Liveness Detection) จะถูกหลอกลวงได้ยากกว่าระบบที่ไม่มีการตรวจจับความมีชีวิต

2.4.4 ประสิทธิภาพ (Performance)

ประสิทธิภาพของข้อมูลชีวภาพที่นำไปใช้จะพิจารณาจากความแม่นยำ ความทนทาน และความเร็วของอุปกรณ์และระบบงาน

2.5 ขั้นตอนการทำงานของระบบชีวภาพ

ระบบชีวภาพนั้นทำงานโดยการรวบรวมและเก็บคุณลักษณะทางชีวภาพ และพฤติกรรมของปัจเจกบุคคลในขั้นตอนของการลงทะเบียน (Enrollment) เพื่อนำมาใช้ในการระบุตัวตน (Identification) หรือยืนยันตัวตน (Authentication) ต่อไป

2.5.1 การลงทะเบียน (Enrollment)

การลงทะเบียนเป็นการเก็บข้อมูลชีวภาพตั้งต้นของบุคคล (sample) เพื่อใช้อ้างอิงในขั้นตอนของการระบุตัวตนหรือยืนยันตัวตนต่อไป หากข้อมูลชีวภาพตั้งต้นของบุคคลนั้น ๆ ไม่ได้ทำการลงทะเบียน ก็จะไม่สามารถทำการระบุตัวตนหรือยืนยันตัวตนได้

1) *การเก็บรวบรวม (collect หรือ acquire)*

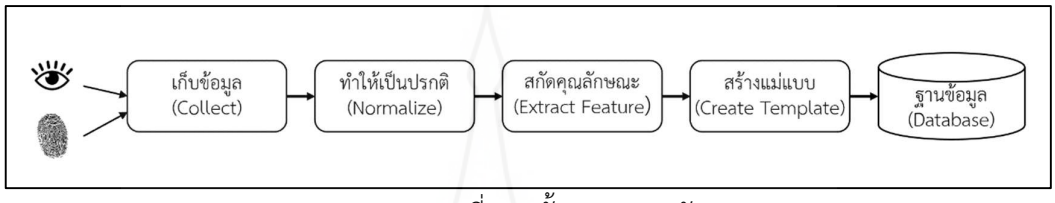
ในขั้นตอนนี้ระบบจะทำการเก็บข้อมูลชีวภาพจากปัจเจกบุคคล โดยอุปกรณ์ที่ใช้เก็บข้อมูลนั้นจะขึ้นอยู่กับชนิดของข้อมูล เช่น กล้องถ่ายรูปและกล้องวงจรปิดใช้สำหรับเก็บรวบรวมใบหน้า เครื่องสแกนลายนิ้วมือใช้สำหรับเก็บลายนิ้วมือ หรือเครื่องอ่านม่านตาใช้สำหรับอ่านม่านตา เป็นต้น

2) *การทำให้เป็นปรกติ (normalized หรือ pre-process)*

เมื่อทำการเก็บข้อมูลแล้ว ขั้นตอนต่อไปคือการกำจัดข้อมูลไม่พึงประสงค์หรือข้อมูลที่เป็นการรบกวน (noise) ออกจากข้อมูลตั้งต้น และเพิ่มคุณภาพของข้อมูลชีวภาพที่ได้ทำการเก็บมา

3) *การสกัดคุณลักษณะ และการสร้างแม่แบบ (feature extraction and template generation)*

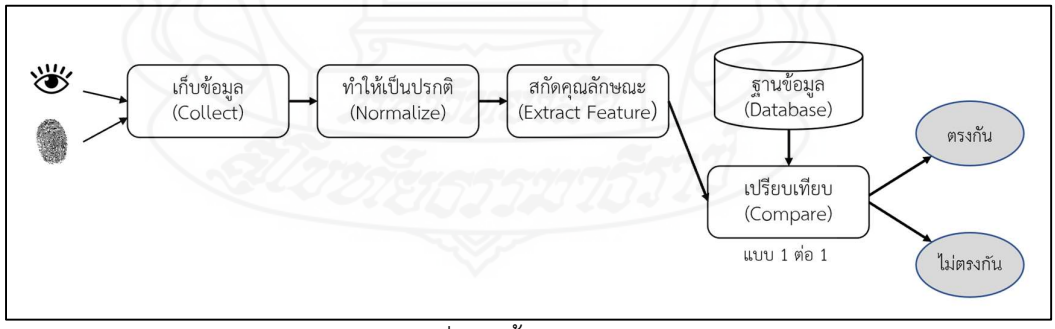
เมื่อได้ข้อมูลชีวภาพที่กำจัดสิ่งไม่พึงประสงค์ออกจากข้อมูลหลักแล้ว ระบบจะทำการดึงคุณลักษณะของข้อมูลออกมาเพื่อสร้างเป็นแม่แบบและนำแม่แบบไปจัดเก็บไว้ในฐานข้อมูล



ภาพที่ 2.1 ขั้นตอนการสมัคร

2.5.2 การยืนยันตัวตน (Verification)

การยืนยันตัวตนใช้วิธีการเปรียบเทียบแบบหนึ่งต่อหนึ่ง (one-to-one matching) กล่าวคือการนำข้อมูลแม่แบบชีวภาพที่ได้จากขั้นตอนการสมัคร (enroll หรือ registration) มาเปรียบเทียบกับข้อมูลแม่แบบที่สร้างจากขั้นตอนการขอยืนยันตัวตน ผลที่ได้คือคะแนนจากการเปรียบเทียบ (match score) บ่งถึงระดับความเหมือน (degree of similarities) ซึ่งหากคะแนนที่ได้สูงหมายถึงข้อมูลชีวภาพของผู้ที่ขอยืนยันตัวตนมีความเหมือนกับข้อมูลแม่แบบในฐานข้อมูลมาก ส่วนคะแนนต่ำหมายถึงข้อมูลของผู้ที่ขอยืนยันตัวตนมีความเหมือนกับข้อมูลแม่แบบในฐานข้อมูลน้อย การทำงานในลักษณะนี้มักใช้เพื่อการขอเข้าใช้ (request for entry or request for access) ไม่ว่าจะเป็นการขอเข้าใช้งานระบบคอมพิวเตอร์ หรือการขอเข้าสถานที่ เช่น การเข้าระบบธุรกรรมออนไลน์ของธนาคาร หรือการเข้าพื้นที่หวงห้ามต่าง ๆ เป็นต้น

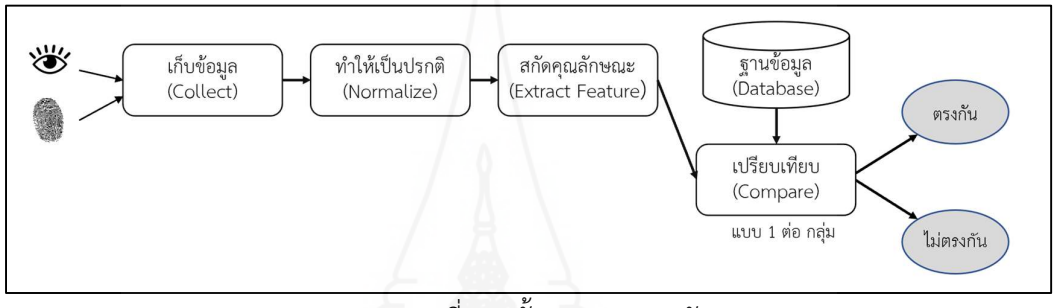


ภาพที่ 2.2 ขั้นตอนการยืนยันตัวตน

2.5.3 การระบุตัวตน (Identification)

สำหรับขั้นตอนการระบุตัวตน ระบบจะนำแม่แบบที่สร้างขึ้นในขั้นตอนการระบุตัวตนมาเปรียบเทียบกับข้อมูลแม่แบบที่เก็บไว้ในฐานข้อมูลในลักษณะหนึ่งต่อกลุ่ม (one-to-many matching) เพื่อการระบุว่าบุคคลผู้นั้นคือใคร กล่าวคือการนำข้อมูลแม่แบบชีวภาพที่ได้จาก

ขั้นตอนการลงทะเบียน (registration) มาเปรียบเทียบกับข้อมูลแม่แบบที่มีอยู่ในฐานข้อมูล โดยเปรียบเทียบกับกลุ่มของแม่แบบ ผลที่ได้คือคะแนนจากการเปรียบเทียบ (match score) บ่งถึงระดับความเหมือน (degree of similarities) ซึ่งหากคะแนนที่ได้สูงหมายถึงข้อมูลชีวภาพของผู้ที่ระบุตัวตนมีความเหมือนกับข้อมูลแม่แบบในฐานข้อมูลมาก ส่วนคะแนนต่ำหมายถึงข้อมูลของผู้ที่ขอระบุตัวตนมีความเหมือนกับข้อมูลแม่แบบในฐานข้อมูลน้อย ซึ่งมักใช้โดยหน่วยงานบังคับใช้กฎหมาย หรือในการรักษาความปลอดภัย เช่น การรักษาความปลอดภัยของสนามบิน การตรวจคนเข้าเมือง และการจับคนร้าย เป็นต้น



ภาพที่ 2.3 ขั้นตอนการระบุตัวตน

2.6 ข้อมูลชีวภาพที่นิยมใช้

ข้อมูลชีวภาพที่นิยมใช้มักจะเป็นข้อมูลทางสรีระ (physiological) หรือทางชีวภาพ (biological) ที่สามารถใช้วัดได้โดยระบบอัตโนมัติ

2.6.1 ภาพถ่ายใบหน้า (Face Image)

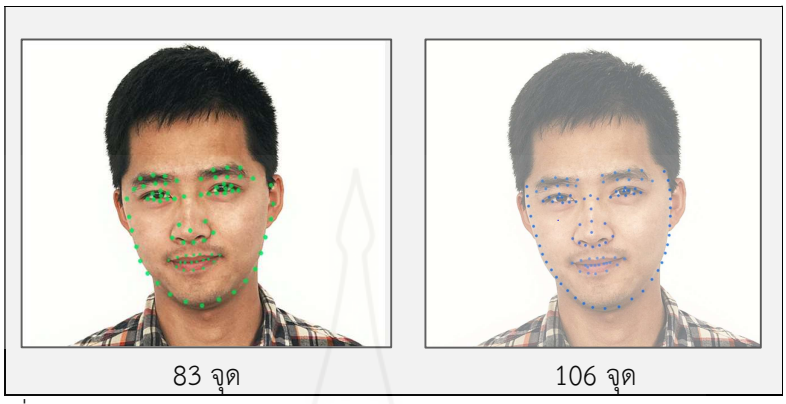
การถ่ายภาพใบหน้าสามารถทำได้ง่าย จากระยะไกล โดยเจ้าของข้อมูลอาจทราบ หรือไม่ทราบว่ามีการถ่ายภาพตนเองอยู่ การถ่ายภาพใบหน้าสามารถทำได้โดยกล้องถ่ายรูปหรือกล้องวิดีโอและถ่ายได้ทั้งแบบสองมิติและสามมิติ การถ่ายภาพใบหน้านั้นเป็นการเก็บข้อมูลชีวภาพที่ไม่เป็นการลุกล้ำ (intrusive) และเป็นที่นิยมใช้กันอย่างแพร่หลาย

การวิเคราะห์ภาพถ่ายใบหน้าสามารถทำได้หลายวิธี เช่น การวัดระยะห่างระหว่างจุดบนใบหน้า การจำลองมิติของหน้าในเชิงเรขาคณิต (face geometry) หรือ แม้กระทั่งดูความเรียบเนียนหรือความหยาบของผิวหน้า (skin texture) ได้อีกด้วย[34]

ใบหน้าคนนั้นประกอบไปด้วยจุดสำคัญ (nodal points หรือ landmark points) ประมาณ 80 จุด ซึ่งคือจุดสูงสุดและต่ำสุดบนใบหน้าของแต่ละคน ในเทคโนโลยีการจดจำใบหน้าโดยใช้ระยะห่างจากจุดสำคัญนั้นจะใช้จุดสำคัญต่าง ๆ ในการสร้างแม่แบบในระบบ เช่น ระยะห่างระหว่างตา ความกว้างของจมูก โหนกแก้ม กราม และคาง เป็นต้น ซึ่งความแม่นยำในการ

[34] Kindt, E. J. (2013). *Privacy and Data Protection Issues of Biometrics Applications*. New York: Springer.. p 25.

ระบุตัวตนนั้นส่วนหนึ่งขึ้นอยู่กับจำนวนจุดสำคัญ และขึ้นอยู่กับความซับซ้อนของกระบวนการแก้ปัญหา หรือ อัลกอริทึม (algorithm) ที่ใช้



ภาพที่ 2.4 แสดงการเปรียบเทียบจำนวนจุดสำคัญ (Nodal หรือ Landmark points)

ที่มา: Face++, https://console.faceplusplus.com/documents/5679127

2.6.2 ลายนิ้วมือ (Fingerprint)

ลายนิ้วมือของมนุษย์ประกอบไปด้วย เส้นนูน (ridges) และร่อง (valleys) รอยนูนที่อยู่สูงกว่าผิวหนังส่วนนอกเรียกว่าเส้นนูน ส่วนเส้นร่อง คือรอยลึกที่อยู่ต่ำกว่าระดับของเส้นนูน ลายเส้นที่อยู่บนนิ้วมือ ฝ่ามือ และ ฝ่าเท้า ของมนุษย์จะประกอบด้วยลายเส้นที่มีลักษณะเฉพาะในแต่ละคน โดยมีลักษณะสำคัญพิเศษ หรือจุดตำหนิที่ทำให้แยกลายนิ้วมือ ลายฝ่ามือ หรือ ฝ่าเท้าของแต่ละบุคคลออกจากกันได้ และมักมีการใช้จุดตำหนิตั้งแต่ 10 จุดขึ้นไปในการยืนยันว่าเป็นลายนิ้วมือของบุคคลคนเดียวกัน

การใช้ลายนิ้วมือ หรือลายฝ่ามือในการยืนยันตัวตนนั้นมีมาตั้งแต่สมัยโบราณ โดยมีการค้นพบลายฝ่ามือในบริเวณภาพวาดที่มีอายุราว 3,600 ปี บนผนังถ้ำในประเทศฝรั่งเศส โดยเชื่อกันว่าผู้ที่วาดภาพนั้นได้ทำการประทับลายฝ่ามือไว้เพื่อเป็นการแสดงว่าตนเองเป็นผู้วาดภาพนั้น[35]

การเก็บลายนิ้วมือด้วยเซ็นเซอร์เป็นการเก็บลายนิ้วมือแบบที่ต้องการความร่วมมือจากเจ้าของข้อมูล แต่การเก็บลายนิ้วมือแฝง (latent fingerprint) นั้นอาจเก็บได้จากวัตถุที่เจ้าของข้อมูลได้ทำการสัมผัส เช่น แก้วน้ำ ด้ามปืน เป็นต้น โดยเจ้าของข้อมูลอาจทราบหรือไม่ทราบถึงการเก็บข้อมูลนั้น ทั้งนี้คุณภาพของลายนิ้วมือที่เก็บนั้นมีความสำคัญอย่างมากต่อความแม่นยำในการระบุหรือยืนยันตัวตน โดยทั่วไปการใช้ลายนิ้วมือในการยืนยัน หรือระบุตัวตนมีความแม่นยำค่อนข้างสูงและอุปกรณ์ที่ใช้มีราคาไม่แพงจึงเป็นที่นิยมใช้ทั่วไป

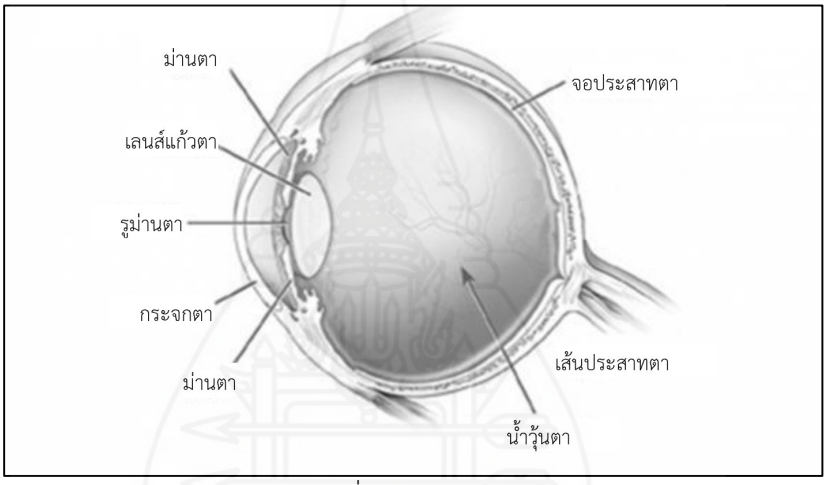
---

[35] Kindt, E. J. (2013). *Privacy and Data Protection Issues of Biometrics Applications*. New York: Springer. p 15.

2.6.3 ม่านตา (Iris)

ม่านตาคือวงกลมที่ล้อมรอบรูม่านตา (pupil) โดยสีของม่านตานั้นจะแตกต่างกันไปขึ้นอยู่กับเชื้อชาติ บางเชื้อชาติมีม่านตาสีเขียว บางเชื้อชาติมีม่านตาสีฟ้า คนไทยนั้นมักมีม่านตาสีน้ำตาล หรือดำ ม่านตามีความเป็นเอกลักษณ์สูง แม้ฝาแฝดยังมีม่านตาที่ไม่เหมือนกัน นอกจากนี้การแก้ไข ดัดแปลง ม่านตายังทำได้ยาก และระบบสามารถตรวจจับการปลอมแปลงม่านตาได้อย่างง่ายดาย[36]

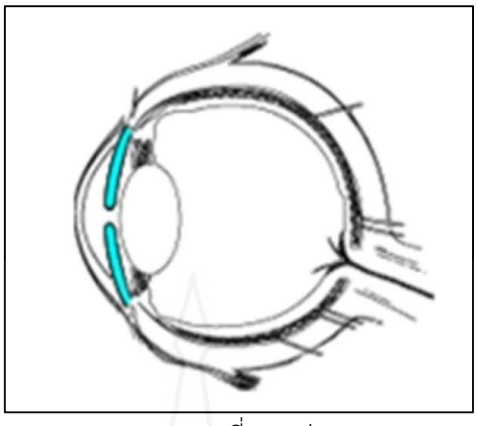
ในอดีตการเก็บข้อมูลม่านตาจะต้องทำผ่านเซ็นเซอร์โดยเจ้าของข้อมูลต้องให้ความร่วมมือเท่านั้น แต่ปัจจุบันการพัฒนาทางเทคโนโลยีทำให้การเก็บข้อมูลม่านตาสามารถกระทำได้จากระยะไกล โดยไม่ต้องการความร่วมมือจากเจ้าของมูลอีกต่อไป



ภาพที่ 2.5 องค์ประกอบของตา

ที่มา: Laser Vision, https://www.laservisionthai.com/health-corner/องค์ประกอบของตา-anatomy-eye

[36] Jian, A. K., Ross, A., & Prabhakar, S. (2004). An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology, 14*(1), 4-20. p. 10.



ภาพที่ 2.6 ม่านตา

ที่มา: Laser Vision, https://www.laservisionthai.com/health-corner/องค์ประกอบของตา-anatomy-eye

2.6.4 รูปทรงของมือ (Hand Geometry)

รูปทรงและขนาดของมือเป็นข้อมูลชีวภาพอีกชนิดหนึ่งที่สามารถนำมาใช้ในการยืนยัน หรือระบุตัวตนได้ โดยพิจารณาจากขนาดของฝ่ามือ ความยาว ความกว้าง และความหนาของนิ้วแต่ละนิ้ว รวมถึงความโค้งและตำแหน่งสัมพันธ์ (relative location) ของส่วนประกอบทั้งหมดของมือ การเก็บข้อมูลรูปทรงของมือจะไม่รวมข้อมูลที่อยู่ระดับผิวหนังของมือ เช่น ลายนิ้วมือ ลายฝ่ามือ แผลเป็น และ สีผิว เป็นต้น

การเก็บรวบรวมข้อมูลรูปทรงของมือนั้นจะต้องได้รับความร่วมมือจากเจ้าของข้อมูลเสมอ การเก็บข้อมูลโดยไม่ได้รับความร่วมมือจากเจ้าของข้อมูลนั้นแทบเป็นไปไม่ได้เลย แต่ความเป็นเอกลักษณ์ของรูปทรงของมืออาจไม่สูงมากนัก การใช้รูปทรงของมือในการยืนยันและระบุตัวตนจึงอาจไม่เหมาะกับการนำไปใช้กับคนจำนวนมาก นอกจากนี้รูปทรงของมือยังอาจมีการเปลี่ยนแปลงได้ ไม่ว่าจะเป็นจากอุบัติเหตุ โรคภัยไข้เจ็บ น้ำหนักที่มากขึ้นหรือน้อยลง อายุที่มากขึ้น หรือแม้แต่การสวมใส่เครื่องประดับ เช่น แหวน เป็นต้น

2.6.5 ลายฝ่ามือ (Palm Print)

ลายมือ หรือลายฝ่ามือนั้นมีความเป็นเอกลักษณ์เช่นเดียวกับลายนิ้วมือ และประกอบไปด้วยเส้นนูน และร่องเช่นเดียวกับลายนิ้วมือ การใช้ลายฝ่ามือเป็นข้อมูลชีวภาพในการยืนยัน หรือระบุตัวตนนั้นอาจมีการใช้ร่วมกับรูปทรงของมือเพื่อเพิ่มความแม่นยำของระบบ

การเก็บข้อมูลลายฝ่ามือนั้นต้องการความร่วมมือจากเจ้าของข้อมูล แต่อาจมีบางกรณีที่สามารถเก็บข้อมูลลายฝ่ามือโดยเจ้าของข้อมูลมิได้ให้ความร่วมมือ เช่น กรณีตำรวจเก็บ

ข้อมูลลายฝ่ามือแฝง (latent palm prints) เพื่อนำไปเปรียบเทียบกับข้อมูลลายฝ่ามือของผู้กระทำความผิดในฐานข้อมูล

2.6.6 เสียง (Voice)

เสียงเป็นข้อมูลชีวภาพที่เป็นทั้งลักษณะทางพฤติกรรม (Behavioural Characteristics) และทางสรีระ (Physiological Characteristics) โดยเจ้าของข้อมูลไม่จำเป็นต้องให้ความร่วมมือในการเก็บตัวอย่างเสียงซึ่งเป็นข้อมูลตั้งต้น

เสียงสามารถใช้ได้สำหรับทั้งการระบุตัวตน และยืนยันตัวตน ซึ่งเป็นที่นิยมใช้ในนิติเวชศาสตร์ แต่ยังไม่ค่อยเป็นที่นิยมนักในภาคธุรกิจ อย่างไรก็ดีเริ่มมีการนำเสียงมาใช้ในภาคธุรกิจมากขึ้น เช่น การยืนยันตัวตนเพื่อใช้บริการผ่านโทรศัพท์ของธนาคารซิตี้แบงก์[37] หรือธนาคารไทยพาณิชย์[38] เป็นต้น

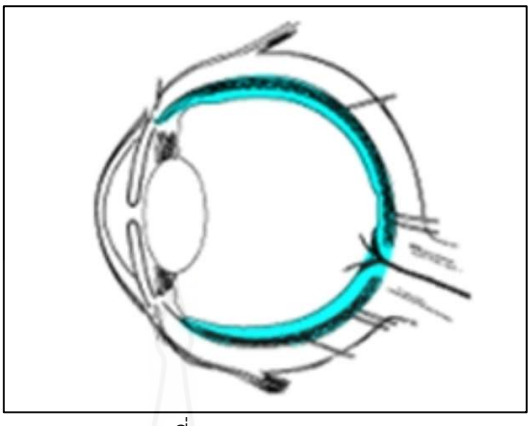
2.6.7 จอประสาทตา (Retina)

จอประสาทตามีความเป็นเอกลักษณ์เฉพาะบุคคล และสามารถใช้ได้ทั้งในการยืนยันตัวตนและระบุตัวตน โดยการสแกนจอประสาทตาจะมีการวิเคราะห์เส้นเลือดและเส้นประสาทตาซึ่งอยู่ในผนังชั้นในด้านหลังของลูกตา การเก็บข้อมูลจอประสาทตาจะต้องได้รับความร่วมมือจากผู้เป็นเจ้าของข้อมูลเสมอเนื่องจากความยากในการเก็บข้อมูลจากเจ้าของข้อมูลและราคาของเครื่องมือจัดเก็บที่ค่อนข้างสูงทำให้การใช้จอประสาทตาไม่ค่อยเป็นที่นิยมและมักใช้กันในสถานที่ที่ต้องการให้มีการรักษาความปลอดภัยในระดับสูงเท่านั้น เช่น ศูนย์วิจัยทางด้านพลังงานนิวเคลียร์ หรือสถานที่เก็บอาวุธนิวเคลียร์ เป็นต้น นอกจากนี้การสแกนจอประสาทตาอาจทำให้เห็นถึงโรคประจำตัว เช่น ความดันสูง ได้ การใช้จอประสาทตาในระบบข้อมูลชีวภาพจึงไม่ค่อยเป็นที่ยอมรับสักเท่าไหร่

---

[37] ซิตี้ ยกระดับการเงิน ใช้นวัตกรรม “Voice Biometrics” ยืนยันตัวตนด้วย “เสียงพูด”. (2559, 10 พฤศจิกายน 2559). สยามรัฐออนไลน์. Retrieved from https://siamrath.co.th/n/5050

[38] 'เอสซีบี'ยืนยันตัวตนลูกค้าสายคอลเซนเตอร์ด้วยเสียง. (2561). เดลินิวส์. สืบค้นจาก เดลินิวส์ website: https://www.dailynews.co.th/economic/636183



ภาพที่ 2.7 จอประสาทตา

ที่มา: Laser Vision, https://www.laservisionthai.com/health-corner/องค์ประกอบของตา-anatomy-eye

2.6.8 รูปแบบของหลอดเลือดดำ (Vein Pattern)

รูปแบบของหลอดเลือดดำ ในนิ้ว มือ ฝ่ามือ หรือแม้แต่ข้อมือของแต่ละคนมีความเป็นเอกลักษณ์เฉพาะตัวและไม่เหมือนกันแม้กระทั่งในฝาแฝดแท้ (identical twins) ทั้งนี้การแตกแขนงของหลอดเลือด ความหนาของหลอดเลือด และองศาของหลอดเลือดในแต่ละคนนั้นทำให้รูปแบบของหลอดเลือดดำนั้นมีความเป็นเอกลักษณ์

การเก็บข้อมูลรูปแบบของหลอดเลือดดำต้องทำด้วยกล้องที่มีความชัดเจนสูงประกอบกับอินฟราเรด (Infrared) หรืออินฟราเรดคลื่นสั้น (Near Infrared) นอกจากนี้การเก็บข้อมูลต้องการความร่วมมือจากเจ้าของข้อมูล อย่างไรก็ดี ความก้าวหน้าทางเทคโนโลยีอาจทำให้สามารถเก็บข้อมูลได้โดยที่เจ้าของข้อมูลไม่ต้องสัมผัสอุปกรณ์โดยตรงและสามารถเก็บได้แม้กระทั่งขณะที่เจ้าของข้อมูลกำลังเคลื่อนไหวได้อีกด้วย

2.6.9 ใบหู (Ear)

รูปทรงของใบหูและโครงสร้างของกระดูกอ่อนในแต่ละคนมีความแตกต่างกันและสามารถใช้แยกแยะบุคคลได้ในระดับหนึ่ง การใช้ข้อมูลใบหูในระบบชีวภาพทำโดยการวัดระยะห่างระหว่างจุดที่โดดเด่นบนใบหู แต่เนื่องจากข้อมูลใบหูไม่มีความเป็นเอกลักษณ์เพียงพอที่จะใช้ระบุตัวตนได้จึงอาจต้องใช้ประกอบกับข้อมูลชีวภาพอื่นเพื่อให้ได้ผลลัพธ์ที่ดีขึ้น

2.6.10 ดีเอ็นเอ (DNA)

การใช้ดีเอ็นเอในนิติเวชศาสตร์มีมาเป็นเวลานาน ไม่ว่าจะเป็นการหาตัวผู้กระทำความผิดหรือการตรวจสอบทางพันธุกรรม อย่างไรก็ดี แม้ว่าดีเอ็นเอจะมีความเป็นเอกลักษณ์แต่ฝาแฝดแท้ (identical twins) มีดีเอ็นเอที่เหมือนกันและความก้าวหน้าทางการแพทย์ในการปลูก

ถ่ายอวัยวะทำให้ผู้ได้รับการปลูกถ่ายอวัยวะได้รับดีเอ็นเอของผู้บริจาคอวัยวะ ทั้งนี้มีรายงานว่าพบดีเอ็นเอของผู้บริจาคไตอยู่ในกระแสเลือดของผู้ได้รับการปลูกถ่ายไตภายหลังการปลูกถ่ายอวัยวะผ่านไปแล้ว 2 ปี[39] นอกจากนี้ยังมีรายงานว่าการปลูกถ่ายไขกระดูกนอกจากจะพบดีเอ็นเอของผู้บริจาคได้ในเลือดหรือในกระพุ้งแก้มของผู้รับบริจาคแล้วดีเอ็นเอในอสุจิของผู้รับบริจาคล้วนแต่เป็นดีเอ็นเอของผู้บริจาคทั้งหมดโดยไม่มีดีเอ็นเอของผู้รับบริจาคเลย[40]

การเก็บข้อมูลดีเอ็นเอมีความเสี่ยงเนื่องจากอาจเกิดการปนเปื้อนได้ง่ายและวิธีการเก็บข้อมูลยังเป็นการล่วงล้ำความเป็นส่วนตัวสูง นอกจากนี้ การประมวลผลนั้นยังต้องใช้ผู้ชำนาญการในการประมวลผล จึงอาจไม่เหมาะที่จะนำดีเอ็นเอมาใช้ในระบบข้อมูลชีวภาพ

2.6.11 ข้อมูลชีวภาพอื่น ๆ

นอกจากข้อมูลชีวภาพที่นิยมใช้ที่ได้กล่าวมาแล้ว ยังมีข้อมูลชีวภาพอื่น ๆ ที่น่าสนใจอีกหลายชนิด ดังต่อไปนี้

1) *ท่าเดิน (Gait)*

เราอาจเคยได้ยินเสียงเดินของบางคนแล้วจำได้ว่าเป็นใคร เนื่องจากท่าทางการเดิน จังหวะการเดินและรองเท้าที่ใส่ทำให้เกิดเสียงที่มีลักษณะเฉพาะของแต่ละคน ท่าเดินถือเป็นข้อมูลชีวภาพประเภทลักษณะของพฤติกรรม โดยท่าเดินของแต่ละคนนั้นมีลักษณะเฉพาะที่สามารถใช้ในการแยกแยะบุคคลได้ในระดับหนึ่งและสามารถใช้ระบุตัวตนได้แม้ในระยะไกล ท่าเดินอาจมีการเปลี่ยนแปลงได้เมื่อเจ้าของข้อมูลมีน้ำหนักที่มากขึ้นหรือน้อยลง หรือมีการอาการบาดเจ็บจึงทำให้อาจไม่เหมาะนักที่จะนำมาใช้ในการยืนยันและ/หรือระบุตัวตน มีการศึกษาค้นคว้าการนำท่าเดินมาใช้แต่การพัฒนาในด้านนี้ยังไม่ก้าวหน้ามากนักเมื่อเทียบกับข้อมูลชีวภาพชนิดอื่น นอกจากนี้ยังมีการศึกษาค้นคว้าเกี่ยวกับการนำท่านั่งมาใช้เป็นข้อมูลชีวภาพอีกด้วย[41]

2) *จังหวะการพิมพ์ (Keystroke Dynamics)*

จังหวะการพิมพ์ของแต่ละคนสามารถนำมาใช้เป็นข้อมูลชีวภาพได้ เนื่องจากแต่ละคนมีจังหวะการพิมพ์และการกดปุ่มผิดไม่เหมือนกัน โดยระบบสามารถเก็บข้อมูลไว้เพื่อนำไปเปรียบเทียบกับข้อมูลตั้งต้น (sample) ที่เคยเก็บไว้ก่อนหน้า จังหวะการพิมพ์มักใช้ร่วมกับ

---

[39] Rutkowska J, Interewiczi B, Rydzewski A, Swietek M, Dominiak A, Durlik M, Olszewski WL. Donor DNA is detected in recipient blood for years after kidney transplantation using sensitive forensic medicine methods. Ann Transplant. 2007;12(3):12-4.

[40] Houser, K. (2019). After Bone Marrow Tranplant, Man's Semen Contains Only Donor's DNA. *Neoscope, 2019*.

[41] Kindt, E. J. (2013). *Privacy and Data Protection Issues of Biometrics Applications*. New York: Springer. p. 31.

พาสเวิร์ด เพื่อตรวจสอบว่าพาสเวิร์ดนั้นพิมพ์โดยคนคนเดียวกันหรือไม่ การจับจังหวะการพิมพ์นั้นต้องการความร่วมมือจากเจ้าของข้อมูล แต่เจ้าของข้อมูลอาจไม่ทราบว่ามีการเก็บข้อมูลอยู่

3) *ลายเซ็น (Signature)*

ลายเซ็นนั้นเป็นสิ่งที่ใช้ยืนยันตัวตนกันมายาวนาน ในอดีตการเปรียบเทียบลายเซ็นนั้นจะใช้คนเปรียบเทียบด้วยตาเปล่า แต่ลายเซ็นในระบบข้อมูลชีวภาพจะจับวิธีการเซ็นชื่อที่ใช้ปากกาอัจฉริยะ (smart pen) โดยวัดแรงกด ความเร็ว และทิศทาง เพื่อนำไปเปรียบเทียบกับข้อมูลตั้งต้นที่เก็บไว้ในฐานข้อมูล อย่างไรก็ดีลายเซ็นอาจมีการเปลี่ยนแปลงได้เมื่อเวลาผ่านไป และมักได้รับผลกระทบจากปัจจัยทางร่างกายหรืออารมณ์ของเจ้าของข้อมูล

4) *กลิ่น (Odor)*

กลิ่นเป็นข้อมูลชีวภาพที่มีลักษณะเฉพาะบุคคล ทำให้สามารถใช้ในการแยกแยะบุคคลได้ การวิเคราะห์กลิ่นจะทำโดยการวิเคราะห์องค์ประกอบของสารเคมีที่อยู่ในกลิ่น

5) *คลื่นสมอง และ จังหวะการเต้นของหัวใจ (Brain Patterns and Heart Rhythms)*

เครื่องมือ Electrocardiograms (EKG) สามารถใช้บันทึกจังหวะการเต้นของหัวใจได้และเครื่อง Electroencephalography (EEG) สามารถใช้บันทึกคลื่นสมองได้ เครื่องมือสองชนิดนี้เป็นเครื่องมือทางการแพทย์ที่เราใช้กันอยู่ในปัจจุบัน การนำคลื่นสมองและจังหวะการเต้นของหัวใจมาใช้เป็นข้อมูลชีวภาพยังอยู่ในขั้นตอนการทดลองและยังไม่มีการนำมาใช้จริง

2.7 การนำเทคโนโลยีชีวภาพไปใช้

ดังที่ได้กล่าวมาแล้ว เทคโนโลยีชีวภาพนั้นสามารถนำไปใช้ได้ใน 2 ลักษณะ คือการยืนยันตัวตนและการระบุตัวตน ซึ่งในปัจจุบันได้มีการนำเทคโนโลยีชีวภาพมาใช้อย่างแพร่หลาย

2.7.1 การยืนยันตัวตน (Authenticate)

เทคโนโลยีชีวภาพได้ถูกนำไปใช้ในขั้นตอนการยืนยันตัวตนเพื่อวัตถุประสงค์ต่าง ๆ เช่น เพื่อทำธุรกรรมของธนาคารโดยให้ลูกค้าทำการยืนยันตัวตนเพื่อเข้าสู่ระบบธุรกรรมบนอุปกรณ์สื่อสารเคลื่อนที่ หรือโมบายแบงก์กิ้ง (mobile banking) ซึ่งขณะนี้ธนาคารในประเทศไทยได้นำเทคโนโลยีนี้มาใช้อย่างแพร่หลาย โดยลูกค้าสามารถทำธุรกรรมต่าง ๆ ผ่านโทรศัพท์มือถือสมาร์ทโฟนหรือแท็บเล็ตได้อย่างสะดวกสบาย ขั้นตอนของการทำงานในลักษณะนี้คือผู้ขอใช้บริการจะต้องทำการสมัคร (enroll) เพื่อขอใช้บริการ โดยระบบจะเก็บข้อมูลชีวภาพตั้งต้น จากนั้นระบบจะทำการแปลงข้อมูลที่เก็บได้ให้เป็นปรกติ และนำไปสร้างเป็นแม่แบบ หลังจากการสมัครแล้วเมื่อบุคคลนั้นต้องการจะเข้าสู่ระบบในครั้งถัด ๆ ไป ระบบจะทำการเก็บข้อมูลตั้งต้นของบุคคลนั้นอีกครั้งแล้วนำไปสร้างแม่แบบ จากนั้นจึงนำแม่แบบที่สร้างใหม่ไปเปรียบเทียบกับแม่แบบที่ได้สร้างไว้ในขั้นตอนการสมัคร

นอกจากการใช้ยืนยันตัวตนเพื่อทำธุรกรรมออนไลน์แล้ว การยืนยันตัวตนด้วยชีวภาพนั้นยังถูกนำไปใช้ในการเช็คเวลาเข้า-ออกของพนักงาน หรือนักเรียน และหลายประเทศยังได้นำเทคโนโลยีนี้ไปใช้ในพาสปอร์ตเพื่อใช้ในการตรวจคนเข้าเมืองอีกด้วย

2.7.2 การระบุตัวตน (Identify)

ผู้ค้าปลีกอาจนำเทคโนโลยีชีวภาพไปใช้ในการโฆษณาแบบเจาะจง โดยการใช้ระบบชีวภาพเก็บภาพของผู้ที่เดินผ่าน และนำไปการวิเคราะห์ความรู้สึก กริยาท่าทาง อายุ หรือเพศของคนที่เดินผ่านป้ายและแสดงเนื้อหาของป้ายนั้น ๆ ให้เหมาะสมกับผู้ที่เดินผ่านป้าย การนำมาใช้ในลักษณะนี้เป็นการเปรียบเทียบแบบหนึ่งต่อกลุ่ม ระบบจะต้องทำการเก็บแม่แบบของบุคคลไว้ในฐานข้อมูลเป็นจำนวนมากเพื่อนำมาใช้เปรียบเทียบกับข้อมูลของผู้ที่เดินผ่านป้าย โดยที่ไม่จำเป็นต้องระบุว่าคนผู้นั้นเป็นใคร หากเพียงแต่ระบุได้ว่าคนผู้นั้นอายุเท่าไหร่ เพศอะไร และกำลังมีความรู้สึกเช่นไร ก็สามารถแสดงโฆษณาที่คาดว่าน่าจะเป็นที่สนใจของบุคคลผู้นั้นได้ ตลาดของการโฆษณาแบบเจาะจง (target advertising) นี้เติบโตขึ้นถึง 3.2 พันล้านเหรียญสหรัฐภายในระยะเวลา 6 ปี (ระหว่าง พ.ศ. 2553 ถึง พ.ศ.2559)[42]

3. หลักการคุ้มครองข้อมูลส่วนบุคคลชีวภาพ

แนวคิดเรื่องความเป็นส่วนตัวสำหรับข้อมูลชีวภาพกำหนดให้เจ้าของข้อมูลส่วนบุคคลต้องสามารถควบคุมการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลของตนเองได้ โดยสามารถกำหนดได้ว่าให้ผู้ใดสามารถเก็บรวบรวม ใช้ และเปิดเผยข้อมูลของตนได้ รวมถึงสามารถควบคุมวิธีการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลชีวภาพของตน[43] เนื่องจากข้อมูลชีวภาพเป็นข้อมูลที่มีความอ่อนไหวสูง หากมีผู้นำไปใช้ในทางที่ผิด หรือมีการรั่วไหลออกไปจะสร้างความเสียหายรุนแรงและไม่มีที่สิ้นสุดแก่เจ้าของข้อมูลส่วนบุคคล ดังนั้นหลักการคุ้มครองข้อมูลส่วนบุคคลชีวภาพที่เหมาะสม คือ[44]

3.1 หลักความยินยอม

ความยินยอมของเจ้าของข้อมูลส่วนบุคคลและการให้ทางเลือกกับเจ้าของข้อมูลส่วนบุคคลเป็นสิ่งสำคัญในบริบทของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลชีวภาพ การเก็บรวบรวมข้อมูลส่วนบุคคลชีวภาพควรถูกนำไปใช้เพื่อวัตถุประสงค์ที่ได้กำหนดไว้เท่านั้น ไม่ว่าจะเป็น

---

[42] Coseraru, R. (2017). Facial Recognition Systems and their Data Protection Risks Under the GDPR. (Master Thesis), Tilburg University, Retrieved from http://arno.uvt.nl/show.cgi?fid=143731. p 18.

[43] Kindt, E. J. (2009). The Use of Privacy Enhancing Technologies for Biometric Systems Analysed from a Legal Perspective. *Privacy and Identity Management for Life, 5th IFIP WG 9.2, 9.6/11.4, 11.6, 11.7/ PrimeLife International Summer School (PRIMELIFE)*, 134-145.

[44] Toli, C.-A. (2018). *Secure and Privacy-Preserving Biometric Systems.* (Doctor of Engineering Science (PhD)), Katholieke Universiteit Leuven, Retrieved from https://www.esat.kuleuven.be/cosic/publications/thesis-308.pdf . pp 35-37.

เพื่อการระบุตัวตน หรือการยืนยันตัวตน ทั้งนี้ไม่ว่าวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลชีวภาพคือการระบุตัวตน หรือการยืนยันตัวตนจำต้องมีกฎระเบียบหรือแนวปฏิบัติที่ชัดเจน

หลักความยินยอมควรอยู่บนพื้นฐานที่เจ้าของข้อมูลส่วนบุคคลได้รับทราบขอบเขตของการเก็บรวบรวม และประมวลผลข้อมูลส่วนบุคคลชีวภาพอย่างชัดเจน เพื่อป้องกันการละเมิดหลักความเป็นส่วนตัวไม่ควรมีการเก็บข้อมูลส่วนบุคคลชีวภาพในฐานข้อมูลชีวภาพกลาง (Centralized Biometric Database) เนื่องจากการกระทำดังกล่าวเป็นการเพิ่มความเสี่ยงต่อภัยคุกคามความเป็นส่วนตัว แต่ในกรณีที่จำเป็นการเก็บข้อมูลส่วนบุคคลชีวภาพในฐานข้อมูลชีวภาพกลางควรมีเพื่อวัตถุประสงค์ในการยืนยันตัวตน (Authentication) เท่านั้น และควรเป็นไปตามหลักปฏิบัติที่เป็นสากล เช่น ISO/IEC 24745:2011[45] หรือ ISO/IEC 19092:2008[46] เป็นต้น

3.2 หลักความโปร่งใสและความรับผิดชอบ

หลักความโปร่งใสในการคุ้มครองข้อมูลส่วนบุคคลชีวภาพคือการที่เจ้าของข้อมูลส่วนบุคคลได้รับการแจ้งข้อมูลที่ชัดเจนและโปร่งใสเกี่ยวกับวิธีการที่องค์กรต่าง ๆ ที่รับผิดชอบในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลชีวภาพจะนำข้อมูลชีวภาพไปใช้ นอกจากนี้เจ้าของข้อมูลส่วนบุคคลต้องได้รับแจ้งเกี่ยวกับกลไกการเข้ารหัสที่ใช้ป้องกันการรั่วไหลของข้อมูลชีวภาพ รวมถึงความแม่นยำของระบบและอัตราความผิดพลาดที่อาจนำไปสู่ความล้มเหลวของระบบ ส่วนความรับผิดชอบคือการที่องค์กรนั้น ๆ ได้ดำเนินการตามขั้นตอนที่เหมาะสมเพื่อให้แน่ใจว่าทุกฝ่ายที่เกี่ยวข้องปฏิบัติตามหลักการดังกล่าว

3.3 หลักการเลือกปฏิบัติ

ดังที่กล่าวมาแล้ว ข้อมูลส่วนบุคคลชีวภาพเป็นข้อมูลที่ละเอียดอ่อนและข้อมูลส่วนบุคคลชีวภาพบางชนิดอาจเปิดเผยให้เห็นถึงสถานะทางสรีรวิทยา พยาธิวิทยา หรืออาการเจ็บป่วยของเจ้าของข้อมูลส่วนบุคคลชีวภาพได้ จอประสาทตา (retina) สามารถบอกถึงปัญหาสุขภาพ เช่น ไขมันในเส้นเลือดสูง หรือเบาหวานได้ นอกจากนี้ ข้อมูลชีวภาพที่ใช้ลักษณะทางสรีระ เช่น ท่าเดิน หรือจังหวะการพิมพ์ อาจทำให้เห็นถึงอาการป่วยทางสมองของเจ้าของข้อมูลส่วนบุคคลชีวภาพนั้นได้ ดังนั้นเพื่อมิให้เกิดการเลือกปฏิบัติ การนำข้อมูลที่อ่อนไหวเหล่านี้ไปใช้ควรอยู่ภายใต้การคุ้มครองที่แน่นหนา โดยไม่อนุญาตให้มีการนำไปใช้นอกเหนือจากวัตถุประสงค์ที่ได้กำหนดไว้ และต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลชีวภาพก่อนเสมอ หลักการนี้เป็นการป้องกันการระบุตัวตนที่แอบแฝง เช่น การระบุตัวตนของผู้คนในฝูงชน เป็นต้น

---

[45] ISO/IEC 24745:2011 - Information Technology – Security Techniques – Biometric Information Protection, 2011.

[46] ISO/IEC 19092:2008 – Financial Services – Biometrics – Security Framework, 2008.

3.4 หลักความถูกต้องและการแก้ไข

หลักการนี้กำหนดให้ข้อมูลส่วนบุคคลต้องมีความถูกต้องและควรได้รับการปรับปรุงให้ทันสมัยอยู่เสมอ ซึ่งเกี่ยวข้องกับข้อปฏิบัติด้านการรักษาความปลอดภัยโดยการเพิกถอนและการต่ออายุ ซึ่งองค์กรต่าง ๆ ที่เก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลชีวภาพต้องจัดให้มีแนวปฏิบัติในการรักษาความปลอดภัยของข้อมูล เพื่อให้แน่ใจว่าข้อมูลชีวภาพที่ไม่ถูกต้อง หรือไม่สมบูรณ์ได้ถูกลบยกเลิก หรือ แก้ไข

3.5 หลักการจำกัดข้อมูล

หลักการจำกัดข้อมูลคือการกำหนดทั้งจำนวน และขอบเขตของการใช้งานของข้อมูลชีวภาพ โดยการใช้ข้อมูลชีวภาพควรจำกัดเฉพาะสิ่งที่จำเป็น และต้องมีการระบุวัตถุประสงค์ที่ชัดเจนและถูกต้องตามกฎหมาย การเก็บรวบรวมข้อมูลชีวภาพควรเก็บเท่าที่เกี่ยวข้องและจำกัด เฉพาะที่จำเป็น หลักการของการจำกัดข้อมูลห้ามมิให้ดำเนินการเพื่อวัตถุประสงค์ในการระบุตัวตนบุคคลหากไม่ได้รับความยินยอมอย่างชัดเจนจากเจ้าของข้อมูลส่วนบุคคล อย่างไรก็ตามหลักการนี้อาจทำได้โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการจ้างงาน การประกันสังคม การคุ้มครองทางสังคมและเพื่อประโยชน์สาธารณะในด้านสาธารณสุขแต่ยังคงต้องรักษาหลักการของการจำกัดข้อมูลไว้

3.6 หลักการไม่เปิดเผยตัวตน

หลักการการไม่เปิดเผยตัวตนใช้เพื่อลดปัญหาการละเมิดความเป็นส่วนตัวในการทำธุรกรรมหรือการระบุตัวตนข้ามระบบงาน หรือฐานข้อมูล ในทางปฏิบัติการไม่เปิดเผยตัวตนสามารถทำได้โดยการรวมแนวทางการปฏิบัติด้านการรักษาความปลอดภัยที่เกี่ยวกับการทำให้ย้อนกลับไม่ได้ (non-invertibility) การทำให้เชื่อมโยงไม่ได้ (un-linkability) การยกเลิก (cancelability) และการต่ออายุ (renewability) การไม่เปิดเผยตัวตนหมายถึงตัวตนของเจ้าของข้อมูลส่วนบุคคลจะไม่สามารถถูกแยกออกมาจากกลุ่มของเจ้าของข้อมูลส่วนบุคคลหรือกลุ่มบุคคลใดได้ นอกจากนี้ยังหมายถึงผู้ที่เกี่ยวข้องและผู้รับข้อมูลชีวภาพซึ่งต้องไม่เปิดเผยตัวตนเพื่อลดความเป็นไปได้ที่จะระบุได้ว่าใครเป็นผู้เก็บรวบรวมข้อมูลซึ่งอาจทำให้มีการย้อนกลับไประบุตัวตนของเจ้าของข้อมูลส่วนบุคคลได้ในที่สุด

4. ความเสี่ยงของการใช้ข้อมูลชีวภาพ

ระบบข้อมูลชีวภาพนั้นมีความเสี่ยงหลายประการ โดยความเสี่ยงดังกล่าวอาจเกิดจากธรรมชาติของข้อมูลชีวภาพเอง หรือเกิดจากความผิดพลาดของระบบข้อมูลชีวภาพที่มีสาเหตุจากวิธีการทำงานของระบบเอง หรือเกิดจากโจมตีจากภายนอก

4.1 ความเสี่ยงต่อความปลอดภัยของสังคม

เนื่องจากธรรมชาติของข้อมูลชีวภาพบางชนิด ยิ่งมีการนำข้อมูลชีวภาพมาใช้มากเท่าไหร่ยิ่งทำให้เกิดความเสี่ยงมากขึ้นเท่านั้น การรักษาความมั่นคงปลอดภัยของประชาชนอาจได้รับผลกระทบจากการใช้ข้อมูลชีวภาพ เนื่องจากการปลอมแปลงลายนิ้วมือทำได้ง่ายโดยสามารถค้นหาวิธีปลอมลายนิ้วมือได้จากอินเตอร์เน็ต ในการกระทำความผิดคนร้ายอาจทิ้งลายนิ้วมือของผู้อื่นไว้ในสถานที่เกิดเหตุแทนลายนิ้วมือของตน เมื่อทำการตรวจหาลายนิ้วมือคนร้ายจากสถานที่เกิดเหตุกลับไม่พบลายนิ้วมือของผู้ก่อเหตุ แต่พบลายนิ้วมือของผู้อื่นแทน ดังนั้นผู้สุจริตอาจกลายเป็นผู้ต้องหาและถูกลงโทษโดยมิได้กระทำความผิด

การนำลายนิ้วมือมาใช้มากขึ้นทำให้เกิดการปลอมแปลงและการขโมยข้อมูลลายนิ้วมือมากขึ้นตามไปด้วย และไม่เป็นที่แน่ชัดว่าเจ้าหน้าที่จะปราบปรามกระบวนการปลอมแปลงข้อมูลลายนิ้วมือหรือไม่ เนื่องจากในบางครั้งเจ้าหน้าที่อาจต้องใช้บริการของกระบวนการดังกล่าว เช่น ในกรณีที่โน้ตบุ๊คของผู้ต้องสงสัยใช้ลายนิ้วมือในการเปิด เจ้าหน้าที่ในบางประเทศจะไม่สามารถบังคับให้ผู้ต้องสงสัยเปิดโน้ตบุ๊คให้เจ้าหน้าที่ตรวจสอบได้ เนื่องจากกฎหมายในบางประเทศไม่อนุญาตให้เจ้าหน้าที่บังคับผู้ต้องสงสัยให้กระทำการอย่างใดอย่างหนึ่งหากการกระทำนั้นอาจนำไปสู่หลักฐานซึ่งจะผูกมัดตัวผู้ต้องสงสัย หรือเครือญาติได้

อนึ่ง การนำข้อมูลชีวภาพมาใช้ยังอาจทำให้อัตราการเกิดอาชญากรรม เช่น การลักพาตัว หรือการขโมยชิ้นส่วนมนุษย์ หรือการฆาตกรรมสูงขึ้นได้ ตัวอย่างเช่น กรณีเจ้าของรถเมอร์เซเดส-เบนซ์ เอสคลาสในประเทศมาเลเซียได้ถูกขโมยตัดนิ้วเพื่อนำไปสตาร์ทรถ[47] การใช้ม่านตา หรือจอประสาทตาเพื่อเข้าสู่สถานที่ที่ต้องมีการรักษาความปลอดภัยสูงก็อาจทำให้มีการขโมยดวงตาเกิดขึ้นได้ แม้ว่าจะสามารถเพิ่มฟังก์ชั่นของระบบให้ตรวจเช็คการมีชีวิต (liveness detection) ได้ แต่นั่นก็เป็นเพียงการเปลี่ยนความเสี่ยงจากการตัดชิ้นส่วนของร่างกายไปเป็นการลักพาตัวหรือการข่มขู่กรรโชกแทน นอกจากนี้ การใช้ข้อมูลชีวภาพเพื่อระบุตัวตนยังอาจทำให้ผู้ที่ต้องปกปิดตัวตนด้วยเหตุผลที่จำเป็นและอยู่ภายใต้กฎหมายได้รับอันตรายโดยไม่จำเป็น เช่น ตำรวจนอกเครื่องแบบ หรือพยานที่ต้องการการคุ้มครอง เป็นต้น[48]

---

[47] Kent, J. (2005). Malaysia car thieves steal finger. สืบค้นจาก http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm

[48] Pfitzmann, A. (2008). Biometrics - How to Put to Use and How Not at All? ใน S. Furnell, S. K. Katsikas, & A. Lioy (Eds.), *Trust, Privacy and Security in Digital Business, LNCS* (Vol. 5185, pp. 3-5). Springer-Verlag Berlin Heidelberg: TrustBus 2008.

4.2 ความเสี่ยงที่เกิดจากความผิดพลาดของระบบข้อมูลชีวภาพ

ความผิดพลาดของระบบข้อมูลชีวภาพ เป็นความผิดพลาดที่เกิดจากธรรมชาติของวิธีการทำงานของระบบเอง (intrinsic error) ที่อาจเกิดขึ้นได้ไม่ว่าระบบนั้นจะดีเพียงใด การผิดพลาดของระบบข้อมูลชีวภาพสามารถเกิดขึ้นได้ในระหว่างขั้นตอนต่าง ๆ ได้ดังนี้

4.2.1 ความล้มเหลวในขั้นตอนการสมัคร

ในขั้นตอนของการสมัครมีความเป็นไปได้ที่เจ้าของข้อมูลไม่สามารถทำการสมัครได้ อาจเป็นเพราะเจ้าของข้อมูลขาดคุณลักษณะในการสมัคร เช่น ไม่มีลายนิ้วมือ หรือนิ้วมือขาดเนื่องจากอุบัติเหตุ เป็นต้น ทำให้เจ้าของข้อมูลส่วนบุคคลไม่สามารถใช้ระบบข้อมูลชีวภาพได้ ความผิดพลาดในขั้นตอนนี้เรียกว่า ความล้มเหลวในการสมัคร (Failure to Enroll - FTE)[49]

4.2.2 ความล้มเหลวในการได้มา

ความล้มเหลวในการได้มา (Failure to Acquire – FTA) อาจเกิดขึ้นได้เช่นเดียวกับความล้มเหลวในขั้นตอนการสมัคร ความล้มเหลวในการได้มาอาจเกิดขึ้นระหว่างการเก็บรวบรวมข้อมูลจากเจ้าของข้อมูลที่เคยสมัครไว้แล้ว หรือการนำข้อมูลไปสร้างแม่แบบ หรือระหว่างการเปรียบเทียบข้อมูลที่เก็บรวบรวมกับข้อมูลแม่แบบที่เก็บไว้ในระบบ นอกจากนี้ ความล้มเหลวในการได้มาหมายความรวมถึงความล้มเหลวในการเก็บรวบรวม (Failure to Capture - FTC) และ ความล้มเหลวในการเปรียบเทียบ (Failure to Compare – FTM)[50] อีกด้วย

4.2.3 ความผิดพลาดในการยืนยัน หรือระบุตัวตน

ความผิดพลาดของระบบข้อมูลชีวภาพอาจเกิดขึ้นในขั้นตอนของการยืนยันตัวตน หรือระบุตัวตนได้ ซึ่งความผิดพลาดนั้นแบ่งได้เป็น 2 ประเภท คือ อัตราการปฏิเสธที่ผิดพลาด (False Rejection Rate - FRR) และ อัตราการยอมรับที่ผิดพลาด (False Acceptance Rate - FAR)

1) อัตราการปฏิเสธที่ผิดพลาด (False Rejection Rate - FRR) หมายถึง ในการเปรียบเทียบข้อมูลชีวภาพของผู้ที่ต้องการระบุตัวตน หรือยืนยันตัวตน กับข้อมูลแม่แบบจากฐานข้อมูลแล้ว ระบบปฏิเสธว่าข้อมูลชีวภาพนั้นมิใช่ของเจ้าของข้อมูล เช่น การปฏิเสธผู้ใช้ที่มีสิทธิใช้ระบบไม่ให้เข้าใช้ระบบ

2) อัตราการยอมรับที่ผิดพลาด (False Acceptance Rate - FAR) หมายถึง ในการเปรียบเทียบข้อมูลชีวภาพของผู้ที่ต้องการระบุตัวตน หรือยืนยันตัวตนกับข้อมูลแม่แบบจากฐานข้อมูลแล้ว ระบบยอมรับว่าผู้ที่ไม่ใช่เจ้าของข้อมูลนั้นเป็นเจ้าของข้อมูล เช่น การยอมรับให้ผู้ที่ไม่มีสิทธิใช้ระบบเข้าระบบ

---

[49] Kindt, E. J. (2013). *Privacy and Data Protection Issues of Biometrics Applications*. New York: Springer. p. 48.

[50] Kindt, E. J. (2013). *Privacy and Data Protection Issues of Biometrics Applications*. New York: Springer. p. 49.

อัตราการปฏิเสธที่ผิดพลาดและอัตราการยอมรับที่ผิดพลาดที่สูงหรือต่ำเกินไปย่อมมีผลกระทบต่อระดับความปลอดภัยและความสะดวกในการใช้ระบบ อัตราความผิดพลาดทั้งสองนี้มีความสัมพันธ์กันอย่างใกล้ชิด การลดลงของอัตราการยอมรับที่ผิดพลาด (FAR) จะทำให้อัตราการปฏิเสธที่ผิดพลาด (FRR) สูงขึ้น ในทางกลับกันการลดลงของอัตราการปฏิเสธที่ผิดพลาด (FRR) จะทำให้อัตราการยอมรับที่ผิดพลาด (FAR) สูงขึ้น

FRR และ FAR มีความเกี่ยวข้องกับการกำหนดระดับที่รับได้ (Threshold) ของระบบข้อมูลชีวภาพ สำหรับระบบที่ต้องการความปลอดภัยสูงอัตราของการยอมรับที่ผิดพลาดจะต้องต่ำ เนื่องจากไม่สามารถให้คนที่ไม่ได้รับอนุญาตเข้าระบบได้ ในทางกลับกันระบบที่ไม่ได้ต้องการความปลอดภัยสูงสามารถรับอัตราของการยอมรับที่ผิดพลาดที่สูงกว่าได้

ระดับของ FRR และ FAR นั้นจะเกิดขึ้นจากระบบ และกฎเกณฑ์ในการตัดสินใจที่ใช้ในระบบ เช่น จำนวนครั้งในการเก็บข้อมูล จำนวนแม่แบบที่ใช้ในการเปรียบเทียบ เป็นต้น แต่ยังมีความผิดพลาดอีก 2 ชนิด ที่เกิดจากความผิดพลาดของอัลกอริทึมที่ใช้ คือ อัตราการยอมรับว่าตรงกันที่ผิดพลาด (False Match Rate - FMR) และ อัตราการไม่ยอมรับว่าตรงกันที่ผิดพลาด (False Non-match Rate – FNMR) ตัวอย่างเช่น การที่สองรูปเป็นคนละคนกันแต่ระบบบอกว่าเป็นคนเดียวกัน ถือว่าเป็น FMR และการที่สองรูปเป็นของคนคนเดียวกัน แต่ระบบบอกว่าเป็นคนละคนกัน คือ FNMR

โดยสรุป อาจกล่าวได้ว่าอัตราความผิดพลาดของระบบข้อมูลชีวภาพที่เกิดจากธรรมชาติของวิธีการทำงานของระบบเอง (intrinsic error) ขึ้นอยู่กับคุณภาพของข้อมูลชีวภาพรวมไปถึงวิธีการและขั้นตอนในการเก็บรวบรวม นอกจากนี้ยังขึ้นอยู่กับคุณภาพของอัลกอริทึมที่ใช้ในการจับคู่อีกด้วย

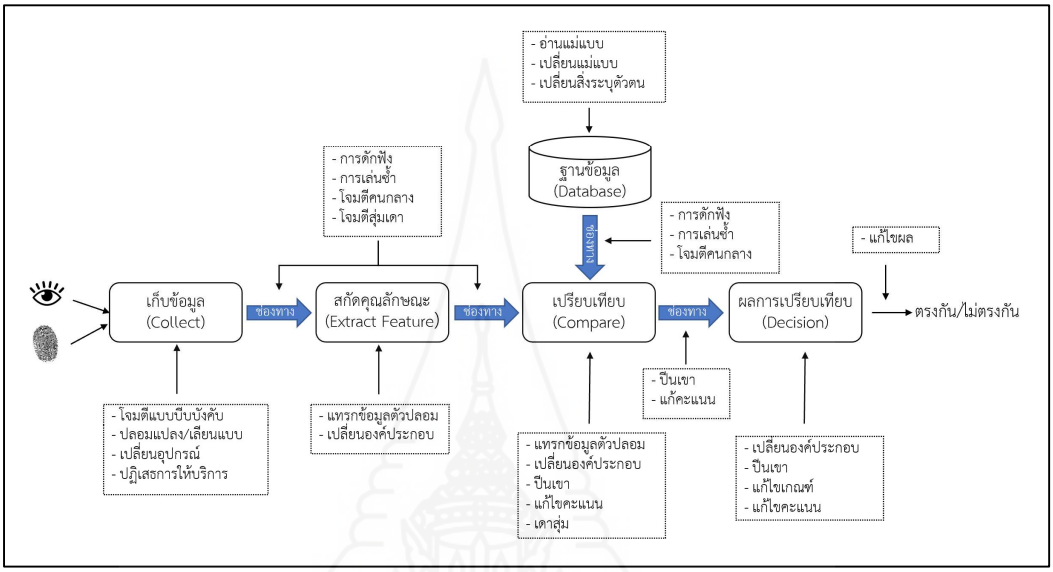
4.3 ความเสี่ยงต่อการโจมตีจากภายนอก

องค์กรที่เก็บรวบรวมข้อมูลส่วนบุคคลไว้มากย่อมมีความเสี่ยงที่จะถูกโจมตีโดยผู้ไม่หวังดี การพัฒนาของเทคโนโลยีทำให้มีการโจมตีองค์กรเหล่านี้มากขึ้น ในปี ค.ศ. 2014 ได้มีการโจมตีสำนักงานฝ่ายบริหารงานบุคคลของสหรัฐอเมริกา (U.S. Office of Personnel Management) ในสหรัฐอเมริกา ซึ่งทำให้ข้อมูลของบุคคลถึง 22.1 ล้านคนถูกขโมย ซึ่งถือได้ว่าเป็นการโจมตีที่รุนแรงครั้งหนึ่งเนื่องจากข้อมูลที่ถูกขโมยไปนั้นเป็นข้อมูลที่มีความอ่อนไหวสูง เช่น ข้อมูลพฤติกรรมทางเพศและลายนิ้วมือ เป็นต้น[51]

---

[51] Fruhlinger, J. (2020). The OPM hack explained: Bad security practices meet China's Captain America. *CSO ASEAN*. สืบค้นจาก https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

ดังที่ได้กล่าวมาแล้วระบบข้อมูลชีวภาพที่มีอัตราการยอมรับที่ผิดพลาด (False Acceptance Rate - FAR) สูงจะมีความเสี่ยงต่อการโดนโจมตีจากภายนอกสูง เนื่องจากระบบจะยอมรับข้อมูลที่ผิดพลาดได้มากกว่าระบบที่มีอัตราการยอมรับที่ผิดพลาดต่ำ การโจมตีจากภายนอกนั้นสามารถโจมตีระบบข้อมูลส่วนบุคคลได้หลายจุด ดังต่อไปนี้[52]



ภาพที่ 2.8 การโจมตีระบบข้อมูลชีวภาพ

ที่มา: Toli, C.-A. (2018). Secure and Privacy-Preserving Biometric Systems. (Doctor of Engineering Science (PhD)), Katholieke Universiteit Leuven.

4.3.1 อุปกรณ์อ่านข้อมูลชีวภาพ (Sensor)

การโจมตีที่มุ่งเป้าไปยังเครื่องอ่านข้อมูลชีวภาพ หรือเซนเซอร์นั้นเป็นการโจมตีโดยตรง ซึ่งอาจทำได้หลายวิธี เช่น

1) *การโจมตีแบบบีบบังคับ (Coercive Attack)*

การโจมตีชนิดนี้คือการที่ผู้โจมตีแอบอ้างว่าเป็นผู้ได้รับอนุญาตให้เข้าระบบโดยบังคับให้ผู้มีอำนาจอนุญาตให้เข้าถึงระบบได้

2) *การปลอมแปลงและการเลียนแบบ (Spoofing and Mimic)*

การโจมตีแบบนี้ใช้การปลอมแปลงและการเลียนแบบคุณลักษณะทางชีวภาพของผู้ใช้ที่ลงทะเบียนโดยวิธีการต่าง ๆ เพื่อหลอกลวงระบบ

---

[52] Toli, C.-A. (2018). *Secure and Privacy-Preserving Biometric Systems.* (Doctor of Engineering Science (PhD)), Katholieke Universiteit Leuven, Retrieved from https://www.esat.kuleuven.be/cosic/publications/thesis-308.pdf

3) *การเปลี่ยนอุปกรณ์อ่านข้อมูล (Device Substitution)*

การโจมตีวิธีนี้เป็นการเปลี่ยนอุปกรณ์อ่านข้อมูลชีวภาพเป็นอุปกรณ์ที่ผ่านการดัดแปลงมาแล้ว

4) *การปฏิเสธการให้บริการ (Denial of Service)*

เป็นอีกรูปแบบหนึ่งของการโจมตีที่ผู้ไม่หวังดีส่งคำขอเข้าระบบเป็นจำนวนมาก ระบบไม่สามารถรับคำขอเข้าถึงจำนวนมากได้จนทำให้ระบบล้มเหลว จนไม่สามารถใช้งานได้

4.3.2 การสกัดคุณลักษณะ (Feature Extraction)

ในขั้นตอนของการสกัดคุณลักษณะผู้โจมตีสามารถบังคับให้ระบบข้อมูลชีวภาพสร้างคุณลักษณะชีวภาพที่ผู้โจมตีต้องการได้โดยการแทรกข้อมูลของตัวปลอมที่ต้องการเข้าไปในระบบ หรือเปลี่ยนองค์ประกอบบางส่วนเพื่อให้ระบบข้อมูลชีวภาพอ้างถึงซอฟต์แวร์หรือฮาร์ดแวร์ของผู้โจมตี เพื่อให้ผู้โจมตีสามารถควบคุมพฤติกรรมของระบบข้อมูลชีวภาพและสร้างชุดคุณลักษณะเฉพาะเองได้

4.3.3 ฐานข้อมูล (Database)

เมื่อระบบได้ทำการสกัดคุณลักษณะและสร้างแม่แบบแล้ว ข้อมูลแม่แบบนั้นจะถูกจัดเก็บไว้ในฐานข้อมูล ซึ่งฐานข้อมูลนั้นอาจเป็นฐานข้อมูลที่อยู่ในเครื่อง (local database) หรือฐานข้อมูลระยะไกล (remote database) นอกจากนี้ข้อมูลยังอาจถูกเก็บแบบกระจาย (distributed) อยู่บนหลายเซิร์ฟเวอร์ได้ ผู้โจมตีอาจเลือกโจมตีฐานข้อมูลโดยการอ่านแม่แบบ หรือเปลี่ยนแม่แบบที่เก็บไว้ในฐานข้อมูล หรือเปลี่ยนความเชื่อมโยงระหว่างข้อมูลชีวภาพกับข้อมูลส่วนบุคคลที่เป็นสิ่งระบุตัวตน เช่น ชื่อ เป็นต้น การโจมตีในลักษณะนี้จะทำให้ผู้ที่ไม่ควรเข้าระบบได้สามารถเข้าสู่ระบบได้ หรือทำให้ผู้ที่ควรเข้าระบบได้ไม่สามารถเข้าสู่ระบบได้

4.3.4 การเปรียบเทียบ (Matching)

ขั้นตอนของการเปรียบเทียบคือ การนำข้อมูลแม่แบบชีวภาพที่ได้จากขั้นตอนการสมัคร (enroll หรือ registration) มาเปรียบเทียบกับข้อมูลแม่แบบที่สร้างจากขั้นตอนการยืนยันตัวตน การโจมตีระบบข้อมูลชีวภาพในขั้นตอนของการเปรียบเทียบอาจทำได้โดยการเปลี่ยนแปลงผลของการเปรียบเทียบให้เป็นผลที่ผู้โจมตีต้องการ โดยการแทรกข้อมูลของผู้ปลอมตัว การทดแทนส่วนประกอบบางส่วนหรือการเปลี่ยนแปลงผลการเปรียบเทียบโดยการโจมตีแบบการคาดเดา (guessing) หรือการปีนเขา (hill-climbing) การโจมตีในลักษณะดังกล่าวผู้โจมตีจะทำการแทนที่ส่วนประกอบของซอฟต์แวร์หรือฮาร์ดแวร์ก่อนการสรุปผลการเปรียบเทียบของระบบโดยการพยายามแก้ไขคะแนนอยู่ตลอดเวลาเพื่อให้เกินเกณฑ์การตัดสินใจ

4.3.5 ช่องทางเชื่อมต่อ (Channel)

ช่องทางเชื่อมต่อเป็นตัวเชื่อมต่อระหว่างขั้นตอนต่าง ๆ ของระบบข้อมูลชีวภาพ เช่น ระหว่างอุปกรณ์อ่านข้อมูลชีวภาพและการสกัดคุณลักษณะ หรือ การสกัดคุณลักษณะและการเปรียบเทียบ และการเปรียบเทียบกับผลการเปรียบเทียบ โดยช่องทางถือว่าเป็นจุดอ่อนของระบบ ทั้งนี้ผู้โจมตีสามารถโจมตีได้ในระหว่างขั้นตอนต่าง ๆ

ผู้บุกรุกอาจโจมตีช่องทางการเชื่อมต่อระหว่างอุปกรณ์อ่านข้อมูลชีวภาพและการสกัดคุณลักษณะ และระหว่างการสกัดคุณลักษณะและการเปรียบเทียบ โดยการสกัดกั้น และยึดการควบคุม หนึ่งในวิธีการโจมตีช่องทางเชื่อมต่อคือการดักฟัง (eavesdropping) โดยผู้บุกรุกจะดักฟังการส่งข้อมูลชีวภาพ สำหรับการโจมตีแบบเล่นซ้ำ (replay) ผู้โจมตีจะส่งสัญญาณซ้ำ ๆ เข้าไปที่ช่องทางเชื่อมต่อเพื่อเจาะเข้าระบบโดยไม่ต้องผ่านอุปกรณ์อ่านข้อมูลชีวภาพ สำหรับการโจมตีแบบคนตรงกลาง (man in the middle attack) ผู้โจมตีสามารถจัดการกับข้อมูลที่ส่งระหว่างสองฝ่ายโดยทั้งสองฝ่ายไม่ทราบว่ามีการโจมตีระหว่างการเชื่อมต่อ หากการรับ-ส่งข้อมูลนั้นเป็นการรับ-ส่งภายในเครื่องเดียวกันโอกาสของการโจมตีในลักษณะนี้แทบจะเป็นไปไม่ได้เลย แต่หากเป็นการส่งข้อมูลระยะไกล (remote) การโจมตีในลักษณะนี้ถือว่าเป็นภัยคุกคามร้ายแรงต่อระบบข้อมูลชีวภาพ ส่วนการโจมตีแบบการสุ่มเดา (brute force attack) คือการสุ่มเดาข้อมูลไปเรื่อย ๆ จนกว่าจะพบข้อมูลที่ตรงกันกับข้อมูลที่ถูกต้องในระบบ สำหรับช่องทางเชื่อมต่อระหว่างแม่แบบที่จัดเก็บไว้และการเปรียบเทียบอาจสามารถถูกโจมตีได้เมื่อแม่แบบชีวภาพถูกส่งไปยังขั้นตอนการเปรียบเทียบโดยมีการสกัดกั้นข้อมูล หรือเปลี่ยนแปลงข้อมูลระหว่างทาง สำหรับขั้นตอนสุดท้ายคือช่องระหว่างการเปรียบเทียบกับผลของการเปรียบเทียบอาจถูกโจมตีโดยการแก้ไขคะแนน หรือเปลี่ยนค่าของการเปรียบเทียบหรือโดยการโจมตีด้วยการเปลี่ยนค่าคะแนนไปเรื่อย ๆ (hill-climbing) จนกว่าจะได้คะแนนที่ดีที่สุด

4.3.1 ผลการเปรียบเทียบ (Decision)

ผู้โจมตีอาจทำการเปลี่ยนแปลงผลการเปรียบเทียบในขั้นตอนสุดท้ายของการทำงานของระบบข้อมูลชีวภาพ แม้ว่าระบบข้อมูลชีวภาพนั้นจะแม่นยำเพียงใดการโจมตีในลักษณะนี้อาจทำให้ระบบข้อมูลชีวภาพหมดความหมายได้

4.4 ความเสี่ยงที่อาจเกิดขึ้นต่อเจ้าของข้อมูลชีวภาพ

4.4.1 ความเสี่ยงต่อการละเมิดความเป็นส่วนตัว

ดังที่กล่าวมาแล้วข้างต้น ข้อมูลชีวภาพสามารถนำมาใช้ในการระบุตัวตน และการยืนยันตัวตนได้ อย่างไรก็ตามการนำข้อมูลชีวภาพมาใช้ในการระบุตัวตนนั้นทำให้เกิดความเสี่ยงต่อการละเมิดความเป็นส่วนตัว เนื่องจากข้อมูลชีวภาพเป็นข้อมูลที่อ่อนไหวเปราะบาง และข้อมูลชีวภาพบางชนิดอาจทำให้ผู้เก็บรวบรวมได้ล่วงรู้ข้อมูลเกี่ยวกับเจ้าของข้อมูลที่เจ้าของข้อมูลไม่ต้องการ

เปิดเผยให้ผู้อื่นทราบ เช่น จอประสาทตาอาจบอกถึงความเจ็บป่วย สภาวะของโรค หรือแม้แต่การบริโภคแอลกอฮอล์[53] ส่วนลายนิ้วมืออาจบอกได้ถึงพฤติกรรมทางเพศหรือความสนใจในเพศเดียวกันของผู้ชาย[54] ซึ่งทำให้การเก็บรวบรวมข้อมูลชีวภาพเป็นการละเมิดสิทธิความเป็นส่วนตัว นอกจากนี้บางครั้งการเก็บรวบรวมข้อมูลชีวภาพกระทำโดยเจ้าของข้อมูลไม่ได้รับทราบซึ่งเป็นการละเมิดความเป็นส่วนตัว เช่น ฟังก์ชั่น auto-tagging ของ Facebook เป็นต้น ซึ่ง Facebook ถูกฟ้องคดีในรัฐอิลลินอยส์ สหรัฐอเมริกาและอาจต้องจ่ายค่าเสียหายให้กับเจ้าของข้อมูลส่วนบุคคลถึง 650 ล้านเหรียญสหรัฐ

การใช้ข้อมูลชีวภาพประเภทหนึ่งเพื่อปิดจุดอ่อนของข้อมูลชีวภาพอีกประเภทหนึ่งเป็นสิ่งที่ไม่สมควรทำ เนื่องจากการเพิ่มประเภทของข้อมูลชีวภาพยิ่งจะทำให้ความเสี่ยงที่จะละเมิดความเป็นส่วนตัวเพิ่มมากขึ้นเป็นทวีคูณ นอกจากนี้การลบข้อมูลชีวภาพที่อยู่บนอินเตอร์เน็ตนั้นไม่สามารถแก้ปัญหาการละเมิดความเป็นส่วนตัวได้ เนื่องจากข้อมูลที่อยู่บนอินเตอร์เน็ตอาจมีการส่งต่อกันไปเรื่อย ๆ ทำให้มีข้อมูลอยู่หลายแหล่ง และการตามไปลบข้อมูลออกจากทุกแหล่งนั้นเป็นสิ่งที่แทบจะเป็นไปไม่ได้เลย[55]

4.4.2 ความเสี่ยงต่อการถูกขโมยข้อมูล และการรั่วไหลของข้อมูล

การเก็บรวบรวมข้อมูลส่วนบุคคลชีวภาพ และการติดตามขององค์กรเอกชนต่าง ๆ อาจทำให้เกิดความเสี่ยงต่อเจ้าของข้อมูลส่วนบุคคล (ดูรายละเอียดใน บทที่ 2 หัวข้อ 4.3 ความเสี่ยงต่อการโจมตีจากภายนอก) เมื่อองค์กรเอกชนเก็บข้อมูลส่วนบุคคลยิ่งมากเท่าไหร่ความเสี่ยงต่อการถูกโจมตีจากภายนอกก็ยิ่งมากขึ้นเท่านั้น ในปี ค.ศ. 2016 ได้มีการโจมตีฐานข้อมูลผู้มีสิทธิเลือกตั้งของประเทศฟิลิปปินส์ 55 ล้านคน[56] โดยข้อมูลที่ถูกขโมยไปมี อีเมล 228,605 รายการ หมายเลขหนังสือเดินทางและวันหมดอายุของหนังสือเดินทาง 1.3 ล้านเลขหมายของผู้มีสิทธิเลือกตั้งชาวฟิลิปปินส์ในต่างประเทศ รวมถึงลายนิ้วมืออีก 15.8 ล้านลายนิ้วมือ[57] ซึ่งข้อมูลเหล่านี้ได้ถูก

---

[53] Alcohol's Effects on Eye Health. สืบค้นจาก https://guardionhealth.com/alcohols-effect-eye-health/

[54] Hall, J. A., & Kimura, D. (1994). Dermatoglyphic Asymmetry and Sexual Orientation in Men. *Behavioral Neuroscience, 108*(6), 1203-1206.

[55] Pfitzmann, A. (2008). Biometrics - How to Put to Use and How Not at All? ใน S. Furnell, S. K. Katsikas, & A. Lioy (Eds.), *Trust, Privacy and Security in Digital Business, LNCS* (Vol. 5185, pp. 3-5). Springer-Verlag Berlin Heidelberg: TrustBus 2008.

[56] Mayhew, S. (2016). Fingerprint and Passport Data Leaked in Philippines Voter Database Breach. สืบค้นจาก BiometricUpdate.com website: https://www.biometricupdate.com/201604/fingerprint-and-passport-data-leaked-in-philippines-voter-database-breach

[57] Temperton, J. (2016). The Philippines Election Hack is 'Freaking Huge'. *Wired.* สืบค้นจาก https://www.wired.co.uk/article/philippines-data-breach-fingerprint-data

แพร่กระจายออกไปอย่างกว้างขวางทั้งในเว็บมืดและเว็บทั่วไป[58] ข้อมูลที่ถูกขโมยไปอาจถูกนำไปขายหรือถูกนำไปใช้ในการโจรกรรมเอกลักษณ์ส่วนบุคคล (identity theft) ได้ ซึ่งอาจทำความเสียหายอย่างมหาศาลและไม่สามารถแก้ไขได้ การโจมตีฐานข้อมูลสำนักงานฝ่ายบริหารงานบุคคลของสหรัฐอเมริกา (U.S. Office of Personnel Management) ของรัฐบาลสหรัฐอเมริกาในปี ค.ศ. 2014 ข้อมูลของบุคลากร 22.1 ล้านคนถูกขโมย[59] ซึ่งรวมถึงลายนิ้วมือจำนวน 5.6 ล้านและหมายเลขประกันสังคมของบุคคลจำนวน 21.5 ล้านคน โดยทางรัฐบาลได้จัดตั้งกลุ่มหน่วยงานเพื่อตรวจสอบความเป็นไปได้ที่ข้อมูลที่ถูกขโมยจะถูกนำมากระทำการฉ้อโกงในการชำระเงิน หรือนำไปสร้างตัวตนปลอม แม้ว่าผู้เชี่ยวชาญของรัฐบาลกลางระบุว่าการนำข้อมูลลายนิ้วมือไปใช้ในทางที่ผิดนั้นอาจทำได้ยาก แต่ความน่าจะเป็นของการนำข้อมูลชีวภาพที่ถูกขโมยไปใช้ในทางที่ผิดนั้นนับวันจะเพิ่มขึ้นอย่างไม่ต้องสงสัย[60] อย่างไรก็ตามเป็นที่ทราบกันดีว่าการปลอมแปลงลายนิ้วมือนั้นทำได้ไม่ยากและสามารถค้นหาวิธีทำได้จากยูทูป (YouTube) โดยใช้เวลาไม่นาน

ในขณะที่เมื่อ 6 ปีก่อน ในปี ค.ศ. 2014 ภาพถ่ายลายนิ้วมือของอดีตรัฐมนตรีว่าการกระทรวงกลาโหมเยอรมัน Ursula von der Leyen เมื่อครั้งยังดำรงตำแหน่งรัฐมนตรีว่าการกระทรวงกลาโหมยังสามารถนำไปสร้างลายนิ้วมือเพื่อใช้ในการปลดล็อคไอโฟนได้[61] บ่งบอกถึงความสามารถอันไม่มีขีดจำกัดของเทคโนโลยี และด้วยเทคโนโลยีนำสมัยอย่าง deepfake ที่มิใช่เทคโนโลยีใหม่และในปัจจุบันคนทั่วไปก็สามารถสร้าง deepfake ได้อย่างง่ายดายไม่ยุ่งยากเหมือนในอดีต ทำให้ deepfake เป็นเทคโนโลยีที่มีความน่ากลัวเนื่องจากการนำไปใช้อาจก่อให้เกิดอันตรายต่อการใช้ข้อมูลชีวมาตร ไปจนถึงสังคมโดยส่วนรวมได้ การเลียนแบบเสียง (voice pattern)

---

[58] เว็บไซต์นั้นมีด้วยกัน 3 ระดับ คือ 1) Surface Web หรือเว็บไซต์ทั่วไปที่เราใช้งานกัน ซึ่งสามารถถูกค้นหาได้จากเครื่องมือค้นหา (Search Engine) ทั่วไป เช่น Google หรือ Yahoo เป็นต้น 2) Deep Web หรือเว็บส่วนลึกซึ่งเป็นเว็บไซต์ที่ไม่สามารถถูกค้นหาได้จากเครื่องมือค้นหาทั่วไป โดยเว็บส่วนลึกจะมีการเปลี่ยนแปลงข้อมูลอย่างรวดเร็วอยู่ตลอดเวลา การเข้าถึงจำเป็นต้องรู้ที่อยู่ของเว็บไซต์เท่านั้นถึงจะเข้าสู่เว็บไซต์นั้นได้ เว็บส่วนลึกส่วนใหญ่ใช้เก็บความลับ เก็บข้อมูลส่วนตัว หรือเป็นคลังเก็บเอกสารสำคัญของหน่วยงานต่าง ๆ เป็นต้น 3) Dark Web หรือเว็บมืด ต้องใช้เครื่องมือพิเศษในการเข้าถึง และใช้เป็นพื้นที่ที่เอาไว้ดำเนินกิจกรรมต่าง ๆ ที่ผิดกฎหมาย เช่น การซื้อขายข้อมูลบัญชีธนาคาร บัตรเครดิต ซื้อขายอาวุธ เป็นต้น

[59] Fruhlinger, J. (2020). The OPM hack explained: Bad security practices meet China's Captain America. *CSO ASEAN*. สืบค้นจาก https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

[60] Bergsman, J. (2016). Biometrics are less secure than passwords -- this is why. *Betanews*. สืบค้นจาก https://betanews.com/2016/08/24/unsafe-biometrics/

[61] Scharr, J. (2014). iPhone Hack Fools Touch ID with Hand Photos. *Tom's Guide*. สืบค้นจาก https://www.tomsguide.com/us/iphone-touch-id-hack,news-20066.html

การทำรูปปลอม หรือการทำคลิปอนาจาร ไม่ใช่เรื่องยากสำหรับ deepfake เลย[62] และเมื่อรูปปลอมหรือคลิปอนาจารได้ถูกเผยแพร่ออกไปแล้วนั้นทำให้เกิดความเสียหายแก่บุคคลได้ทันทีและเป็นระยะเวลายาวนาน ไม่อาจลบล้างได้ง่าย ๆ เนื่องจากเราไม่สามารถลบข้อมูลทั้งหมดที่ได้ถูกเผยแพร่ออกไปในอินเตอร์เน็ตได้

ในปี ค.ศ. 2010 เอริก เอเมอร์สัน ชมิดต์ ซึ่งในขณะนั้นดำรงตำแหน่งประธานบริหารของบริษัทกูเกิล ได้กล่าวในงานสัมมนา Techonomy ว่า “เอารูปถ่ายของคุณให้เราดู 14 รูป แล้วเราจะสามารถบอกได้ว่าคุณคือใคร คุณคิดว่าในอินเตอร์เน็ตไม่มีรูปถ่ายของตัวคุณเอง 14 รูปหรือไง ก็รูปถ่ายของคุณใน Facebook ไง”[63] การค้นหารูปถ่ายของบุคคลใดบุคคลหนึ่งสามารถทำได้โดยไม่ยากหากบุคคลเหล่านั้นมีบัญชีผู้ใช้ในโซเชียลเน็ตเวิร์ก เห็นได้ชัดว่ารูปถ่ายเหล่านี้สามารถนำมาใช้ในการระบุตัวตนของบุคคลได้ไม่ยาก

---

[62] Allan, K. (2020). Why deepfakes could threaten everything from biometrics to democracy. สืบค้นจาก ITPro website: https://www.itpro.co.uk/security/357591/why-deepfakes-could-threaten-everything-from-biometrics-to-democracy

[63] Nixon, J. (2010). No anonymity on future web says Google CEO. *Thinq.co.uk*. สืบค้นจาก Thinq.co.uk website: http://www.thinq.co.uk/2010/8/5/no-anonymity-future-web-says-google-ceo/

บทที่ 3
หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลประเภทชีวภาพตามกฎหมายต่างประเทศ

1. หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลประเภทชีวภาพตามกฎหมาย General Data Protection Regulation (GDPR) ของสหภาพยุโรป

กฎข้อบังคับการคุ้มครองข้อมูลส่วนบุคคล หรือ General Data Protection Regulation (GDPR) เป็นกฎหมายกลางที่บังคับใช้กับทุกประเทศสมาชิกของสหภาพยุโรป (European Union - EU) โดยได้มีการลงมติรับเมื่อวันที่ 14 เมษายน พ.ศ. 2559 และเผยแพร่ในวารสารทางการของสหภาพยุโรปเมื่อวันที่ 27 เมษายน พ.ศ. 2559 โดยให้มีผลบังคับใช้ในวันที่ 25 พฤษภาคม พ.ศ. 2561

ก่อนที่จะมีการบัญญัติ GDPR เป็นกฎหมายกลางนั้น สหภาพยุโรปมีการใช้กฎระเบียบการคุ้มครองข้อมูลส่วนบุคคล (The EU Data Protection Directive 95/46/EC) ซึ่งเป็นกรอบการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในรูปแบบของกฎระเบียบ (Directive) ที่แต่ละประเทศสมาชิกต้องบัญญัติกฎหมายภายในให้เป็นไปตามกฎระเบียบดังกล่าว แต่ GDPR หรือ Regulation (EU) 2016/679 เป็นกฎข้อบังคับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป โดยถือเป็นกฎข้อบังคับ (Regulation) ซึ่งมีผลบังคับใช้เป็นกฎหมายกลางทั่วทั้งสหภาพยุโรป

กฎระเบียบการคุ้มครองข้อมูลส่วนบุคคล EU Data Protection Directive 95/46/EC มีการบังคับใช้มาตั้งแต่ปี พ.ศ. 2538 ซึ่งเป็นระยะเริ่มแรกของการนำอินเตอร์เน็ตมาใช้ และเนื่องจากการพัฒนาอย่างก้าวกระโดดของเทคโนโลยี สหภาพยุโรปจึงเห็นถึงความจำเป็นในการปรับปรุงกฎระเบียบเพื่อให้ทันต่อความก้าวหน้าทางด้านเทคโนโลยี นอกจากนั้นแล้วการไหลเวียนของข้อมูลจำนวนมหาศาล ไม่ว่าจะเป็นระหว่างประเทศสมาชิกของสหภาพยุโรปด้วยกันเองและระหว่างประเทศสมาชิกของสหภาพยุโรปกับประเทศนอกสหภาพยุโรป ทำให้สหภาพยุโรปมองเห็นถึงความจำเป็นที่จะต้องมีกฎหมายสำหรับการคุ้มครองข้อมูลส่วนบุคคลที่เป็นมาตรฐานเดียวกัน เพื่อให้ประเทศสมาชิกของสหภาพยุโรปมีความพร้อมในการรองรับการคุ้มครองข้อมูลส่วนบุคคลในยุคสมัยดิจิทัล จึงได้มีการบัญญัติกฎข้อบังคับการคุ้มครองข้อมูลส่วนบุคคล (GDPR) ขึ้นมาใช้แทนที่กฎระเบียบการคุ้มครองข้อมูลส่วนบุคคล EU Data Protection Directive 95/46/EC

1.1 ขอบเขตการบังคับใช้

มาตรา 2 ของ GDPR กำหนดให้ใช้ GDPR กับการประมวลผลข้อมูลส่วนบุคคลไม่ว่าจะเป็นทั้งหมด หรือบางส่วน ไม่ว่าจะเป็นโดยวิธีการอัตโนมัติ หรือวิธีการอื่นใด ซึ่งเป็นส่วนหนึ่งของระบบการจัดเก็บข้อมูล หรือเป็นส่วนหนึ่งของระบบการจัดเก็บข้อมูล ทั้งนี้ไม่รวมถึงการประมวลผลข้อมูลส่วนบุคคล ดังต่อไปนี้[64]

---

[64] GDPR, Article 2.

1) ในกิจการซึ่งอยู่นอกขอบเขตการบังคับของกฎหมายสหภาพยุโรป

2) โดยประเทศสมาชิกในการดำเนินกิจการที่อยู่ภายใต้ขอบเขตของ หมวดที่ 2 หัวข้อ 5 ของสนธิสัญญาสหภาพยุโรป (TEU)

3) โดยบุคคลธรรมดาในกิจการส่วนบุคคล หรือกิจการในครัวเรือน

4) โดยพนักงานเจ้าหน้าที่ที่มีความสามารถเพื่อวัตถุประสงค์ในการป้องกัน การสืบสวนสอบสวน การดำเนินคดีหรือการลงโทษทางอาญา รวมถึงมาตรการการรักษาความปลอดภัยและป้องกันการคุกคามต่อความมั่นคงของประชาชนทั่วไป

นอกจากนี้ใน มาตรา 3 ของ GDPR กำหนดให้ใช้บังคับกับ การประมวลผลข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งมีสถานประกอบการที่ตั้งอยู่ในสหภาพยุโรป ไม่ว่าการประมวลผลนั้นจะกระทำอยู่ในสหภาพยุโรปหรือไม่ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลไม่มีสถานประกอบการอยู่ในสหภาพยุโรป กฎข้อบังคับนี้จะใช้บังคับกับการประมวลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลที่อยู่ในสหภาพยุโรปเมื่อการประมวลผลข้อมูลส่วนบุคคลนั้นเป็นการนำเสนอสินค้าหรือบริการแก่เจ้าของข้อมูลส่วนบุคคลโดยมิต้องคำนึงถึงว่ามีการชำระเงินโดยเจ้าของข้อมูลส่วนบุคคลหรือไม่ หรือเป็นการติดตามตรวจสอบพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในสหภาพยุโรป นอกจากนี้ GDPR ยังใช้บังคับการประมวลผลข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมิได้มีสถานประกอบการอยู่ในสหภาพยุโรป แต่อยู่ในประเทศที่กฎหมายของประเทศสมาชิกให้ใช้บังคับโดยอาศัยอำนาจตามกฎหมายระหว่างประเทศแผนกคดีเมือง[65]

1.2 ความหมายของข้อมูลส่วนบุคคล และข้อมูลส่วนบุคคลประเภทชีวภาพ

1.2.1 ความหมายของข้อมูลส่วนบุคคล

มาตรา 4 (1) ของ GDPR ได้ให้คำจำกัดความของ “ข้อมูลส่วนบุคคล” ว่าเป็นข้อมูลที่เกี่ยวข้องกับบุคคลธรรมดาซึ่งใช้ระบุตัวตน (Identified) หรืออาจระบุตัวตน (Identifiable) บุคคลนั้นได้ ไม่ว่าโดยทางตรงหรือทางอ้อม ซึ่งนอกเหนือจาก ชื่อ นามสกุล หมายเลขบัตรประจำตัวประชาชนแล้ว ยังรวมไปถึง ข้อมูลตำแหน่งที่ตั้ง (Location Data) สิ่งระบุตัวบุคคลออนไลน์ (Online Identifier) และข้อมูลสรีรวิทยา พันธุกรรม จิตใจ เศรษฐกิจ วัฒนธรรม หรือ สังคมของบุคคลนั้นอีกด้วย[66]

ดังนั้น ข้อมูลส่วนบุคคลตามคำจำกัดความของ GDPR จึงมิได้จำกัดอยู่เพียงแค่ ชื่อ นามสกุล ที่อยู่ หมายเลขโทรศัพท์ เท่านั้น แต่รวมถึงข้อมูลใด ๆ ที่สามารถใช้ระบุตัวตนของเจ้าของข้อมูลด้วยวิธีการที่เหมาะสม (all means reasonable)[67] ไม่ว่าจะเป็นโดยทางตรงหรือทางอ้อม ข้อมูลเหล่านั้นย่อมถือว่าเป็นข้อมูลส่วนบุคคลตามความจำกัดความของ GDPR

ส่วนข้อมูลตำแหน่งที่ตั้ง หรือ Location Data คือตำแหน่งที่ตั้งทางภูมิศาสตร์ที่เจ้าของข้อมูลส่วนบุคคลนั้นได้เดินทางไป ซึ่งข้อมูลตำแหน่งที่ตั้งนี้สามารถได้มาจากหลายทาง เช่น

---

[65] GDPR, Article 3.

[66] GDPR, Article 4 (1).

[67] GDPR, Recital 26.

ระบบระบุตำแหน่งบนพื้นโลก (Global Positioning System - GPS) สัญญาณ Wi-Fi หรือ สัญญาณโทรศัพท์มือถือ เป็นต้น ดังนั้นอุปกรณ์ที่เราใช้ในชีวิตประจำวันแทบจะทุกชนิด ไม่ว่าจะเป็นอุปกรณ์มือถือ สมาร์ทโฟน หรือนาฬิกาอัจฉริยะ (Smart Watch) ล้วนแต่สามารถใช้ระบุตำแหน่งที่ตั้งของบุคคลที่ใช้อุปกรณ์นั้น ๆ ได้ และในยุคดิจิทัลนี้องค์กรธุรกิจต่าง ๆ สามารถนำข้อมูลตำแหน่งที่ตั้งไปใช้ประโยชน์ทางด้านการตลาดและเพิ่มยอดขายได้ โดยอาจจะเสนอโปรโมชั่นหรือบริการพิเศษ หรือวิเคราะห์พฤติกรรมของบุคคล เป็นต้น

สำหรับ “สิ่งระบุตัวบุคคลออนไลน์ (Online Identifier)” นั้น Recital 30 ของ GDPR ได้ยกตัวอย่างไว้ดังนี้ หมายเลขประจำเครื่องคอมพิวเตอร์ในระบบเครือข่าย (Internet Protocol Addresses หรือ IP Address) ชิ้นส่วนของข้อมูลที่ได้ถูกจัดเก็บไว้ในคอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่ (Cookies) และ ป้ายที่อ่านข้อมูลโดยใช้คลื่นความถี่วิทยุ (Radio Frequency Identification Tags หรือ RFID)[68] นอกจากนี้สิ่งที่สามารถถือว่าเป็นสิ่งระบุตัวบุคคลออนไลน์ได้นั้นยังรวมถึง ชุดตัวเลขที่ทางผู้ผลิตระบุไว้ให้กับการ์ดเครือข่ายในคอมพิวเตอร์ (MAC Address) และชื่อที่บุคคลใช้แทนตัวเองในโซเชียลมิเดีย เช่น ชื่อไอจี (Instagram Name) และ ชื่อเฟซบุ๊ก (Facebook Name) เป็นต้น

1.2.2 ความหมายของข้อมูลส่วนบุคคลประเภทชีวภาพ

สำหรับข้อมูลชีวภาพนั้น GDPR มาตรา 4 (14) ได้ให้คำจำกัดความของ “ข้อมูลชีวภาพ” ว่าหมายถึง ข้อมูลส่วนบุคคลที่เกิดจากการประมวลผลโดยใช้เทคนิคพิเศษที่เกี่ยวกับลักษณะทางกายภาพ ทางสรีรวิทยาหรือพฤติกรรมของบุคคลซึ่งสามารถนำไปใช้เพื่อระบุตัวตน หรือใช้เพื่อยืนยันตัวตนของบุคคล เช่น ภาพใบหน้า หรือข้อมูลลายนิ้วมือ[69]

คำจำกัดความของข้อมูลชีวภาพ สามารถแบ่งได้ออกเป็น 4 ส่วน ดังต่อไปนี้

1) เป็นข้อมูลส่วนบุคคล (personal data)

2) เกิดจากการประมวลผลโดยใช้เทคนิคพิเศษ (resulting from specific technical processing)

3) เกี่ยวกับลักษณะทางกายภาพ ทางสรีรวิทยาหรือพฤติกรรมของบุคคล (relating to the physical, physiological or behavioural characteristics of a natural person)

4) สามารถนำไปใช้เพื่อระบุตัวตน หรือเพื่อยืนยันตัวตนของบุคคลธรรมดา (allow or confirm the unique identification of that natural person)

จากการวิเคราะห์คำจำกัดความของข้อมูลชีวภาพภายใต้ GDPR ดังกล่าว สามารถสรุปได้ว่า ข้อมูลชีวภาพถือว่าเป็นข้อมูลส่วนบุคคลเนื่องจากสามารถนำไปใช้ระบุตัวบุคคลได้ แต่จะถือว่าเป็นข้อมูลส่วนบุคคลประเภทชีวภาพเมื่อมีองค์ประกอบครบทั้ง 4 ข้อที่กล่าวมาข้างต้น คือ เมื่อข้อมูลนั้นเป็นข้อมูลส่วนบุคคลเกี่ยวกับลักษณะทางกายภาพ ทางสรีรวิทยาหรือพฤติกรรมของบุคคลที่เกิดจาก “การประมวลผลด้วยเทคนิคพิเศษ” และ “สามารถนำไปใช้เพื่อระบุตัวตน หรือเพื่อ

---

[68] GDPR, Recital 30 and Article 4(14).

[69] GDPR, Article 4(14).

ยืนยันตัวตน” ดังนั้นหากข้อมูลส่วนบุคคลใด ๆ เกี่ยวกับลักษณะทางกายภาพ ทางสรีรวิทยาหรือพฤติกรรมของบุคคลนั้นไม่ได้เกิดจากการประมวลผลทางเทคนิคพิเศษ และไม่สามารถนำไปใช้เพื่อการระบุตัวตน หรือไม่ได้ใช้เพื่อการยืนยันตัวตนของบุคคลแล้ว ข้อมูลส่วนบุคคลนั้นจะไม่ถือว่าเป็นข้อมูลชีวภาพตามคำจำกัดความของ GDPR ข้อมูลส่วนบุคคลที่เกี่ยวกับลักษณะทางกายภาพ ทางสรีรวิทยาหรือพฤติกรรมของบุคคลดังกล่าวถือเป็นเพียงข้อมูลส่วนบุคคลธรรมดา ดังนั้น ภาพถ่ายของบุคคล หรือรูปถ่ายลายนิ้วมือ ที่มิได้เกิดจากการประมวลผลทางเทคนิคพิเศษ และมิได้นำไปยืนยันการระบุเอกลักษณ์ของบุคคล หรือไม่สามารถนำไปยืนยันตัวตนได้ จึงเป็นข้อมูลส่วนบุคคล แต่มิได้เป็นข้อมูลส่วนบุคคลประเภทชีวภาพ

การประมวลผลข้อมูลส่วนบุคคลที่เป็นภาพถ่ายโดยทั่วไปอาจไม่ถือว่าเป็นการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว หากมิได้มีการประมวลผลด้วยเทคนิคพิเศษเพื่อทำการระบุเอกลักษณ์ของบุคคล หรือยืนยันเอกลักษณ์ของบุคคล โดยการประมวลผลข้อมูลส่วนบุคคลประเภทชีวภาพกระทำได้ต่อเมื่อกฎหมายสหภาพยุโรปหรือกฎหมายประเทศสมาชิกอนุญาตให้ทำได้เป็นการเฉพาะเจาะจง[70]

1.3 หลักการคุ้มครองข้อมูลส่วนบุคคล

ใน มาตรา 5 ของ GDPR ได้มีการกำหนดหลักการในการประมวลผลข้อมูลส่วนบุคคลไว้ดังนี้[71]

1.3.1 หลักความชอบด้วยกฎหมาย เป็นธรรม และโปร่งใส (Lawfully, fairly and in a transparent manner) [72]

การประมวลผลข้อมูลส่วนบุคคลนั้นจะต้องกระทำโดยชอบด้วยกฎหมาย มีความเป็นธรรมและมีความโปร่งใสต่อเจ้าของข้อมูลส่วนบุคคล สำหรับหลักการประมวลผลข้อมูลส่วนบุคคลโดยชอบด้วยกฎหมายนั้น GDPR ได้มีการบัญญัติไว้ใน มาตรา 6 ซึ่งใช้กับข้อมูลส่วนบุคคลธรรมดา สำหรับหลักการประมวลผลโดยชอบด้วยกฎหมายของข้อมูลส่วนบุคคลที่มีความอ่อนไหวได้ถูกบัญญัติไว้ใน มาตรา 9 นอกเหนือจากหลักการที่ได้ระบุไว้ใน GDPR แล้ว การกระทำใด ๆ ที่ถือว่าเป็นการกระทำอันมิชอบด้วยกฎหมายภายใต้กฎหมายอื่นที่เกี่ยวข้องย่อมถือว่าเป็นการกระทำที่มิชอบด้วยกฎหมายเช่นกัน นอกจากนี้การประมวลผลอาจเป็นการประมวลผลที่มิชอบด้วยกฎหมายหากมีการละเมิดลิขสิทธิ์ หรือผิดข้อตกลงตามสัญญา หรือผิดกฎระเบียบข้อบังคับต่าง ๆ ของภาคอุตสาหกรรม

หลักความเป็นธรรม หมายถึง การได้มาซึ่งข้อมูลส่วนบุคคลและการประมวลผลข้อมูลส่วนบุคคลนั้นจะต้องมองถึงผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูลเป็นสำคัญ การเก็บข้อมูลส่วนบุคคลต้องกระทำด้วยความเป็นธรรม โดยมิได้มีการหลอกลวงเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคล นอกจากนี้การประมวลผลข้อมูลส่วนบุคคลควรกระทำด้วยความเป็นธรรมต่อเจ้าของข้อมูลและเป็นไปตามความคาดหมายของเจ้าของข้อมูล คือ ไม่นำข้อมูลส่วนบุคคลนั้นไปทำในสิ่งที่

---

[70] GDPR, Recital 51.

[71] GDPR, Article 5(1).

[72] GDPR, Article 5(1)(a).

นอกเหนือจากความคาดหมายของเจ้าของข้อมูล ทั้งนี้องค์กรที่ทำการประมวลข้อมูลส่วนบุคคลจะต้องมีความชัดเจน และซื่อสัตย์กับเจ้าของข้อมูล โดยแจ้งให้เจ้าของข้อมูลทราบถึงเหตุผลของการเก็บ และประมวลผลข้อมูลส่วนบุคคล

หลักความโปร่งใสนั้นมีความเกี่ยวเนื่องกับหลักความเป็นธรรม หมายถึง ผู้ทำการประมวลผลข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลทราบก่อนการเก็บรวบรวมข้อมูลส่วนบุคคล ทั้งนี้เป็นไปตามสิทธิของเจ้าของข้อมูลที่จะได้รับการแจ้งให้ทราบ นอกจากนี้ผู้ที่เก็บรวบรวมข้อมูลจะต้องทำให้ข้อความที่ใช้สื่อสารกับเจ้าของข้อมูลนั้นเข้าถึงได้ง่าย รวมทั้งใช้ถ้อยคำที่สามารถเข้าใจได้ง่ายอีกด้วย โดยต้องมีการระบุชื่อองค์กรที่เป็นผู้ประมวลผลข้อมูลส่วนบุคคล รวมถึงวัตถุประสงค์ของการเก็บข้อมูลส่วนบุคคลไว้อย่างชัดเจน[73]

ภายใต้หลักความชอบด้วยกฎหมาย เป็นธรรม และโปร่งใสนี้ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการให้ครบถ้วนตามหลักการที่ได้กล่าวมาทั้งสามข้อ จะขาดข้อใดข้อหนึ่งเสียมิได้

1.3.2 หลักจำกัดตามวัตถุประสงค์ (purpose limitation)[74]

การจำกัดตามวัตถุประสงค์ หมายถึง การประมวลผลข้อมูลส่วนบุคคลนั้นได้กระทำภายใต้วัตถุประสงค์ที่ผู้เก็บรวบรวมได้ระบุไว้โดยชัดแจ้งและชอบด้วยกฎหมาย[75] โดยไม่สามารถนำไปใช้สำหรับวัตถุประสงค์อื่นใดที่ขัดกับวัตถุประสงค์ที่ได้ระบุไว้ เว้นแต่การประมวลผลข้อมูลส่วนบุคคลเพื่อประโยชน์สาธารณะ หรือการวิจัยทางวิทยาศาสตร์หรือประวัติศาสตร์ หรือวัตถุประสงค์ทางสถิติ ไม่ถือว่าเป็นการขัดต่อวัตถุประสงค์ที่ได้ระบุไว้

การประเมินว่าวัตถุประสงค์นั้นขัดกับวัตถุประสงค์ที่ได้ระบุไว้หรือไม่จะต้องประเมินถึงความเกี่ยวเนื่องกับวัตถุประสงค์ที่ได้ระบุไว้ อีกทั้งยังต้องเป็นไปตามความคาดหมายของเจ้าของข้อมูล การดำเนินการจะต้องไม่เกิดผลกระทบต่อเจ้าของข้อมูล และต้องมีมาตรการในการคุ้มครองความปลอดภัยของข้อมูล

1.3.3 หลักการจัดเก็บข้อมูลเท่าที่จำเป็น (Data Minimization)[76]

ภายใต้หลักการเก็บข้อมูลเท่าที่จำเป็นนี้ การประมวลผลข้อมูลส่วนบุคคลจะต้องกระทำโดยใช้เฉพาะข้อมูลที่จำเป็น และเกี่ยวข้องกับวัตถุประสงค์ที่ทำการประมวลผลเท่านั้น โดยจะต้องไม่มีการใช้ข้อมูลส่วนบุคคลเกินความจำเป็นสำหรับวัตถุประสงค์นั้น โดยผู้ประมวลผล หรือผู้ควบคุมข้อมูลต้องทำการประเมินความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล และเลือกเพียงเท่าที่จำเป็น นอกจากนี้ข้อมูลส่วนบุคคลจะต้องถูกจัดเก็บไว้ในระยะเวลาเท่าที่จำเป็น และต้องมีการกำหนดระยะเวลาในการเก็บข้อมูล โดยเก็บไว้ในระยะเวลาเท่าที่จำเป็นที่สั้นที่สุด และมีการกำหนดระยะเวลาในการลบข้อมูลหรือตรวจสอบข้อมูล[77]

---

[73] GDPR, Recital 39.

[74] GDPR, Article 5(1)(b).

[75] GDPR, Recital 39.

[76] GDPR, Article 5(1)(c).

[77] GDPR, Recital 39.

1.3.4 หลักความถูกต้องของข้อมูล (Accuracy)[78]

ข้อมูลส่วนบุคคลที่เก็บรวบรวม ใช้ และเปิดเผยจะต้องมีความถูกต้องและในกรณีที่จำเป็นข้อมูลนั้นต้องเป็นปัจจุบัน สำหรับข้อมูลส่วนบุคคลที่ไม่ถูกต้องจำเป็นต้องได้รับการแก้ไขให้ถูกต้องหรือลบทิ้งในทันที ทั้งนี้ความถูกต้องหรือเป็นปัจจุบันของข้อมูลขึ้นอยู่กับวัตถุประสงค์ของการเก็บข้อมูล การเก็บข้อมูลที่ไม่ถูกต้อง หรือไม่เป็นปัจจุบันอาจเป็นไปได้หากการเก็บข้อมูลนั้นไม่มีผลกับข้อเท็จจริงโดยรวม เช่น การเก็บข้อมูลเพื่อวัตถุประสงค์ทางสถิติหรือการวิจัยทางประวัติศาสตร์ไม่จำเป็นต้องใช้ข้อมูลที่เป็นปัจจุบัน

1.3.5 หลักข้อจำกัดในการจัดเก็บ (Storage Limitation)[79]

ข้อมูลส่วนบุคคลจะถูกเก็บอยู่ในรูปแบบที่สามารถระบุตัวตนของเจ้าของข้อมูลได้ไม่นานเกินกว่าความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวม ข้อยกเว้นที่ทำให้การเก็บข้อมูลเป็นเวลานานสามารถทำได้เมื่อเป็นการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยเพื่อประโยชน์สาธารณะ หรือการวิจัยทางวิทยาศาสตร์ หรือประวัติศาสตร์ หรือวัตถุประสงค์ทางสถิติ อย่างไรก็ดี การเก็บข้อมูลส่วนบุคคลภายใต้ข้อยกเว้นเหล่านี้จะต้องมีมาตรการในการปกป้องสิทธิและเสรีภาพของเจ้าของข้อมูลตามความเหมาะสมอีกด้วย

แม้ใน GDPR มิได้มีการกำหนดระยะเวลาของการเก็บข้อมูลส่วนบุคคลไว้ หากแต่ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลต้องทำการกำหนดระยะเวลาให้สอดคล้องกับวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล โดยกำหนดเป็นนโยบายในการเก็บรักษาและลบข้อมูลส่วนบุคคล อนึ่ง การลบข้อมูลที่ไม่จำเป็นนั้นยังสอดคล้องกับหลักการลดปริมาณข้อมูล และหลักความถูกต้องของข้อมูลอีกด้วย นอกจากนี้ยังเป็นการลดภาระที่อาจเกิดขึ้นจากการที่เจ้าของข้อมูลติดต่อสอบถามเกี่ยวกับระยะเวลาการเก็บข้อมูลและ/หรือขอให้ลบข้อมูลอีกด้วย

1.3.6 หลักความสมบูรณ์ของข้อมูล และหลักการรักษาความลับ (Integrity and Confidentiality)[80]

การเก็บรวมรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลนั้นจะต้องมีมาตรการทางเทคนิคหรือมาตรการขององค์กรในด้านความปลอดภัยที่เหมาะสม เพื่อคุ้มครองความสมบูรณ์ของข้อมูลและรักษาข้อมูลนั้นให้เป็นความลับ โดยจะต้องมีการป้องกันการเข้าถึงข้อมูลโดยมิได้รับอนุญาตหรือโดยไม่ชอบด้วยกฎหมาย รวมทั้งต้องมีการป้องกันการทำลายข้อมูล หรือทำให้ข้อมูลเสียหาย โดยเทคนิคการคุ้มครองข้อมูลนั้นอาจรวมถึงการเข้ารหัสข้อมูล (encryption) หรือการใช้การยืนยันตัวตน (authentication) หรือการกำหนดระดับการอนุญาตให้เข้าถึงข้อมูล (authorization)

ทั้งนี้ GDPR มีข้อกำหนดในการรักษาความปลอดภัยของการประมวลผลข้อมูลส่วนบุคคล ตาม มาตรา 32 (1) โดยกำหนดให้ผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูลส่วนบุคคลมีมาตรการทางเทคนิคและมาตรการทางองค์กรที่เหมาะสมโดยคำนึงถึงความทันสมัยของเทคโนโลยี ค่าใช้จ่ายในการนำมาใช้ ลักษณะ ขอบเขต และบริบท รวมทั้งวัตถุประสงค์ในการ

---

[78] GDPR, Article 5(1)(d).

[79] GDPR, Article 5(1)(e).

[80] GDPR, Article 5(1)(f).

ประมวลผล รวมทั้งความเสี่ยงที่อาจเกิดกับสิทธิและเสรีภาพของเจ้าของข้อมูลทั้งหมด ไม่ว่าจะมีระดับความเป็นไปได้มากหรือน้อยเพียงใด และระดับความรุนแรงของผลกระทบจะมากหรือน้อยเพียงใด[81] โดยรวมถึงมาตรการดังต่อไปนี้

1) การเปลี่ยนข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถระบุตัวตนได้ และการเข้ารหัสข้อมูลส่วนบุคคล (Pseudonymization and Encryption)

2) มีความสามารถที่ทำให้มั่นใจว่ามีการเก็บรักษาความลับอย่างต่อเนื่อง ด้วยความซื่อสัตย์ ความพร้อม และความยืดหยุ่นของระบบการประมวลผลและการบริการที่เกี่ยวข้อง

3) มีความสามารถที่จะกู้คืนและเข้าถึงข้อมูลส่วนบุคคลทันทีที่มีอุบัติการณ์ (incident) เกิดขึ้นไม่ว่าจะเป็นทางกายภาพหรือทางเทคนิค

4) มีกระบวนการในการทดสอบ วิเคราะห์ และประเมินประสิทธิภาพของมาตรการทั้งทางด้านเทคนิคและทางด้านองค์กรอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าการประมวลผลเป็นไปอย่างปลอดภัย

1.3.7 หลักความรับผิดชอบ (Accountability)[82]

ทั้งนี้ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องมีความรับผิดชอบในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล และสามารถแสดงให้เห็นว่ามีการดำเนินการตามหลักการที่กล่าวมาข้างต้นทั้ง 6 ข้อ ภายใต้ มาตรา 5 (1) โดยต้องมีการกำหนดมาตรการที่เหมาะสม และจัดเก็บหลักฐานว่าได้มีการปฏิบัติตามหลักการเหล่านี้แล้ว

1.4 การประมวลผลข้อมูลส่วนบุคคลที่ชอบด้วยกฎหมาย

1.4.1 ข้อมูลส่วนบุคคลธรรมดา

ใน มาตรา 6 ของ GDPR ได้มีการบัญญัติฐานในการประมวลผลข้อมูลส่วนบุคคลที่ชอบด้วยกฎหมาย ไว้ดังนี้[83]

1) ฐานความยินยอม (Consent)

ภายใต้ข้อบังคับของ GDPR การประมวลผลข้อมูลส่วนบุคคลนั้นไม่สามารถทำได้ ยกเว้นกรณีที่กฎหมายอนุญาตให้ทำได้ หรือได้รับความยินยอมจากเจ้าของข้อมูล โดย GDPR ได้กำหนดเงื่อนไขไว้ว่าผู้ควบคุมข้อมูลจะต้องสามารถแสดงให้เห็นว่าได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล[84] โดยที่ความยินยอมนั้นจะต้องเป็นการแสดงออกโดยอิสระ เฉพาะเจาะจง ชัดแจ้ง และชัดเจน[85] การให้ความยินยอมโดยอิสระ หมายถึง เจ้าของข้อมูลส่วนบุคคลจะต้องมีความสมัครใจที่จะให้มีการประมวลผลข้อมูลส่วนบุคคลของตน โดยที่เจ้าของข้อมูลส่วนบุคคลสามารถตัดสินใจได้ว่าจะให้ หรือไม่ให้มีการประมวลผลข้อมูลส่วนบุคคลของตน โดยการตัดสินใจของเจ้าของข้อมูลส่วนบุคคลนั้นจะต้องปราศจากความกดดัน หรือการชี้นำใด ๆ เช่น ความสัมพันธ์ระหว่างลูกจ้าง

---

[81] GDPR, Article 32(1).

[82] GDPR, Article 5(2).

[83] GDPR, Article 6

[84] GDPR, Article 7(1).

[85] GDPR, Article 4(11).

และนายจ้าง อาจมีผลทำให้ลูกจ้างผู้ซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลตัดสินใจให้ความยินยอม เนื่องจากกังวลถึงผลกระทบที่จะได้รับหากไม่ให้ความยินยอม ดังนั้น GDPR จึงได้กำหนดว่า การพิจารณาว่าความยินยอมนั้นได้ให้โดยอิสระหรือไม่ต้องคำนึงถึงเงื่อนไขในการให้ความยินยอม หากความยินยอมดังกล่าวจำเป็นต่อการปฏิบัติตามสัญญา หรือการให้บริการ ถือได้ว่าเป็นการยินยอมที่ให้โดยอิสระ แต่หากความยินยอมดังกล่าวไม่มีความจำเป็นต่อการปฏิบัติตามสัญญา หรือการให้บริการ ถือว่าความยินยอมนั้นมิได้เป็นความยินยอมที่ให้โดยอิสระ[86,87] ดังนั้นผู้ประมวลผลข้อมูลส่วนบุคคล หรือผู้ควบคุมข้อมูลส่วนบุคคลจึงสามารถเก็บข้อมูลส่วนบุคคลได้เพียงเท่าที่มีความจำเป็นในการปฏิบัติตามสัญญาหรือการให้บริการเท่านั้น และในการขอความยินยอมต้องระบุชื่อองค์กรของผู้ควบคุมข้อมูล ประเภทของข้อมูลส่วนบุคคลที่จะนำไปใช้ในการประมวลผล รวมถึงวิธีการนำไปใช้และวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลอีกด้วย ซึ่งการระบุรายละเอียดดังกล่าวในคำขอความยินยอมเป็นการป้องกันมิให้มีการเพิ่มเติมได้ในภายหลังโดยที่เจ้าของข้อมูลส่วนบุคคลมิได้ให้ความยินยอม นอกจากนี้ผู้ควบคุมข้อมูลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบหากมีการใช้ระบบการตัดสินใจอัตโนมัติ (Automated Decision-Making) ในการประมวลผลอีกด้วย

ความยินยอมสามารถอยู่ในรูปแบบของลายลักษณ์อักษร ไม่ว่าจะเป็นทางกระดาษ หรืออิเล็กทรอนิกส์ หรือในรูปแบบของวาจาก็ได้ โดยอาจเป็นการทำเครื่องหมายในช่องทำเครื่องหมาย (check box) หรือการตั้งค่าทางเทคนิค หรือการกระทำใด ๆ ที่แสดงให้เห็นโดยชัดแจ้งว่าได้มีการให้ความยินยอมโดยเจ้าของข้อมูลส่วนบุคคล ทั้งนี้เพื่อหลีกเลี่ยงการเข้าใจผิดว่าได้มีการให้ความยินยอมหรือไม่ สำหรับการทำเครื่องหมายล่วงหน้าในช่องทำเครื่องหมาย (pre-tick checkbox) หรือการไม่กระทำการใด ๆ ไม่ถือว่าเป็นการให้ความยินยอม นอกจากนี้การให้ความยินยอมยังต้องครอบคลุมวัตถุประสงค์ทั้งหมดที่ใช้ในการประมวลผลข้อมูลส่วนบุคคล ต้องมีการระบุวัตถุประสงค์ทั้งหมดหากมีวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลมากกว่าหนึ่งวัตถุประสงค์ และสำหรับกรณีที่มีการขอให้เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมโดยผ่านระบบอิเล็กทรอนิกส์ การขอความยินยอมจะต้องให้มีความชัดเจน กระชับ และไม่เป็นการเก็บข้อมูลนอกเหนือจากที่จำเป็นสำหรับการปฏิบัติตามสัญญาหรือการให้บริการ[88]

ในกรณีที่มีการขอความยินยอมเป็นลายลักษณ์อักษรสำหรับประเด็นใดประเด็นหนึ่งร่วมกับการขอความยินยอมสำหรับอีกประเด็นหนึ่ง การขอความยินยอมนั้นต้องนำเสนอให้เห็นว่ามีการแยกประเด็นอย่างชัดเจน รวมถึงต้องอยู่ในรูปแบบที่เข้าใจง่าย เข้าถึงได้ง่ายและใช้ภาษาธรรมดาที่ชัดเจนอีกด้วย หากคำขอความยินยอมขัดกับข้อบังคับนี้ความยินยอมย่อมไม่ผูกพันเจ้าของข้อมูลส่วนบุคคล[89] ดังนั้นการขอความยินยอมสำหรับการประมวลผลข้อมูลส่วนบุคคลกับการขอความยินยอมตามข้อตกลงในสัญญาจึงต้องมีการแยกออกจากกันอย่างชัดเจน

---

[86] สราวุธ ปิติยาศักดิ์. (2561b). โครงการวิจัย นโยบายคลาวด์และการคุ้มครองข้อมูลส่วนบุคคลในระบบคลาวด์ระหว่างสหภาพยุโรป สหรัฐอเมริกา ออสเตรเลียและอาเซียน: มุมมองของไทย (รายงานฉบับสมบูรณ์). สำนักงานสนับสนุนกองทุนการวิจัย (สกว.), น.60.

[87] GDPR, Article 7(4).

[88] GDPR, Recital 32.

[89] GDPR, Article 7(2).

เมื่อให้ความยินยอมแล้วเจ้าของข้อมูลส่วนบุคคลสามารถถอนความยินยอมเสียเมื่อใดก็ได้ โดยการเพิกถอนความยินยอมนั้นจะไม่มีผลกระทบต่อการประมวลผลที่ชอบด้วยกฎหมายที่เกิดขึ้นก่อนการเพิกถอนความยินยอมนั้น ทั้งนี้ต้องมีการแจ้งสิทธิในการเพิกถอนความยินยอมให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนมีการให้ความยินยอม และการถอนความยินยอมนั้นจะต้องให้เจ้าของข้อมูลส่วนบุคคลสามารถดำเนินการได้โดยง่ายอีกด้วย[90]

หากผู้ควบคุมข้อมูลส่วนบุคคลได้ใช้ฐานความยินยอมเพื่อการประมวลผลข้อมูลส่วนบุคคลแล้ว หากมีการเพิกถอนความยินยอมโดยเจ้าของข้อมูลส่วนบุคคลแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลจะไม่สามารถยกฐานอื่นขึ้นมาเป็นเหตุผลในการประมวลผลข้อมูลส่วนบุคคลได้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องหยุดการประมวลผลข้อมูลส่วนบุคคลทั้งหมดเมื่อมีการเพิกถอนความยินยอมโดยเจ้าของข้อมูลส่วนบุคคล[91]

สำหรับความยินยอมที่ได้รับก่อนการประกาศใช้ GDPR หากความยินยอมที่ได้รับมาก่อนการบังคับใช้ GDPR ไม่สอดคล้องกับข้อกำหนดใน GDPR ผู้ควบคุมข้อมูลต้องทำการแก้ไขให้ถูกต้องตามข้อกำหนด โดยต้องทำการขอความยินยอมใหม่ หากไม่สามารถทำการแก้ไขให้ถูกต้องได้ผู้ควบคุมข้อมูลส่วนบุคคลนั้นจะต้องหยุดการประมวลผลข้อมูลส่วนบุคคลดังกล่าว

2) ฐานสัญญา (Contract)

การประมวลผลข้อมูลส่วนบุคคลสำหรับการปฏิบัติตามสัญญาใช้ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา[92] ผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูลส่วนบุคคลไม่สามารถประมวลผลภายใต้เงื่อนไขนี้ได้หากข้อมูลส่วนบุคคลนั้นไม่มีความจำเป็นในการปฏิบัติตามสัญญา[93] หรือข้อมูลส่วนบุคคลที่ใช้ประมวลผลมิได้เป็นของคู่สัญญา

ฐานการปฏิบัติตามสัญญาใช้ในกรณีที่มีความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลเพื่อปฏิบัติตามสัญญา หรือใช้ในกิจการที่เกี่ยวข้องกับการชำระหนี้ตามสัญญา หรือในกรณีที่ต้องดำเนินการก่อนการทำสัญญา เช่น ทำการประเมินราคาสินค้า หรือการบริการที่ต้องใช้ข้อมูลส่วนบุคคลในการจัดทำ ซึ่งในกรณีนี้ถือเป็นการปฏิบัติตามสัญญาแม้สัญญาจะเกิดขึ้นหรือไม่ก็ตาม

ตัวอย่าง เจ้าของข้อมูลส่วนบุคคลได้ขอให้บริษัทประกันรถยนต์ประเมินเบี้ยประกันสำหรับการประกันภัยรถยนต์ของตนเอง บริษัทประกันภัยจำเป็นต้องใช้ข้อมูลรถยนต์ ไม่ว่าจะเป็นรุ่น ยี่ห้อ ทะเบียน อายุ และข้อมูลส่วนบุคคลอื่น ๆ ในการคำนวณเบี้ยประกัน

---

[90] GDPR, Article 7(3).

[91] GDPR, Data Protection Working Party (WP29).

[92] GDPR, Article 6(1)(b).

[93] สราวุธ ปิติยาศักดิ์. (2561b). โครงการวิจัย นโยบายคลาวด์และการคุ้มครองข้อมูลส่วนบุคคลในระบบคลาวด์ระหว่างสหภาพยุโรป สหรัฐอเมริกา ออสเตรเลียและอาเซียน: มุมมองของไทย (รายงานฉบับสมบูรณ์). สำนักงานสนับสนุนกองทุนการวิจัย (สกว.), น. 60.

ข้อมูลส่วนบุคคลที่ใช้เพื่อประมวลผลสำหรับการปฏิบัติตามสัญญาไม่สามารถนำไปใช้เพื่อวัตถุประสงค์อื่นในองค์กรของผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูลส่วนบุคคลได้ แม้ว่าในสัญญาระบุว่าสามารถทำได้ก็ตาม

ในกรณีที่ก่อนเข้าทำสัญญา การประมวลผลข้อมูลส่วนบุคคลสำหรับการปฏิบัติตามสัญญาใช้ได้สำหรับกรณีที่เป็นการดำเนินตามคำขอของเจ้าของข้อมูลส่วนบุคคลเท่านั้น ไม่สามารถใช้ในกรณีที่ผู้อื่นนอกเหนือจากเจ้าของข้อมูลส่วนบุคคลเป็นผู้ร้องขอได้

3) ฐานการปฏิบัติหน้าที่ตามกฎหมาย (Legal Obligation)

การประมวลผลข้อมูลส่วนบุคคลภายใต้การปฏิบัติหน้าที่ตามกฎหมายเป็นการประมวลผลโดยผู้ควบคุมข้อมูลส่วนบุคคลเนื่องจากความจำเป็นที่จะต้องปฏิบัติตามกฎหมาย[94] โดยความจำเป็นดังกล่าวจะต้องเป็นหลักเกณฑ์ที่ถูกกำหนดโดยกฎหมายสหภาพยุโรปหรือกฎหมายของประเทศสมาชิกของผู้ควบคุมข้อมูลส่วนบุคคล[95] ทั้งนี้กฎหมายดังกล่าวไม่จำเป็นต้องเป็นลายลักษณ์อักษร แต่ต้องมีความชัดเจนและแน่นอน โดยการนำไปปฏิบัติจะต้องเป็นที่คาดหมายได้ของผู้ควบคุมข้อมูล[96]

ตัวอย่าง ธนาคารพาณิชย์ต้องรายงานพฤติกรรมทางการเงินที่น่าสงสัยหรือนายจ้างต้องส่งข้อมูลลูกจ้าง ให้กับหน่วยงานที่เกี่ยวข้อง

อย่างไรก็ดี การปฏิบัติตามสัญญาต่างจากการปฏิบัติตามกฎหมาย และไม่สามารถอ้างการปฏิบัติตามกฎหมายเป็นการปฏิบัติตามสัญญาได้ ทั้งนี้การประมวลผลข้อมูลส่วนบุคคลภายใต้การปฏิบัติตามกฎหมายจะต้องมีความเหมาะสม และเป็นสัดส่วนกันกับวัตถุประสงค์ การประมวลข้อมูลส่วนบุคคลภายใต้หลักเกณฑ์นี้ไม่สามารถใช้อ้างได้หากมีวิธีอื่นที่สามารถปฏิบัติตามกฎหมายได้โดยมิต้องมีการประมวลผลข้อมูลส่วนบุคคล

เนื่องจากการประมวลผลข้อมูลส่วนบุคคลเป็นการประมวลผลโดยใช้ฐานการปฏิบัติตามกฎหมาย เจ้าของข้อมูลส่วนบุคคลจึงถูกจำกัดสิทธิในการเรียกให้ผู้ควบคุมข้อมูลส่วนบุคคลลบข้อมูลส่วนบุคคลของตน[97] เนื่องจากถูกจำกัดสิทธิในการเรียกให้ผู้ควบควบคุมข้อมูลส่วนบุคคลลบข้อมูลส่วนบุคคลของตนจึงไม่สามารถใช้สิทธิในการย้ายข้อมูลส่วนบุคคลของตนไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยเสรีได้ และเจ้าของข้อมูลส่วนบุคคลไม่สามารถใช้สิทธิในการโต้แย้งคัดค้านได้หากประโยชน์จากการประมวลผลข้อมูลส่วนบุคคลเพื่อการปฏิบัติตามกฎหมายนั้นเหนือกว่าประโยชน์หรือสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล[98]

4) ฐานประโยชน์สำคัญต่อชีวิต (Vital Interest)

การประมวลผลข้อมูลส่วนบุคคลเพื่อประโยชน์สำคัญต่อชีวิต คือการประมวลผลที่เป็นการจำเป็นเพื่อปกป้องผลประโยชน์ที่สำคัญของเจ้าของข้อมูลส่วนบุคคล หรือของ

---

[94] GDPR, Article 6(1)(c).

[95] GDPR, Article 6(3).

[96] GDPR, Recital 41.

[97] GDPR, Article 17(1)(c).

[98] GDPR, Article 6(1)(f).

บุคคลอื่น[99] ซึ่งอาจเป็นการกระทำเพื่อรักษาชีวิต หรือประโยชน์อื่นใดที่มีความสำคัญ ทั้งนี้การประมวลผลข้อมูลส่วนบุคคลด้วยหลักเกณฑ์นี้จะต้องกระทำเนื่องจากมีความจำเป็นเท่านั้น ดังนั้นจึงไม่สามารถใช้หลักเกณฑ์นี้ได้หากมีวิธีอื่นที่จะสามารถกระทำเพื่อปกป้องผลประโยชน์ที่สำคัญของเจ้าของข้อมูลส่วนบุคคล หรือของบุคคลอื่นได้

กรณีการประมวลผลข้อมูลส่วนบุคคลเพื่อประโยชน์สำคัญต่อชีวิตของบุคคลอื่นอาจนำไปใช้กับการประมวลผลที่จำเป็นสำหรับวัตถุประสงค์ด้านมนุษยธรรม เช่น การตรวจสอบการระบาดของโรค หรือสำหรับเหตุฉุกเฉินด้านมนุษยธรรม เช่น การตอบสนองภัยพิบัติ กรณีที่มีการประมวลผลข้อมูลส่วนบุคคลเพื่อผลประโยชน์ที่สำคัญของบุคคลอื่นควรใช้เฉพาะในกรณีที่ไม่มีพื้นฐานทางกฎหมายอื่น ๆ รองรับเท่านั้น[100]

สำหรับข้อมูลที่เกี่ยวกับสุขภาพ หากเจ้าของข้อมูลส่วนบุคคลสามารถให้ความยินยอมได้ ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถอ้างหลักเกณฑ์ประโยชน์สำคัญต่อชีวิตได้ และจะต้องใช้หลักเกณฑ์การขอความยินยอมแทน

ตัวอย่าง เมื่อมีผู้ประสบอุบัติเหตุ ได้รับบาดเจ็บสาหัส ไม่ได้สติ และมีความจำเป็นต้องได้รับการผ่าตัดเพื่อรักษาชีวิต เนื่องจากผู้ประสบอุบัติเหตุไม่มีสติสัมปชัญญะ ผู้ควบคุมข้อมูลส่วนบุคคลจึงไม่สามารถขอความยินยอมในการประมวลผลข้อมูลส่วนบุคคลได้ การประมวลข้อมูลส่วนบุคคลในกรณีนี้จึงต้องใช้พื้นฐานเพื่อประโยชน์สำคัญต่อชีวิต แต่หากผู้ประสบอุบัติเหตุมีสติสัมปชัญญะ รู้สึกตัวดี การประมวลข้อมูลส่วนบุคคลด้วยหลักเกณฑ์เพื่อประโยชน์สำคัญต่อชีวิตก็ไม่สามารถใช้ได้

ตัวอย่าง เมื่อเด็กป่วยหนักเป็นอันตรายถึงชีวิต และต้องได้รับการรักษาโดยทันที อาจมีความจำเป็นต้องใช้หลักเกณฑ์การประมวลผลข้อมูลส่วนบุคคลเพื่อประโยชน์สำคัญต่อชีวิตผู้อื่นในการประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับสุขภาพของบิดาและมารดา

การประมวลผลข้อมูลส่วนบุคคลเพื่อประโยชน์สำคัญต่อชีวิตมักเกี่ยวข้องกับข้อมูลด้านสุขภาพ ซึ่งเป็นข้อมูลส่วนบุคคลที่ละเอียดอ่อน การประมวลผลข้อมูลส่วนบุคคลเพื่อประโยชน์สำคัญต่อชีวิตจึงต้องคำนึงถึงบทบัญญัติเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลที่ละเอียดอ่อนภายใต้ มาตรา 9 อีกด้วย

5) ฐานภารกิจของรัฐ (Public Task)

การประมวลผลข้อมูลส่วนบุคคลเพื่อภารกิจของรัฐ คือการประมวลผลข้อมูลส่วนบุคคลที่เป็นการจำเป็นต่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะ หรือในการใช้อำนาจรัฐของผู้ควบคุมข้อมูลส่วนบุคคล[101] โดยความจำเป็นดังกล่าวจะต้องเป็นหลักเกณฑ์ที่ถูกกำหนดภายใต้กฎหมายสหภาพยุโรป หรือกฎหมายของประเทศสมาชิกของผู้ควบคุมข้อมูลส่วนบุคคล[102] ทั้งนี้ไม่ต้องมีกฎหมายที่ให้อำนาจผู้ควบคุมข้อมูลส่วนบุคคลเพื่อกระทำการประมวลผลข้อมูลส่วนบุคคล

---

[99] GDPR, Article 6(1)(d).

[100] GDPR, Recital 46.

[101] GDPR, Article 6(1)(e).

[102] GDPR, Article 6(3).

อย่างชัดเจน หากแต่ภารกิจที่ต้องกระทำนั้นจะต้องมีหลักเกณฑ์ที่ต้องกระทำตามกฎหมาย[103] การประมวลผลข้อมูลส่วนบุคคลด้วยหลักเกณฑ์ภารกิจของรัฐต้องกระทำด้วยความจำเป็น นอกจากนี้ยังต้องมีความเหมาะสมและเป็นสัดส่วนกับวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล หากมีวิธีอื่นที่จะสามารถกระทำเพื่อภารกิจของรัฐได้ ผู้ควบคุมข้อมูลส่วนบุคคลจะไม่สามารถใช้หลักเกณฑ์นี้ในการประมวลผลข้อมูลส่วนบุคคลได้ ทั้งนี้ผู้ควบคุมข้อมูลส่วนบุคคลที่ประมวลผลข้อมูลส่วนบุคคลโดยใช้หลักเกณฑ์ประโยชน์สาธารณะ และอำนาจของรัฐไม่จำเป็นต้องเป็นองค์กรของรัฐเสมอไป

เนื่องจากการประมวลผลข้อมูลส่วนบุคคลเป็นการประมวลผลโดยใช้หลักเกณฑ์ประโยชน์สาธารณะและอำนาจของรัฐ เจ้าของข้อมูลส่วนบุคคลจึงถูกจำกัดสิทธิในการเรียกให้ผู้ควบคุมข้อมูลส่วนบุคคลลบข้อมูลส่วนบุคคลของตน รวมทั้งไม่สามารถใช้สิทธิในการย้ายข้อมูลส่วนบุคคลของตนไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยเสรีได้ อย่างไรก็ดี เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิในการโต้แย้งคัดค้านได้ เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลสามารถพิสูจน์ให้เห็นได้ว่าเหตุตามกฎหมายของการประมวลผลข้อมูลส่วนบุคคลอยู่เหนือผลประโยชน์ สิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรืออยู่เหนือการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิ เรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย[104]

6) ฐานประโยชน์อันชอบธรรม (Legitimate Interest)

การประมวลผลข้อมูลส่วนบุคคลภายใต้ฐานประโยชน์อันชอบธรรม คือ การประมวลผลข้อมูลส่วนบุคคลเมื่อมีความจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายสำหรับผู้ควบคุมข้อมูลส่วนบุคคล หรือของบุคคลที่สาม มีข้อยกเว้นในกรณีที่ประโยชน์ดังกล่าวด้อยกว่าประโยชน์หรือสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล โดยเฉพาะกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นเด็ก[105] หลักเกณฑ์ข้อนี้นับได้ว่าเป็นหลักเกณฑ์ที่มีความยืดหยุ่นมากกว่าฐานการประมวลผลข้อมูลส่วนบุคคลอื่น ๆ ที่ได้กล่าวมาแล้วข้างต้น แต่อาจมิใช่ฐานที่เหมาะสมที่สุด

ฐานประโยชน์อันชอบธรรมเหมาะแก่การใช้สำหรับกรณีการประมวลผลข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลทั่วไปสามารถคาดเดาได้ และมีผลกระทบต่อความเป็นส่วนตัวน้อย หรือมีเหตุผลอันไม่อาจหลีกเลี่ยงได้ เช่น การประมวลผลข้อมูลส่วนบุคคลเพื่อป้องกันการฉ้อโกง[106] เมื่อใช้ฐานนี้ในการประมวลผลข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องคำนึงถึงสิทธิ และเสรีภาพของเจ้าของข้อมูลส่วนบุคคลให้มากเนื่องจากมีโอกาสเกิดการละเมิดสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลได้โดยง่าย

การประมวลผลข้อมูลส่วนบุคคลของพนักงานภายในกลุ่มกิจการ เพื่อวัตถุประสงค์ในการบริหารจัดการ สามารถถือว่าเป็นการประมวลผลข้อมูลส่วนบุคคลเพื่อประโยชน์อันชอบธรรมได้[107]

---

[103] GDPR, Recital 41.

[104] GDPR, Article 21(1).

[105] GDPR, Article 6(1)(f).

[106] GDPR, Recital 47.

[107] GDPR, Recital 48.

อย่างไรก็ดีการประมวลผลข้อมูลส่วนบุคคลภายใต้ฐานประโยชน์อันชอบธรรมไม่ว่าจะเป็นประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูล หรือของผู้อื่น และไม่ว่าจะเป็นความชอบธรรมเพื่อผลประโยชน์เชิงพาณิชย์ ผลประโยชน์ส่วนตัว หรือผลประโยชน์ของสังคมโดยรวม จะต้องมีความจำเป็น เช่นเดียวกับการประมวลผลข้อมูลส่วนบุคคลภายใต้ฐานอื่น ๆ หากสามารถได้ผลลัพธ์ที่คล้ายกันโดยมิต้องใช้ข้อมูลส่วนบุคคล ให้ถือว่ามิได้มีความจำเป็นต้องใช้ข้อมูลส่วนบุคคล และไม่สามารถอ้างหลักเกณฑ์ประโยชน์อันชอบธรรมได้

1.4.2 ข้อมูลส่วนบุคคลประเภทชีวภาพ[108]

GDPR ได้บัญญัติให้ข้อมูลชีวภาพเป็นข้อมูลส่วนบุคคลชนิดพิเศษ[109] ซึ่งถือว่าเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว (sensitive data) ดังนั้นจึงห้ามมิให้ประมวลผลข้อมูลชนิดนี้ยกเว้นกรณีดังต่อไปนี้[110]

1) ความยินยอมโดยชัดแจ้ง (Explicit consent)

การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลเพื่อประมวลผลตามวัตถุประสงค์ที่ได้ระบุไว้ อย่างไรก็ดีหากกฎหมายสหภาพยุโรป หรือกฎหมายของประเทศสมาชิกมีการกำหนดห้ามมิให้เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมสำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว ความยินยอมนั้นย่อมไม่มีผล[111]

เนื่องจากการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวมีความเสี่ยงมากกว่าการประมวลผลข้อมูลส่วนบุคคลธรรมดา เจ้าของข้อมูลส่วนบุคคลต้องสามารถควบคุมข้อมูลของตนได้ในระดับที่สูงกว่าข้อมูลส่วนบุคคลธรรมดา การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวจึงต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล[112] และไม่สามารถอ้างการทำตามสัญญาเป็นหลักเกณฑ์ในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่ชอบด้วยกฎหมายได้

ภายใต้ GDPR ความยินยอมในการให้ประมวลผลข้อมูลส่วนบุคคลธรรมดามีข้อกำหนดที่เข้มงวดอยู่แล้ว ดังนั้นการได้รับความยินยอมโดยชัดแจ้ง จึงต้องให้เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมโดยแสดงข้อความในการให้ความยินยอมอย่างชัดเจนเหนือกว่าการให้ความยินยอมในการให้ประมวลผลข้อมูลส่วนบุคคลธรรมดา การอนุมานจากการกระทำบางอย่างของเจ้าของข้อมูลส่วนบุคคลไม่สามารถถือได้ว่าเป็นการให้ความยินยอมอย่างชัดแจ้ง การให้ความยินยอมอย่างชัดแจ้งอาจทำเป็นลายลักษณ์อักษร โดยผู้ควบคุมข้อมูลส่วนบุคคลอาจขอให้เจ้าของข้อมูลส่วนบุคคลเซ็นให้ความยินยอมในเอกสารที่ระบุข้อความให้ความยินยอมที่ผู้ควบคุมข้อมูลส่วนบุคคลได้เตรียมไว้ อย่างไรก็ดี การให้เจ้าของข้อมูลส่วนบุคคลเซ็นให้ความยินยอมในเอกสารมิใช่ทางเดียวที่จะ

---

[108] GDPR, Article 9(2).

[109] GDPR, Article 9(1).

[110] GDPR, Article 9

[111] GDPR, Article 9(2)(a).

[112] Article 29 Working Party. Guidelines on consent under Regulation 2016/679 (WP259 rev.01), (2018).

ได้มาซึ่งความยินยอมโดยชัดแจ้ง สำหรับกิจกรรมที่ดำเนินการผ่านระบบดิจิทัลการให้ความยินยอมโดยชัดแจ้งสามารถกระทำได้หลายวิธี เช่น การกรอกฟอร์มออนไลน์ การส่งอีเมล การสแกนเอกสารที่มีลายเซ็นของเจ้าของข้อมูลส่วนบุคคลเข้าระบบ การทำเครื่องหมายในช่องทำเครื่องหมาย (check box) หรือแม้กระทั่งการใช้ลายเซ็นดิจิทัล เป็นต้น การให้ความยินยอมอย่างชัดแจ้งด้วยวาจานั้นอาจทำได้ แต่การพิสูจน์ว่าความยินยอมนั้นได้มาอย่างถูกต้องภายใต้ข้อกำหนดของ GDPR อาจเป็นไปได้ยาก[113]

2) ความจำเป็นสำหรับการปฏิบัติหน้าที่ (Employment, social security and social protection)

การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นการจำเป็นสำหรับการปฏิบัติหน้าที่ รวมถึงการใช้สิทธิเฉพาะของผู้ควบคุมข้อมูลส่วนบุคคล หรือของเจ้าของข้อมูลส่วนบุคคล ตามกฎหมายแรงงาน กฎหมายประกันสังคม หรือกฎหมายคุ้มครองสังคม ภายใต้อำนาจที่ได้รับจากกฎหมายสหภาพ หรือกฎหมายของประเทศสมาชิก หรือตามข้อตกลงร่วมกันของประเทศสมาชิก ทั้งนี้ต้องมีมาตรการที่เหมาะสมในการปกป้องสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลด้วย[114]

ตัวอย่าง บริษัทประกอบการรถทัวร์ที่ให้บริการเดินรถอาจจัดให้มีการตรวจวัดแอลกอฮอล์และสารเสพติดพนักงานขับรถทุกคนเป็นประจำ ทั้งนี้บริษัทรถทัวร์มีหน้าที่และความรับผิดชอบต่อความปลอดภัยของผู้โดยสารทุกคน โดยการควบคุมไม่ให้พนักงานขับรถใช้แอลกอฮอล์และสารเสพติดในระหว่างการทำงาน ซึ่งบริษัทฯ สามารถใช้หลักเกณฑ์ความจำเป็นในการปฏิบัติหน้าที่ได้ แต่ไม่สามารถจัดให้มีการตรวจวัดแอลกอฮอล์และสารเสพติดพนักงานที่ไม่ได้มีความรับผิดชอบในการขับรถได้เนื่องจากไม่มีความจำเป็นในการปฏิบัติงาน

3) ประโยชน์สำคัญต่อชีวิต (Vital interests)

การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวสามารถทำได้หากเป็นการจำเป็นเพื่อปกป้องประโยชน์ที่สำคัญต่อชีวิตของเจ้าของข้อมูลส่วนบุคคลหรือของบุคคลอื่นในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าจะทางพฤตินัย หรือนิตินัย[115]

การประมวลผลข้อมูลส่วนบุคคลภายใต้หลักเกณฑ์นี้มีไว้เพื่อปกป้องประโยชน์สำคัญที่จำเป็นต่อชีวิต ไม่ว่าจะเป็นชีวิตของเจ้าของข้อมูลส่วนบุคคลหรือของบุคคลอื่น[116] จึงมีขอบเขตการใช้ที่จำกัด และมักใช้ในกรณีที่เป็นเรื่องของความเป็นความตาย และใช้ในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมทางพฤตินัย หรือนิตินัยได้ ดังนั้น การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวภายใต้หลักเกณฑ์นี้ไม่สามารถทำได้หากเจ้าของข้อมูลส่วนบุคคลสามารถให้ความยินยอมได้ และต้องขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลจึงชอบด้วยกฎหมาย

---

[113] Article 29 Working Party. Guidelines on consent under Regulation 2016/679 (WP259 rev.01), (2018).

[114] GDPR, Article 9(2)(b).

[115] GDPR, Article 9(2)(c).

[116] GDPR, Recital 46.

4) กิจกรรมโดยชอบขององค์กรไม่แสวงหาผลกำไร (Not-for-profit bodies)

การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่ชอบด้วยกฎหมายสามารถทำได้สำหรับการดำเนินการกิจกรรมที่ชอบด้วยกฎหมายขององค์กรที่ไม่แสวงหาผลกำไร เช่น มูลนิธิ สมาคม หรือองค์กรไม่แสวงหาผลกำไรอื่นที่มีวัตถุประสงค์ทางการเมือง ปรัชญา ศาสนา หรือสหภาพแรงงาน โดยมีเงื่อนไขว่าการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวนั้นจะต้องเกี่ยวข้องเฉพาะสมาชิก หรือ อดีตสมาชิกขององค์กร หรือบุคคลที่มีการติดต่อกับองค์กรเป็นปรกติ ภายใต้วัตถุประสงค์ขององค์กร และข้อมูลส่วนบุคคลที่มีความอ่อนไหวต้องไม่ถูกเปิดเผยออกไปภายนอกองค์กรหากมิได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล[117]

5) เปิดเผยข้อมูลต่อสาธารณชน (Made public by the data subject)

การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวสามารถทำได้โดยชอบด้วยกฎหมายหากเจ้าของข้อมูลส่วนบุคคลนั้นได้เปิดเผยข้อมูลส่วนบุคคลดังกล่าวต่อสาธารณชนด้วยตนเอง[118] ซึ่งการเปิดเผยนั้นต้องเป็นการเปิดเผยที่เจ้าของข้อมูลส่วนบุคคลกระทำไปโดยมีความตั้งใจที่จะเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวต่อสาธารณชน การรั่วไหลของข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่ทำให้สาธารณชนได้ทราบข้อมูลดังกล่าว ไม่ถือว่าเป็นการเปิดเผยข้อมูลต่อสาธารณชนด้วยตนเองของเจ้าของข้อมูลส่วนบุคคล

ความคิดเห็นทางการเมืองถือเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่เจ้าของข้อมูลส่วนบุคคลบางคนอาจเปิดเผยต่อสาธารณชนด้วยตนเอง อย่างไรก็ดีการนำข้อมูลส่วนบุคคลที่มีความอ่อนไหวไปใช้ภายใต้ฐานนี้ควรกระทำด้วยความระมัดระวัง เนื่องจากต้องดูพื้นฐานในการเปิดเผยข้อมูลว่าเจ้าของข้อมูลต้องการเปิดเผยให้แค่คนใกล้ชิด เช่น เพื่อนในโซเชียลมีเดีย หรือต้องการเปิดเผยให้สาธารณชนทราบ

การเปิดเผยให้สาธารณชนทราบ หมายถึง การเปิดเผยที่บุคคลทั่วไปสามารถเข้าถึงได้ มิใช่เข้าถึงได้แค่เฉพาะกลุ่ม การที่บุคคลใดบุคคลหนึ่งสามารถเข้าถึงข้อมูลได้มิได้หมายความว่าทุกคนสามารถเข้าถึงข้อมูลดังกล่าวได้ ดังนั้นการที่บุคคลใดบุคคลหนึ่ง หรือกลุ่มใดกลุ่มหนึ่งสามารถเข้าถึงข้อมูลได้มิได้หมายความว่าข้อมูลดังกล่าวเป็นข้อมูลที่เปิดเผยให้สาธารณชนทราบ

ทั้งนี้ การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวโดยใช้หลักเกณฑ์นี้อาจต้องมีการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบหากตกอยู่ภายใต้ข้อกำหนดที่ต้องแจ้ง (ดูรายละเอียด บทที่ 3 หัวข้อ 1.5.1 สิทธิในการได้รับทราบ (The right to be informed))

6) ฐานสิทธิเรียกร้องตามกฎหมาย (Legal claims or judicial acts)

การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวสามารถกระทำได้โดยชอบด้วยกฎหมายหากเป็นการจำเป็นสำหรับการก่อให้เกิดสิทธิเรียกร้อง การใช้สิทธิเรียกร้อง หรือการป้องกันสิทธิเรียกร้องตามกฎหมาย หรือในการพิจารณาคดีของศาล[119] ทั้งนี้ผู้ควบคุมข้อมูลส่วน

---

[117] GDPR, Article 9(2)(d).

[118] GDPR, Article 9(2)(e).

[119] GDPR, Article 9(2)(f).

บุคคลที่มีความอ่อนไหวจะต้องสามารถแสดงให้เห็นได้ว่าวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลดังกล่าวคือเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องทางกฎหมาย หรือเพื่อการพิจารณาคดีของศาล ซึ่งรวมถึงการขอคำปรึกษาทางด้านกฎหมาย และขั้นตอนการเตรียมสำหรับการดำเนินคดีทางกฎหมาย

ตัวอย่าง นายจ้างกำลังถูกลูกจ้างฟ้องร้องในคดีที่เกี่ยวกับอุบัติเหตุที่เกิดขึ้นในสถานที่ทำการของนายจ้าง นายจ้างต้องปรึกษาทนายเพื่อขอคำแนะนำ การนำข้อมูลที่เกี่ยวข้องกับอุบัติเหตุรวมถึงข้อมูลการบาดเจ็บของลูกจ้างซึ่งเป็นข้อมูลสุขภาพที่เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวไปเปิดเผยกับทนายของนายจ้าง ถือว่าเป็นการกระทำโดยชอบด้วยกฎหมายเนื่องจากเป็นการจำเป็นภายใต้หลักเกณฑ์สิทธิเรียกร้องตามกฎหมาย

ตัวอย่าง การที่ผู้อนุบาลทำนิติกรรมแทนผู้ไร้ความสามารถอาจต้องมีการเปิดเผยข้อมูลให้ผู้ที่เข้าทำนิติกรรมด้วยทราบว่าเป็นการกระทำการแทนผู้ไร้ความสามารถ ถือว่าเป็นการเปิดเผยข้อมูลสุขภาพซึ่งนับว่าเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว การเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวในกรณีนี้สามารถทำได้โดยชอบด้วยกฎหมาย

7) ประโยชน์สาธารณะที่สำคัญ (Reasons of substantial public interest)

การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวในกรณีที่เป็นการจำเป็นสำหรับประโยชน์สาธารณะที่สำคัญตามหลักเกณฑ์ของกฎหมายสหภาพ หรือกฎหมายของประเทศสมาชิกเป็นอีกหลักเกณฑ์หนึ่งในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่ชอบด้วยกฎหมาย โดยการประมวลผลจะต้องเหมาะสมได้สัดส่วนตามวัตถุประสงค์ของการประมวลผล และให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล อีกทั้งยังต้องจัดให้มีมาตรการการปกป้องสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลที่เหมาะสมด้วย[120]

8) ประโยชน์สาธารณะด้านการคุ้มครองและประกันสังคม (Health or social care)

การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวสามารถทำได้หากเป็นการจำเป็นสำหรับวัตถุประสงค์ทางการแพทย์ด้านเวชศาสตร์ป้องกัน หรืออาชีวเวชศาสตร์ เพื่อการประเมินความสามารถในการทำงานของพนักงาน การวินิจฉัยทางการแพทย์ การดูแลสุขภาพและสังคม หรือการรักษาหรือการจัดการระบบและการให้บริการที่เกี่ยวกับสุขภาพและสังคมตามหลักเกณฑ์ของกฎหมายสหภาพหรือกฎหมายของประเทศสมาชิก หรือเป็นไปตามสัญญากับผู้ประกอบอาชีพที่เกี่ยวกับสุขภาพ (Health Professionals) ทั้งนี้ต้องเป็นไปตามเงื่อนไขและมาตรการที่กำหนดไว้[121]

อนึ่ง การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวอาจถูกประมวลผลภายใต้หลักเกณฑ์นี้เมื่อข้อมูลเหล่านั้นถูกประมวลผลโดยหรือภายใต้ความรับผิดชอบของผู้เชี่ยวชาญที่มีหน้าที่รักษาความลับตามจรรยาบรรณของวิชาชีพ ทั้งนี้ตามหลักเกณฑ์ของกฎหมายสหภาพยุโรป

---

[120] GDPR, Article 9(2)(g).

[121] GDPR, Article 9(2)(h).

หรือกฎหมายของประเทศสมาชิก หรือภายใต้หลักเกณฑ์ที่กำหนดโดยหน่วยงานระดับชาติ หรือโดยบุคคลซึ่งมีหน้าที่เก็บรักษาความลับภายใต้กฎหมายสหภาพยุโรป หรือกฎหมายของประเทศสมาชิกหรือหลักเกณฑ์ของหน่วยงานระดับชาติ[122]

เนื่องจากการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวควรได้รับการคุ้มครองในระดับที่สูงกว่าข้อมูลส่วนบุคคลอื่น จึงควรใช้เฉพาะในกรณีที่จำเป็นเพื่อวัตถุประสงค์ที่เกี่ยวข้องกับสุขภาพและใช้เพียงเท่าที่จำเป็นเพื่อให้บรรลุวัตถุประสงค์เหล่านั้นเพื่อประโยชน์ของบุคคลธรรมดาและสังคมโดยรวม โดยเฉพาะอย่างยิ่งในบริบทของการบริหารจัดการระบบการบริการทางด้านสุขภาพและสังคม การประมวลผลเพื่อการควบคุมคุณภาพโดยผู้บริหารและหน่วยงานกลางที่รับผิดชอบด้านสาธารณสุข การจัดการและการกำกับดูแลทั่วไปของข้อมูลด้านสุขภาพและสังคมในระดับชาติและระดับท้องถิ่นเพื่อการดูแลสุขภาพและสังคม การดูแลสุขภาพอย่างต่อเนื่องไม่ว่าจะเป็นการดูแลข้ามพรมแดนหรือการดูแลความปลอดภัยทางด้านสุขภาพ การตรวจสอบและแจ้งเตือนเพื่อประโยชน์สาธารณะ การวิจัยทางวิทยาศาสตร์หรือประวัติศาสตร์หรือวัตถุประสงค์ทางสถิติตามกฎหมายของสหภาพหรือประเทศสมาชิกที่จะต้องบรรลุวัตถุประสงค์ด้านสาธารณะประโยชน์ เช่นเดียวกับการดำเนินการศึกษาวิจัยเพื่อประโยชน์ด้านสาธารณสุข เมื่อมีความต้องการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่เกี่ยวกับสุขภาพ จะต้องมีการกำหนดเงื่อนไขที่สอดคล้องกัน โดยเฉพาะอย่างยิ่งเมื่อมีการประมวลผลข้อมูลดังกล่าวเพื่อจุดประสงค์ด้านสุขภาพโดยบุคคลที่อยู่ภายใต้บังคับของกฎหมายในการรักษาความลับโดยอาชีพ นอกจากนี้กฎหมายของสหภาพหรือประเทศสมาชิกควรจัดให้มีมาตรการเฉพาะและเหมาะสมเพื่อปกป้องสิทธิขั้นพื้นฐานและข้อมูลส่วนบุคคลของบุคคลธรรมดา ทั้งนี้ สำหรับข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลสุขภาพ GDPR ได้กำหนดให้ประเทศสมาชิกสามารถคงไว้ หรือเพิ่มเงื่อนไขที่เฉพาะเจาะจง และข้อจำกัดเกี่ยวกับการประมวลข้อมูลส่วนบุคคลดังกล่าวได้[123]

9) ประโยชน์ด้านสาธารณสุข (Public health)

การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวสามารถทำได้หากเป็นการจำเป็นสำหรับวัตถุประสงค์เพื่อประโยชน์ด้านสาธารณสุข เช่น การป้องกันจากภัยคุกคามข้ามพรมแดนอันอาจเป็นอันตรายร้ายแรงต่อสุขภาพ หรือเพื่อการรับรองมาตรฐานด้านคุณภาพ และความปลอดภัยของผลิตภัณฑ์ยา และเครื่องมืออุปกรณ์ทางการแพทย์ ภายใต้หลักเกณฑ์ของกฎหมายสหภาพหรือกฎหมายของประเทศสมาชิก ซึ่งมีมาตรการที่เหมาะสม และเฉพาะเจาะจงในการปกป้องสิทธิและเสรีภาพของเจ้าของข้อมูล โดยเฉพาะในการเก็บรักษาความลับตามจริยธรรมของผู้ประกอบวิชาชีพ[124]

การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวภายใต้หลักเกณฑ์ประโยชน์ด้านสาธารณสุขมีวัตถุประสงค์เพื่อป้องกัน และควบคุมโรคติดต่อ รวมถึงภัยคุกคามอื่นซึ่งอาจเป็นอันตรายต่อสุขภาพโดยเน้นไปที่ภัยคุกคามข้ามพรมแดน

---

[122] GDPR, Article 9(3).

[123] GDPR, Recital 53.

[124] GDPR, Article 9(2)(i).

การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวอาจมีความจำเป็นเพื่อเหตุผลสาธารณะประโยชน์ในด้านสาธารณสุขโดยไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูล อย่างไรก็ดี การประมวลผลดังกล่าวควรอยู่ภายใต้มาตรการที่เหมาะสมและเฉพาะเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของบุคคลธรรมดา คำว่า “สาธารณสุข” ควรตีความตามที่กำหนดไว้ใน Regulation (EC) No 1338/2008 of the European Parliament and of the Council (11) หมายถึง องค์ประกอบทั้งหมดที่เกี่ยวข้องกับสุขภาพ ได้แก่ สถานะของสุขภาพ รวมถึงอาการเจ็บป่วยและความพิการ ปัจจัยที่มีผลต่อสถานะสุขภาพ ความต้องการการดูแลสุขภาพ ทรัพยากรที่จัดสรรให้กับการดูแลสุขภาพ การจัดหาและการเข้าถึงระบบการดูแลสุขภาพ การใช้จ่ายด้านการดูแลสุขภาพและการเงิน และสาเหตุของการตาย การประมวลผลข้อมูลที่เกี่ยวข้องกับสุขภาพเพื่อผลประโยชน์สาธารณะนี้ไม่ควรส่งผลให้มีการประมวลผลเพื่อวัตถุประสงค์อื่นโดยบุคคลที่สาม เช่น นายจ้าง บริษัทประกันภัย และธนาคาร[125]

ตัวอย่าง การประมวลข้อมูลส่วนบุคคลที่มีความอ่อนไหวด้านสุขภาพเพื่อการตรวจสอบและควบคุมทางด้านสาธารณสุข การป้องกันโรคระบาด การทดสอบประสิทธิภาพทางคลินิกของยาใหม่หรืออุปกรณ์ทางการแพทย์ใหม่โดยการทดลองกับมนุษย์ การอนุมัติขึ้นทะเบียนยาเพื่อนำไปใช้กับประชากรทั่วไป สามารถทำได้โดยชอบด้วยกฎหมายภายใต้หลักเกณฑ์ประโยชน์ด้านสาธารณสุข

10) จดหมายเหตุ การวิจัยหรือทางสถิติ (Archiving, research and statistics)

การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวสามารถทำได้หากเป็นการจำเป็นสำหรับวัตถุประสงค์ในการจัดเก็บในลักษณะจดหมายเหตุเพื่อประโยชน์สาธารณะ เพื่อการวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือเพื่อวัตถุประสงค์ทางสถิติ[126] การประมวลผลดังกล่าวต้องได้สัดส่วนตามวัตถุประสงค์ของการประมวลผลข้อมูลและให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล อีกทั้งยังต้องจัดให้มีมาตรการที่เหมาะสมและเฉพาะเจาะจงในการปกป้องสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล[127]

ดังนั้น การวิจัยที่มิใช่การวิจัยทางวิทยาศาสตร์ หรือประวัติศาสตร์จึงไม่สามารถอ้างฐานนี้ในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวได้ นอกจากนี้การวิจัยดังกล่าวอาจเป็นการวิจัยที่จัดทำโดยทั้งภาครัฐและภาคเอกชน แต่ต้องเป็นการวิจัยเพื่อประโยชน์สาธารณะ

การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการจัดเก็บเพื่อประโยชน์สาธารณะ เพื่อการวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือวัตถุประสงค์ทางสถิติ ต้องอยู่ภายใต้มาตรการป้องกันที่เหมาะสมในการคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูล โดยต้องทำให้มั่นใจว่ามีมาตรการทางเทคนิคและมาตรการทางองค์กรที่ยึดหลักการใช้ข้อมูลให้น้อยที่สุด ซึ่งรวมถึงมาตรการการเปลี่ยนข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถระบุตัวตนได้ (pseudonymization) หากการ

---

[125] GDPR, Recital 54.

[126] GDPR, Article 89(1).

[127] GDPR, Article 9(2)(j).

เปลี่ยนข้อมูลสามารถทำให้บรรลุวัตถุประสงค์ดังกล่าวได้ ในกรณีที่วัตถุประสงค์ดังกล่าวสามารถบรรลุได้โดยมีการประมวลผลข้อมูลเพิ่มเติมซึ่งทำให้ไม่สามารถระบุตัวตนของเจ้าของข้อมูลได้ วัตถุประสงค์ดังกล่าวสามารถดำเนินการต่อไปในลักษณะเช่นนั้นได้[128]

เนื่องจากข้อมูลส่วนบุคคลที่มีความอ่อนไหวถือว่าเป็นข้อมูลส่วนบุคคล ดังนั้น การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวจึงต้องใช้ฐานในการประมวลผลข้อมูลส่วนบุคคลที่ชอบด้วยกฎหมายภายใต้มาตรา 6 ประกอบกับหลักเกณฑ์ในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่ชอบด้วยกฎหมายภายใต้มาตรา 9 เสมอ หลักเกณฑ์ในการประมวลประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวไม่สามารถใช้โดยลำพังโดยไม่มีฐานในการประมวลผลข้อมูลส่วนบุคคลที่ชอบด้วยกฎหมายได้ ทั้งนี้ฐานในการประมวลผลข้อมูลส่วนบุคคลอาจมีความสัมพันธ์กับหลักเกณฑ์ในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวในบางกรณี เช่น หากฐานในการประมวลผลข้อมูลส่วนบุคคลคือฐานประโยชน์สำคัญต่อชีวิตแล้ว การใช้หลักเกณฑ์ประโยชน์สำคัญต่อชีวิตในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวจึงมีความสอดคล้องกัน และในกรณีฐานในการประมวลผลข้อมูลส่วนบุคคลคือฐานความยินยอมก็อาจเป็นไปได้ที่หลักเกณฑ์ในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นหลักเกณฑ์ความยินยอมโดยชัดแจ้งเช่นกัน แต่หากฐานในการประมวลผลข้อมูลส่วนบุคคลคือฐานประโยชน์สำคัญต่อชีวิตแต่ใช้หลักเกณฑ์ความยินยอมโดยชัดแจ้งในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวนั้นไม่สามารถเป็นไปได้ ในบางกรณีมีความเป็นไปได้ที่ฐานในการประมวลผลข้อมูลส่วนบุคคลนั้นอาจดูเหมือนไม่มีความสัมพันธ์โดยตรงกับหลักเกณฑ์ในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว เช่น หากฐานในการประมวลผลข้อมูลส่วนบุคคลคือฐานประโยชน์อันชอบธรรมหรือฐานปฏิบัติตามสัญญา แต่หลักเกณฑ์ในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวอาจเป็นความยินยอมโดยชัดแจ้งได้ ดังนั้นหลักเกณฑ์ในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวนั้นจึงต้องมีการคำนึงถึงวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวสูงเป็นสำคัญ เพื่อให้มั่นใจได้ว่าการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวสูงนั้นมีความจำเป็นสำหรับวัตถุประสงค์นั้น

ในบางกรณีอาจมีการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล แต่ผู้ควบคุมข้อมูลส่วนบุคคลไม่ได้ใช้หลักเกณฑ์ความยินยอมในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว เช่น ในกรณีการทดลองวัคซีนผู้ทำการวิจัยและทดลองวัคซีนอาจได้รับความยินยอมอย่างชัดแจ้งจากผู้รับการทดลองวัคซีนเป็นเพื่อนำผลในการทดลองไปใช้ แต่ผู้ทำการวิจัยอาจใช้ฐานภารกิจของรัฐตามมาตรา 6(1)(e) ในการประมวลผลข้อมูลส่วนบุคคลประกอบกับหลักเกณฑ์ประโยชน์ด้านสาธารณสุขตามมาตรา 9(2)(i) ในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว ทั้งนี้การใช้หลักเกณฑ์ประโยชน์ด้านสาธารณสุขและฐานภารกิจของรัฐนั้นเป็นการป้องกันในกรณีที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิในการถอนความยินยอม เนื่องจากวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวนั้นคือเพื่อประโยชน์ด้านสาธารณสุขนั่นเอง

1.5 สิทธิของเจ้าของข้อมูลส่วนบุคคล

ภายใต้ข้อกำหนดของ GDPR เจ้าของข้อมูลส่วนบุคคลมีสิทธิ ดังนี้

---

[128] GDPR, Article 89(1).

1.5.1 สิทธิในการได้รับทราบ (The right to be informed)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการได้รับทราบถึงรายละเอียดเกี่ยวกับการเก็บรวบรวม การนำไปใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลของตน ทั้งนี้การประมวลผลข้อมูลส่วนบุคคลภายใต้ GDPR ต้องดำเนินการโดยโปร่งใส โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องเปิดเผยให้เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียด เช่น วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล ระยะเวลาที่ข้อมูลส่วนบุคคลดังกล่าวจะถูกจัดเก็บ และนอกจากผู้ควบคุมข้อมูลแล้วมีองค์กรใดนำข้อมูลดังกล่าวไปใช้บ้าง

ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลทราบถึงรายละเอียดของการประมวลผลข้อมูลส่วนบุคคล ไม่ว่าผู้ควบคุมข้อมูลจะเป็นผู้เก็บรวมรวมข้อมูลส่วนบุคคลด้วยตนเอง หรือได้รับข้อมูลส่วนบุคคลดังกล่าวมาจากผู้อื่น สำหรับรายละเอียดที่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคล มีดังนี้

ตารางที่ 3.1 รายละเอียดที่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคล

รายละเอียดที่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคล	ผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้เก็บรวบรวมข้อมูล[129]	ผู้ควบคุมข้อมูลส่วนบุคคลมิได้เป็นผู้เก็บรวบรวมข้อมูล[130]
ตัวตน และรายละเอียดในการติดต่อผู้ควบคุมข้อมูลส่วนบุคคลและผู้แทนผู้ควบคุมส่วนบุคคล (ถ้ามี)	✓	✓
รายละเอียดในการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (ถ้ามี)	✓	✓
วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล รวมถึงฐานในการประมวลผลข้อมูลส่วนบุคคล	✓	✓
ประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมส่วนบุคคลหรือของบุคคลที่สาม ในกรณีที่การประมวลผลข้อมูลส่วนบุคคลเป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายสำหรับผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลที่สาม	✓	✓
ผู้รับข้อมูลส่วนบุคคลหรือประเภทของผู้รับข้อมูลส่วนบุคคล (ถ้ามี)	✓	✓
รายละเอียดเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังประเทศที่สาม หรือองค์การระหว่างประเทศ	✓	✓

[129] GDPR, Article 13.

[130] GDPR, Article 14.

ตารางที่ 3.1 (ต่อ)

รายละเอียดที่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคล	ผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้เก็บรวบรวมข้อมูล[130]	ผู้ควบคุมข้อมูลส่วนบุคคลมิได้เป็นผู้เก็บรวบรวมข้อมูล[131]
ระยะเวลาที่ข้อมูลส่วนบุคคลจะถูกจัดเก็บ	✓	✓
สิทธิต่าง ๆ ของเจ้าของข้อมูลที่เกี่ยวกับการประมวลผลข้อมูล เช่น สิทธิในการเข้าถึงข้อมูล หรือสิทธิเรียกให้ลบข้อมูลส่วนบุคคล เป็นต้น	✓	✓
สิทธิถอนความยินยอม	✓	✓
สิทธิยื่นคำร้องต่อหน่วยงานกำกับดูแล	✓	✓
แหล่งที่มาของข้อมูลส่วนบุคคล	✗	✓
รายละเอียดเกี่ยวกับการให้ข้อมูลส่วนบุคคลว่า เป็นไปตามบทบัญญัติของกฎหมาย หรือข้อกำหนดตามสัญญา หรือข้อบังคับที่จำเป็นในการเข้าทำสัญญา	✓	✗
รายละเอียดเกี่ยวกับการตัดสินและการจัดเก็บข้อมูลโดยวิธีการอัตโนมัติ และการทำโปรไฟลิ่ง	✓	✓

ที่มา : GDPR มาตรา 13 และ 14

ระยะเวลาที่จะต้องแจ้งรายละเอียดต่อเจ้าของข้อมูลส่วนบุคคลสำหรับทั้งกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้เก็บรวบรวมข้อมูล และ ผู้ควบคุมข้อมูลส่วนบุคคลมิได้เป็นผู้เก็บรวบรวมข้อมูลส่วนบุคคล มีดังนี้

ตารางที่ 3.2 ระยะเวลาที่ต้องแจ้งรายละเอียดต่อเจ้าของข้อมูล

	ระยะเวลาที่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคล
ผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้เก็บรวบรวมข้อมูล	ก่อนการเก็บรวบรวมข้อมูลส่วนบุคคล
ผู้ควบคุมข้อมูลส่วนบุคคลมิได้เป็นผู้เก็บรวบรวมข้อมูล	1. ภายในระยะเวลาตามสมควร แต่ต้องไม่เกินหนึ่งเดือนนับแต่วันที่เก็บรวบรวมข้อมูล 2. ขณะเวลาติดต่อสื่อสารครั้งแรกกับเจ้าของข้อมูลส่วนบุคคล 3. ขณะเวลาที่ข้อมูลส่วนบุคคลถูกเปิดเผยเป็นครั้งแรก ในกรณีเป็นการเปิดเผยกับผู้รับอื่น

ที่มา : GDPR มาตรา 13 และ 14

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้เก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลไม่จำเป็นต้องแจ้งเจ้าของข้อมูลหากเจ้าของข้อมูลส่วนบุคคลทราบรายละเอียดดังกล่าวแล้ว ทั้งนี้หากผู้ควบคุมข้อมูลส่วนบุคคลได้ข้อมูลมาจากแหล่งอื่นไม่ได้เป็นผู้เก็บรวบรวมข้อมูลด้วยตนเอง ผู้ควบคุมข้อมูลส่วนบุคคลไม่ต้องแจ้งรายละเอียดให้เจ้าของข้อมูลส่วนบุคคลในกรณีดังต่อไปนี้[131]

1) เจ้าของข้อมูลส่วนบุคคลได้ทราบรายละเอียดดังกล่าวแล้ว

2) การแจ้งรายละเอียดให้เจ้าของข้อมูลส่วนบุคคลเป็นไปไม่ได้ หรือการแจ้งรายละเอียดให้เจ้าของข้อมูลส่วนบุคคลต้องใช้ความพยายามเกินควร

3) การแจ้งข้อมูลให้เจ้าของข้อมูลส่วนบุคคลอาจเป็นอุปสรรค ทำให้วัตถุประสงค์ของการประมวลผลส่วนบุคคลนั้นเป็นไปไม่ได้ หรือเสียหายร้ายแรง

4) ผู้ควบคุมข้อมูลส่วนบุคคลจำต้องเก็บรวบรวม หรือเปิดเผยข้อมูลส่วนบุคคลโดยอาศัยอำนาจตามกฎหมายของสหภาพยุโรป หรือกฎหมายของประเทศสมาชิกที่ผู้ควบคุมข้อมูลส่วนบุคคลอยู่ภายใต้บังคับ

5) ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่รักษาความลับตามมาตรฐานวิชาชีพภายใต้กฎหมายของสหภาพยุโรป หรือกฎหมายของประเทศสมาชิกที่ผู้ควบคุมข้อมูลส่วนบุคคลอยู่ภายใต้บังคับ รวมถึงหน้าที่ตามกฎหมายในการรักษาความลับนั้น

1.5.2 สิทธิในการเข้าถึงข้อมูล (The right of access)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของตน โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลแสดงให้เห็นว่าผู้ควบคุมข้อมูลส่วนบุคคลได้เก็บข้อมูลอะไร และข้อมูลดังกล่าวกำลังถูกประมวลผลอยู่หรือไม่ รวมทั้งการประมวลผลนั้นชอบด้วยกฎหมายหรือไม่ กรณีนี้รวมถึงข้อมูลส่วนบุคคลด้านสุขภาพ เช่น ข้อมูลในเวชระเบียนของเจ้าของข้อมูลส่วนบุคคลที่มีข้อมูลการวินิจฉัย ผลการตรวจ การประเมินการรักษาของแพทย์ และการ

[131] GDPR, Article 14(5).

รักษาที่เจ้าของข้อมูลส่วนบุคคลได้รับ เป็นต้น และเมื่อเป็นไปได้ผู้ควบคุมข้อมูลส่วนบุคคลควรจัดให้เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงข้อมูลของตนจากระยะไกล (remote access) ได้โดยผ่านระบบที่ปลอดภัยโดยไม่กระทบสิทธิ และเสรีภาพของผู้อื่น[132] ทั้งนี้การร้องขอนั้นเจ้าของข้อมูลส่วนบุคคลสามารถทำได้ด้วยวาจา ทำเป็นลายลักษณ์อักษร หรือด้วยวิธีทางอิเล็กทรอนิกส์[133] ทั้งนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำตามคำร้องขอภายใน 1 เดือน[134] ในกรณีที่คำร้องของเจ้าของข้อมูลเป็นคำร้องที่ไม่มีมูล หรือเกินสมควร ผู้ควบคุมอาจปฏิเสธคำร้องดังกล่าวได้[135]

เจ้าของข้อมูลส่วนบุคคลมีสิทธิเข้าถึงข้อมูลส่วนบุคคลของตน และรายละเอียด ดังต่อไปนี้[136]

1) วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล

2) ประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้อง

3) ผู้รับหรือประเภทของผู้รับที่ข้อมูลส่วนบุคคลจะถูกส่งให้ หรือถูกเปิดเผยโดยเฉพาะผู้รับในประเทศที่สาม หรือองค์การระหว่างประเทศ

4) ระยะเวลาที่ข้อมูลส่วนบุคคลนั้นจะถูกจัดเก็บ หรือหากไม่สามารถกำหนดระยะเวลาได้ต้องระบุเกณฑ์ที่ใช้เพื่อกำหนดระยะเวลานั้น

5) สิทธิเข้าถึงข้อมูลและสิทธิให้แก้ไขข้อมูล หรือสิทธิเรียกให้ลบข้อมูล หรือสิทธิจำกัดการประมวลผลข้อมูลส่วนบุคคล หรือสิทธิคัดค้านการประมวลผลข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลส่วนบุคคล รวมถึงสิทธิเคลื่อนย้ายข้อมูล

6) สิทธิในการร้องเรียนต่อหน่วยงานกำกับดูแล

7) แหล่งที่มาของข้อมูลส่วนบุคคล ในกรณีที่ข้อมูลส่วนบุคคลไม่ได้ถูกเก็บรวบรวมจากเจ้าของข้อมูลส่วนบุคคล

8) การตัดสินและการจัดเก็บข้อมูลโดยอัตโนมัติตามมาตรา 22(1) และมาตรา 22(4) และอย่างน้อยต้องระบุรายละเอียดที่สำคัญเกี่ยวกับเหตุผลที่เกี่ยวข้อง รวมถึงความสำคัญและผลกระทบของการประมวลผลข้อมูลส่วนบุคคลที่มีต่อเจ้าของข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถเรียกเก็บค่าใช้จ่ายในการดำเนินตามคำร้องขอของเจ้าของข้อมูลได้[137] ยกเว้นการจัดทำสำเนาของข้อมูลส่วนบุคคลเพิ่มเติมซึ่งผู้ควบคุมข้อมูลส่วนบุคคลอาจเรียกเก็บค่าธรรมเนียมโดยคำนวณจากค่าใช้จ่ายในการทำสำเนาได้[138]

---

[132] GDPR, Recital 63.

[133] GDPR, Article 12(1).

[134] GDPR, Article 12(3).

[135] GDPR, Article 12(5).

[136] GDPR, Article 15(1).

[137] GDPR, Recital 59.

[138] GDPR, Article 15(3).

1.5.3 สิทธิให้แก้ไขข้อมูล (The right to rectification)

เมื่อพบว่าข้อมูลส่วนบุคคลของตนไม่ถูกต้องหรือไม่สมบูรณ์ เจ้าของข้อมูลส่วนบุคคลมีสิทธิเรียกให้ผู้ควบคุมข้อมูลส่วนบุคคลแก้ไขข้อมูลเกี่ยวกับตนที่ไม่ถูกต้องหรือทำให้ส่วนที่ไม่สมบูรณ์นั้นสมบูรณ์ครบถ้วน รวมทั้งจัดทำรายละเอียดประกอบด้วย[139] โดยคำร้องสามารถทำด้วยวาจา ทำเป็นลายลักษณ์อักษรหรือด้วยวิธีทางอิเล็กทรอนิกส์ได้[140] โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการแก้ไขให้ถูกต้องครบถ้วนภายใน 1 เดือน[141]

ผู้ควบคุมข้อมูลอาจเรียกค่าใช้จ่ายในการดำเนินการตามความเหมาะสมในกรณีที่คำร้องเป็นที่ชัดแจ้งว่าคำร้องไม่มีมูล หรือเป็นการเกินสมควร และผู้ควบคุมข้อมูลส่วนบุคคลสามารถปฏิเสธไม่ให้มีการแก้ไขข้อมูลส่วนบุคคล หรือทำข้อมูลที่ไม่สมบูรณ์ให้สมบูรณ์สำหรับกรณีคำร้องซึ่งเป็นที่ชัดแจ้งว่าคำร้องไม่มีมูล หรือเป็นการเกินสมควร หรือเป็นการร้องขอซ้ำ[142] หรือเป็นการจำกัดสิทธิเจ้าของข้อมูลส่วนบุคคลในกรณีเฉพาะ[143]

1.5.4 สิทธิเรียกให้ลบ (The right to erasure)

สิทธิเรียกให้ลบ หรือสิทธิที่จะถูกลืม (right to be forgotten) คือเจ้าของข้อมูลส่วนบุคคลมีสิทธิเรียกให้ผู้ควบคุมข้อมูลส่วนบุคคลลบข้อมูลส่วนบุคคลที่เกี่ยวกับตนเสีย โดยเจ้าของข้อมูลส่วนบุคคลอาจต้องการถอนความยินยอมที่เคยให้ไว้ หรือไม่ต้องการได้รับการติดต่อจากผู้ควบคุมข้อมูลส่วนบุคคล ไม่ว่าจะเป็นการส่งเมล์โฆษณา หรือการติดต่อทางโทรศัพท์ เจ้าของข้อมูลส่วนบุคคลสามารถร้องขอด้วยวาจา ทำเป็นลายลักษณ์อักษรหรือด้วยวิธีทางอิเล็กทรอนิกส์[144] โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการภายใน 1 เดือนนับจากวันที่ได้รับคำร้องขอ[145] ทั้งนี้ สิทธิให้ลบนี้มิใช่สิทธิสมบูรณ์ และใช้ได้ในบางสถานการณ์ โดยเมื่อได้รับคำร้องผู้ควบคุมข้อมูลส่วนบุคคลต้องลบข้อมูลส่วนบุคคลในกรณีดังต่อไปนี้[146]

1) ไม่มีความจำเป็นต้องเก็บรวบรวม หรือประมวลผลตามวัตถุประสงค์ในการเก็บรวบรวม หรือประมวลผลอีกต่อไป

2) เจ้าของข้อมูลส่วนบุคคลถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคลตามมาตรา 6(1)(a) หรือ มาตรา 9(2)(a) และไม่มีเหตุตามกฎหมายอื่นสำหรับการประมวลผลข้อมูลส่วนบุคคลอีก

---

[139] GDPR, Article 16.

[140] GDPR, Article 12(1).

[141] GDPR, Article 12(3).

[142] GDPR, Article 12(5).

[143] GDPR, Article 23.

[144] GDPR, Article 12(1).

[145] GDPR, Article 12(3).

[146] GDPR, Article 17(1).

3) เจ้าของข้อมูลส่วนบุคคลคัดค้านการประมวลผลข้อมูลส่วนบุคคลตาม มาตรา 21(1) และไม่มีเหตุตามกฎหมายที่สำคัญกว่าสำหรับการประมวลผลข้อมูลส่วนบุคคล หรือเจ้าของข้อมูลส่วนบุคคลคัดค้านการประมวลผลข้อมูลส่วนบุคคลตาม มาตรา 21(2)

4) ข้อมูลส่วนบุคคลถูกประมวลผลโดยผิดกฎหมาย

5) ข้อมูลส่วนบุคคลต้องถูกลบเพื่อให้สอดคล้องกับหน้าที่ตามกฎหมายสหภาพยุโรปหรือกฎหมายของประเทศสมาชิกที่ผู้ควบคุมข้อมูลส่วนบุคคลอยู่ภายใต้บังคับ

6) ข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมโดยกิจกรรมที่เกี่ยวข้องกับการให้บริการทางอิเล็กทรอนิกส์ (information society services)[147] ตามมาตรา 8(1)

ผู้ควบคุมข้อมูลส่วนบุคคลไม่ต้องปฏิบัติตามคำร้องขอให้ลบข้อมูลส่วนบุคคลในกรณีที่การประมวลผลข้อมูลส่วนบุคคลดังกล่าวมีความจำเป็นเพื่อ[148]

1) การใช้สิทธิเสรีภาพในการแสดงออกและการเข้าถึงข้อมูล

2) การปฏิบัติตามกฎหมายภายใต้กฎหมายสหภาพ หรือกฎหมายของประเทศสมาชิกที่ผู้ควบคุมข้อมูลส่วนบุคคลอยู่ภายใต้บังคับ หรือเพื่อการดำเนินการเพื่อประโยชน์สาธารณะ หรือการใช้อำนาจรัฐของผู้ควบคุมข้อมูลส่วนบุคคล

3) ประโยชน์สาธารณะเกี่ยวกับสุขภาพของประชาชน ตามมาตรา 9(2)(h) และมาตรา 9(2)(i) รวมถึงมาตรา 9(3)

4) วัตถุประสงค์ในการเก็บรวบรวมเพื่อประโยชน์สาธารณะ เพื่อการวิจัยทางวิทยาศาสตร์ หรือประวัติศาสตร์ หรือวัตถุประสงค์ทางสถิติ ภายใต้เงื่อนไขและการป้องกันตามมาตรา 89(1) หรือการลบข้อมูลส่วนบุคคลดังกล่าวจะทำให้วัตถุประสงค์ดังกล่าวไม่สามารถกระทำได้ หรือหากกระทำได้จะมีผลกระทบอย่างร้ายแรง

5) การก่อ การใช้ หรือการป้องกันสิทธิเรียกร้องตามกฎหมาย

นอกจากนี้ ในกรณีที่เป็นที่ชัดแจ้งว่าคำร้องไม่มีมูล หรือเป็นการเกินสมควร ผู้ควบคุมข้อมูลส่วนบุคคลสามารถปฏิเสธที่จะปฏิบัติตามการร้องขอให้ลบข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลได้ หรือผู้ควบคุมข้อมูลส่วนบุคคลอาจเรียกค่าใช้จ่ายในการดำเนินการตามความเหมาะสม[149]

1.5.5 สิทธิจำกัดการประมวลผล (The right to restrict processing)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการร้องให้ผู้ควบคุมข้อมูลส่วนบุคคลจำกัดการประมวลผลข้อมูลส่วนบุคคลของตน ทั้งนี้ในการจำกัดการประมวลผลผู้ควบคุมข้อมูลส่วนบุคคลเพียงแต่ต้องทำการจำกัดการประมวลผล แต่ผู้ควบคุมข้อมูลส่วนบุคคลยังสามารถเก็บข้อมูลส่วนบุคคลไว้ได้ ในการร้องขอให้จำกัดการประมวลผลเจ้าของข้อมูลส่วนบุคคลสามารถร้องขอด้วยวาจา

---

[147] Directive 98/48/EC has defined “information society service” as “any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.”

[148] GDPR, Article 17(3).

[149] GDPR, Article 12(5).

ทำเป็นลายลักษณ์อักษร หรือด้วยวิธีทางอิเล็กทรอนิกส์ก็ได้[150] โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการภายใน 1 เดือนนับจากวันที่ได้รับคำร้องขอ[151] ทั้งนี้ สิทธิให้จำกัดการประมวลผลนี้มิใช่สิทธิสมบูรณ์ และใช้ได้ในบางสถานการณ์เท่านั้น โดยเจ้าของข้อมูลส่วนบุคคลอาจห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลประมวลผลข้อมูลส่วนบุคคลของตนได้ด้วยเหตุอย่างหนึ่งอย่างใดดังต่อไปนี้[152]

1) เจ้าของข้อมูลส่วนบุคคลโต้แย้ง หรือคัดค้านความถูกต้องของข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคลมีสิทธิจำกัดการประมวลผลข้อมูลส่วนบุคคลในระหว่างที่ผู้ควบคุมข้อมูลส่วนบุคคลทำการตรวจสอบ ยืนยันความถูกต้องของข้อมูลส่วนบุคคล

2) การประมวลผลข้อมูลส่วนบุคคลนั้นมิชอบด้วยกฎหมาย และเจ้าของข้อมูลส่วนบุคคลคัดค้านการลบข้อมูลส่วนบุคคล และร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลจำกัดการประมวลผลข้อมูลส่วนบุคคลเหล่านั้นแทน

3) ผู้ควบคุมข้อมูลส่วนบุคคลไม่มีความจำเป็นต้องใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลอีกต่อไป แต่ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำตามข้อเรียกร้องของเจ้าของข้อมูลส่วนบุคคล ในการก่อตั้ง การใช้ และการป้องกันสิทธิเรียกร้องทางกฎหมาย

4) เจ้าของข้อมูลส่วนบุคคลโต้แย้ง หรือคัดค้านความถูกต้องของข้อมูลส่วนบุคคลตามมาตรา 21(1) เพื่อรอการพิสูจน์ข้ออ้างตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลว่ามีอำนาจเหนือสิทธิของเจ้าของข้อมูลส่วนบุคคลหรือไม่

หากผู้ควบคุมข้อมูลส่วนบุคคลได้ทำการจำกัดการประมวลผลข้อมูลส่วนบุคคลภายใต้เหตุดังกล่าวข้างต้น และผู้ควบคุมข้อมูลส่วนบุคคลต้องการยกเลิกการจำกัดการประมวลผลข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนการยกเลิก[153]

ตัวอย่าง เจ้าของข้อมูลส่วนบุคคลโต้แย้งความถูกต้องของข้อมูลส่วนบุคคลของตน ในระหว่างที่ผู้ควบคุมส่วนบุคคลทำการตรวจสอบยืนยันความถูกต้องของข้อมูล เจ้าของข้อมูลส่วนบุคคลมีสิทธิเรียกร้องให้ผู้ควบคุมข้อมูลส่วนบุคคลจำกัดการประมวลผลข้อมูลส่วนบุคคลของตน และเมื่อผู้ควบคุมข้อมูลส่วนบุคคลได้ทำการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลเป็นที่เรียบร้อยแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเจ้าของข้อมูลส่วนบุคคลว่าได้ทำการยืนยันความถูกต้องของข้อมูลแล้ว และต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนการยกเลิกการจำกัดการประมวลผลข้อมูลส่วนบุคคล

ในกรณีที่เป็นที่ชัดแจ้งว่าคำร้องของเจ้าของข้อมูลส่วนบุคคลเพื่อให้จำกัดการประมวลผลนั้นไม่มีมูล หรือเป็นการเกินสมควร ผู้ควบคุมข้อมูลส่วนบุคคลสามารถปฏิเสธที่จะปฏิบัติ

---

[150] GDPR, Article 12(1).

[151] GDPR, Article 12(3).

[152] GDPR, Article 18(1).

[153] GDPR, Article 18(3).

ตามการร้องขอของเจ้าของข้อมูลส่วนบุคคลได้ หรือ ผู้ควบคุมข้อมูลส่วนบุคคลอาจเรียกค่าใช้จ่ายในการดำเนินการได้ตามความเหมาะสม[154]

1.5.6 สิทธิในการย้ายข้อมูล (The right to data portability)

สิทธิในการย้ายข้อมูลทำให้เจ้าของข้อมูลส่วนบุคคลสามารถนำข้อมูลของตนไปใช้เพื่อวัตถุประสงค์ของเจ้าของข้อมูลส่วนบุคคลได้โดยสะดวก ปลอดภัยและไม่มีผลกระทบต่อการนำข้อมูลไปใช้งาน ทั้งนี้เจ้าของข้อมูลมีสิทธิในการได้รับข้อมูลส่วนบุคคลของตนที่ได้ให้กับผู้ควบคุมข้อมูลส่วนบุคคลในรูปแบบที่ใช้กันทั่วไปและเครื่องคอมพิวเตอร์สามารถอ่านได้ นอกจากนี้เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการย้ายข้อมูลไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยเสรี ปราศจากการขัดขวางจากผู้ควบคุมข้อมูลส่วนบุคคลที่เป็นผู้จัดเก็บข้อมูลดังกล่าว ในกรณีดังต่อไปนี้[155]

1) การประมวลผลข้อมูลส่วนบุคคลเป็นไปตามความยินยอม ในมาตรา 6(1)(a) หรือมาตรา 9(2)(a) หรือโดยสัญญาตามมาตรา 6(1)(b) และ

2) การประมวลผลข้อมูลส่วนบุคคลโดยวิธีการอัตโนมัติ

เจ้าของข้อมูลส่วนบุคคลอาจยื่นคำร้องขอย้ายข้อมูลต่อผู้ควบคุมข้อมูลด้วยวาจา หรือเป็นลายลักษณ์อักษรหรือด้วยวิธีทางอิเล็กทรอนิกส์ก็ได้[156] โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการภายใน 1 เดือนนับจากวันที่ได้รับคำร้องขอ[157] เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิในการย้ายข้อมูลได้ในกรณีที่การประมวลผลโดยผู้ควบคุมข้อมูลส่วนบุคคลได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (consent) หรือการประมวลผลข้อมูลส่วนบุคคลเป็นการจำเป็นสำหรับการปฏิบัติตามสัญญา (contract) และสิทธิในการย้ายข้อมูลนี้ไม่ก่อให้เกิดพันธกรณีแก่ผู้ควบคุมข้อมูลในการจัดเตรียมระบบงานที่มีความเข้ากันได้ในทางเทคนิค (technically compatible) [158]

ทั้งนี้สิทธิในการย้ายข้อมูลจำกัดเฉพาะข้อมูลที่เจ้าของข้อมูลได้เคย “ให้” กับผู้ควบคุมส่วนบุคคล หากมิได้ครอบคลุมเพียงแค่ข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้มอบให้กับผู้ควบคุมข้อมูลส่วนบุคคลโดยตรง แต่หมายความรวมถึงข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ทำการเก็บรวบรวมจากเจ้าของข้อมูลส่วนบุคคล[159] เช่น

1) ข้อมูลประวัติการใช้เว็บไซต์ (website usage) และประวัติการค้นหา (search history)

2) ข้อมูลการเดินทาง (traffic data) และข้อมูลสถานที่ (location data)

3) ข้อมูลที่เก็บจากอุปกรณ์ที่เชื่อมต่อผ่านระบบอินเตอร์เน็ต เช่น อุปกรณ์ IoT หรืออุปกรณ์สวมใส่ (wearable devices) อย่างสมาร์ทวอช หรือกล้องวงจรปิด เป็นต้น

---

[154] GDPR, Article 12(5).

[155] GDPR, Article 20(1).

[156] GDPR, Article 12(1).

[157] GDPR, Article 12(3).

[158] GDPR, Recital 68.

[159] Information Commissioner's Office. (2019). *Guide to the General Data Protection Regulation (GDPR).* In Information Commissioner's Office (Ed.). , p.139.

สำหรับข้อมูลที่ได้จากข้อมูลส่วนบุคคล ไม่ว่าจากการอนุมาน หรือเป็นผลที่ได้มาจากการประมวลผลข้อมูลส่วนบุคคล ถือว่าเป็นข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลต้องส่งมอบให้กับเจ้าของข้อมูลส่วนบุคคลเมื่อมีการร้องขอทั้งสิ้น ทั้งนี้ไม่รวมถึงข้อมูลที่เกิดจากการประมวลผลโดยผู้ควบคุมข้อมูลหากข้อมูลที่ได้จากการประมวลผลนั้นไม่ถือว่าเป็นข้อมูลส่วนบุคคล เช่น เมื่อข้อมูลนั้นมีการนำไปทำให้ไม่สามารถระบุตัวตนได้โดยทำให้เป็นข้อมูลนิรนาม (anonymized) แต่หากเป็นการแฝงข้อมูล (pseudonymized) ยังถือว่าข้อมูลนั้นเป็นข้อมูลส่วนบุคคลอยู่ ผู้ควบคุมข้อมูลส่วนบุคคลจึงต้องส่งมอบข้อมูลแฝงให้เจ้าของข้อมูลส่วนบุคคล แต่ไม่ต้องส่งมอบข้อมูลนิรนาม[160]

ผู้ควบคุมข้อมูลส่วนบุคคลสามารถปฏิเสธคำร้องของเจ้าของข้อมูลส่วนบุคคลได้ในกรณีที่เป็นที่ชัดแจ้งว่าคำร้องของเจ้าของข้อมูลส่วนบุคคลเพื่อย้ายข้อมูลนั้นไม่มีมูล หรือเป็นการเกินสมควร หรือผู้ควบคุมข้อมูลส่วนบุคคลอาจเรียกค่าใช้จ่ายในการดำเนินการได้ตามความเหมาะสม[161]

1.5.7 สิทธิโต้แย้งคัดค้าน (The right to object)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะโต้แย้งคัดค้านการประมวลผลข้อมูลส่วนบุคคลของตนเอง ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้ข้อมูลส่วนบุคคลนั้นเพื่อการตลาดแบบขายตรง (direct marketing)[162] ซึ่งรวมถึงการทำโปรไฟลิ่งที่เกี่ยวข้องกับการตลาดแบบขายตรง[163] โดยสิทธิในการคัดค้านการตลาดแบบขายตรงดังกล่าวเป็นสิทธิสมบูรณ์ของเจ้าของข้อมูล ซึ่งผู้ควบคุมข้อมูลส่วนบุคคลไม่อาจโต้แย้งได้

เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะคัดค้านการประมวลผลข้อมูลส่วนบุคคลในกรณีดังต่อไปนี้

1) ผู้ควบคุมข้อมูลส่วนบุคคลอ้างการประมวลผล และการจัดเก็บข้อมูลเป็นการจำเป็นสำหรับการปฏิบัติหน้าที่อันเป็นไปเพื่อประโยชน์สาธารณะ หรือเพื่อใช้อำนาจรัฐของผู้ควบคุมข้อมูลส่วนบุคคล ตามมาตรา 6(1)(e) หรือ ผู้ควบคุมข้อมูลส่วนบุคคลอ้างการประมวลผลเป็นการจำเป็นต่อวัตถุประสงค์อันเป็นประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือบุคคลที่สามตาม มาตรา 6(1)(f) แต่เจ้าของข้อมูลส่วนบุคคลไม่สามารถคัดค้านได้ หากประโยชน์จากการประมวลผลข้อมูลส่วนบุคคลเพื่อการปฏิบัติตามกฎหมายนั้นเหนือกว่าประโยชน์หรือสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล[164] โดยภาระการพิสูจน์ตกอยู่กับผู้ควบคุมข้อมูลส่วนบุคคล[165]

---

[160] Information Commissioner's Office. (2019). Guide to the General Data Protection Regulation (GDPR). In Information Commissioner's Office (Ed.). , p.139.

[161] GDPR, Article 12(5).

[162] GDPR, Article 21(2).

[163] GDPR, Recital 70.

[164] GDPR, Article 21(1).

[165] GDPR, Recital 69.

2) ผู้ควบคุมข้อมูลส่วนบุคคลอ้างการประมวลผลข้อมูลส่วนบุคคลเพื่อการวิจัยทางวิทยาศาสตร์ หรือประวัติศาสตร์ หรือวัตถุประสงค์ตามสถิติ ตามมาตรา 89(1) เจ้าของข้อมูลส่วนบุคคลมีสิทธิโต้แย้งคัดค้านการประมวลผลข้อมูลส่วนบุคคลของตน เว้นแต่การประมวลผลข้อมูลส่วนบุคคลเป็นการจำเป็นสำหรับการทำงานเพื่อประโยชน์สาธารณะ[166] ทั้งนี้ภาระการพิสูจน์ตกอยู่กับผู้ควบคุมข้อมูลส่วนบุคคล[167]

3) ในบริบทของการประมวลผลที่เกี่ยวข้องกับการให้บริการทางอิเล็กทรอนิกส์ (Information Society Services) โดยไม่คำนึงถึงกฎระเบียบที่ 2002/58/EC เจ้าของข้อมูลส่วนบุคคลอาจใช้สิทธิโต้แย้งคัดค้านด้วยวิธีอัตโนมัติโดยใช้ข้อกำหนดทางเทคนิค[168]

เมื่อเจ้าของข้อมูลส่วนบุคคลคัดค้านการประมวลผลข้อมูลส่วนบุคคล มีผลให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องหยุดประมวลผลข้อมูลส่วนบุคคล การคัดค้านการประมวลผลข้อมูลส่วนบุคคลนั้นอาจเป็นการคัดค้านข้อมูลส่วนบุคคลของเจ้าของข้อมูลเพียงบางส่วน หรือทั้งหมด หรือเป็นการคัดค้านการประมวลผลสำหรับวัตถุประสงค์บางประการ

เจ้าของข้อมูลส่วนบุคคลอาจยื่นคำร้องคัดค้านโต้แย้งข้อมูลต่อผู้ควบคุมข้อมูลด้วยวาจา หรือเป็นลายลักษณ์อักษรหรือด้วยวิธีทางอิเล็กทรอนิกส์ก็ได้[169] โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการภายใน 1 เดือนนับจากวันที่ได้รับคำร้องขอ[170]

ในกรณีที่เป็นที่ชัดแจ้งว่าคำร้องของเจ้าของข้อมูลส่วนบุคคลเพื่อโต้แย้งคัดค้านนั้นไม่มีมูล หรือเป็นการเกินสมควร ผู้ควบคุมข้อมูลส่วนบุคคลสามารถปฏิเสธคำร้องของเจ้าของข้อมูลส่วนบุคคลได้ หรือ ผู้ควบคุมข้อมูลส่วนบุคคลอาจเรียกค่าใช้จ่ายในการดำเนินการได้ตามความเหมาะสม[171]

1.5.8 สิทธิไม่ต้องตกอยู่ภายใต้การตัดสินและการประมวลผลโดยอัตโนมัติ (Rights in relation to automated decision making and profiling)

ใน มาตรา 22 ของ GDPR มีข้อกำหนดที่เกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับ

1) การตัดสินใจด้วยวิธีอัตโนมัติเพียงอย่างเดียวโดยไม่มีส่วนร่วมของมนุษย์ (Automated individual decision-making) และ

2) การทำโปรไฟลิ่ง (Profiling) ซึ่งคือการประมวลผลข้อมูลส่วนบุคคลโดยอัตโนมัติเพื่อประเมินบางสิ่งเกี่ยวกับบุคคลใดบุคคลหนึ่ง การทำโปรไฟลิ่งอาจเป็นส่วนหนึ่งของกระบวนการตัดสินใจอัตโนมัติ

---

[166] GDPR, Article 21(6).

[167] GDPR, Recital 69.

[168] GDPR, Article 21(5).

[169] GDPR, Article 12(1).

[170] GDPR, Article 12(3).

[171] GDPR, Article 12(5).

โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิไม่ต้องตกอยู่ภายใต้การตัดสินใจด้วยวิธีอัตโนมัติเพียงอย่างเดียวโดยไม่มีส่วนร่วมของมนุษย์ และการทำโปรไฟลิ่งที่อาจก่อให้เกิดผลทางกฎหมายหรือส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลอย่างมีนัยสำคัญ[172]

ตัวอย่าง การขออนุมัติสินเชื่อ หรือการสอบคัดเลือกสมัครเข้าทำงาน หากขั้นตอนการอนุมัติหรือการคัดเลือกกระทำการโดยระบบอัตโนมัติ และมิได้มีมนุษย์เข้ามาเกี่ยวข้องในขั้นตอนใดขั้นตอนหนึ่ง ถือได้ว่าเป็นการตัดสินใจด้วยวิธีอัตโนมัติเพียงอย่างเดียวโดยไม่มีส่วนร่วมของมนุษย์ซึ่งส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลอย่างมีนัยสำคัญ

สำหรับการทำโปรไฟลิ่ง (Profiling) นั้น คือการเก็บข้อมูลส่วนบุคคลจากแหล่งต่าง ๆ ไม่ว่าจะเป็นข้อมูลเกี่ยวกับการซื้อสินค้า การค้นหาข้อมูลทางอินเตอร์เน็ต ข้อมูลการดำเนินชีวิตและพฤติกรรมที่สามารถรวบรวมจากโทรศัพท์มือถือ โซเชียลเน็ตเวิร์ค กล้องวงจรปิด และ IoT (Internet of Things) เป็นต้น ข้อมูลเหล่านี้จะถูกนำมาวิเคราะห์ เพื่อจำแนกบุคคลออกเป็นกลุ่ม โดยการใช้ อัลกอริทึม (algorithm) และการเรียนรู้ด้วยเครื่อง (machine learning) โดยการวิเคราะห์นี้สามารถกำหนดความเชื่อมโยงระหว่างพฤติกรรมและ คุณลักษณะเฉพาะเพื่อสร้างโปรไฟล์สำหรับบุคคล โดยทั่วไป วัตถุประสงค์ของการทำโปรไฟลิ่งมักใช้เพื่อคาดการณ์พฤติกรรมของแต่ละบุคคลและใช้ในการตัดสินใจ เช่น การสร้างโปรไฟล์สำหรับกลุ่มลูกค้าเพื่อนำไปทำการตลาดโดยผ่านอีเมลโดยเลือกที่จะส่งแคมเปญที่ตรงกับเป้าหมายได้

สำหรับการทำโปรไฟลิ่งนั้น GDPR ได้ให้คำจำกัดความไว้ ดังนี้[173]

1) การประมวลผลข้อมูลโดยวิธีอัตโนมัติ

2) ใช้ข้อมูลส่วนบุคคลในการประเมินลักษณะส่วนตัวบางประการของบุคคลใด

3) ใช้ในการวิเคราะห์หรือคาดการณ์เกี่ยวกับประสิทธิภาพของบุคคลในการทำงาน สถานภาพทางเศรษฐกิจ สุขภาพ ความชอบหรือความสนใจส่วนบุคคล ความน่าเชื่อถือพฤติกรรม สถานที่อยู่ หรือการเดินทาง

อย่างไรก็ดี การตัดสินใจโดยวิธีการอัตโนมัติ รวมถึงการทำโปรไฟลิ่งนั้น อาจทำได้หากกฎหมายสหภาพยุโรป หรือกฎหมายของประเทศสมาชิกที่ผู้ควบคุมข้อมูลส่วนบุคคลอยู่ภายใต้บังคับได้มีข้อกำหนดให้ทำได้โดยเฉพาะ ซึ่งรวมถึงเพื่อวัตถุประสงค์ในการตรวจสอบและป้องกันการฉ้อโกงและการหลีกเลี่ยงภาษีที่ดำเนินการตามระเบียบมาตรฐานและคำแนะนำของสถาบัน หรือหน่วยงานกำกับดูแลระดับชาติและเพื่อให้มั่นใจในความปลอดภัยและความน่าเชื่อถือของบริการของผู้ควบคุมข้อมูลส่วนบุคคล หรือจำเป็นสำหรับการทำสัญญา หรือปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคล หรือเมื่อได้รับความยินยอมอย่างชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล ทั้งนี้การประมวลผลดังกล่าวต้องมีมาตรการการป้องกันที่เหมาะสมซึ่งควรรวมถึงข้อมูลที่เฉพาะเจาะจงกับเจ้าของข้อมูลส่วนบุคคล สิทธิในการได้รับการแทรกแซงจาก

---

[172] GDPR, Article 22(1).

[173] GDPR, Article 4(4).

มนุษย์ สิทธิแสดงมุมมองของเจ้าของข้อมูลส่วนบุคคล สิทธิได้รับคำอธิบายของการตัดสินใจ และสิทธิโต้แย้งการตัดสินใจ[174]

เพื่อให้มั่นใจว่าการประมวลผลเป็นธรรมและโปร่งใสสำหรับเจ้าของข้อมูลส่วนบุคคล โดยคำนึงถึงสถานการณ์และบริบทเฉพาะในการประมวลผลข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลควรใช้กระบวนการทางคณิตศาสตร์หรือสถิติที่เหมาะสมในการทำโปรไฟลิ่ง และใช้มาตรการด้านเทคนิคและด้านองค์กรที่เหมาะสม เพื่อให้มั่นใจว่าปัจจัยที่ส่งผลให้เกิดความไม่ถูกต้องในข้อมูลส่วนบุคคลได้รับการแก้ไข และลดความเสี่ยงของการเกิดข้อผิดพลาด มีการรักษาความปลอดภัยของข้อมูลส่วนบุคคลในลักษณะที่คำนึงถึงความเสี่ยงที่อาจเกิดขึ้นกับผลประโยชน์และสิทธิของเจ้าของข้อมูลส่วนบุคคล และป้องกันผลกระทบจากการเลือกปฏิบัติต่อบุคคลบนพื้นฐานของเชื้อชาติหรือชาติพันธุ์ ความคิดเห็นทางการเมือง ศาสนาหรือความเชื่อ สมาชิกสหภาพแรงงาน สถานะทางพันธุกรรม หรือสุขภาพ หรือรสนิยมทางเพศ หรือการประมวลผลอันใดที่อาจทำให้เกิดมาตรการดังกล่าว ทั้งนี้การตัดสินใจด้วยวิธีอัตโนมัติ และการทำโปรไฟลิ่งโดยใช้ข้อมูลส่วนบุคคลที่มีความอ่อนไหวควรให้สามารถทำได้เฉพาะภายใต้เงื่อนไขที่เฉพาะเจาะจงเท่านั้น[175]

เจ้าของข้อมูลส่วนบุคคลอาจยื่นคำร้องไม่ให้ต้องตกอยู่ภายใต้การตัดสินและการประมวลผลโดยอัตโนมัติต่อผู้ควบคุมข้อมูลด้วยวาจา หรือเป็นลายลักษณ์อักษรหรือด้วยวิธีทางอิเล็กทรอนิกส์ก็ได้[176] โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการภายใน 1 เดือนนับจากวันที่ได้รับคำร้องขอ[177] ทั้งนี้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถปฏิเสธคำร้องของเจ้าของข้อมูลส่วนบุคคลได้ในกรณีที่เป็นที่ชัดแจ้งว่าคำร้องของเจ้าของข้อมูลส่วนบุคคลเพื่อโต้แย้งข้อมูลนั้นไม่มีมูล หรือเป็นการเกินสมควร หรือผู้ควบคุมข้อมูลส่วนบุคคลอาจเรียกค่าใช้จ่ายในการดำเนินการได้ตามความเหมาะสม[178]

1.6 การรักษาความปลอดภัยของข้อมูลส่วนบุคคล

การรักษาความปลอดภัยของข้อมูลส่วนบุคคลนั้นเป็นหน้าที่สำคัญของผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคล หมายถึง บุคคลธรรมดาหรือนิติบุคคล หน่วยงานภาครัฐ สำนักงานผู้แทน หรือองค์กรอื่นใด ไม่ว่าจะด้วยตนเองหรือร่วมกับผู้อื่นกำหนดวัตถุประสงค์ และวิธีการประมวลผลข้อมูลส่วนบุคคล ในกรณีที่วัตถุประสงค์ และวิธีการประมวลผลข้อมูลดังกล่าวถูกกำหนดโดยกฎหมายสหภาพยุโรปหรือกฎหมายของประเทศสมาชิก ให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือเกณฑ์ที่ใช้ในการกำหนดผู้ควบคุมข้อมูลส่วนบุคคลเป็นไปตามกฎหมายสหภาพยุโรปหรือ

---

[174] GDPR, Recital 71.

[175] GDPR, Recital 71.

[176] GDPR, Article 12(1).

[177] GDPR, Article 12(3).

[178] GDPR, Article 12(5).

กฎหมายของประเทศสมาชิก[179,180] ในกรณีมีผู้ควบคุมข้อมูลส่วนบุคคลตั้งแต่สองคนขึ้นไปร่วมกันกำหนดวัตถุประสงค์และวิธีการประมวลผลข้อมูลส่วนบุคคล ให้ถือว่าผู้ควบคุมข้อมูลส่วนบุคคลนั้นเป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วม[181] โดยส่วนใหญ่ผู้ควบคุมข้อมูลส่วนบุคคลมักเป็นผู้ประมวลผลข้อมูลส่วนบุคคลที่ได้เก็บรวมรวมมาด้วยตนเอง แต่ในบางกรณีผู้ควบคุมข้อมูลส่วนบุคคลอาจมีความจำเป็นต้องให้บุคคลที่สามทำการประมวลผลข้อมูลส่วนบุคคลให้ เช่น การวิเคราะห์ข้อมูล เป็นต้น อย่างไรก็ดีผู้ควบคุมข้อมูลส่วนบุคคลยังคงเป็นผู้กำหนดวัตถุประสงค์ และวิธีการในการประมวลผลข้อมูลส่วนบุคคล แม้ว่าการประมวลผลนั้นจะกระทำโดยผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นบุคคลที่สามก็ตาม

ผู้ประมวลผลข้อมูลส่วนบุคคล หมายถึง บุคคลธรรมดาหรือนิติบุคคล หน่วยงานภาครัฐ สำนักงานผู้แทน หรือองค์กรอื่นใด ทำการประมวลผลข้อมูลส่วนบุคคลในนามผู้ควบคุมข้อมูลส่วนบุคคล[182,183] โดยผู้ควบคุมข้อมูลส่วนบุคคลทำการส่งข้อมูลส่วนบุคคลให้ผู้ประมวลผลข้อมูลส่วนบุคคลทำการประมวลผลให้ภายใต้วัตถุประสงค์ และวิธีการที่ผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้กำหนด โดยผู้ประมวลผลข้อมูลส่วนบุคคลไม่ถือว่าเป็นผู้ควบคุมข้อมูลส่วนบุคคลดังกล่าว และผู้ประมวลผลข้อมูลส่วนบุคคลไม่สามารถเปลี่ยนแปลงวัตถุประสงค์ หรือวิธีการในการประมวลผลข้อมูลส่วนบุคคลนั้นได้

ตัวอย่าง บริษัท A เป็นผู้เก็บรวบรวมข้อมูลการใช้งานเว็บไซต์ โดยมีการเก็บข้อมูลว่าผู้ใช้งานเข้าสู่เว็บไซต์ผ่านหน้าใดเป็นหน้าแรก และลำดับหน้าที่ผู้ใช้งานเข้าใช้งาน รวมถึงเวลาในการเข้าใช้งานแต่ละหน้า บริษัท A เป็นผู้กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลดังกล่าว ดังนั้น บริษัท A จึงเป็นผู้ควบคุมข้อมูลส่วนบุคคล เมื่อบริษัท A ได้ว่าจ้างบริษัท B ให้ทำการวิเคราะห์ข้อมูลการเข้าใช้งานเว็บไซต์ บริษัท B จึงเป็นผู้ประมวลผลข้อมูลส่วนบุคคล

ข้อกำหนด GDPR ที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูลส่วนบุคคล มีดังต่อไปนี้

1.6.1 ใช้มาตรการทางด้านเทคนิค และทางด้านองค์กรที่เหมาะสมเพื่อรักษาความปลอดภัยของการประมวลผลข้อมูลส่วนบุคคล (Data Security)

ผู้ควบคุมข้อมูลส่วนบุคคล ต้องใช้มาตรการทางด้านเทคนิค และมาตรการทางด้านองค์กรที่เหมาะสมเพื่อทำให้มั่นใจและแสดงให้เห็นว่าการประมวลผลข้อมูลส่วนบุคคลได้ดำเนินการตามข้อกำหนด และมาตรการเหล่านั้นต้องได้รับการทบทวน และปรับปรุงโดยผู้ควบคุมข้อมูลส่วนบุคคลให้ทันสมัยเท่าที่จำเป็นเสมอ[184]

---

[179] GDPR, Article 4(7).

[180] สราวุธ ปิติยาศักดิ์. (2561a). โครงการวิจัย นโยบายคลาวด์และการคุ้มครองข้อมูลส่วนบุคคลในระบบคลาวด์ระหว่างสหภาพยุโรป สหรัฐอเมริกา ออสเตรเลียและอาเซียน: มุมมองของไทย (ภาคผนวก). สำนักงานสนับสนุนกองทุนการวิจัย (สกว.), น. 17.

[181] GDPR, Article 26(1).

[182] GDPR, Article 4(8).

[183] สราวุธ ปิติยาศักดิ์. (2561a). โครงการวิจัย นโยบายคลาวด์และการคุ้มครองข้อมูลส่วนบุคคลในระบบคลาวด์ระหว่างสหภาพยุโรป สหรัฐอเมริกา ออสเตรเลียและอาเซียน: มุมมองของไทย (ภาคผนวก). สำนักงานสนับสนุนกองทุนการวิจัย (สกว.), น. 17.

[184] GDPR, Article 24(1).

นอกจากนี้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ต้องใช้มาตรการทางด้านเทคนิคและมาตรการทางด้านองค์กรที่เหมาะสม เพื่อทำให้มั่นใจว่ามีมาตรการที่เหมาะสมกับระดับความเสี่ยง โดยต้องมีมาตรการต่อไปนี้ตามความเหมาะสม[185]

(1) ทำการเข้ารหัสลับข้อมูล (Encrypt) หรือทำให้เป็นข้อมูลแฝงที่ไม่สามารถระบุตัวตนได้ (Pseudonymized)

(2) ระบบงานและบริการมีความสามารถอย่างต่อเนื่องในการเก็บรักษาความลับ (confidentiality) ความสมบูรณ์ (integrity) การเข้าถึงได้ (accessibility) และความสามารถในการรับมือต่อเหตุต่าง ๆ (resilience)

(3) มีความสามารถในการกู้คืนการเข้าถึงระบบ และข้อมูลส่วนบุคคลได้ทันท่วงทีในกรณีที่มีเหตุการณ์ทางกายภาพ หรือทางเทคนิค

(4) มีกระบวนการในการทดสอบ ประเมินประสิทธิภาพของมาตรการด้านเทคนิคและมาตรการด้านองค์การอย่างสม่ำเสมอ เพื่อให้มั่นใจในความปลอดภัยของการประมวลผลข้อมูลส่วนบุคคล

มาตรการทางด้านเทคนิคและมาตรการทางด้านองค์กร รวมถึงนโยบายคุ้มครองข้อมูลส่วนบุคคลจะต้องเป็นไปตามหลักการคุ้มครองข้อมูลส่วนบุคคลด้วยการออกแบบ (data protection by design) และการคุ้มครองข้อมูลส่วนบุคคลขั้นพื้นฐาน (data protection by default)[186] หลักการคุ้มครองข้อมูลส่วนบุคคลด้วยการออกแบบ (data protection by design) คือ ผู้ควบคุมข้อมูลส่วนบุคคลต้องใช้มาตรการทางเทคนิคและทางการจัดการองค์กรที่เหมาะสมและเพียงพอ ตั้งแต่ขั้นตอนแรกไปจนถึงขั้นตอนสุดท้ายของการออกแบบระบบงาน การบริการ ผลิตภัณฑ์ หรือการดำเนินการ โดยครอบคลุมกระบวนการทำงานตั้งแต่ต้นจนจบ ในลักษณะที่คุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นการป้องกันเชิงรุก โดยเน้นการป้องกันปัญหา เช่น ออกแบบให้ระบบมีการแจ้งเตือนหากมีการเข้าไปสู่เว็บไซต์ที่มีความเสี่ยงสูง หรือ ออกแบบให้มีการเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็น เป็นต้น ส่วนการคุ้มครองข้อมูลส่วนบุคคลโดยค่าพื้นฐาน (data protection by default) คือ ผู้ควบคุมข้อมูลต้องตรวจสอบให้แน่ใจว่าข้อมูลส่วนบุคคลถูกประมวลผลโดยมีการปกป้องความเป็นส่วนตัวสูงสุด มีการเก็บข้อมูลส่วนบุคคล และการประมวลผลเท่าที่จำเป็น และเก็บไว้เพียงระยะเวลาที่จำเป็นเท่านั้น ซึ่งหลักการนี้เชื่อมโยงกับหลักการคุ้มครองข้อมูลส่วนบุคคลในเรื่องหลักจำกัดตามวัตถุประสงค์ (Purpose Limitation) หลักการจัดเก็บข้อมูลเฉพาะที่จำเป็น (Data Minimization) และหลักข้อจำกัดในการจัดเก็บ (Storage Limitation)

1.6.2 แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer – DPO) เป็นบุคคล ซึ่งอาจเป็นพนักงานประจำของผู้ควบคุมข้อมูลส่วนบุคคลหรือของผู้ประมวลผลข้อมูลส่วนบุคคล หรือเป็นพนักงานตามสัญญาจ้างบริการก็ได้[187] ที่ได้รับมอบหมายอย่างเป็นทางการให้

---

[185] GDPR, Article 32(1).

[186] GDPR, Article 25, and Recital 78.

[187] GDPR, Article 37(6).

รับผิดชอบดูแลการปฏิบัติตามกระบวนการปกป้องข้อมูลภายในองค์กรภายใต้ GDPR ทั้งนี้ GDPR ได้มีการกำหนดแนวทางเกี่ยวกับการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและแนวทางปฏิบัติไว้ใน Guidelines for Data Protection Officers188 แต่การนำไปปฏิบัติอาจแตกต่างกันระหว่างประเทศสมาชิก เช่น กรณีที่ GDPR มิได้กำหนดให้มีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลแต่ในบางประเทศสมาชิก (เช่น ประเทศเยอรมนี และประเทศสวีเดน) ได้กำหนดให้ทุกองค์กรต้องจัดตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

อย่างไรก็ตาม GDPR ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ในกรณีดังต่อไปนี้[189]

1) การประมวลผลข้อมูลส่วนบุคคลนั้นดำเนินการโดยหน่วยงาน หรือองค์กรภาครัฐ เว้นแต่เป็นการพิจารณาคดีของศาล

2) กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลประกอบด้วยการประมวลผลข้อมูลส่วนบุคคล ซึ่งโดยลักษณะของขอบเขตและ/หรือวัตถุประสงค์ จำเป็นต้องมีการติดตามตรวจสอบข้อมูลส่วนบุคคลจำนวนมากอย่างเป็นระบบและเป็นปรกติ หรือ

3) กิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลประกอบด้วยการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว ตามมาตรา 9 และข้อมูลส่วนบุคคลที่เกี่ยวกับความผิดและโทษทางอาญาตามมาตรา 10 เป็นจำนวนมาก

ดังนั้นผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่มีการประมวลผลข้อมูลส่วนบุคคลชีวภาพ ซึ่งเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นจำนวนมากจะต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล อย่างไรก็ดีถึงแม้ว่าผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลจะไม่ตกอยู่ภายใต้ข้อบังคับที่กำหนดให้แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลอาจเลือกที่จะแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเพื่อควบคุมดูแลข้อมูลส่วนบุคคลเพื่อให้การปฏิบัติเป็นไปตามข้อกำหนดภายใต้ GDPR ได้

แม้ GDPR ไม่ได้ให้คำจำกัดความของคำว่า “จำนวนมาก” ไว้ แต่คณะทำงาน Article 29 Data Protection Working Party (WP29) ได้กำหนดแนวทางไว้ว่าควรพิจารณาจากปัจจัยดังต่อไปนี้[190]

1) จำนวนเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง ไม่ว่าจะเป็นจำนวนที่เจาะจงหรือเป็นสัดส่วนของจำนวนประชากรที่เกี่ยวข้อง

2) ปริมาณของข้อมูล และ/หรือความหลากหลายของข้อมูลที่ใช้ประมวลผล

3) ระยะเวลา หรือ ความถาวรของการประมวลผลข้อมูล

4) ขอบเขตทางภูมิศาสตร์ของกิจกรรมการประมวลผล

---

[188] Article 29 Data Protection Working Party, WP243.

[189] GDPR, Article 37(1).

[190] Article 29 Data Protection Working Party, WP243.

ตัวอย่างของการประมวลผลข้อมูลจำนวนมาก ได้แก่

1) การประมวลผลข้อมูลคนไข้ในการดำเนินกิจการตามปรกติของโรงพยาบาล

2) การประมวลผลข้อมูลการเดินทางของเจ้าของข้อมูลที่ใช้ระบบขนส่งสาธารณะ เช่น การติดตามการเดินทางด้วยบัตรเดินทาง

3) การประมวลผลตำแหน่งทางภูมิศาสตร์แบบ real time ของลูกค้าที่ใช้บริการร้านอาหารจานด่วนที่มีสาขาในประเทศต่าง ๆ ทั่วโลกเพื่อวัตถุประสงค์ด้านสถิติโดยผู้ประมวลผลที่เชี่ยวชาญในกิจกรรมเหล่านี้

4) การประมวลผลข้อมูลของลูกค้าในการดำเนินกิจการตามปรกติของบริษัทประกัน หรือธนาคาร

5) การประมวลผลข้อมูลส่วนบุคคลเพื่อนำไปใช้ในการโฆษณาโดยวิเคราะห์จากการใช้ระบบการค้นหา (search engine) ในการสืบค้นข้อมูลในอินเตอร์เน็ต

6) การประมวลผลข้อมูล ไม่ว่าจะเป็น เนื้อหา ปริมาณการเข้าถึง หรือตำแหน่งที่ตั้ง โดยผู้ให้บริการโทรศัพท์ หรือ ผู้ให้บริการอินเตอร์เน็ต

การประมวลผลข้อมูลส่วนบุคคลตามตัวอย่างดังต่อไปนี้ ไม่ถือว่าเป็นการประมวลผลจำนวนมาก

1) การประมวลผลข้อมูลส่วนบุคคลของคนไข้โดยแพทย์แต่ละคน

2) การประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับความผิดและโทษทางอาญาโดยทนายแต่ละคน

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องได้รับการคัดเลือกจากคุณสมบัติทางวิชาชีพ โดยต้องมีความรู้ความชำนาญในกฎหมายคุ้มครองข้อมูลส่วนบุคคลและแนวทางการปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล[191] รวมถึงความสามารถในการดำเนินงานตามภารกิจของตนอีกด้วย ภารกิจของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีอย่างน้อยดังต่อไปนี้[192]

1) แจ้งให้ทราบและให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างที่ดำเนินการประมวลผลข้อมูลส่วนบุคคลตามหน้าที่ ซึ่งข้อกำหนดตาม GDPR และบทบัญญัติคุ้มครองข้อมูลอื่น ๆ ที่เกี่ยวข้องของสหภาพยุโรป หรือของประเทศสมาชิก

2) ติดตามการตรวจสอบการปฏิบัติตามข้อกำหนดของ GDPR และบทบัญญัติคุ้มครองข้อมูลอื่น ๆ ที่เกี่ยวข้องของสหภาพยุโรป หรือของประเทศสมาชิก และตามนโยบายของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในส่วนที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รวมถึงมอบหมายความรับผิดชอบ การสร้างความตระหนัก และทำการฝึกอบรมพนักงานที่มีส่วนร่วมในการประมวลผลข้อมูลส่วนบุคคลและการตรวจสอบที่เกี่ยวข้อง

---

[191] GDPR, Article 37(5).

[192] GDPR, Article 39.

3) ให้คำแนะนำเกี่ยวกับการประเมินผลกระทบการคุ้มครองข้อมูลส่วนบุคคลและตรวจสอบการปฏิบัติตามมาตรา 35 เมื่อได้รับการร้องขอ

4) ให้ความร่วมมือกับหน่วยงานกำกับดูแล

5) ทำหน้าที่เป็นผู้ประสานงาน (contact point) กับหน่วยงานกำกับดูแลในประเด็นที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล รวมทั้งการปรึกษากับหน่วยงานกำกับดูแลตามมาตรา 36 และปรึกษาตามควรในเรื่องอื่น (ถ้ามี)

6) ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลเกี่ยวกับการประเมินผลกระทบการคุ้มครองข้อมูลส่วนบุคคลเมื่อได้รับการร้องขอ[193]

ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องทำให้มั่นใจได้ว่าเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลดำเนินการอย่างถูกต้องและทันการในทุกประเด็นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล[194] ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องให้การสนับสนุนการปฏิบัติงานตามมาตรา 39 ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล โดยจัดหาทรัพยากรที่จำเป็นในการดำเนินงาน การเข้าถึงข้อมูลส่วนบุคคลและการดำเนินการประมวลผลข้อมูลส่วนบุคคล และสนับสนุนการเสริมสร้างความรู้ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเพื่อให้คงระดับความเชี่ยวชาญอยู่เสมอ[195] เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องมีอิสระในการปฏิบัติหน้าที่โดยไม่ต้องรับคำสั่งจากผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล และต้องไม่ถูกไล่ออกหรือลงโทษโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเนื่องจากการปฏิบัติงานของตน เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องขึ้นตรงต่อผู้บริหารระดับสูงสุดของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล[196]

1.6.3 การประเมินผลกระทบการคุ้มครองข้อมูลส่วนบุคคลสำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูง

ผู้ควบคุมข้อมูลส่วนบุคคลต้องประเมินผลกระทบของการประมวลผลข้อมูลส่วนบุคคล (Data Privacy Impact Assessment - DPIA) ก่อนดำเนินการประมวลผลข้อมูลส่วนบุคคลในกรณีที่มีการประมวลผลข้อมูลส่วนบุคคลด้วยเทคโนโลยีใหม่ และเมื่อคำนึงถึงลักษณะ ขอบเขต บริบท และวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล มีแนวโน้มก่อให้เกิดความเสี่ยงอย่างสูงต่อสิทธิและเสรีภาพของบุคคล[197] โดยผู้ควบคุมข้อมูลส่วนบุคคลอาจขอคำแนะนำจากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเมื่อดำเนินการประเมินผลกระทบการคุ้มครองข้อมูลส่วนบุคคล[198]

---

[193] GDPR, Article 35.

[194] GDPR, Article 38(1).

[195] GDPR, Article 38(2).

[196] GDPR, Article 38(3).

[197] GDPR, Article 35(1).

[198] GDPR, Article 35(2).

ทั้งนี้การประเมินผลกระทบการคุ้มครองข้อมูลส่วนบุคคลครั้งเดียวอาจสามารถนำไปใช้กับการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงคล้ายกันเป็นชุดได้[199]

การประมวลผลข้อมูลส่วนบุคคลที่มีแนวโน้มก่อให้เกิดความเสี่ยงอย่างสูงต่อสิทธิและเสรีภาพของบุคคล ได้แก่[200]

1) การประมวลผลข้อมูลส่วนบุคคลและการจัดเก็บข้อมูลโดยวิธีการอัตโนมัติที่ส่งผลกระทบทางกฎหมายหรือผลกระทบทางอื่นที่คล้ายคลึงกันอย่างมีนัยสำคัญต่อเจ้าของข้อมูลส่วนบุคคล

2) การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวจำนวนมากตามมาตรา 9(1) หรือข้อมูลส่วนบุคคลที่เกี่ยวกับความผิดและโทษทางอาญาตามมาตรา 10 หรือ

3) การติดตามตรวจสอบอย่างเป็นระบบในส่วนที่สาธารณชนจำนวนมากสามารถเข้าถึงได้

หากผู้ควบคุมข้อมูลส่วนบุคคลทำการประเมินผลกระทบการคุ้มครองข้อมูลส่วนบุคคลแล้วผลของการประเมินชี้ให้เห็นว่าหากปราศจากมาตรการบริหารจัดการเพื่อลดความเสี่ยง (risk mitigation) โดยผู้ควบคุมข้อมูลส่วนบุคคลแล้วจะก่อให้เกิดความเสี่ยงสูง ผู้ควบคุมข้อมูลส่วนบุคคลต้องปรึกษาหน่วยงานกำกับดูแลก่อนดำเนินการประมวลผลข้อมูล[201]

1.6.4 การแจ้งถึงการรั่วไหลของข้อมูลส่วนบุคคล (Data Breach Notification)

ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งการรั่วไหลของข้อมูลส่วนบุคคลแก่หน่วยงานกำกับดูแลโดยไม่ชักช้า และภายในเวลาไม่เกิน 72 ชั่วโมงนับแต่เวลาที่ทราบถึงการรั่วไหลของข้อมูลส่วนบุคคล เว้นแต่การรั่วไหลนั้นไม่น่าเกิดความเสี่ยงต่อสิทธิและเสรีภาพของบุคคล[202] และบันทึกการรั่วไหลของข้อมูลส่วนบุคคลไว้ในเอกสาร[203] โดยการแจ้งจะต้องมีรายละเอียดดังนี้[204]

1) ลักษณะในการรั่วไหลของข้อมูลส่วนบุคคล และหากเป็นไปได้

2) ให้รวมถึงประเภทและจำนวนของเจ้าของข้อมูลส่วนบุคคล และประเภทและจำนวนรายการของข้อมูลส่วนบุคคลที่รั่วไหลด้วย

3) ชื่อและรายละเอียดในการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) หรือสถานที่ติดต่ออื่นที่สามารถขอข้อมูลเพิ่มเติมได้

4) ผลกระทบที่คาดว่าอาจเกิดจากการรั่วไหลของข้อมูลส่วนบุคคล

---

[199] GDPR, Article 35(1).

[200] GDPR, Article 35(3).

[201] GDPR, Article 36(1).

[202] GDPR Article 33(1)

[203] GDPR, Article 33(4).

[204] GDPR, Article 33(3).

5) มาตรการที่ใช้ในการดำเนินการ หรือข้อเสนอที่จะใช้ในการดำเนินการกับการรั่วไหลของข้อมูลส่วนบุคคล และในกรณีที่จำเป็นให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งมาตรการเพื่อลดผลกระทบที่อาจเกิดขึ้นได้

ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งการรั่วไหลของข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลเมื่อมีการรั่วไหลของข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงต่อสิทธิและเสรีภาพของบุคคลโดยไม่ชักช้า[205]ด้วยภาษาที่ชัดเจนและเข้าใจง่าย[206] แต่ไม่ต้องแจ้งหากผู้ควบคุมข้อมูลส่วนบุคคลมีมาตรการด้านเทคนิค และมาตรการด้านองค์กรที่เหมาะสม และมาตรการนั้นได้ถูกนำมาใช้บังคับกับข้อมูลส่วนบุคคลที่รั่วไหล โดยเฉพาะมาตรการที่ทำให้ข้อมูลส่วนบุคคลไม่สามารถอ่านได้โดยบุคคลที่ไม่ได้รับอนุญาตให้เข้าถึง เช่น การเข้ารหัส (encryption) หรือผู้ควบคุมข้อมูลส่วนบุคคลมีมาตรการที่ทำให้มั่นใจได้ว่าความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลได้หมดไปแล้ว หรือการแจ้งเตือนไม่ได้สัดส่วนกับความเสี่ยง ในกรณีเช่นนี้ ต้องมีการแจ้งไปยังสาธารณะแทนหรือมีมาตรการที่ได้ผลคล้ายกันกับการแจ้งไปยังเจ้าของข้อมูลโดยตรง[207]

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลยังไม่ได้แจ้งการรั่วไหลของข้อมูลส่วนบุคคลไปยังเจ้าของข้อมูลส่วนบุคคล หากหน่วยงานกำกับดูแลพิจารณาความน่าจะเป็นของความเสี่ยงที่อาจเกิดต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคลแล้ว หน่วยงานกำกับดูแลอาจกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการแจ้ง หรือไม่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคลได้[208]

สำหรับผู้ประมวลผลข้อมูลส่วนบุคคลต้องแจ้งการรั่วไหลของข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่ชักช้า[209]

1.6.5 การบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลและผู้แทนผู้ควบคุมข้อมูลส่วนบุคคลจะต้องมีการบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคลภายใต้ความรับผิดชอบของตน โดยมีรายละเอียดดังต่อไปนี้[210]

1) ชื่อและรายละเอียดในการติดต่อผู้ควบคุมข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลร่วม ผู้แทนผู้ควบคุมข้อมูลส่วนบุคคล และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

2) วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล

3) รายละเอียดของประเภทของเจ้าของข้อมูลส่วนบุคคล และประเภทของข้อมูลส่วนบุคคล

4) ประเภทของผู้รับข้อมูลส่วนบุคคลที่ได้รับ หรือจะได้รับการเปิดเผยข้อมูล รวมถึงผู้รับในประเทศที่สาม หรือองค์การระหว่างประเทศ

---

[205] GDPR, Article 34(1).

[206] GDPR, Article 34(2).

[207] GDPR, Article 34(3).

[208] GDPR, Article 34(4).

[209] GDPR, Article 33(2).

[210] GDPR, Article 30(1).

5) การโอนข้อมูลส่วนบุคคลไปยังประเทศที่สาม หรือองค์การระหว่างประเทศ รวมทั้งการระบุตัวตนของผู้รับโอนในประเทศที่สาม หรือองค์การระหว่างประเทศ และในกรณีของการโอนไม่ซ้ำซ้อน หรือเกี่ยวข้องกับเจ้าของข้อมูลส่วนบุคคลจำนวนจำกัด หรือเป็นการจำเป็นสำหรับวัตถุประสงค์ของผลประโยชน์ที่ชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล และผู้ควบคุมข้อมูลส่วนบุคคลได้ประเมินสถานการณ์เกี่ยวกับการโอนข้อมูลส่วนบุคคล และได้วางมาตรการป้องกันที่เหมาะสมในการคุ้มครองข้อมูลส่วนบุคคล[211]

6) ระยะเวลาในการลบข้อมูลประเภทต่าง ๆ ในกรณีที่ระบุได้

7) คำอธิบายทั่วไปของมาตรการด้านเทคนิคและมาตรการเกี่ยวกับองค์กรในการรักษาความปลอดภัย เช่น การเปลี่ยนข้อมูลให้ทำการเข้ารหัสลับข้อมูล (Encrypt) หรือทำให้เป็นข้อมูลแฝงที่ไม่สามารถระบุตัวตนได้ (Pseudonymized) ความสามารถอย่างต่อเนื่องในการเก็บรักษาความลับ (confidentiality) ความสมบูรณ์ (integrity) การเข้าถึงได้ (accessibility) และความสามารถในการรับมือต่อเหตุต่าง ๆ (resilience) และ มีความสามารถในการกู้คืนการเข้าถึงระบบ และข้อมูลส่วนบุคคลได้ทันท่วงทีในกรณีที่มีเหตุการณ์ทางกายภาพ หรือทางเทคนิค รวมถึงมีกระบวนการในการทดสอบ ประเมินประสิทธิภาพของมาตรการด้านเทคนิค และมาตรการด้านองค์การอย่างสม่ำเสมอ เพื่อให้มั่นใจในความปลอดภัยของการประมวลผลข้อมูลส่วนบุคคล[212]

ผู้ประมวลผลข้อมูลส่วนบุคคลและผู้แทนผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องมีการบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคลทุกประเภทที่ดำเนินการในนามของผู้ควบคุมข้อมูลส่วนบุคคล โดยมีรายละเอียด เช่น ชื่อและรายละเอียดในการติดต่อผู้ประมวลผลข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลอื่น ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้แทนผู้ควบคุมข้อมูลส่วนบุคคล และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล รายละเอียดของประเภทของเจ้าของข้อมูลส่วนบุคคล และประเภทของข้อมูลส่วนบุคคล เป็นต้น[213]

สำหรับผู้ควบคุมข้อมูลส่วนบุคคลที่มีพนักงานน้อยกว่า 250 คน ไม่ต้องเก็บรักษาเอกสารที่เกี่ยวกับกิจกรรมการประมวลผล เว้นแต่การประมวลผลข้อมูลส่วนบุคคลมีแนวโน้มส่งผลให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือการประมวลผลเป็นครั้งคราว หรือการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวตามมาตรา 9(1) หรือข้อมูลส่วนบุคคลที่เกี่ยวกับความผิดและโทษทางอาญาตามมาตรา 10

ดังนั้น หากมีการประมวลผลข้อมูลส่วนบุคคลประเภทชีวภาพ ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลต้องทำการบันทึกกิจกรรมการประมวลผลที่เกี่ยวกับข้อมูลส่วนบุคคลประเภทชีวภาพเสมอ

---

[211] GDPR, Article 49(1) paragraph 2.

[212] GDPR, Article 32(1).

[213] GDPR, Article 30(2).

1.7 หน้าที่อื่น ๆ ของผู้ควบคุมข้อมูลส่วนบุคคล

1.7.1 หลักการในการประมวลผลข้อมูลส่วนบุคคล (Principle of Data Processing)

ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการให้เป็นไปตามหลักการของการประมวลผลข้อมูลส่วนบุคคล (ดูรายละเอียดในบทที่ 3 หัวข้อ 1.3 หลักการคุ้มครองข้อมูลส่วนบุคคล) และมีการกำหนดฐานในการประมวลผลข้อมูลส่วนบุคคลที่ชอบด้วยกฎหมาย (ดูรายละเอียดในบทที่ 3 หัวข้อ 1.4 การประมวลผลข้อมูลส่วนบุคคลที่ชอบด้วยกฎหมาย)

1.7.2 ประกาศแจ้งรายละเอียดความเป็นส่วนตัว (Privacy Notice)

ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดทำประกาศแจ้งรายละเอียดความเป็นส่วนตัว เพื่อแจ้งให้เจ้าของข้อมูลรับทราบถึงรายละเอียดในการเก็บรวบรวม และประมวลผลข้อมูลส่วนบุคคล เช่น วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล ระยะเวลาที่ข้อมูลส่วนบุคคลดังกล่าวจะถูกจัดเก็บ และนอกเหนือจากผู้ควบคุมข้อมูลแล้วมีองค์กรใดนำข้อมูลดังกล่าวไปใช้บ้าง เป็นต้น (ดูรายละเอียดเพิ่มเติมได้ใน ตารางที่ 3.1 รายละเอียดที่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคล)

1.7.3 การทำสัญญากับผู้ประมวลผลข้อมูลส่วนบุคคล

สำหรับการทำสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับผู้ประมวลผลข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ดังต่อไปนี้

1) ผู้ควบคุมข้อมูลส่วนบุคคลต้องเลือกใช้เฉพาะผู้ประมวลผลข้อมูลส่วนบุคคลที่สามารถให้การประกันได้ตามสมควรว่าจะใช้มาตรการด้านเทคนิค และมาตรการด้านองค์กรที่เหมาะสมในการประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามข้อจำกัดของ GDPR และสามารถสร้างความมั่นใจในการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล[214]

2) ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่กำหนดลักษณะ และระยะเวลาของการประมวลผลข้อมูลส่วนบุคคล วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล ประเภทของข้อมูลส่วนบุคคล ประเภทของเจ้าของข้อมูลส่วนบุคคล โดยมีการกำหนดไว้ในสัญญาหรือการกระทำทางกฎหมายอื่นภายใต้กฎหมายสหภาพยุโรปหรือกฎหมายของประเทศสมาชิกที่มีผลผูกพันระหว่างผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล[215]

ผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ดังต่อไปนี้

1) ผู้ประมวลผลข้อมูลส่วนบุคคลต้องไม่มอบหมายให้ผู้ประมวลผลข้อมูลส่วนบุคคลอื่นประมวลผลข้อมูลส่วนบุคคลโดยมิได้รับอนุญาตเป็นลายลักษณ์อักษรเป็นการเฉพาะหรือเป็นการทั่วไป สำหรับกรณีที่การอนุญาตเป็นการทั่วไปผู้ประมวลผลข้อมูลส่วนบุคคลต้องแจ้งผู้ควบคุมข้อมูลส่วนบุคคลให้ทราบถึงการเปลี่ยนแปลงเกี่ยวกับการเพิ่มผู้ประมวลผลข้อมูลส่วนบุคคลอื่น หรือการทดแทนผู้ประมวลผลข้อมูลส่วนบุคคลอื่น ซึ่งทำให้ผู้ควบคุมข้อมูลส่วนบุคคลมีโอกาสคัดค้านการเปลี่ยนแปลงดังกล่าว[216]

---

[214] GDPR, Article 28(1).

[215] GDPR, Article 28(3).

[216] GDPR, Article 28(2).

2) ผู้ประมวลผลข้อมูลส่วนบุคคลต้องประมวลผลข้อมูลส่วนบุคคลเฉพาะตามคำสั่งที่เป็นเอกสารจากผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งรวมทั้งเรื่องการโอนข้อมูลส่วนบุคคลไปยังประเทศที่สาม หรือองค์การระหว่างประเทศด้วย ยกเว้นแต่มีความจำเป็นที่ต้องดำเนินการประมวลผลข้อมูลตามกฎหมายสหภาพยุโรปหรือกฎหมายของประเทศสมาชิกที่ผู้ประมวลผลข้อมูลส่วนบุคคลอยู่ใต้บังคับ ทั้งนี้ผู้ประมวลผลข้อมูลส่วนบุคคลต้องแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบก่อนการประมวลผลข้อมูลส่วนบุคคล เว้นแต่กฎหมายห้ามมิให้แจ้งด้วยเหตุผลของประโยชน์สาธารณะ[217]

3) ผู้ประมวลผลข้อมูลส่วนบุคคลต้องทำให้เป็นที่มั่นใจว่าผู้มีอำนาจในการประมวลผลได้ผูกพันตนในการเก็บรักษาความลับ หรืออยู่ภายใต้หน้าที่ตามกฎหมายในการเก็บรักษาความลับ[218]

4) ผู้ประมวลผลข้อมูลส่วนบุคคลต้องใช้มาตรการการรักษาความปลอดภัยทั้งหมดที่จำเป็นตามมาตรา 32[219]

5) สำหรับการปฏิบัติตามหน้าที่ของผู้ควบคุมส่วนบุคคลในการตอบคำร้องขอในการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลต้องให้ความช่วยเหลือผู้ควบคุมข้อมูลส่วนบุคคลโดยมาตรการด้านเทคนิค และมาตรการด้านองค์กรที่เหมาะสมเท่าที่เป็นไปได้[220]

6) ผู้ประมวลผลข้อมูลส่วนบุคคลต้องให้ความช่วยเหลือผู้ควบคุมข้อมูลส่วนบุคคลในการตรวจสอบการปฏิบัติหน้าที่ตามมาตรา 32 ถึง 36[221]

7) ภายหลังสิ้นสุดการให้บริการเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลต้องทำการลบ หรือส่งกลับข้อมูลส่วนบุคคลทั้งหมดไปยังผู้ควบคุมส่วนบุคคล โดยเป็นไปตามความประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคล และลบสำเนาทั้งหมดที่มีอยู่ เว้นแต่กฎหมายสหภาพยุโรป หรือกฎหมายของประเทศสมาชิกกำหนดให้ต้องเก็บรักษาข้อมูลส่วนบุคคลนั้นไว้[222]

8) ผู้ประมวลผลข้อมูลส่วนบุคคลต้องเปิดเผยข้อมูลทั้งหมดที่จำเป็นต่อการพิสูจน์ให้เห็นถึงการปฏิบัติตามหน้าที่ตามที่กำหนดไว้ในมาตรา 28 รวมทั้งต้องแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบโดยทันทีหากคำสั่งใดละเมิดข้อกำหนด GDPR หรือบทบัญญัติใดที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป หรือของประเทศสมาชิก[223]

---

[217] GDPR, Article 28(3)(a).

[218] GDPR, Article 28(3)(b).

[219] GDPR, Article 28(3)(c).

[220] GDPR, Article 28(3)(e).

[221] GDPR, Article 28(3)(f).

[222] GDPR, Article 28(3)(g).

[223] GDPR, Article 28(3)(h).

9) หากผู้ประมวลผลข้อมูลส่วนบุคคลได้มอบหมายให้ผู้ประมวลผลข้อมูลส่วนบุคคลอื่นดำเนินการประมวลผลข้อมูลส่วนบุคคลเฉพาะส่วนในนามของผู้ควบคุมข้อมูลส่วนบุคคล หน้าที่คุ้มครองข้อมูลส่วนบุคคลที่กำหนดไว้ในสัญญาหรือการกระทำทางกฎหมายระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับผู้ประมวลผลข้อมูลส่วนบุคคล จะถูกนำไปใช้บังคับกับผู้ประมวลผลข้อมูลส่วนบุคคลอื่นภายใต้กฎหมายสหภาพยุโรป หรือกฎหมายของประเทศสมาชิก โดยเฉพาะการมีหลักประกันอย่างเพียงพอในการใช้มาตรการด้านเทคนิค และมาตรการด้านองค์การที่เหมาะสมในการประมวลผลข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลแรกต้องรับผิดอย่างเต็มที่ต่อผู้คุ้มครองข้อมูลส่วนบุคคลในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลอื่นไม่ปฏิบัติตามหน้าที่คุ้มครองข้อมูลส่วนบุคคล[224]

1.7.4 กำหนดหน้าที่ความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคลร่วม

ผู้ควบคุมข้อมูลส่วนบุคคลร่วมต้องกำหนดหน้าที่ความรับผิดชอบของแต่ละคนอย่างโปร่งใส และต้องสอดคล้องกับหน้าที่ตาม GDPR โดยเฉพาะในส่วนที่เกี่ยวข้องกับสิทธิของเจ้าของข้อมูลส่วนบุคคลและการปฏิบัติหน้าที่ในการให้ข้อมูลตามมาตรา 13 และ 14 การกำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลร่วมนั้นให้กระทำโดยข้อตกลง เว้นแต่กฎหมายสหภาพยุโรป หรือกฎหมายของประเทศสมาชิกที่ผู้ควบคุมข้อมูลส่วนบุคคลอยู่ภายใต้บังคับได้กำหนดหน้าที่ความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคลร่วมไว้เป็นการเฉพาะ ทั้งนี้ข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลร่วมอาจกำหนดสถานที่ติดต่อให้แก่เจ้าของข้อมูลด้วยก็ได้[225]

1.7.5 แจ้งการแก้ไข หรือการลบข้อมูลส่วนบุคคล หรือการจำกัดการประมวลผลข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่แจ้งการแก้ไข หรือการลบข้อมูลส่วนบุคคลหรือการจำกัดการประมวลผลข้อมูลส่วนบุคคลตามมาตรา 16 มาตรา 17(1) และมาตรา 18 ไปยังผู้รับการเปิดเผยข้อมูลส่วนบุคคลแต่ละคน เว้นแต่ไม่อาจแจ้งได้หรือได้ใช้ความพยายามอย่างเพียงพอในการแจ้งแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเจ้าของข้อมูลส่วนบุคคลเกี่ยวกับผู้รับเหล่านั้นหากเจ้าของข้อมูลส่วนบุคคลได้ร้องขอ[226]

1.8 การร้องเรียน

1.8.1 หน่วยงานกำกับดูแล

GDPR กำหนดให้ประเทศสมาชิกจัดตั้งหน่วยงานอิสระเพื่อกำกับดูแล (supervisory authority) อย่างน้อยหนึ่งหน่วยงาน โดยทำหน้าที่รับผิดชอบในการตรวจสอบการบังคับใช้กฎข้อบังคับของ GDPR เพื่อคุ้มครองสิทธิและเสรีภาพขั้นพื้นฐานของบุคคลธรรมดาที่เกี่ยวกับการประมวลข้อมูล และอำนวยความสะดวกในการไหลเวียนโดยเสรีของข้อมูลภายในสหภาพยุโรป[227] อีกทั้งต้องนำกฎข้อบังคับของ GDPR ไปใช้บังคับให้สอดคล้องเป็นมาตรฐานเดียวกันทั่วทั้ง

---

[224] GDPR, Article 28(4).

[225] GDPR, Article 26(1).

[226] GDPR, Article 19.

[227] GDPR, Article 51(1).

สหภาพยุโรป[228] ในกรณีที่ประเทศสมาชิกจัดตั้งหน่วยงานกำกับดูแลมากกว่าหนึ่งหน่วยงานให้ประเทศสมาชิกกำหนดให้หน่วยงานกำกับดูแลหนึ่งหน่วยงานเป็นผู้แทนของหน่วยงานทั้งหมด[229]

หน่วยงานกำกับดูแลต้องมีความอิสระอย่างสมบูรณ์ในการปฏิบัติภารกิจและการใช้อำนาจ[230] ที่ได้รับมอบหมายอย่างเป็นทางการโดยสอดคล้องกับข้อกำหนด GDPR ภายในประเทศของตน[231] ทั้งนี้หน่วยงานกำกับดูแลไม่มีอำนาจหน้าที่ในการกำกับดูแลการประมวลผลข้อมูลส่วนบุคคลของศาลในการพิจารณาพิพากษาคดี[232]

อำนาจหน้าที่ของหน่วยงานกำกับดูแลครอบคลุมถึงการประมวลผลข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลในประเทศของตน รวมถึงการประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการโดยหน่วยงานภาครัฐ หน่วยงานภาคเอกชนที่ดำเนินงานเพื่อประโยชน์สาธารณะ และการประมวลผลข้อมูลส่วนบุคคลที่กระทบเจ้าของข้อมูลส่วนบุคคลที่อยู่ในประเทศตน หรือการประมวลผลข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลที่มิได้อยู่ในสหภาพยุโรปสำหรับกรณีที่เจ้าของข้อมูลส่วนบุคคลอยู่ในประเทศของตน นอกจากนี้หน่วยงานกำกับดูแลยังมีหน้าที่ดำเนินการเกี่ยวกับคำร้องจากเจ้าของข้อมูลส่วนบุคคล ดำเนินการสืบสวนเกี่ยวกับการบังคับใช้ข้อกำหนด GDPR ส่งเสริมให้ประชาชนตระหนักรู้ถึงความเสี่ยง กฎระเบียบ และการคุ้มครอง รวมถึงสิทธิต่าง ๆ ที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล[233] นอกจากนี้ยังมีหน้าที่สำคัญตามข้อกำหนด GDPR ดังที่บัญญัติไว้ในมาตรา 57 เช่น ติดตามตรวจสอบและบังคับใช้ข้อกำหนด GDPR ให้ความร่วมมือ แบ่งปันข้อมูลและให้ความช่วยเหลือหน่วยงานกำกับดูแลอื่น ตรวจสอบพัฒนาการที่มีผลกระทบต่อการคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะพัฒนาการทางด้านเทคโนโลยีสารสนเทศ และการสื่อสาร เป็นต้น

อำนาจที่สำคัญของหน่วยงานกำกับดูแลในการดำเนินงาน ได้แก่

1) อำนาจตรวจสอบหาความจริง เช่น สั่งให้ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล ผู้แทนผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้แทนผู้ประมวลผลข้อมูลส่วนบุคคลให้ข้อมูลที่ต้องใช้สำหรับการปฏิบัติงานของตน แจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลทราบข้อกล่าวหาการละเมิดข้อบังคับ เข้าถึงข้อมูลส่วนบุคคลและข้อมูลทั้งหมดในความดูแลของผู้ควบคุมข้อมูลส่วนบุคคล และ ผู้ประมวลผลข้อมูลส่วนบุคคลเท่าที่จำเป็นสำหรับการทำงานของตน[234] เป็นต้น

2) อำนาจสั่งให้ดำเนินการแก้ไขให้ถูกต้อง เช่น สั่งผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ให้ดำเนินการประมวลผลข้อมูลให้สอดคล้องกับบทบัญญัติของ

---

[228] GDPR, Article 51(2).

[229] GDPR, Article 51(3).

[230] GDPR, Article 52(1).

[231] GDPR, Article 55(1).

[232] GDPR, Article 55(3).

[233] GDPR, Recital 122.

[234] GDPR, Article 58(1).

ข้อกำหนดนี้ สั่งผู้ควบคุมข้อมูลส่วนบุคคลให้แจ้งการรั่วไหลของข้อมูลส่วนบุคคลไปยังเจ้าของข้อมูลส่วนบุคคล กำหนดค่าปรับทางปกครองตามมาตรา 83 หรือมาตรการทดแทนที่ขึ้นอยู่กับสถานการณ์ของแต่ละกรณี สั่งให้ระงับการส่งหรือโอนข้อมูลไปยังผู้รับในประเทศที่สามหรือองค์การระหว่างประเทศ[235] เป็นต้น

3) อนุมัติและให้คำปรึกษาในกรณีต่าง ๆ เช่น ให้คำแนะนำผู้ควบคุมข้อมูลส่วนบุคคลตามขั้นตอนการให้คำปรึกษาก่อนการประมวลผล ให้ความเห็นและอนุมัติร่างประมวลจริยธรรม ให้การรับรองกฎเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร[236] เป็นต้น

1.8.2 กระบวนการร้องเรียน

หากเจ้าของข้อมูลส่วนบุคคลพิจารณาแล้วเห็นว่าการประมวลผลข้อมูลส่วนบุคคลของตนละเมิดข้อกำหนด GDPR เจ้าของข้อมูลส่วนบุคคลมีสิทธิยื่นคำร้องต่อหน่วยงานกำกับดูแลของประเทศสมาชิกซึ่งเป็นถิ่นที่อยู่ หรือสถานที่ทำงานของตน หรือสถานที่ของการทำละเมิด หน่วยงานกำกับดูแลดังกล่าวมีหน้าที่ดำเนินการเกี่ยวกับคำร้องจากเจ้าของข้อมูลส่วนบุคคล และแจ้งความคืบหน้าของการตรวจสอบหรือผลของคำร้อง รวมถึงความเป็นไปได้ของการได้รับการเยียวยาทางศาลให้เจ้าของข้อมูลส่วนบุคคลทราบ[237] โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิได้รับการเยียวยาทางศาลที่มีประสิทธิภาพตามกฎหมาย[238] ทั้งนี้หน่วยงานกำกับดูแลจะต้องแจ้งความคืบหน้าหรือผลของการร้องเรียนภายใน 3 เดือนนับแต่ได้รับคำร้อง[239] เจ้าของข้อมูลส่วนบุคคลมีสิทธิได้รับการเยียวยาทางศาลตามมาตรา 47 ของกฎบัตรเกี่ยวกับสิทธิขั้นพื้นฐานของสหภาพยุโรป (Charter of Fundamental Rights of the European Union) หากสิทธิของเจ้าของข้อมูลส่วนบุคคลภายใต้ข้อกำหนด GDPR ถูกละเมิด หรือเมื่อหน่วยงานกำกับดูแลไม่ตอบสนองคำร้อง ปฏิเสธคำร้องหรือยกคำร้องไม่ว่าจะบางส่วนหรือทั้งหมด หรือไม่ปฏิบัติหน้าที่ในการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล โดยเจ้าของข้อมูลส่วนบุคคลสามารถยื่นคำร้องได้ทั้งด้วยวาจาหรือโดยลายลักษณ์อักษรหรือทางอิเล็กทรอนิกส์[240]

เจ้าของข้อมูลส่วนบุคคลมีสิทธิยื่นฟ้องหน่วยงานกำกับดูแล โดยยื่นคำฟ้องต่อศาลของประเทศสมาชิกที่หน่วยงานกำกับดูแลนั้นตั้งอยู่[241] ทั้งนี้เจ้าของข้อมูลส่วนบุคคลมีสิทธิยื่นฟ้องหน่วยงานกำกับดูแลในกรณีที่หน่วยงานกำกับดูแลไม่ดำเนินการจัดการกับคำร้อง หรือไม่แจ้งเจ้าของข้อมูลส่วนบุคคลให้ทราบถึงความคืบหน้าหรือผลของคำร้องภายใน 3 เดือน หรือเจ้าของข้อมูลส่วนบุคคลต้องการอุทธรณ์คำตัดสินของหน่วยงานกำกับดูแล[242]

---

[235] GDPR, Article 58(2).

[236] GDPR, Article 58(3).

[237] GDPR, Article 77.

[238] GDPR, Article 78(1).

[239] GDPR, Article 78(2).

[240] GDPR, Recital 141.

[241] GDPR, Article 78(3).

[242] GDPR, Article 78(4).

เมื่อเจ้าของข้อมูลส่วนบุคคลเห็นว่าผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลกระทำการละเมิดสิทธิของตนภายใต้ข้อกำหนด GDPR เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการฟ้องคดีต่อผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล โดยฟ้องยังศาลของประเทศสมาชิกที่ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลมีสถานประกอบการอยู่ หรือฟ้องยังศาลของประเทศสมาชิกที่เจ้าของข้อมูลส่วนบุคคลมีถิ่นที่อยู่ เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นหน่วยงานรัฐของประเทศสมาชิก[243]

1.9 การเยียวยา และบทลงโทษ

1.9.1 การเยียวยา

ภายใต้ข้อกำหนด GDPR บุคคลที่ได้รับความเดือดร้อนหรือความเสียหายแก่ทรัพย์สิน หรือสิ่งอื่นใดอันเป็นผลจากการละเมิดข้อกำหนดนี้ มีสิทธิได้รับค่าสินไหมทดแทนจากผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลสำหรับความเสียหายที่เกิดขึ้นนั้น[244] ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นจากการประมวลผลข้อมูลส่วนบุคคลที่ละเมิดข้อกำหนดนี้ ส่วนผู้ประมวลผลข้อมูลส่วนบุคคลต้องรับผิดชอบจากการประมวลผลข้อมูลส่วนบุคคลต่อเมื่อกระทำการขัดกับหน้าที่ที่กำหนดไว้โดยเฉพาะสำหรับประมวลผลข้อมูลส่วนบุคคลตามข้อกำหนดนี้ หรือขัดกับคำสั่งที่ชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล[245] แต่ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลสามารถพิสูจน์ได้ว่าตนไม่ต้องรับผิดชอบต่อเหตุการณ์ที่ก่อให้เกิดความเสียหายนั้น ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอาจหลุดพ้นความรับผิดได้[246]

เจ้าของข้อมูลส่วนบุคคลอาจมอบอำนาจให้องค์กรที่ไม่แสวงหาผลกำไร ซึ่งเป็นองค์กรหรือสมาคมที่จัดตั้งขึ้นโดยชอบด้วยกฎหมายของประเทศสมาชิกที่มีวัตถุประสงค์เพื่อประโยชน์สาธารณะ และทำงานด้านการคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลทำการใช้สิทธิเรียกค่าสินไหมทดแทนในนามของเจ้าของข้อมูลส่วนบุคคลได้[247] ทั้งนี้ประเทศสมาชิกอาจกำหนดให้องค์กรดังกล่าวมีสิทธิในการยื่นฟ้องกับหน่วยงานกำกับดูแลที่มีอำนาจตามมาตรา 77 และใช้สิทธิตามมาตรา 78 และ 79 โดยมิต้องได้รับการแต่งตั้งจากเจ้าของข้อมูลส่วนบุคคล หากเห็นว่ามีการละเมิดสิทธิของเจ้าของข้อมูลส่วนบุคคลภายใต้ข้อกำหนดนี้เนื่องจากการประมวลผลข้อมูลส่วนบุคคล[248]

ตัวอย่าง ในปี ค.ศ. 2018 สององค์กร None Of Your Business (“NOYB”) องค์กรไม่แสวงหากำไรที่มีสำนักงานใหญ่อยู่ในประเทศออสเตรีย และ La Quadrature du Net (“LQDN”) องค์กรไม่แสวงหากำไรในประเทศฝรั่งเศส ได้ยื่นคำร้องต่อหน่วยงานกำกับดูแลของ

---

[243] GDPR, Article 79.

[244] GDPR, Article 82(1).

[245] GDPR, Article 82(2).

[246] GDPR, Article 82(3).

[247] GDPR, Article 80(1).

[248] GDPR, Article 80(2).

ประเทศฝรั่งเศส National Data Protection Commission (CNIL) โดย LQDN ได้รับการแต่งตั้งจากเจ้าของข้อมูลส่วนบุคคล 10,000 คนเพื่อให้เป็นตัวแทนในการเรียกค่าสินไหมทดแทนในนามของเจ้าของข้อมูลส่วนบุคคล ซึ่ง CNIL ได้ตัดสินให้ปรับ Google เป็นจำนวนเงิน 50 ล้านยูโร จากการละเมิดหลักการความโปร่งใส ตามมาตรา 5 การให้รายละเอียด และการเข้าถึงข้อมูลตามมาตรา 13 และมาตรา 14 และการประมวลผลโดยชอบด้วยกฎหมายตามมาตรา 6[249]

ตัวอย่าง เจ้าของข้อมูลส่วนบุคคลซึ่งเป็นอดีตพนักงานของบริษัทแห่งหนึ่งในสาธารณรัฐเช็กได้ยื่นคำร้องต่อหน่วยงานกำกับดูแลในสาธารณรัฐเช็ก Czech Data Protection Authority (UOOU) ว่าบริษัทดังกล่าวไม่ยอมลบข้อมูลส่วนบุคคลของตนแม้ว่าเจ้าของข้อมูลส่วนบุคคลจะมิได้เป็นพนักงานของบริษัทดังกล่าวแล้วก็ตาม บริษัทดังกล่าวได้ถูกปรับเป็นเงินจำนวน 388 ยูโร จากการละเมิดการประมวลผลโดยชอบด้วยกฎหมายตามมาตรา 6[250]

1.9.2 บทลงโทษ

ข้อกำหนด GDPR ได้กำหนดบทลงโทษสำหรับผู้กระทำการฝ่าฝืนข้อกำหนดในรูปของค่าปรับทางปกครอง โดยหน่วยงานกำกับดูแลมีหน้าที่ต้องทำให้เชื่อมั่นได้ว่าค่าปรับทางปกครองสำหรับการละเมิดข้อกำหนด GDPR นั้นมีประสิทธิภาพ ได้สัดส่วน และป้องปรามการกระทำในแต่ละคดีได้[251]

ทั้งนี้ค่าปรับขึ้นอยู่กับสถานการณ์ของแต่ละคดี โดยหน่วยงานกำกับดูแลอาจกำหนดเพิ่มเติมจากค่าปรับหรือแทนที่ค่าปรับด้วยมาตรการดังต่อไปนี้[252]

1) ออกคำเตือนไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่การดำเนินการประมวลผลข้อมูลส่วนบุคคลมีแนวโน้มที่จะละเมิดบทบัญญัติของข้อกำหนดนี้

2) ออกคำตำหนิไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่การดำเนินการประมวลผลข้อมูลส่วนบุคคลได้ละเมิดบทบัญญัติของข้อกำหนดนี้

3) สั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติตามคำร้องขอในการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามข้อกำหนด

4) สั่งผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลให้ดำเนินการประมวลผลข้อมูลส่วนบุคคลให้สอดคล้องกับบทบัญญัติของข้อกำหนด ในลักษณะที่ระบุไว้และภายในระยะเวลาที่กำหนด

5) สั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งการรั่วไหลของข้อมูลส่วนบุคคลไปยังเจ้าของข้อมูลส่วนบุคคล

6) กำหนดข้อจำกัดชั่วคราว หรือข้อกำหนดเด็ดขาดซึ่งอาจรวมถึงการห้ามการประมวลผลข้อมูลส่วนบุคคล

---

[249] CNIL. (2019). The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC. สืบค้นจาก https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

[250] ที่มา: https://www.privacyaffairs.com/gdpr-fines/

[251] GDPR, Article 83(1).

[252] GDPR, Article 83(2).

7) สั่งให้มีการปรับปรุงแก้ไขหรือลบข้อมูลส่วนบุคคลหรือข้อจำกัดของการประมวลผลข้อมูลส่วนบุคคลตามมาตรา 16 มาตรา 17 และมาตรา 18 และแจ้งการกระทำดังกล่าวไปยังผู้รับซึ่งได้รับการเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 17(2) และมาตรา 19

8) ถอนใบรับรองหรือสั่งให้องค์กรที่ออกใบรับรองถอนใบรับรองที่ออกตามมาตรา 42 และมาตรา 43 หรือสั่งองค์กรที่ออกใบรับรองให้ไม่ออกใบรับรองในกรณีคุณสมบัติการได้ใบรับรองไม่ครบหรือขาดคุณสมบัติ

9) สั่งระงับการโอนข้อมูลส่วนบุคคลไปยังผู้รับในประเทศที่สามหรือองค์การระหว่างประเทศ

ทั้งนี้ ในการพิจารณากำหนดจำนวนเงินค่าปรับทางปกครองหน่วยงานกำกับดูแลต้องคำนึงถึงประเด็นต่าง ๆ ดังต่อไปนี้[253]

1) ลักษณะ ความรุนแรง และระยะเวลาของการละเมิด โดยคำนึงถึงขอบเขตลักษณะ หรือวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล รวมถึงจำนวนเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ และระดับความเสียหายของเจ้าของข้อมูลส่วนบุคคลที่ได้รับความเดือดร้อน

2) การกระทำละเมิดนั้นเป็นการกระทำโดยเจตนา หรือเป็นการกระทำโดยประมาท

3) การดำเนินการที่ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลได้กระทำเพื่อบรรเทาความเสียหายที่เกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล

4) ระดับความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงมาตรการด้านเทคนิคและมาตรการด้านองค์กรที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลตามมาตรา 25 และมาตรา 32

5) การละเมิดครั้งก่อนหน้าที่เกิดจากการกระทำของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล

6) ระดับของการให้ความร่วมมือกับหน่วยงานกำกับดูแลโดยผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลเพื่อแก้ไขการละเมิดสิทธิ หรือบรรเทาผลกระทบที่อาจเกิดขึ้นจากการละเมิด

7) ประเภทของข้อมูลส่วนบุคคลที่ได้รับผลกระทบจากการละเมิด

8) วิธีการที่หน่วยงานกำกับดูแลได้รับทราบถึงการละเมิดข้อมูลส่วนบุคคลและการแจ้งการละเมิดข้อมูลส่วนบุคคลได้กระทำโดยผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลหรือไม่

9) หน่วยงานกำกับดูแลได้เคยใช้อำนาจสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการแก้ไขตามมาตรา 58(2) ในประเด็นเดียวกันหรือไม่

10) ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลได้ปฏิบัติตามประมวลจริยธรรมตามมาตรา 40 หรือกลไกการออกใบรับรองตามมาตรา 42 หรือไม่

---

[253] GDPR, Article 83(2).

11) เหตุเพิ่มโทษหรือลดโทษอื่นที่ใช้บังคับได้กับกรณี เช่น ประโยชน์ทางการเงินที่ได้รับ หรือความเสียหายที่อาจหลีกเลี่ยงได้ ไม่ว่าจะเป็นทั้งโดยตรงหรือโดยอ้อม

กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลจงใจหรือประมาทเลินเล่อในการประมวลผลข้อมูลส่วนบุคคลกรรมเดียว หรือหลายกรรมต่อเนื่องกัน โดยละเมิดบทบัญญัติในข้อกำหนดหลายบท ให้กำหนดจำนวนเงินค่าปรับได้ไม่เกินจำนวนเงินค่าปรับที่มีอัตราสูงสุด[254]

การละเมิดบทบัญญัติของ GDPR ต้องระวางโทษทางปกครองไม่เกิน 10,000,000 ยูโร หรือในกรณีขององค์กรธุรกิจ (undertakings[255]) ต้องระวางค่าปรับทางปกครองไม่เกินร้อยละ 2 ของมูลค่ายอดขายทั่วโลกของปีงบประมาณก่อนหน้า แล้วแต่จำนวนใดจะสูงกว่า ในกรณีดังต่อไปนี้[256]

1) หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลตามมาตรา 8 มาตรา 11 มาตรา 25 ถึงมาตรา 39 มาตรา 42 และมาตรา 43

2) หน้าที่ขององค์กรที่ได้รับการรับรองตามมาตรา 42 และมาตรา 43

3) หน้าที่ขององค์กรติดตามการตรวจสอบตามมาตรา 41(4)

การละเมิดบทบัญญัติ GDPR ต้องระวางโทษทางปกครองไม่เกิน 20,000,000 ยูโร หรือในกรณีขององค์กรธุรกิจ (undertakings) ต้องระวางค่าปรับทางปกครองไม่เกินร้อยละ 4 ของมูลค่ายอดขายทั่วโลกของปีงบประมาณก่อนหน้า แล้วแต่จำนวนใดจะสูงกว่า ในกรณีดังต่อไปนี้[257]

1) หลักเกณฑ์สำหรับการประมวลผลข้อมูลส่วนบุคคลรวมทั้งเงื่อนไขในการได้รับความยินยอม ตามมาตรา 5 มาตรา 6 มาตรา 7 และมาตรา 9

2) สิทธิของเจ้าของข้อมูลส่วนบุคคล ตามมาตรา 12 ถึงมาตรา 22

3) การโอนข้อมูลส่วนบุคคลไปยังผู้รับในประเทศที่สาม หรือองค์การระหว่างประเทศตามมาตรา 44 ถึงมาตรา 49

4) หน้าที่ใด ๆ ตามกฎหมายของประเทศสมาชิกที่รับรองภายใต้หมวด 9

5) การไม่ปฏิบัติตามคำสั่ง หรือข้อจำกัดชั่วคราว หรือถาวรเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล หรือระงับการโอนข้อมูลส่วนบุคคลของหน่วยงานกำกับดูแลตามมาตรา 58(2) หรือการไม่จัดให้มีการเข้าถึงข้อมูลอันเป็นการละเมิดตามมาตรา 58(1)

นอกจากนี้ การไม่ปฏิบัติตามคำสั่งของหน่วยงานกำกับดูแลตามมาตรา 58(2) ต้องระวางโทษทางปกครองไม่เกิน 20,000,000 ยูโร หรือในกรณีขององค์กรธุรกิจ (undertakings)

---

[254] GDPR, Article 83(3).

[255] undertakings หมายถึงองค์กรธุรกิจ (จาก วาทิณี คำดี. (2561). ปัญหากฎหมายเกี่ยวกับการดำเนินคดีเพื่อเรียกร้องค่าเสียหายกรณีร่วมกัน กำหนดราคาอันเป็นการผูกขาดหรือลดการแข่งขันหรือจำกัดการแข่งขัน. (นิติศาสตรมหาบัณฑิต กลุ่มวิชากฎหมายธุรกิจ), มหาวิทยาลัยศรีปทุม, กรุงเทพฯ. น.41.)

[256] GDPR, Article 83(4).

[257] GDPR, Article 83(5).

ต้องระวางค่าปรับทางปกครองไม่เกินร้อยละ 4 ของมูลค่ายอดขายทั่วโลกของปีงบประมาณก่อนหน้า แล้วแต่จำนวนใดจะสูงกว่า[258]

ตัวอย่าง หน่วยงานกำกับดูแลของประเทศเนเธอร์แลนด์ (The Dutch Data Protection Authority - AP) ได้สั่งปรับบริษัทแห่งหนึ่งเป็นจำนวนเงิน 725,000 ยูโร เมื่อพบว่าบริษัทนั้นได้กระทำการละเมิดบทบัญญัติของ GDPR เนื่องจากมีการเก็บข้อมูลชีวภาพโดยมิชอบด้วยกฎหมาย หลังจากการพิจารณาสอบสวนแล้ว AP พบว่าบริษัทแห่งนั้นไม่สามารถแสดงให้เห็นถึงความจำเป็นในการใช้ข้อมูลชีวภาพไม่ว่าจะเป็นเพื่อการยืนยันตัวตน หรือเพื่อการรักษาความปลอดภัย[259]

2. หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลประเภทชีวภาพตามกฎหมายสหราชอาณาจักร

เมื่อ GDPR มีผลบังคับใช้ในวันที่ 25 พฤษภาคม พ.ศ. 2561 ในขณะที่สหราชอาณาจักรยังมีสถานะเป็นหนึ่งในประเทศสมาชิกของสหภาพยุโรป ดังนั้น GDPR จึงมีผลบังคับใช้ในสหราชอาณาจักรเช่นเดียวกับประเทศสมาชิกอื่น ๆ อย่างไรก็ดี สหราชอาณาจักรได้ออกจากการเป็นประเทศสมาชิกของสหภาพยุโรปอย่างเป็นทางการ เมื่อวันที่ 31 มกราคม พ.ศ. 2563 และได้เข้าสู่ช่วงการเปลี่ยนผ่าน ซึ่งกินเวลาทั้งหมด 11 เดือน และจะสิ้นสุดลงในวันที่ 31 ธันวาคม พ.ศ. 2563 ในช่วงการเปลี่ยนผ่านนั้น สหราชอาณาจักรยังคงอยู่ภายใต้บังคับของกฎหมายสหภาพยุโรป ซึ่งรวมถึง GDPR ด้วย อย่างไรก็ดีสหราชอาณาจักรได้บัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือ Data Protection Act 2018 (DPA) ซึ่งนำเอาหลักการของ GDPR มาใช้ ทั้งนี้ในช่วงของการเปลี่ยนผ่านกฎหมาย GDPR และ DPA จะมีผลบังคับใช้ในสหราชอาณาจักรทั้งสองฉบับ เมื่อหมดช่วงการเปลี่ยนผ่านสหราชอาณาจักรไม่อยู่ภายใต้กฎหมายสหภาพยุโรปอีกต่อไปจะมีการแปลง GDPR เป็นกฎหมายภายในของสหราชอาณาจักรภายใต้ European Union (Withdrawal) Act โดยอาจมีการแก้ไขปรับเปลี่ยนในบางส่วน ดังนั้น กฎหมายภายในฉบับดังกล่าวจะเป็นกฎหมายที่คุ้มครองข้อมูลส่วนบุคคลที่สหราชอาณาจักรใช้ควบคู่ไปกับ DPA อย่างไรก็ตาม GDPR ได้อนุญาตให้ประเทศสมาชิกทำการปรับเปลี่ยนบางอย่างเพื่อให้สอดคล้องกับข้อกำหนดภายในของแต่ประเทศสมาชิกอยู่แล้ว ดังนั้น DPA จึงได้ปรับข้อกำหนดบางส่วนใน GDPR เช่น การกำหนดเงื่อนไขที่เฉพาะเจาะจงสำหรับการประมวลผลข้อมูลที่มีความละเอียดอ่อน และการกำหนดข้อยกเว้นบางอย่างเฉพาะสำหรับสหราชอาณาจักร นอกจากนี้ยังมีกำหนดกฎระเบียบและการบังคับใช้ในสหราชอาณาจักรอีกด้วย[260]

---

[258] GDPR, Article 83(6).

[259] AP imposes GDPR fine for processing biometric data without a demonstrated authentication or security need. (2020). *Insights*. สืบค้นจาก Osborne Clarke website: https://www.osborneclarke.com/insights/ap-imposes-gdpr-fine-processing-biometric-data-without-demonstrated-authentication-security-need/

[260] Information Commissioner's Office. *An overview of the Data Protection Act 2018*. In. Retrieved from https://ico.org.uk/media/for-organisations/documents/2614158/ico-introduction-to-the-data-protection-bill.pdf p.4.

ทั้งนี้ DPA ประกอบไปด้วยระบบการคุ้มครองข้อมูลส่วนบุคคลที่แตกต่างกัน 4 ระบบ โดยแบ่งระบบตามประเภทของข้อมูลส่วนบุคคลแต่ละประเภท หรือตามประเภทของการประมวลผลข้อมูลส่วนบุคคล ดังนี้[261]

1) การประมวลผลส่วนบุคคลภายในขอบเขตของ GDPR

2) การประมวลผลข้อมูลส่วนบุคคลนอกเหนือขอบเขตของ GDPR

3) การประมวลผลข้อมูลส่วนบุคคลโดยหน่วยงานที่มีอำนาจเพื่อการบังคับใช้กฎหมาย

4) การประมวลผลข้อมูลส่วนบุคคลโดยหน่วยงานข่าวกรอง หรือหน่วยงานราชการลับ

2.1 ขอบเขตการบังคับใช้

เนื่องจากในขณะนี้ DPA ยังมีผลบังคับใช้ในสหราชอาณาจักรควบคู่ไปกับ GDPR และดังที่กล่าวมาแล้ว DPA ประกอบด้วยระบบการคุ้มครองข้อมูลส่วนบุคคลที่แตกต่างกัน 4 ระบบ ดังนั้นสำหรับการประมวลผลส่วนบุคคลภายในขอบเขตของ GDPR ขอบเขตการบังคับใช้จึงอ้างอิงตาม GDPR ซึ่งกำหนดให้ใช้ GDPR กับการประมวลผลข้อมูลส่วนบุคคลไม่ว่าจะเป็นทั้งหมด หรือบางส่วน ไม่ว่าจะเป็นโดยวิธีการอัตโนมัติ หรือวิธีการอื่นใด ซึ่งเป็นส่วนหนึ่งของระบบการจัดเก็บข้อมูล หรือเป็นส่วนหนึ่งของระบบการจัดเก็บข้อมูล ทั้งนี้ไม่รวมถึงการประมวลผลข้อมูลส่วนบุคคลดังต่อไปนี้[262]

1) ในกิจการซึ่งอยู่นอกขอบเขตการบังคับของกฎหมายสหภาพยุโรป

2) โดยประเทศสมาชิกในการดำเนินกิจการที่อยู่ภายใต้ขอบเขตของหมวดที่ 2 หัวข้อ 5 ของสนธิสัญญาสหภาพยุโรป (Treaty on European Union - TEU)

3) โดยบุคคลธรรมดาในกิจการส่วนบุคคล หรือกิจการในครัวเรือน

4) โดยพนักงานเจ้าหน้าที่ที่มีความสามารถเพื่อวัตถุประสงค์ในการป้องกัน การสืบสวนสอบสวน การดำเนินคดีหรือการลงโทษทางอาญา รวมถึงมาตรการการรักษาความปลอดภัยและป้องกันการคุกคามต่อความมั่นคงของประชาชนทั่วไป

นอกจากนี้ GDPR กำหนดให้ใช้บังคับกับการประมวลผลข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งมีสถานประกอบการที่ตั้งอยู่ในสหภาพยุโรป ไม่ว่าการประมวลผลนั้นจะกระทำอยู่ในสหภาพยุโรปหรือไม่ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลไม่มีสถานประกอบการอยู่ในสหภาพยุโรปกฎข้อบังคับนี้จะใช้บังคับกับการประมวลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลที่อยู่ในสหภาพยุโรปเมื่อการประมวลผลข้อมูลส่วนบุคคลนั้นเป็นการนำเสนอสินค้าหรือบริการแก่เจ้าของข้อมูลส่วนบุคคลโดยมิต้องคำนึงถึงว่ามีการชำระเงินโดยเจ้าของข้อมูลส่วนบุคคลหรือไม่ หรือเป็นการติดตามตรวจสอบพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในสหภาพยุโรป นอกจากนี้ GDPR ยังใช้บังคับการ

---

[261] Information Commissioner's Office. *An overview of the Data Protection Act 2018*. In. Retrieved from https://ico.org.uk/media/for-organisations/documents/2614158/ico-introduction-to-the-data-protection-bill.pdf. p.5.

[262] GDPR, Article 2.

ประมวลผลข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมิได้มีสถานประกอบการอยู่ในสหภาพยุโรป แต่อยู่ในประเทศที่กฎหมายของประเทศสมาชิกให้ใช้บังคับโดยอาศัยอำนาจตามกฎหมายระหว่างประเทศแผนกคดีเมือง[263]

2.2 ความหมายของข้อมูลส่วนบุคคล

2.2.1 ความหมายของข้อมูลส่วนบุคคล

DPA ได้ให้คำจำกัดความของ “ข้อมูลส่วนบุคคล” ว่าหมายถึงข้อมูลใด ๆ ที่เกี่ยวข้องกับบุคคลที่มีชีวิตอยู่ที่สามารถระบุตัวตนหรืออาจนำไปใช้ระบุตัวตนบุคคลนั้นได้[264] และยังได้ให้คำจำกัดความของ “บุคคลที่มีชีวิตอยู่ที่อาจระบุตัวตนได้ (Identifiable living individual)” ว่าหมายถึง

“บุคคลที่มีชีวิตอยู่ที่สามารถถูกระบุตัวตนได้ ไม่ว่าจะเป็นทางตรง หรือทางอ้อมโดยการอ้างอิงถึง 1) สิ่งระบุตัวตน เช่น ชื่อ หมายเลขประจำตัว ข้อมูลตำแหน่งที่ตั้ง หรือ สิ่งระบุตัวบุคคลออนไลน์ หรือ 2) ปัจจัยที่มีความเฉพาะเจาะจงด้านร่างกาย สรีรวิทยา พันธุกรรม เอกลักษณ์ สภาวะทางจิต เศรษฐกิจ วัฒนธรรม หรือสังคมของแต่ละบุคคล” [265]

สำหรับคำจำกัดความของ “ข้อมูลส่วนบุคคล” ใน DPA นั้นมิได้มีการระบุรายละเอียดว่าสิ่งระบุตัวตนออนไลน์ครอบคลุมสิ่งใดบ้าง ต่างจาก GDPR ที่ได้ทำการยกตัวอย่างสิ่งระบุตัวตนออนไลน์ไว้อย่างละเอียดใน Recital 30

2.2.2 ความหมายของข้อมูลส่วนบุคคลประเภทชีวภาพ

สำหรับความหมายของ “ข้อมูลชีวภาพ” นั้น DPA ได้ให้คำจำกัดความว่า “ข้อมูลชีวภาพ” หมายถึงข้อมูลส่วนบุคคลที่เกิดจากการประมวลผลโดยใช้เทคนิคพิเศษที่เกี่ยวกับลักษณะทางกายภาพ ทางสรีรวิทยาหรือพฤติกรรมของบุคคลซึ่งสามารถนำไปใช้เพื่อระบุตัวตน หรือใช้เพื่อยืนยันตัวตนของบุคคล เช่น ภาพใบหน้า หรือข้อมูลลายนิ้วมือ[266]

คำจำกัดความของ “ข้อมูลชีวภาพ” ภายใต้ DPA นั้นมีความหมายเหมือนกันกับ“ข้อมูลชีวภาพ” ภายใต้ GDPR โดย “ข้อมูลชีวภาพ” จะต้องประกอบไปด้วย 4 ส่วน ดังต่อไปนี้

1) เป็นข้อมูลส่วนบุคคล (personal data)

2) เกิดจากการประมวลผลข้อมูลส่วนบุคคลด้วยเทคนิคพิเศษ (resulting from specific technical processing)

3) เกี่ยวกับลักษณะทางกายภาพ ทางสรีรวิทยาหรือพฤติกรรมของบุคคล (relating to the physical, physiological or behavioural characteristics of a natural person)

4) สามารถนำไปใช้เพื่อระบุตัวตน หรือใช้เพื่อยืนยันตัวตนของบุคคล (allow or confirm the unique identification of that natural person

---

[263] GDPR, Article 3.

[264] BPA, Article 3(2).

[265] BPA, Article 3(3).

[266] BPA, Article 205(1).

ดังนั้นข้อมูลส่วนบุคคลจะถือว่าเป็นข้อมูลส่วนบุคคลประเภทชีวภาพเมื่อมีองค์ประกอบครบทั้ง 4 ข้อ คือเมื่อข้อมูลนั้นเป็นข้อมูลส่วนบุคคลเกี่ยวกับลักษณะทางกายภาพ ทางสรีรวิทยาหรือพฤติกรรมของบุคคลที่เกิดจาก “การประมวลผลด้วยเทคนิคพิเศษ” และ “ช่วยยืนยันการระบุเอกลักษณ์ของบุคคล” ดังนั้นหากข้อมูลส่วนบุคคลใด ๆ เกี่ยวกับลักษณะทางกายภาพ ทางสรีรวิทยาหรือพฤติกรรมของบุคคลนั้นไม่ได้เกิดจากการประมวลผลทางเทคนิคพิเศษ และไม่ได้ช่วยยืนยันการระบุเอกลักษณ์ของบุคคล ข้อมูลส่วนบุคคลนั้นจะไม่ถือว่าเป็นข้อมูลชีวภาพตามคำจำกัดความของ DPA ข้อมูลส่วนบุคคลที่เกี่ยวกับลักษณะทางกายภาพ ทางสรีรวิทยาหรือพฤติกรรมของบุคคลดังกล่าวถือเป็นเพียงข้อมูลส่วนบุคคลธรรมดา ดังนั้น ภาพถ่ายของบุคคล หรือรูปถ่ายลายนิ้วมือที่มิได้เกิดจากการประมวลผลทางเทคนิคพิเศษ และมิได้ช่วยยืนยันการระบุเอกลักษณ์ของบุคคล จึงเป็นเพียงข้อมูลส่วนบุคคล มิได้เป็นข้อมูลส่วนบุคคลประเภทชีวภาพ

การประมวลผลข้อมูลส่วนบุคคลที่เป็นภาพถ่ายโดยทั่วไปไม่ถือว่าเป็นการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว เนื่องจากข้อมูลส่วนบุคคลจะถือว่าเป็นข้อมูลชีวภาพได้ต่อเมื่อมีการประมวลผลด้วยเทคนิคพิเศษเพื่อทำการระบุเอกลักษณ์ของบุคคล หรือยืนยันเอกลักษณ์ของบุคคล โดยการประมวลผลข้อมูลส่วนบุคคลประเภทชีวภาพกระทำได้ต่อเมื่อกฎหมายสหภาพยุโรปหรือกฎหมายประเทศสมาชิกอนุญาตให้ทำได้เป็นการเฉพาะเจาะจง[267]

2.3 หลักการคุ้มครองข้อมูลส่วนบุคคล

หลักการคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร จะใช้ตามข้อกำหนดของ GDPR (อ่านรายละเอียดในบทที่ 3 หัวข้อ 1.3 หลักการคุ้มครองข้อมูลส่วนบุคคล) เนื่องจากใน DPA ไม่ได้มีการกำหนดไว้ อย่างไรก็ดีใน Data Protection Act 1998 (DPA 1998) ซึ่งถูกแทนที่โดย DPA เมื่อ DPA ประกาศใช้ในปี 2018 ได้มีการวางหลักการคุ้มครองข้อมูลส่วนบุคคลไว้ 8 ข้อ ดังต่อไปนี้

1) หลักความชอบด้วยกฎหมาย
2) หลักจำกัดตามวัตถุประสงค์
3) หลักการจัดเก็บข้อมูลเท่าที่จำเป็น
4) หลักความถูกต้องของข้อมูล
5) หลักข้อจำกัดในการจัดเก็บ
6) หลักสิทธิของบุคคล
7) หลักความปลอดภัย
8) หลักการไม่โอนข้อมูลส่วนบุคคลออกนอกราชอาณาจักร

ทั้งนี้หลักการคุ้มครองข้อมูลส่วนบุคคลที่บัญญัติไว้ใน DPA 1998 นั้นมีความต่างกับหลักการคุ้มครองข้อมูลส่วนบุคคลที่บัญญัติไว้ใน GDPR ดังนี้

---

[267] GDPR, Recital 51.

ตารางที่ 3.3 ความแตกต่างระหว่างหลักการคุ้มครองข้อมูลส่วนบุคคล DPA 1998 กับ GDPR

	DPA 1998	GDPR
หลักความชอบด้วยกฎหมาย	ข้อมูลส่วนบุคคลจะต้องได้รับการประมวลผลอย่างเป็นธรรมและชอบด้วยกฎหมายและอยู่ภายใต้เงื่อนไข	ข้อมูลส่วนบุคคลต้องได้รับการประมวลผลโดยชอบด้วยกฎหมาย เป็นธรรมในลักษณะที่โปร่งใสในส่วนที่เกี่ยวข้องกับเจ้าของข้อมูล
หลักจำกัดตามวัตถุประสงค์	การเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องกระทำภายใต้วัตถุประสงค์ที่เจาะจงและชอบด้วยกฎหมายอย่างน้อยหนึ่งวัตถุประสงค์และจะไม่ถูกประมวลผลเพิ่มเติมในลักษณะใด ๆ ที่ไม่สอดคล้องกับวัตถุประสงค์ดังกล่าว	การเก็บรวบรวมข้อมูลส่วนบุคคล ต้องกระทำภายใต้วัตถุประสงค์ที่ได้มีการระบุชัดเจนและถูกต้องตามกฎหมายเท่านั้น โดยไม่มีการนำไปประมวลผลในลักษณะที่ไม่สอดคล้องกับวัตถุประสงค์ที่ได้ระบุไว้
หลักการจัดเก็บข้อมูลเท่าที่จำเป็น	การเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องเพียงพอ มีความเกี่ยวข้องและไม่มากเกินไปเมื่อเทียบกับวัตถุประสงค์ในการประมวลผล	การเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องเพียงพอ มีความเกี่ยวข้องและจำกัดเฉพาะสิ่งที่จำเป็นเพื่อวัตถุประสงค์ในการประมวลผล
หลักความถูกต้องของข้อมูล	ข้อมูลส่วนบุคคลนั้นต้องมีความถูกต้อง และเป็นปัจจุบัน (ในกรณีที่จำเป็น)	ข้อมูลส่วนบุคคลต้องมีความถูกต้อง และเป็นปัจจุบัน (ในกรณีที่จำเป็น) โดยมีขั้นตอนที่เหมาะสมเพื่อลบ หรือแก้ไขข้อมูลที่ไม่ถูกต้องโดยไม่ชักช้า

ตารางที่ 3.3 (ต่อ)

	DPA 1998	GDPR
หลักข้อจำกัดในการจัดเก็บ	ข้อมูลส่วนบุคคลที่นำมาประมวลผลไม่ควรเก็บนานเกินกว่าจำเป็นเพื่อบรรลุวัตถุประสงค์	ข้อมูลส่วนบุคคลที่จัดเก็บในรูปแบบที่ทำให้สามารถระบุตัวตนของเจ้าของข้อมูลส่วนบุคคลได้ จะต้องไม่มีการจัดเก็บนานเกินกว่าจำเป็นเพื่อบรรลุวัตถุประสงค์ในการประมวลผล ข้อมูลส่วนบุคคลอาจมีการจัดเก็บนานเกินกว่าจำเป็นเพื่อบรรลุวัตถุประสงค์ หากวัตถุประสงค์ในการเก็บนั้นคือเพื่อสาธารณะประโยชน์ เหตุผลทางวิทยาศาสตร์ หรือการค้นคว้าทางประวัติศาสตร์ หรือเพื่อวัตถุประสงค์ทางสถิติ
หลักสิทธิของบุคคล	การประมวลผลข้อมูลส่วนบุคคลต้องเป็นไปตามสิทธิของเจ้าของข้อมูลส่วนบุคคล	GDPR มิได้ระบุหลักสิทธิของบุคคล แต่มีการระบุสิทธิในการเข้าถึงไว้ในบทที่ 3 ของ GDPR
หลักความปลอดภัย	ต้องใช้มาตรการทางเทคนิคและทางองค์กรที่เหมาะสมเพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตและการประมวลผลข้อมูลส่วนบุคคลที่มิชอบด้วย อีกทั้งยังต้องป้องกันการสูญเสีย หรือการทำลายโดยไม่ได้ตั้งใจและความเสียหายที่อาจเกิดขึ้นต่อข้อมูลส่วนบุคคล	การประมวลผลข้อมูลส่วนบุคคลจะต้องใช้มาตรการทางเทคนิคหรือทางองค์กรเพื่อรับประกันความปลอดภัย เพื่อป้องกันการประมวลผลที่ไม่ได้รับอนุญาต หรือผิดกฎหมายและป้องกันการสูญเสียโดยไม่ได้ตั้งใจ การทำลาย หรือความเสียหายต่อข้อมูลส่วนบุคคล

ตารางที่ 3.3 (ต่อ)

	DPA 1998	GDPR
หลักการไม่โอนข้อมูลส่วนบุคคลออกนอกราชอาณาจักร	ต้องไม่มีการโอนข้อมูลส่วนบุคคลไปยังประเทศหรือดินแดนอื่นใดนอกสหภาพยุโรป เว้นแต่ประเทศหรือดินแดนนั้นจะสามารถรับรองว่ามีการป้องกันสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลในระดับที่เพียงพอ	GDPR มิได้ระบุหลักสิทธิของบุคคล แต่มีการระบุการโอนข้อมูลไปต่างประเทศไว้ในบทที่ 5 ของ GDPR
หลักความรับผิดชอบ		ผู้ควบคุมข้อมูลส่วนบุคคลต้องรับผิดชอบ และสามารถแสดงให้เห็นได้ว่ามีการกระทำตามหลักการคุ้มครองข้อมูลส่วนบุคคล

ที่มา : https://ico.org.uk/

2.1 การประมวลผลข้อมูลส่วนบุคคลที่ชอบด้วยกฎหมาย

2.1.1 ข้อมูลส่วนบุคคลธรรมดา

สำหรับฐานในการประมวลผลข้อมูลส่วนบุคคลธรรมดา สหราชอาณาจักรจะใช้ข้อกำหนดตาม GDPR (อ่านรายละเอียดในบทที่ 3 หัวข้อ 1.4.1 ข้อมูลส่วนบุคคล) ทั้งนี้ใน DPA ได้มีการกำหนดเพิ่มเติมว่า หากเป็นการประมวลผลข้อมูลส่วนบุคคลโดยอ้างฐานภารกิจของรัฐ (Public Task) คือเป็นการประมวลผลข้อมูลส่วนบุคคลที่เป็นการจำเป็นต่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะ หรือในการใช้อำนาจรัฐของผู้ควบคุมข้อมูลส่วนบุคคลนั้น รวมถึง[268]

1) การบริหารงานด้านความยุติธรรม
2) การใช้อำนาจหน้าที่ของสภาผู้แทนราษฎร
3) การใช้อำนาจหน้าที่ของบุคคลที่ได้รับมอบตามกฎหมาย
4) การใช้พระราชอำนาจของพระราชวงศ์ รัฐมนตรีแห่งพระราชวงศ์ หรือหน่วยงานรัฐบาล หรือ
5) กิจกรรมที่สนับสนุน หรือส่งเสริมการมีส่วนร่วมในระบอบประชาธิปไตย

[268] DPA, Section 8.

2.1.2 ข้อมูลส่วนบุคคลประเภทชีวภาพ

การประมวลผลข้อมูลส่วนบุคคลประเภทชีวภาพซึ่งถือเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว ภายใต้ GDPR และ DPA นั้น ห้ามมิให้ประมวลผลข้อมูลชนิดนี้ ยกเว้นในกรณีดังต่อไปนี้ ดังต่อไปนี้[269,270]

1) ความยินยอมโดยชัดแจ้ง (Explicit consent)

GDPR กำหนดว่าการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวจะกระทำได้แต่ต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลเพื่อประมวลผลตามวัตถุประสงค์ที่ได้ระบุไว้ อย่างไรก็ดี หากกฎหมายสหภาพยุโรป หรือกฎหมายของประเทศสมาชิกมีการกำหนดห้ามมิให้เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมสำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวความยินยอมนั้นย่อมไม่มีผล[271]

เนื่องจากการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวมีความเสี่ยงมากกว่าการประมวลผลข้อมูลส่วนบุคคลธรรมดา เจ้าของข้อมูลส่วนบุคคลต้องควบคุมข้อมูลของตนได้ในระดับที่สูงกว่าข้อมูลส่วนบุคคลธรรมดาการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวจึงต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล[272] และไม่สามารถอ้างการทำตามสัญญาเป็นหลักเกณฑ์ในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่ชอบด้วยกฎหมายได้

ภายใต้ GDPR ความยินยอมในการให้ประมวลผลข้อมูลส่วนบุคคลธรรมดามีข้อกำหนดที่เข้มงวดอยู่แล้ว ดังนั้นการได้รับความยินยอมโดยชัดแจ้ง จึงต้องให้เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมโดยแสดงข้อความในการให้ความยินยอมอย่างชัดเจนเหนือกว่าการให้ความยินยอมในการให้ประมวลผลข้อมูลส่วนบุคคลธรรมดา การอนุมานจากการกระทำบางอย่างของเจ้าของข้อมูลส่วนบุคคลไม่สามารถถือได้ว่าเป็นการให้ความยินยอมอย่างชัดแจ้ง การให้ความยินยอมอย่างชัดแจ้งอาจทำเป็นลายลักษณ์อักษร โดยผู้ควบคุมข้อมูลส่วนบุคคลอาจขอให้เจ้าของข้อมูลส่วนบุคคลเซ็นให้ความยินยอมในเอกสารที่ระบุข้อความให้ความยินยอมที่ผู้ควบคุมข้อมูลส่วนบุคคลได้เตรียมไว้ อย่างไรก็ดี การให้เจ้าของข้อมูลส่วนบุคคลเซ็นให้ความยินยอมในเอกสารมิใช่ทางเดียวที่จะได้มาซึ่งความยินยอมโดยชัดแจ้ง สำหรับกิจกรรมที่ดำเนินการผ่านระบบดิจิทัลการให้ความยินยอมโดยชัดแจ้งสามารถกระทำได้หลายวิธี เช่น การกรอกฟอร์มออนไลน์ การทำเครื่องหมายในช่องทำเครื่องหมาย (check box) การส่งอีเมล การสแกนเอกสารที่มีลายเซ็นของเจ้าของข้อมูลส่วนบุคคลเข้าระบบ หรือแม้กระทั่งการใช้ลายเซ็นดิจิทัล เป็นต้น การให้ความยินยอมอย่างชัดแจ้งด้วยวาจานั้นอาจทำได้ แต่การพิสูจน์ว่าความยินยอมนั้นได้มาอย่างถูกต้องภายใต้ข้อกำหนดของ GDPR อาจเป็นไปได้ยาก[273]

---

[269] GDPR, Article 9

[270] DPA, Section 10.

[271] GDPR, Article 9(2)(a).

[272] Article 29 Working Party. Guidelines on consent under Regulation 2016/679 (WP259 rev.01), (2018).

[273] Ibid.

2) ความจำเป็นสำหรับการปฏิบัติหน้าที่ (Employment, social security and social protection)

GDPR กำหนดว่าการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวนั้นสามารถทำได้หากการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นการจำเป็นสำหรับการปฏิบัติหน้าที่ รวมถึงการใช้สิทธิเฉพาะของผู้ควบคุมข้อมูลส่วนบุคคล หรือของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายแรงงาน กฎหมายประกันสังคม หรือกฎหมายคุ้มครองสังคม ภายใต้อำนาจที่ได้รับจากกฎหมายสหภาพ หรือกฎหมายของประเทศสมาชิก หรือตามข้อตกลงร่วมกันของประเทศสมาชิก ทั้งนี้ต้องมีมาตรการที่เหมาะสมในการปกป้องสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลด้วย[274]

ในขณะที่ DPA กำหนดว่าการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวนั้นสามารถทำได้หากการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นการประมวลผลภายใต้หลักเกณฑ์ความจำเป็นสำหรับการปฏิบัติหน้าที่ รวมถึงการใช้สิทธิเฉพาะของผู้ควบคุมข้อมูลส่วนบุคคล หรือของเจ้าของข้อมูลส่วนบุคคล ตามกฎหมายแรงงาน กฎหมายประกันสังคม หรือกฎหมายคุ้มครองสังคม หรือตามข้อตกลงร่วมกันของประเทศสมาชิก และการประมวลผลมีความจำเป็นเพื่อวัตถุประสงค์ในการดำเนินการหรือเรียกร้องภายใต้สิทธิตามกฎหมายที่เกี่ยวข้องกับการจ้างงาน ประกันสังคมหรือการคุ้มครองทางสังคม และเมื่อมีการประมวลผลดังกล่าวผู้ควบคุมข้อมูลส่วนบุคคลจะต้องมีเอกสารนโยบายที่เหมาะสม[275]

3) ประโยชน์สำคัญต่อชีวิต (Vital interests)

ภายใต้บทบัญญัติของ GDPR การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวสามารถทำได้หากเป็นการจำเป็นเพื่อปกป้องประโยชน์ที่สำคัญต่อชีวิตของเจ้าของข้อมูลส่วนบุคคลหรือของบุคคลอื่นในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ไม่ว่าจะทางพฤตินัย หรือนิตินัย[276]

การประมวลผลข้อมูลส่วนบุคคลภายใต้หลักเกณฑ์นี้มีไว้เพื่อปกป้องประโยชน์สำคัญที่จำเป็นต่อชีวิต ไม่ว่าจะเป็นชีวิตของเจ้าของข้อมูลส่วนบุคคลหรือของบุคคลอื่น[277] จึงมีขอบเขตการใช้ที่จำกัด และมักใช้ในกรณีที่เป็นเรื่องของความเป็นความตาย และใช้ในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมทางพฤตินัยหรือนิตินัยได้ ดังนั้นการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวภายใต้หลักเกณฑ์นี้ไม่สามารถทำได้หากเจ้าของข้อมูลส่วนบุคคลสามารถให้ความยินยอมได้ และต้องขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลจึงชอบด้วยกฎหมาย

---

[274] GDPR, Article 9(2)(b).

[275] DPA, Schedule 1, Part 1(1).

[276] GDPR, Article 9(2)(c).

[277] GDPR, Recital 46.

4) กิจกรรมโดยชอบขององค์กรไม่แสวงหาผลกำไร (Not-for-profit bodies)

ภายใต้ GDPR การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่ชอบด้วยกฎหมายสามารถทำได้สำหรับการดำเนินการกิจกรรมที่ชอบด้วยกฎหมายขององค์กรที่ไม่แสวงหาผลกำไร เช่น มูลนิธิ สมาคม หรือองค์กรไม่แสวงหาผลกำไรอื่นที่มีวัตถุประสงค์ทางการเมือง ปรัชญา ศาสนา หรือสหภาพแรงงาน โดยมีเงื่อนไขว่าการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวนั้นจะต้องเกี่ยวข้องเฉพาะสมาชิก หรืออดีตสมาชิกขององค์กร หรือบุคคลที่มีการติดต่อกับองค์กรเป็นปรกติ ภายใต้วัตถุประสงค์ขององค์กร และข้อมูลส่วนบุคคลที่มีความอ่อนไหวต้องไม่ถูกเปิดเผยออกไปภายนอกองค์กรหากมิได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล[278]

5) เปิดเผยข้อมูลต่อสาธารณชน (Made public by the data subject)

GDPR กำหนดว่าการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวสามารถทำได้โดยชอบด้วยกฎหมายหากเจ้าของข้อมูลส่วนบุคคลนั้นได้เปิดเผยข้อมูลส่วนบุคคลดังกล่าวต่อสาธารณชนด้วยตนเอง[279] ซึ่งการเปิดเผยนั้นต้องเป็นการเปิดเผยที่เจ้าของข้อมูลส่วนบุคคลกระทำไปโดยมีความตั้งใจที่จะเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวต่อสาธารณชน การรั่วไหลของข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่ทำให้สาธารณชนได้ทราบข้อมูลดังกล่าว ไม่ถือว่าเป็นการเปิดเผยข้อมูลต่อสาธารณชนด้วยตนเองของเจ้าของข้อมูลส่วนบุคคล

ความคิดเห็นทางการเมืองถือเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่เจ้าของข้อมูลส่วนบุคคลบางคนอาจเปิดเผยต่อสาธารณชนด้วยตนเอง อย่างไรก็ดีการนำข้อมูลส่วนบุคคลที่มีความอ่อนไหวไปใช้ภายใต้หลักเกณฑ์นี้ควรกระทำด้วยความระมัดระวัง เนื่องจากต้องดูพื้นฐานในการเปิดเผยข้อมูลว่าเจ้าของข้อมูลต้องการเปิดเผยให้แค่คนใกล้ชิด เช่น เพื่อนในโซเชียลมีเดีย หรือต้องการเปิดเผยให้สาธารณชนทราบ

การเปิดเผยให้สาธารณชนทราบ หมายถึง การเปิดเผยที่บุคคลทั่วไปสามารถเข้าถึงได้ มิใช่เข้าถึงได้แค่เฉพาะกลุ่ม การที่บุคคลใดบุคคลหนึ่งสามารถเข้าถึงข้อมูลได้มิได้หมายความว่าทุกคนสามารถเข้าถึงข้อมูลดังกล่าวได้ ดังนั้นการที่บุคคลใดบุคคลหนึ่ง หรือกลุ่มใดกลุ่มหนึ่งสามารถเข้าถึงข้อมูลได้มิได้หมายความว่าข้อมูลดังกล่าวเป็นข้อมูลที่เปิดเผยให้สาธารณชนทราบ

6) สิทธิเรียกร้องตามกฎหมาย (Legal claims or judicial acts)

ภายใต้ GDPR การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวสามารถกระทำได้โดยชอบด้วยกฎหมายหากเป็นการจำเป็นสำหรับการก่อให้เกิดสิทธิเรียกร้อง การใช้สิทธิเรียกร้อง หรือการป้องกันสิทธิเรียกร้องตามกฎหมาย หรือในการพิจารณาคดีของศาล[280] ทั้งนี้ผู้ควบคุมข้อมูลส่วนบุคคลที่มีความอ่อนไหวจะต้องสามารถแสดงให้เห็นได้ว่าวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลดังกล่าวคือเพื่อการก่อให้เกิดสิทธิเรียกร้อง การใช้สิทธิเรียกร้อง หรือการ

---

[278] GDPR, Article 9(2)(d).

[279] GDPR, Article 9(2)(e).

[280] GDPR, Article 9(2)(f).

ป้องกันสิทธิเรียกร้องตามกฎหมาย หรือเพื่อการพิจารณาคดีของศาล ซึ่งรวมถึงการขอคำปรึกษาทางด้านกฎหมาย และขั้นตอนการเตรียมสำหรับการดำเนินคดีทางกฎหมาย

ตัวอย่าง นายจ้างกำลังถูกลูกจ้างฟ้องร้องในคดีที่เกี่ยวกับอุบัติเหตุที่เกิดขึ้นในสถานที่ทำการของนายจ้าง นายจ้างต้องปรึกษาทนายเพื่อขอคำแนะนำ การนำข้อมูลที่เกี่ยวข้องกับอุบัติเหตุรวมถึงข้อมูลการบาดเจ็บของลูกจ้างซึ่งเป็นข้อมูลสุขภาพที่เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวไปเปิดเผยกับทนายของนายจ้าง ถือว่าเป็นการกระทำโดยชอบด้วยกฎหมาย เนื่องจากเป็นการจำเป็นภายใต้หลักเกณฑ์สิทธิเรียกร้องตามกฎหมาย

ตัวอย่าง การที่ผู้อนุบาลทำนิติกรรมแทนผู้ไร้ความสามารถอาจต้องมีการเปิดเผยข้อมูลให้ผู้ที่เข้าทำนิติกรรมด้วยทราบว่าเป็นการกระทำการแทนผู้ไร้ความสามารถ ซึ่งถือว่าเป็นการเปิดเผยข้อมูลสุขภาพ ซึ่งเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว การเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวในกรณีนี้สามารถทำได้โดยชอบด้วยกฎหมาย

7) ประโยชน์สาธารณะที่สำคัญ (Reasons of substantial public interest)

ภายใต้ GDPR การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวในกรณีที่เป็นการจำเป็นสำหรับประโยชน์สาธารณะที่สำคัญตามหลักเกณฑ์ของกฎหมายสหภาพ หรือกฎหมายของประเทศสมาชิกเป็นอีกหลักเกณฑ์หนึ่งในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่ชอบด้วยกฎหมาย โดยการประมวลผลจะต้องเหมาะสมได้สัดส่วนตามวัตถุประสงค์ของการประมวลผล และให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล อีกทั้งยังต้องจัดให้มีมาตรการการปกป้องสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลที่เหมาะสม[281]

สำหรับ DPA การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวสามารถทำได้หากการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวในกรณีที่เป็นการจำเป็นสำหรับประโยชน์สาธารณะที่สำคัญตามหลักเกณฑ์ของกฎหมายสหภาพ หรือกฎหมายของประเทศสมาชิก นอกจากการประมวลผลจะต้องเหมาะสมได้สัดส่วนตามวัตถุประสงค์ของการประมวลผล และให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล และต้องจัดให้มีมาตรการการปกป้องสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลที่เหมาะสม[282] DPA ได้กำหนดให้การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวสามารถทำได้ หากการประมวลผลดังกล่าวอยู่ภายใต้เงื่อนไขดังต่อไปนี้[283]

(1) เพื่อวัตถุประสงค์ทางกฎหมายและของรัฐ (Statutory and government purposes)

(2) เพื่อดำเนินการตามกระบวนการยุติธรรมหรือทางรัฐสภา (Administration of justice and parliamentary purposes)

(3) เพื่อความเสมอภาคและเท่าเทียมกัน (Equality of opportunity or treatment)

---

[281] GDPR, Article 9(2)(g).

[282] GDPR, Article 9(2)(g).

[283] DPA, Schedule 1, Part 2(6) to (28).

(4) เพื่อความหลากหลายและแตกต่างทางเชื้อชาติ และชาติพันธุ์ในระดับอาวุโส (Racial and ethnic diversity at senior levels)

(5) เพื่อป้องกัน หรือตรวจจับการกระทำอันผิดกฎหมาย (Preventing or detecting unlawful acts)

(6) เพื่อปกป้องส่วนรวม (Protecting the public)

(7) เพื่อให้เป็นไปตามข้อกำหนดของกฎหมาย (Regulatory requirements)

(8) เพื่อสื่อสารมวลชน การศึกษา ศิลปะ หรือวรรณกรรม (Journalism, academia, art and literature)

(9) เพื่อการป้องกันการหลอกลวง (Preventing fraud)

(10) เพื่อตรวจสอบการจัดหาเงินทุนของผู้ก่อการร้ายหรือการฟอกเงิน (Suspicion of terrorist financing or money laundering)

(11) เพื่อสนับสนุนผู้พิการหรือผู้ที่มีปัญหาด้านสุขภาพ (Support for individuals with a particular disability or medical condition)

(12) เพื่อการให้คำปรึกษา (Counselling)

(13) เพื่อป้องกันเด็กและบุคคลที่มีความเสี่ยง (Safeguarding of children and individuals at risk)

(14) เพื่อป้องกันความมั่นคงทางเศรษฐกิจของบุคคลบางคน (Safeguarding of economic well-being of certain individuals)

(15) เพื่อการประกันภัย (Insurance)

(16) เพื่อบำนาญทางวิชาชีพ (Occupational pensions)

(17) เพื่อพรรคการเมือง (Political parties)

(18) เพื่อการตอบคำร้องโดยผู้แทนที่ได้รับเลือกตั้ง (Elected representatives responding to requests)

(19) เพื่อการเปิดเผยต่อผู้แทนที่ได้รับเลือกตั้ง (Disclosure to elected representatives)

(20) เพื่อแจ้งผู้แทนที่ได้รับเลือกตั้งให้ทราบเกี่ยวกับนักโทษ (Informing elected representatives about prisoners)

(21) เพื่อการเผยแพร่คำพิพากษาของศาล (Publication of legal judgments)

(22) เพื่อป้องกันการใช้ยาและสารต้องห้ามในกีฬา (Anti-doping in sport)

(23) เพื่อเป็นการสร้างมาตรฐานพฤติกรรมในกีฬา (Standards of behaviour in sport)

8) ประโยชน์สาธารณะด้านการคุ้มครองและประกันสังคม (Health or social care)

การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว GDPR กำหนดว่าสามารถทำได้หากเป็นการจำเป็นสำหรับวัตถุประสงค์ทางการแพทย์ด้านเวชศาสตร์ป้องกัน หรืออาชีวเวชศาสตร์ เพื่อการประเมินความสามารถในการทำงานของพนักงาน การวินิจฉัยทางการแพทย์ การดูแลสุขภาพและสังคม หรือการรักษาหรือการจัดการระบบและการให้บริการที่เกี่ยวกับสุขภาพและสังคมตามหลักเกณฑ์ของกฎหมายสหภาพหรือกฎหมายของประเทศสมาชิก หรือเป็นไปตามสัญญากับผู้ประกอบอาชีพที่เกี่ยวกับสุขภาพ (Health Professionals) ทั้งนี้ต้องเป็นไปตามเงื่อนไขและมาตรการที่กำหนดไว้[284]

ทั้งนี้การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวอาจถูกประมวลผลภายใต้หลักเกณฑ์นี้เมื่อข้อมูลเหล่านั้นถูกประมวลผลโดยหรือภายใต้ความรับผิดชอบของผู้เชี่ยวชาญที่มีหน้าที่รักษาความลับตามจรรยาบรรณของวิชาชีพ ทั้งนี้ตามหลักเกณฑ์ของกฎหมายสหภาพยุโรปหรือกฎหมายของประเทศสมาชิก หรือภายใต้หลักเกณฑ์ที่กำหนดโดยหน่วยงานระดับชาติ หรือโดยบุคคลซึ่งมีหน้าที่เก็บรักษาความลับภายใต้กฎหมายสหภาพยุโรป หรือกฎหมายของประเทศสมาชิกหรือหลักเกณฑ์ของหน่วยงานระดับชาติ[285]

เนื่องจากการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวควรได้รับการคุ้มครองในระดับที่สูงกว่าข้อมูลส่วนบุคคลอื่น จึงควรใช้เฉพาะในกรณีที่จำเป็นเพื่อวัตถุประสงค์ที่เกี่ยวข้องกับสุขภาพและใช้เพียงเท่าที่จำเป็นเพื่อให้บรรลุวัตถุประสงค์เหล่านั้นเพื่อประโยชน์ของบุคคลธรรมดาและสังคมโดยรวม โดยเฉพาะอย่างยิ่งในบริบทของการบริหารจัดการระบบการบริการทางด้านสุขภาพและสังคม การประมวลผลเพื่อการควบคุมคุณภาพโดยผู้บริหารและหน่วยงานกลางที่รับผิดชอบด้านสาธารณสุข การจัดการและการกำกับดูแลทั่วไปของข้อมูลด้านสุขภาพและสังคมในระดับชาติและระดับท้องถิ่นเพื่อการดูแลสุขภาพและสังคม การดูแลสุขภาพอย่างต่อเนื่องไม่ว่าจะเป็นการดูแลข้ามพรมแดนหรือการดูแลความปลอดภัยทางด้านสุขภาพ การตรวจสอบและแจ้งเตือนเพื่อประโยชน์สาธารณะ การวิจัยทางวิทยาศาสตร์หรือประวัติศาสตร์หรือวัตถุประสงค์ทางสถิติตามกฎหมายของสหภาพหรือประเทศสมาชิกที่จะต้องบรรลุวัตถุประสงค์ด้านสาธารณะประโยชน์ เช่นเดียวกับการดำเนินการศึกษาวิจัยเพื่อประโยชน์ด้านสาธารณสุข เมื่อมีความต้องการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่เกี่ยวกับสุขภาพ จะต้องมีการกำหนดเงื่อนไขที่สอดคล้องกันโดยเฉพาะอย่างยิ่งเมื่อมีการประมวลผลข้อมูลดังกล่าวเพื่อจุดประสงค์ด้านสุขภาพโดยบุคคลที่อยู่ภายใต้บังคับของกฎหมายในการรักษาความลับโดยอาชีพ นอกจากนี้กฎหมายของสหภาพหรือประเทศสมาชิกควรจัดให้มีมาตรการเฉพาะและเหมาะสมเพื่อปกป้องสิทธิขั้นพื้นฐานและข้อมูลส่วนบุคคลของบุคคลธรรมดา ทั้งนี้ สำหรับข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลสุขภาพ GDPR ได้

---

[284] GDPR, Article 9(2)(h).

[285] GDPR, Article 9(3).

กำหนดให้ประเทศสมาชิกสามารถคงไว้ หรือเพิ่มเงื่อนไขที่เฉพาะเจาะจง และข้อจำกัดเกี่ยวกับการประมวลข้อมูลส่วนบุคคลดังกล่าวได้[286]

หากการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นการจำเป็นสำหรับวัตถุประสงค์ทางการแพทย์ด้านเวชศาสตร์ป้องกัน หรืออาชีวเวชศาสตร์ เพื่อการประเมินความสามารถในการทำงานของพนักงาน การวินิจฉัยทางการแพทย์ การดูแลสุขภาพและสังคม หรือการรักษาหรือการจัดการระบบและการให้บริการที่เกี่ยวกับสุขภาพและสังคมตามหลักเกณฑ์ของกฎหมายสหภาพหรือกฎหมายของประเทศสมาชิก หรือเป็นไปตามสัญญากับผู้ประกอบอาชีพที่เกี่ยวกับสุขภาพ (Health Professionals) ทั้งนี้ต้องเป็นไปตามเงื่อนไข และมาตรการที่กำหนดไว้[287] DPA ได้กำหนด “วัตถุประสงค์ทางการแพทย์” ไว้ดังนี้[288]

(1) เพื่ออาชีวเวชศาสตร์หรือเวชศาสตร์ป้องกัน

(2) เพื่อการประเมินความสามารถในการทำงานของพนักงาน

(3) เพื่อการวินิจฉัยโรค

(4) เพื่อการให้บริการทางการแพทย์ หรือการรักษา

(5) เพื่อการให้บริการด้านการดูแลสังคม

(6) การบริหารระบบการดูแลสุขภาพ หรือการให้บริการด้านการดูแลสุขภาพ หรือการบริหารระบบการดูแลสังคม หรือการให้บริการด้านการดูแลสังคม

9) ประโยชน์ด้านสาธารณสุข (Public health)

สำหรับ GDPR นั้นการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวสามารถทำได้หากเป็นการจำเป็นสำหรับวัตถุประสงค์เพื่อประโยชน์ด้านสาธารณสุข เช่น การป้องกันจากภัยคุกคามข้ามพรมแดนอันอาจเป็นอันตรายร้ายแรงต่อสุขภาพ หรือเพื่อการรับรองมาตรฐานด้านคุณภาพ และความปลอดภัยของผลิตภัณฑ์ยา และเครื่องมืออุปกรณ์ทางการแพทย์ ภายใต้หลักเกณฑ์ของกฎหมายสหภาพหรือกฎหมายของประเทศสมาชิก ซึ่งมีมาตรการที่เหมาะสมและเฉพาะเจาะจงในการปกป้องสิทธิและเสรีภาพของเจ้าของข้อมูล โดยเฉพาะในการเก็บรักษาความลับตามจริยธรรมของผู้ประกอบวิชาชีพ[289]

การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวภายใต้ฐานของประโยชน์ด้านสาธารณสุขมีวัตถุประสงค์เพื่อป้องกัน และควบคุมโรคติดต่อ รวมถึงภัยคุกคามอื่นซึ่งอาจเป็นอันตรายต่อสุขภาพโดยเน้นไปที่ภัยคุกคามข้ามพรมแดน

การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวอาจมีความจำเป็นเพื่อเหตุผลสาธารณะประโยชน์ในด้านสาธารณสุขโดยไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูล อย่างไรก็ดี การประมวลผลดังกล่าวควรอยู่ภายใต้มาตรการที่เหมาะสมและเฉพาะเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของบุคคลธรรมดา คำว่า “สาธารณสุข” ควรตีความตามที่กำหนดไว้ใน Regulation (EC)

---

[286] GDPR, Recital 53.

[287] GDPR, Article 9(2)(h).

[288] DPA, Schedule 1, Part 1 (2).

[289] GDPR, Article 9(2)(i).

No 1338/2008 of the European Parliament and of the Council (11) หมายถึง องค์ประกอบทั้งหมดที่เกี่ยวข้องกับสุขภาพ ได้แก่ สถานะของสุขภาพ รวมถึงอาการเจ็บป่วยและความพิการ ปัจจัยที่มีผลต่อสถานะสุขภาพ ความต้องการการดูแลสุขภาพ ทรัพยากรที่จัดสรรให้กับการดูแลสุขภาพ การจัดหาและการเข้าถึงระบบการดูแลสุขภาพ การใช้จ่ายด้านการดูแลสุขภาพและการเงิน และสาเหตุของการตาย การประมวลผลข้อมูลที่เกี่ยวข้องกับสุขภาพเพื่อผลประโยชน์สาธารณะนี้ไม่ควรส่งผลให้มีการประมวลผลเพื่อวัตถุประสงค์อื่นโดยบุคคลที่สาม เช่น นายจ้าง บริษัทประกันภัย และธนาคาร[290]

ตัวอย่าง การประมวลข้อมูลส่วนบุคคลที่มีความอ่อนไหวด้านสุขภาพเพื่อการตรวจสอบและควบคุมทางด้านสาธารณสุข การป้องกันโรคระบาด การทดสอบประสิทธิภาพทางคลินิกของยาใหม่หรืออุปกรณ์ทางการแพทย์ใหม่โดยการทดลองกับมนุษย์ การอนุมัติขึ้นทะเบียนยาเพื่อนำไปใช้กับประชากรทั่วไป สามารถทำได้โดยชอบด้วยกฎหมายภายใต้ฐานประโยชน์ด้านสาธารณสุข

หากการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นการจำเป็นสำหรับวัตถุประสงค์เพื่อประโยชน์ด้านสาธารณสุข DPA ได้กำหนดให้การประมวลผลนั้นต้องอยู่ภายใต้ความรับผิดชอบของผู้ที่มีอาชีพให้บริการด้านสุขภาพ หรือ ผู้ที่มีหน้าที่รักษาความลับภายใต้กฎหมาย[291]

10) จดหมายเหตุ การวิจัยหรือทางสถิติ (Archiving, research and statistics)

การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวภายใต้ GDPR สามารถทำได้หากเป็นการจำเป็นสำหรับวัตถุประสงค์ในการจัดเก็บเพื่อประโยชน์สาธารณะ เพื่อการวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือวัตถุประสงค์ทางสถิติ[292] การประมวลผลดังกล่าวต้องได้สัดส่วนตามวัตถุประสงค์ และให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล อีกทั้งยังต้องจัดให้มีมาตรการที่เหมาะสมและเฉพาะเจาะจงในการปกป้องสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล[293]

ดังนั้นการวิจัยที่มิใช่การวิจัยทางวิทยาศาสตร์หรือประวัติศาสตร์จึงไม่สามารถอ้างหลักเกณฑ์นี้ในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวได้ นอกจากนี้การวิจัยดังกล่าวอาจเป็นการวิจัยที่จัดทำโดยทั้งภาครัฐและภาคเอกชน แต่ต้องเป็นการวิจัยเพื่อประโยชน์สาธารณะเท่านั้น

การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการจัดเก็บเพื่อประโยชน์สาธารณะ เพื่อการวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือวัตถุประสงค์ทางสถิติ ต้องอยู่ภายใต้มาตรการป้องกันที่เหมาะสมในการคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูล โดยต้องทำให้

---

[290] GDPR, Recital 54.

[291] DPA, Schedule 1, Part 1(3).

[292] GDPR, Article 89(1).

[293] GDPR, Article 9(2)(j).

มั่นใจว่ามีมาตรการทางเทคนิค และมาตรการทางองค์กรที่ยึดหลักการใช้ข้อมูลให้น้อยที่สุด ซึ่งรวมถึงมาตรการการเปลี่ยนข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถระบุตัวตนได้ (pseudonymization) หากการเปลี่ยนข้อมูลสามารถทำให้บรรลุวัตถุประสงค์ดังกล่าวได้ ในกรณีที่วัตถุประสงค์ดังกล่าวสามารถบรรลุได้โดยมีการประมวลผลข้อมูลเพิ่มเติมซึ่งทำให้ไม่สามารถระบุตัวตนของเจ้าของข้อมูลได้ วัตถุประสงค์ดังกล่าวสามารถดำเนินการต่อไปในลักษณะเช่นนั้นได้[294]

DPA กำหนดว่าหากการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นการจำเป็นสำหรับวัตถุประสงค์ในการจัดเก็บเพื่อประโยชน์สาธารณะ เพื่อการวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือวัตถุประสงค์ทางสถิติ[295] นอกจากการประมวลผลดังกล่าวต้องได้สัดส่วนตามวัตถุประสงค์และให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลแล้วยังต้องจัดให้มีมาตรการที่เหมาะสมและเฉพาะเจาะจงในการปกป้องสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล[296] นอกจากนี้ DPA ยังได้กำหนดให้การประมวลผลข้อมูลส่วนบุคคลต้องเป็นไปตามมาตรา 89(1) ของ GDPR และต้องเป็นการกระทำเพื่อผลประโยชน์ของส่วนรวมอีกด้วย[297]

2.2 สิทธิของเจ้าของข้อมูลส่วนบุคคล

นอกเหนือจากสิทธิของเจ้าของข้อมูลที่กำหนดโดย GDPR (อ่านรายละเอียดได้ในบทที่ 3 หัวข้อ 1.5 สิทธิของเจ้าของข้อมูลส่วนบุคคล) แล้ว DPA ยังมีข้อกำหนดสำหรับกรณีการประมวลผลข้อมูลส่วนบุคคลภายใต้การตัดสินและการประมวลผลโดยอัตโนมัตินอกเหนือจากข้อกำหนดตาม GDPR ทั้งนี้ GDPR ไม่อนุญาตให้ทำการประมวลผลข้อมูลส่วนบุคคลภายใต้การตัดสินและการประมวลผลโดยอัตโนมัติ แต่มีข้อยกเว้นให้สามารถทำได้หากได้รับอนุญาตตามกฎหมายของสหภาพยุโรปหรือประเทศสมาชิกซึ่งผู้ควบคุมอยู่ภายใต้และมีการวางมาตรการที่เหมาะสมเพื่อปกป้องสิทธิเสรีภาพและผลประโยชน์ที่ชอบด้วยกฎหมายของเจ้าของข้อมูลส่วนบุคคล[298] ซึ่ง DPA มีข้อกำหนดเพิ่มเติมจาก GDPR เพื่อเป็นการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลว่าการประมวลผลข้อมูลส่วนบุคคลภายใต้การตัดสินและการประมวลผลโดยอัตโนมัตินั้นสามารถทำได้หากกฎหมายอนุญาตให้ทำได้ ทั้งนี้นอกจากผู้ควบคุมข้อมูลส่วนบุคคลต้องมีการวางมาตรการที่เหมาะสมเพื่อป้องกันสิทธิและเสรีภาพของเจ้าของข้อมูลแล้ว การตัดสินและการประมวลผลโดยอัตโนมัติดังกล่าวต้องเป็นการตัดสินที่ก่อให้เกิดผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลอย่างมากไม่ว่าจะเป็นผลทางกฎหมายหรือทางอื่นใด อย่างไรก็ดีเมื่อมีการประมวลผลข้อมูลส่วนบุคคลภายใต้การตัดสินและการประมวลผลโดยอัตโนมัติผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงการประมวลผลนั้นภายใน 1 เดือน[299]

---

[294] GDPR, Article 89(1).

[295] GDPR, Article 89(1).

[296] GDPR, Article 9(2)(j).

[297] DPA, Schedule 1, Part 1(4).

[298] GDPR, Article 22(2)(b).

[299] DPA, Section 14.

นอกจากนี้ DPA ยังมีบทจำกัดสิทธิของเจ้าของข้อมูล ไม่ว่าข้อมูลส่วนบุคคลนั้นจะได้ทำการเก็บรวบรวมโดยตรงจากเจ้าของข้อมูลส่วนบุคคล หรือได้มาจากช่องทางอื่น โดยเจ้าของข้อมูลส่วนบุคคลจะถูกจำกัดสิทธิสำหรับการประมวลผลข้อมูลส่วนบุคคลที่ GDPR ได้กำหนดไว้ในมาตรา 5 และมาตรา 13 ถึง 21 ทั้งนี้ DPA ได้กำหนดรายละเอียดไว้ใน Schedule 2 ถึง 4 ยกตัวอย่างเช่น[300]

1) สำหรับการป้องกันอาชญากรรมและการจัดเก็บภาษี หากการประมวลผลข้อมูลส่วนบุคคลนั้นเพื่อเป็นการป้องกัน การตรวจจับอาชญากรรม การจับกุม หรือการดำเนินคดีผู้กระทำความผิด หรือเพื่อการประเมิน การจัดเก็บภาษี เจ้าของข้อมูลส่วนบุคคลจะไม่ได้รับสิทธิในการได้รับทราบข้อมูลตาม GDPR มาตรา 13 และ 14 นอกจากนี้ เจ้าของข้อมูลยังถูกจำกัดสิทธิอื่น ๆ เช่น สิทธิในการเข้าถึงข้อมูล สิทธิให้แก้ไขข้อมูล และสิทธิเรียกให้ลบ เป็นต้น[301]

2) สำหรับการควบคุมการตรวจคนเข้าเมืองให้มีประสิทธิภาพ เจ้าของข้อมูลส่วนบุคคลจะไม่ได้รับสิทธิเรียกให้ลบตาม GDPR มาตรา 17 และสิทธิให้แก้ไขข้อมูล ตาม GDPR มาตรา 16 เป็นต้น[302]

3) สำหรับข้อมูลที่ต้องเปิดเผยตามกฎหมายหรือเกี่ยวข้องกับกระบวนการทางกฎหมาย เช่น หากการเปิดเผยเป็นสิ่งจำเป็นตามบทบัญญัติของกฎหมายหรือเป็นการกระทำตามคำสั่งศาล เจ้าของข้อมูลส่วนบุคคลจะไม่ได้รับสิทธิในการคัดค้านการดำเนินการตาม GDPR มาตรา 21[303]

4) สำหรับฟังก์ชันที่ออกแบบมาเพื่อปกป้องส่วนรวม เช่น สำหรับมาตรการที่ออกแบบมาเพื่อป้องกันพฤติกรรมที่ไม่เหมาะสม การทุจริตต่อหน้าที่ เพื่อรักษาความปลอดภัยด้านสุขภาพและสวัสดิการของลูกจ้างในที่ทำงาน เพื่อป้องกันพฤติกรรมต่อต้านการแข่งขัน เจ้าของข้อมูลส่วนบุคคลจะถูกจำกัดสิทธิในการให้แก้ไขข้อมูล และสิทธิในการเรียกให้ลบ ตาม GDPR มาตรา 16 และ 17 นอกจากนี้บุคคลหรือองค์กรที่มีหน้าที่รับผิดชอบในการปฏิบัติหน้าที่เหล่านี้ยังได้รับการยกเว้นอีกด้วย เช่น หน่วยงานการแข่งขันและการตลาด (Competition and Markets Authority)[304]

5) สำหรับหน่วยงานกำกับดูแลที่เกี่ยวข้องกับการบริการด้านกฎหมาย ด้านสุขภาพ และเด็ก เช่น การตรวจสอบข้อร้องเรียนที่เกี่ยวข้องกับบริการทางกฎหมายหรือสังคม ได้รับการยกเว้นจาก GDPR มาตรา 21 โดยเจ้าของข้อมูลส่วนบุคคลจะไม่ได้รับสิทธิโต้แย้งคัดค้านการดำเนินการ[305]

---

[300] Latham & Watkins LLP. GDPR Resource Center - Derogations Tracker. สืบค้นจาก https://gdpr.lw.com/Home/Derogations

[301] DPA, Schedule 2(2).

[302] DPA, Schedule 2(4).

[303] DPA, Schedule 2(5).

[304] DPA, Schedule 2(7) and Schedule 2(11).

[305] DPA, Schedule 2(10).

6) การปกป้องข้อมูลของผู้อื่นได้รับการยกเว้นจาก GDPR มาตรา 15 โดยเจ้าของข้อมูลส่วนบุคคลจะไม่ได้รับสิทธิในการเข้าถึงข้อมูล หากการเข้าถึงนั้นเป็นการละเมิดข้อมูลของผู้อื่น[306]

7) การจัดการทางการเงินของบริษัท (Corporate Finance) ได้รับการยกเว้นจาก GDPR มาตรา 15 หากการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลในการเข้าถึงข้อมูลทำให้มีผลต่อราคา[307]

8) การพยากรณ์ทางการบริหารหรือการวางแผนการจัดการ ได้รับการยกเว้นจาก GDPR มาตรา 15 หากการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลในการเข้าถึงข้อมูลทำให้มีผลกระทบต่อธุรกิจ หรือ กิจกรรมที่เกี่ยวข้อง[308]

9) การเจรจาต่อรองกับเจ้าของข้อมูลส่วนบุคคล ได้รับการยกเว้นจาก GDPR มาตรา 15 หากการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลในการเข้าถึงข้อมูลเหล่านั้นมีแนวโน้มว่าอาจทำให้เกิดอคติต่อการเจรจา[309]

10) สำหรับวัตถุประสงค์อื่น ๆ ที่ได้รับการยกเว้น เช่น วัตถุประสงค์ด้านการสื่อสารมวลชน ด้านวิชาการ ด้านศิลปะ ด้านวรรณกรรม[310] ด้านการวิจัยทางวิทยาศาสตร์ ด้านประวัติศาสตร์ เพื่อวัตถุประสงค์ทางสถิติ[311] หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ[312]

เมื่อเปรียบเทียบ DPA กับ GDPR แล้ว DPA มีบทจำกัดสิทธิของเจ้าของข้อมูลส่วนบุคคลจากสิทธิที่ GDPR ได้บัญญัติไว้อยู่หลายบท ดังนั้นในสหราชอาณาจักร เจ้าของข้อมูลส่วนบุคคลจึงมีสิทธิน้อยกว่าสิทธิที่ได้บัญญัติไว้ใน GDPR

2.3 การรักษาความปลอดภัยของข้อมูลส่วนบุคคล

สำหรับการรักษาความปลอดภัยของข้อมูลส่วนบุคคลนั้น DPA ไม่ได้มีบทบัญญัติเพิ่มเติมจาก GDPR (ดูรายละเอียดในบทที่ 3 หัวข้อ 1.6 การรักษาความปลอดภัยของข้อมูลส่วนบุคคล) หากแต่มีบทยกเว้นสำหรับการแจ้งถึงการรั่วไหลของข้อมูลส่วนบุคคล (Data Breach Notification) ซึ่งบัญญัติให้มีการยกเว้นมิต้องแจ้งการรั่วไหลของข้อมูลส่วนบุคคลหากการประมวลผลข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อการหลีกเลี่ยงการละเมิดสิทธิของสภาผู้แทนราษฎร[313] และเพื่อวัตถุประสงค์ด้านการสื่อสารมวลชน ด้านวิชาการ ด้านศิลปะ ด้านวรรณกรรม[314]

---

[306] DPA, Schedule 2(16).

[307] DPA, Schedule 2(21).

[308] DPA, Schedule 2(22).

[309] DPA, Schedule 2(23).

[310] DPA, Schedule 2(26).

[311] DPA, Schedule 2(27).

[312] DPA, Schedule 2(28).

[313] DPA, Schedule 2(13).

[314] DPA, Schedule 2(26)(9)(c).

2.4 การร้องเรียน

2.4.1 หน่วยงานกำกับดูแล

ดังที่กล่าวมาแล้วข้างต้น GDPR มีข้อกำหนดให้ประเทศสมาชิกจัดตั้งหน่วยงานอิสระเพื่อกำกับดูแล (supervisory authority) อย่างน้อยหนึ่งหน่วยงาน โดยทำหน้าที่รับผิดชอบในการตรวจสอบการบังคับใช้กฎข้อบังคับของ GDPR เพื่อคุ้มครองสิทธิและเสรีภาพขั้นพื้นฐานของบุคคลธรรมดาที่เกี่ยวกับการประมวลข้อมูล และอำนวยความสะดวกในการไหลเวียนโดยเสรีของข้อมูลภายในสหภาพยุโรป สำนักงานคณะกรรมาธิการข้อมูล (Information Commissioner's Office - ICO) เป็นหน่วยงานกำกับดูแลการประมวลผลข้อมูลส่วนบุคคลที่สหราชอาณาจักรได้จัดตั้งขึ้นภายใต้บทบัญญัติของ GDPR ทั้งนี้ ICO เป็นหน่วยงานอิสระที่มิได้ขึ้นตรงต่อรัฐสภาของสหราชอาณาจักร ICO นั้นได้รับการสนับสนุนจากกรมดิจิทัล วัฒนธรรม สื่อ และการกีฬา และเป็นหน่วยงานกำกับดูแลอิสระที่ถือว่าเป็นหน่วยงานคุ้มครองข้อมูลแห่งชาติ เนื่องจาก ICO ไม่เพียงกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคลภายใต้ DPA และ GDPR แต่ยังกำกับดูแลข้อมูลตามกฎหมายภายในสหราชอาณาจักรอีกหลายฉบับดังต่อไปนี้ ระเบียบว่าด้วยความเป็นส่วนตัวและการสื่อสารทางอิเล็กทรอนิกส์ (ระเบียบ EC) 2003 (Privacy and Electronic Communications (EC Directive) Regulations 2003)[315] Freedom of Information Act 2000[316] และ ข้อบังคับด้านข้อมูลสิ่งแวดล้อม 2004 (Environmental Information Regulations 2004)[317]

DPA ได้มีการกำหนดหน้าที่และความรับผิดชอบของ ICO ไว้อย่างละเอียดในส่วนที่ 5 มาตรา 114 ถึง มาตรา 141 โดยได้มีการกำหนดว่า ICO ต้องกำหนดหลักปฏิบัติสำหรับการประมวลผลข้อมูลส่วนบุคคลในลักษณะต่าง ๆ เช่น หลักปฏิบัติสำหรับการประมวลข้อมูลส่วนบุคคลที่เหมาะสมกับวัยสำหรับผู้เยาว์[318] หรือ หลักปฏิบัติสำหรับการประมวลผลข้อมูลส่วนบุคคลสำหรับการสื่อสารมวลชน[319] เป็นต้น

ในการปฏิบัติงานของ ICO ในฐานะหน่วยงานกำกับดูแล DPA ได้มีบทบัญญัติให้ ICO มีอำนาจในการออกหนังสือ ดังต่อไปนี้

1) หนังสือขอข้อมูล (Information notices)

หนังสือขอข้อมูลคือหนังสือที่ ICO ออกเพื่อขอข้อมูลจากผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเพื่อนำไปใช้ในการดำเนินการตามหน้าที่อย่าง

---

[315] Privacy and Electronic Communications (EC Directive) Regulations 2003 เป็นกฎหมายภายในของสหราชอาณาจักรซึ่งกำกับดูแลการส่งข้อความที่บันทึกโดยอัตโนมัติเพื่อวัตถุประสงค์ทางการตลาดทางตรงผ่านทางโทรศัพท์โดยไม่ได้รับความยินยอมจากผู้ใช้บริการล่วงหน้า

[316] Freedom of Information Act 2000 เป็นกฎหมายภายในสหราชอาณาจักรที่สร้าง "สิทธิในการเข้าถึง" ของสาธารณะต่อข้อมูลที่จัดขึ้นโดยหน่วยงานสาธารณะ ที่มีขอบเขตบังคับใช้ในอังกฤษ เวลส์ และไอร์แลนด์เหนือ และในขอบเขตที่จำกัดในสกอตแลนด์

[317] Environmental Information Regulations 2004 ให้สิทธิ์ตามกฎหมายในการเข้าถึงข้อมูลด้านสิ่งแวดล้อมที่จัดทำโดยหน่วยงานสาธารณะของสหราชอาณาจักร ที่มีขอบเขตบังคับใช้ในอังกฤษ เวลส์ และไอร์แลนด์เหนือ และในขอบเขตที่จำกัดในสกอตแลนด์

[318] DPA, Section 123.

[319] DPA, Section 124.

สมเหตุสมผล นอกจากนี้ ICO ยังสามารถกำหนดให้ "บุคคลใด ๆ" ให้ข้อมูลที่จำเป็นตามสมควรเพื่อวัตถุประสงค์ในการตรวจสอบความบกพร่องในการปฏิบัติตามข้อกำหนดหรือเพื่อพิจารณาว่าการประมวลผลนั้นเป็นการประมวลผลส่วนบุคคลหรือเพื่อใช้ในครัวเรือนซึ่งถือเป็นข้อยกเว้นหรือไม่[320]

2) หนังสือแจ้งเพื่อทำการประเมิน (Assessment Notices)

DPA นั้นกำหนดให้ ICO มีอำนาจพิเศษในการประเมินการประมวลผลข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล โดย ICO สามารถออกหนังสือแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอนุญาตให้ ICO เข้าสู่สถานที่ทำการของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อตรวจสอบเอกสารและอุปกรณ์ที่เกี่ยวข้อง โดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องให้คำอธิบาย ทำสำเนาเอกสารที่เกี่ยวข้องให้กับ ICO และให้ ICO สัมภาษณ์เจ้าหน้าที่ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล[321]

3) หนังสือบังคับใช้ (Enforcement notices)

ในกรณีที่ ICO พบว่าเกิดการละเมิดในการประมวลผลข้อมูลส่วนบุคคล ICO สามารถออกหนังสือบังคับใช้ เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลทำการแก้ไขการละเมิดนั้น[322]

4) หนังสือการลงโทษ (Penalty notice)

ICO สามารถออกหนังสือเพื่อประกาศบทลงโทษในกรณีที่มีการละเมิดข้อกำหนดใน GDPR และ DPA ในการประมวลผลข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล โดยการลงโทษนั้นอยู่ในรูปแบบของค่าปรับ[323]

2.4.2 กระบวนการร้องเรียน

เมื่อเจ้าของข้อมูลส่วนบุคคลพิจารณาแล้วเห็นว่าการประมวลผลข้อมูลส่วนบุคคลของตนละเมิดข้อกำหนดตาม GDPR เจ้าของข้อมูลส่วนบุคคลมีสิทธิยื่นคำร้องต่อ ICO ได้[324] (ดูรายละเอียดเพิ่มเติมจากบทที่ 3 หัวข้อ 1.8 การร้องเรียน) ทั้งนี้หากการร้องเรียนของเจ้าของข้อมูลส่วนบุคคลเป็นการละเมิดสิทธิของเจ้าของข้อมูลส่วนบุคคลภายใต้บทบัญญัติของประเทศสมาชิกอื่นที่มิใช่สหราชอาณาจักร ทาง ICO จะทำการส่งต่อข้อร้องเรียนนั้นให้กับหน่วยงานกำกับดูแลของประเทศสมาชิกดังกล่าวพร้อมกับแจ้งให้กับผู้ร้องเรียนทราบว่าได้มีการส่งต่อข้อร้องเรียนนั้นแล้ว[325]

ICO มีหน้าที่ดำเนินการเกี่ยวกับคำร้องจากเจ้าของข้อมูลส่วนบุคคล และแจ้งความคืบหน้าของการตรวจสอบหรือผลของคำร้อง รวมถึงความเป็นไปได้ของการได้รับการเยียวยา

---

[320] DPA, Section 142.

[321] DPA, Section 146.

[322] DPA, Section 149.

[323] DPA, Section 155-157.

[324] DPA, Section 165(1).

[325] DPA, Section 165(6).

ทางศาลให้เจ้าของข้อมูลส่วนบุคคลทราบ ทั้งนี้ ICO ต้องแจ้งความคืบหน้าหรือผลของการร้องเรียนให้ผู้ร้องทราบภายใน 3 เดือนนับแต่วันได้รับคำร้อง[326]

เจ้าของข้อมูลส่วนบุคคลมีสิทธิยื่นฟ้องผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลต่อศาลหากเจ้าของข้อมูลส่วนบุคคลเห็นว่าผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลกระทำการละเมิดสิทธิของตนภายใต้ข้อกำหนด GDPR และ DPA[327]

2.5 การเยียวยา และบทลงโทษ

2.5.1 การเยียวยา

ภายใต้ข้อกำหนด GDPR บุคคลที่ได้รับความเดือดร้อนหรือความเสียหายแก่ทรัพย์สิน หรือสิ่งอื่นใดอันเป็นผลจากการละเมิดข้อกำหนดนี้ มีสิทธิได้รับค่าสินไหมทดแทนจากผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลสำหรับความเสียหายที่เกิดขึ้นนั้น[328] ทั้งนี้ DPA ได้ให้คำจำกัดความของ “สิ่งอื่นใด” ว่ารวมถึง “ความทุกข์”[329] อย่างไรก็ตาม ศาลอุทธรณ์ของอังกฤษได้พิพากษาว่าความเสียหายที่เจ้าของข้อมูลส่วนบุคคลได้รับจากการละเมิดนั้นมิจำเป็นจะต้องเป็นความเสียหายแก่ทรัพย์สิน หรือสิ่งอื่นใด

ตัวอย่าง ในคดี Lloyd v Google LLC [2019] EWCA Civ 1599 Richard Lloyd อดีตผู้อำนวยการของกลุ่มผู้บริโภค Which? ได้ยื่นฟ้องบริษัท Google ในการดำเนินคดีแบบกลุ่ม (Class Action) เนื่องจากพบว่าบริษัท Google ใช้ช่องโหว่ระบบคุกกี้และการจดจำอดีตหน้าเว็บเพจที่ผู้ใช้เรียกใช้งานในเว็บเบราว์เซอร์ซาฟารีของโทรศัพท์ไอโฟน (iPhone) เพื่อดักเก็บข้อมูลโดยผิดกฎหมาย แม้ว่าผู้ใช้งานจะปิดการตั้งค่าความเป็นส่วนตัวแล้วก็ยังไม่สามารถปิดการทำงานได้อย่างถาวร โดย Google นำข้อมูลเหล่านี้ไปใช้งานในการแนะนำบริการและสินค้าในธุรกิจเครือข่ายโฆษณาของตน โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลในระหว่างปี พ.ศ. 2554-2555 ศาลชั้นต้นได้พิพากษาว่าโจทก์มิได้รับความเสียหายภายใต้บทบัญญัติของ DPA 2018 แต่ในปี พ.ศ. 2562 ศาลอุทธรณ์อังกฤษได้พิพากษากลับคำตัดสินของศาลชั้นต้น โดยพิพากษาว่าถึงแม้ผู้ใช้โทรศัพท์ไอโฟนมิได้เรียกร้องค่าสินไหมทดแทนสำหรับความเสียหายด้านการเงิน หรือความทุกข์ที่เกิดจากการละเมิดข้อมูลส่วนบุคคลของ Google แต่ผู้ใช้ไอโฟนเหล่านั้นได้รับความเสียหายจากการละเมิดการประมวลผลข้อมูลส่วนบุคคลที่ชัดเจน ซ้ำ ๆ และเป็นที่แพร่หลายโดยเจตนาของ Google และศาลพิพากษาว่าการสูญเสียการควบคุมข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลนั้นเป็นถือเป็นความเสียหายซึ่งต้องได้รับการเยียวยา นอกจากเป็นครั้งแรกที่ศาลพิพากษาว่าความเสียหายจากการละเมิดการประมวลผลข้อมูลส่วนบุคคลแม้ยังไม่เกิดความเสียหายที่สามารถจับต้องได้ก็ถือว่าเป็นความเสียหายที่เกิดขึ้นจริงแล้ว ยังเป็นครั้งแรกที่ศาลประเทศอังกฤษได้พิจารณาคดีการละเมิดข้อมูลส่วนบุคคลในลักษณะการดำเนินคดีแบบกลุ่มอีกด้วย ทั้งนี้ศาลตัดสินว่า Richard Lloyd ถือเป็นตัวแทน

---

[326] DPA, Section 166(1).

[327] DPA, Section 167.

[328] GDPR, Article 82(1).

[329] DPA, Section 168(1).

ของผู้ใช้ไอโฟนที่ใช้เว็บเบราว์เซอร์ซาฟารีทั้งหมดในประเทศอังกฤษและเวลส์[330] สำหรับคดีนี้ Google ได้ฎีกาคำพิพากษาของศาลอุทธรณ์ และในขณะที่ทำการวิจัยคดีนี้ยังไม่ถึงที่สิ้นสุด

2.5.2 บทลงโทษ

บทลงโทษสำหรับผู้ฝ่าฝืนข้อกำหนดของ DPA อยู่ในรูปของค่าปรับทางปกครอง โดย ICO หน่วยงานผู้มีหน้าที่กำกับดูแลเป็นผู้มีอำนาจในการลงโทษ โดยอัตราค่าปรับของการละเมิดบทบัญญัติของ DPA นั้นมี 2 ระดับ คือ

1) ระดับสูงสุด คือ ไม่เกิน 20,000,000 ยูโร หรือในกรณีขององค์กรธุรกิจ (undertakings) ต้องระวางค่าปรับทางปกครองไม่เกินร้อยละ 4 ของมูลค่ายอดขายทั่วโลกของปีงบประมาณก่อนหน้า แล้วแต่จำนวนใดจะสูงกว่า[331]

2) ระดับทั่วไป ต้องระวางโทษทางปกครองไม่เกิน 10,000,000 ยูโร หรือในกรณีขององค์กรธุรกิจ (undertakings) ต้องระวางค่าปรับทางปกครองไม่เกินร้อยละ 2 ของมูลค่ายอดขายทั่วโลกของปีงบประมาณก่อนหน้า แล้วแต่จำนวนใดจะสูงกว่า[332]

ตัวอย่าง ในเดือนกรกฎาคม พ.ศ. 2562 ICO ได้สั่งปรับสายการบินบริติชแอร์เวย์เป็นจำนวน 183 ล้านปอนด์ หรือ 1.5% ของรายได้ปี พ.ศ. 2561 หลังจากพบว่าความบกพร่องทางมาตรฐานความปลอดภัยได้ทำให้ข้อมูลส่วนบุคคลของลูกค้า 500,000 รายรั่วไหล การแฮ็กเกิดขึ้นระหว่างวันที่ 21 สิงหาคม ถึง 5 กันยายน พ.ศ. 2561 โดยแฮ็กเกอร์ได้ขโมยชื่อลูกค้า ที่อยู่ อีเมลและข้อมูลบัตรเครดิต เช่น หมายเลขบัตรเครดิต วันหมดอายุ และรหัสสามหลักที่ด้านหลังบัตรเครดิตไป[333] ต่อมาในเดือนพฤศจิกายน พ.ศ. 2561 มีรายงานโดยบริษัทรักษาความปลอดภัยทางไซเบอร์ Flashpoint และ Risk IQ ว่ารายละเอียดบัตรเครดิตของลูกค้าของบริติชแอร์เวย์เกือบ 25,000 รายถูกนำไปขายบนเว็บมืดโดยแฮ็กเกอร์ชาวรัสเซีย ทั้งนี้คำพิพากษาของศาลสูงได้อนุญาตให้ลูกค้าที่ได้รับผลกระทบให้เข้าร่วมการดำเนินคดีแบบกลุ่มได้[334]

อย่างไรก็ดี นับตั้งแต่มีการประกาศใช้ GDPR และ DPA นั้น ICO ยังมิได้มีการสั่งปรับองค์กรใดๆ สำหรับการฝ่าฝืนบทบัญญัติที่เกี่ยวข้องกับข้อมูลส่วนบุคคลชีวภาพ

---

[330] Covington & Burling LLP. (2019). Landmark Case Opens the Door to UK Data Protection Consumer Class Actions. สืบค้นจาก https://www.cov.com/en/news-and-insights/insights/2019/10/landmark-case-opens-the-door-to-uk-data-protection-consumer-class-actions

[331] DPA, Section 157(5).

[332] DPA, Section 157(6).

[333] Cellan-Jones, R. (2019). British Airways faces record £183m fine for data breach. สืบค้นจาก https://www.bbc.com/news/business-48905907

[334] Adams, D. (2019). Five of the Biggest Data Breach Fines Issued by the ICO. สืบค้นจาก https://digit.fyi/five-of-the-biggest-data-breach-fines-issued-by-the-ico/

3. หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลประเภทชีวภาพตามกฎหมายของรัฐอิลลินอยส์ ประเทศสหรัฐอเมริกา

รัฐอิลลินอยส์ ประเทศสหรัฐอเมริกาได้มีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลประเภทชีวภาพ (Biometric Information Privacy Act – BIPA (740 ILCS 14/)) เมื่อวันที่ 3 ตุลาคม 2551 โดยพระราชบัญญัติฉบับนี้นับเป็นพระราชบัญญัติฉบับแรกของประเทศสหรัฐอเมริกาที่ให้ความคุ้มครองข้อมูลส่วนบุคคลประเภทชีวภาพโดยเฉพาะ และถือได้ว่าเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลประเภทชีวภาพที่ครอบคลุมมากที่สุดในสหรัฐอเมริกา อนึ่ง รัฐอิลลินอยส์ได้เห็นความสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคลประเภทชีวภาพเนื่องจากการเจริญเติบโตของการนำข้อมูลชีวภาพมาใช้ในธุรกิจ โดยมักมีการนำข้อมูลส่วนบุคคลประเภทชีวภาพมาใช้ในการทำธุรกรรมทางการเงิน หรือการให้บริการการรักษาความปลอดภัย ทั้งนี้บริษัทขนาดใหญ่หลายแห่งได้เลือกให้เมืองชิคาโก รัฐอิลลินอยส์เป็นเมืองที่ใช้ทดลอง (pilot) ระบบงานที่ใช้ข้อมูลชีวภาพในการทำธุรกรรมทางการเงิน เช่น การสแกนลายนิ้วมือสำหรับการซื้อของที่ร้านขายของชำ สถานีบริการน้ำมัน หรือโรงอาหารของโรงเรียน เป็นต้น[335] ก่อนการประกาศใช้ BIPA รัฐอิลลินอยส์ได้มีการประกาศใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล (Personal Information Protection Act - PIPA (815 ILCS 530/)) ในเดือนมิถุนายน พ.ศ. 2548 ซึ่งมีผลบังคับใช้ในวันที่ 1 มกราคม พ.ศ. 2549

BIPA ได้ประกาศใช้ในปี พ.ศ. 2551 ในขณะที่บริษัท Pay By Touch กำลังยื่นล้มละลาย บริษัท Pay By Touch ดำเนินธุรกิจเกี่ยวกับระบบการสแกนลายนิ้วมือที่ใหญ่ที่สุดในอิลลินอยส์ ซึ่งกำลังทดลองใช้ระบบ (pilot) การชำระเงินด้วยการสแกนลายนิ้วมือที่ร้านขายของชำ สถานีบริการน้ำมัน และโรงอาหารของโรงเรียน การยื่นล้มละลายของ Pay By Touch ทำให้เจ้าของข้อมูลส่วนบุคคลเกิดความวิตกกังวลถึงสิ่งที่อาจเกิดขึ้นกับข้อมูลชีวภาพของตนที่อยู่ในระบบของ Pay By Touch[336]

BIPA กำหนดให้มีการสร้างระบบป้องกัน และขั้นตอนที่เกี่ยวข้องกับการเก็บ รวบรวม เปิดเผยและการทำลายข้อมูลส่วนบุคคลประเภทชีวภาพ เนื่องจากข้อมูลชีวภาพ เป็นลักษณะทางชีวภาพที่เป็นเอกลักษณ์ของบุคคล ไม่ว่าจะเป็น ลายนิ้วมือ (fingerprint) พิมพ์เสียง (voiceprint) ม่านตา หรือรูปทรงใบหน้า ล้วนแล้วแต่เป็นข้อมูลที่ละเอียดอ่อนที่สุดของบุคคล ซึ่งเมื่อข้อมูลส่วนบุคคลประเภทชีวภาพถูกละเมิดจะไม่มีทางแก้ไขได้ และทำให้มีความเสี่ยงสูงในการถูกขโมยตัวตน (identity theft) และมีแนวโน้มที่เจ้าของข้อมูลส่วนบุคคลจะถอนตัวจากการทำธุรกรรมที่ใช้ข้อมูลชีวภาพ[337]

---

[335] 740 ILCS 14/5.

[336] Insler, C. N. (2018). How to ride the litigation rollercoaster driven by the Biometric Information Privacy Act. *Southern Illinois University Law Journal, 43*, 819-826.

[337] 740 ILCS 14/5.

3.1 ขอบเขตของการบังคับใช้

BIPA เป็นกฎหมายระดับรัฐของรัฐอิลลินอยส์ บัญญัติภายใต้อำนาจของรัฐ และเช่นเดียวกันกับกฎหมายระดับรัฐอื่น ๆ มีผลบังคับใช้ในรัฐอิลลินอยส์ โดยมีขอบเขตใช้บังคับกับการประมวลผลข้อมูลส่วนบุคคลประเภทชีวภาพโดยผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งมีสถานประกอบการที่ตั้งอยู่ในรัฐอิลลินอยส์ โดยผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นนิติบุคคล (Private Entity) ซึ่ง BIPA ได้ให้คำจำกัดความของ “นิติบุคคล” ไว้ดังนี้ “บุคคล ห้างหุ้นส่วน บริษัท บริษัทจำกัด สมาคมหรือกลุ่มต่าง ๆ ไม่ว่าจะจัดตั้งอย่างไรก็ตาม นิติบุคคลนั้นไม่รวมถึง หน่วยงานของรัฐทั้งระดับรัฐและระดับท้องถิ่น และไม่รวมถึงศาลของรัฐอิลลินอยส์ เจ้าพนักงานของศาล และผู้พิพากษาของศาลดังกล่าว”[338]

เช่นเดียวกันกับกฎหมายอื่นของรัฐอิลลินอยส์ BIPA เป็นพระราชบัญญัติที่ไม่มีผลบังคับใช้นอกขอบเขตของรัฐอิลลินอยส์ แต่อย่างไรก็ดีในโลกดิจิทัล Google ซึ่งเก็บข้อมูลอยู่ในระบบคลาวด์ได้ถูกฟ้องดำเนินคดีโดยผู้ที่อาศัยอยู่ในรัฐอิลลินอยส์ โดยศาลให้ความเห็นว่าภาพถ่ายที่ Google นำไปประมวลผลด้วยซอฟต์แวร์จดจำใบหน้านั้นถ่ายในรัฐอิลลินอยส์ และถ่ายโดยชาวอิลลินอยส์ โดยอัปโหลดรูปถ่ายนั้นไปยังบริการบนคลาวด์ของ Google-Photos จากที่อยู่ IP ของรัฐอิลลินอยส์ ศาลพิจารณาแล้วมีคำพิพากษาว่าศาลมีอำนาจพิจารณาคดีดังกล่าว แต่ศาลได้ตั้งข้อสังเกตว่าประเด็นปัญหาดังกล่าวเป็นเรื่องซับซ้อน และคู่กรณีไม่ได้ชี้แจงให้ศาลทราบอย่างละเอียด[339]

3.2 ความหมายของข้อมูลส่วนบุคคล

3.2.1 ความหมายของข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของรัฐอิลลินอยส์ (PIPA) ซึ่งประกาศใช้ก่อน BIPA ได้ให้ความหมายของคำว่า “ข้อมูลส่วนบุคคล” ไว้ว่า

“ข้อมูลส่วนบุคคล” หมายถึง[340]

1) *ชื่อ หรืออักษรย่อของชื่อ และนามสกุลของบุคคล ประกอบกับ หนึ่งในองค์ประกอบดังต่อไปนี้ ซึ่งเมื่อชื่อ หรือองค์ประกอบเหล่านี้มิได้มีการเข้ารหัส หรือปิดบัง หรือมีการเข้ารหัส หรือปิดบัง แต่กุญแจสำหรับการถอดรหัส หรือเปิดเผย เพื่ออ่านชื่อ หรือองค์ประกอบเหล่านั้นได้ถูกนำไปโดยมิได้รับอนุญาตจากการละเมิดความปลอดภัย*

(1) หมายเลขบัตรประกันสังคม

(2) หมายเลขใบขับขี่ หรือหมายเลขบัตรประจำตัวที่รัฐออกให้

(3) หมายเลขบัญชี หรือ หมายเลขบัตรเครดิต/บัตรเดบิต หรือหมายเลขบัญชี หรือหมายเลขบัตรเครดิต ประกอบกับ รหัสความปลอดภัย รหัสผ่าน หรือพาสเวิร์ด ซึ่งสามารถนำไปใช้ในการเข้าสู่บัญชีการเงินของแต่ละบุคคลได้

(4) ข้อมูลด้านการแพทย์

(5) ข้อมูลด้านการประกันสุขภาพ

---

[338] 740 ILCS 14/10.

[339] Rivera v. Google Inc., 238 F. Supp. 3d 1088 (N.D. Ill. 2017)

[340] 755 ILCS 50/5.

(6) ข้อมูลชีวภาพที่สร้างขึ้นจากการวัดหรือการวิเคราะห์ทางเทคนิคของลักษณะร่างกายมนุษย์ที่ใช้ในการยืนยันบุคคล เช่น ลายนิ้วมือ จอตา หรือภาพม่านตา หรือลักษณะทางกายภาพที่ไม่ซ้ำกันอื่น ๆ หรือข้อมูลชีวภาพที่อยู่ในรูปแบบดิจิตอล

2) *ชื่อผู้ใช้หรืออีเมล ประกอบกับรหัสผ่าน หรือคำถามเพื่อความปลอดภัย พร้อมคำตอบที่จะทำให้สามารถเข้าถึงบัญชีออนไลน์ เมื่อชื่อผู้ใช้ อีเมล รหัสผ่าน หรือคำถามเพื่อความปลอดภัยและคำตอบไม่ได้ถูกเข้ารหัสหรือปิดบัง หรือถูกเข้ารหัสหรือปิดบัง แต่กุญแจเพื่อถอดรหัสหรือเปิดเผย ได้ถูกนำไปโดยมิได้รับอนุญาตจากการละเมิดความปลอดภัย*

"ข้อมูลส่วนบุคคล" ไม่รวมถึงข้อมูลที่ได้รับการเปิดเผยต่อสาธารณชนโดยชอบด้วยกฎหมายโดยรัฐบาลกลาง รัฐ หรือรัฐบาลท้องถิ่น"

3.2.2 ความหมายของข้อมูลส่วนบุคคลประเภทชีวภาพ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลประเภทชีวภาพของรัฐอิลลินอยส์ (BIPA) ได้ให้ความหมายของ "สิ่งระบุตัวตนชีวภาพ (Biometrics Identifier)" ว่าหมายถึง การสแกนม่านตาหรือจอประสาทตา ลายนิ้วมือ เสียง หรือการสแกนมือ หรือใบหน้า ทั้งนี้สิ่งระบุตัวตนชีวภาพไม่รวมถึงตัวอย่างลายมือ ลายเซ็น ภาพถ่าย ตัวอย่างทางชีวภาพของมนุษย์ที่ใช้สำหรับการทดสอบหรือการคัดกรองทางวิทยาศาสตร์ ข้อมูลประชากร คำอธิบายรอยสัก คำอธิบายทางกายภาพ เช่น ส่วนสูง น้ำหนัก สีผม หรือสีตา นอกจากนี้ สิ่งระบุตัวตนชีวภาพยังไม่รวมถึง อวัยวะ เนื้อเยื่อ หรือชิ้นส่วนที่ได้จากการบริจาคตามที่กำหนดไว้ในพระราชบัญญัติการบริจาคอวัยวะ (Illinois Anatomical Gift Act - 755 ILCS 50/) หรือ เลือด หรือเซรุ่ม ที่เก็บไว้ในนามของผู้รับหรือผู้ที่อาจได้รับการปลูกถ่ายอวัยวะ ไม่ว่าอวัยวะนั้นจะมาจากผู้ที่ยังมีชีวิตอยู่ หรือมาจากผู้ที่เสียชีวิตไปแล้ว และได้รับหรือเก็บรักษาโดยหน่วยงานจัดหาอวัยวะที่ได้รับมอบหมายจากรัฐบาลกลาง สิ่งระบุตัวตนชีวภาพไม่รวมถึงวัสดุชีวภาพที่มีการควบคุมภายใต้พระราชบัญญัติความเป็นส่วนตัวข้อมูลทางพันธุกรรม (Genetic Information Privacy Act) สิ่งระบุตัวตนชีวภาพไม่รวมถึงข้อมูลที่ได้จากผู้ป่วยในการดูแลสุขภาพหรือข้อมูลที่รวบรวมใช้หรือเก็บรักษาเพื่อการรักษาพยาบาล การชำระเงิน หรือการดำเนินงานภายใต้พระราชบัญญัติประกันสุขภาพและความรับผิดชอบต่อหน้าที่ 1996 (Health Insurance Portability and Accountability Act 1996)[341] ของรัฐบาลกลาง สิ่งระบุตัวตนชีวภาพไม่รวมถึงการเอกซเรย์ ไม่ว่าจะเป็นการเอกซเรย์รังสี เอกซเรย์คอมพิวเตอร์ (ซีทีสแกน) เอ็มอาร์ไอ PET/CT สแกน หรือการเอกซเรย์เต้านม (mammography) หรือ ภาพของกายวิภาคของมนุษย์ที่ใช้ในการวินิจฉัยพยากรณ์โรคหรือรักษาโรค หรือสภาวะด้านสุขภาพอื่น ๆ หรือเพื่อตรวจสอบเพิ่มเติมการทดสอบหรือการคัดกรองทางวิทยาศาสตร์[342]

นอกจากนี้ BIPA ยังได้ให้ความหมายของ "ข้อมูลชีวภาพ (Biometric Information)" ว่า หมายถึงข้อมูลสิ่งระบุตัวตนชีวภาพใด ๆ โดยไม่คำนึงถึงวิธีการที่ถูกบันทึก แปลง

---

[341] HIPAA เป็นกฎหมายคุ้มครองข้อมูลด้านสุขภาพที่เกี่ยวข้องกับการรักษาพยาบาลของผู้ป่วยในทุกรูปแบบ โดยข้อมูลด้านสุขภาพจะต้องได้รับการคุ้มครองจากการฉ้อโกงและการโจรกรรมและแก้ปัญหาข้อจำกัดเกี่ยวกับการประกันสุขภาพ (ที่มา : https://www.hipaaguide.net/hipaa-for-dummies/)

[342] 740 ILCS 14/10.

จัดเก็บ หรือใช้ ที่นำไปใช้ในการระบุตัวบุคคล ทั้งนี้ ข้อมูลชีวภาพไม่รวมถึงข้อมูลที่ได้มาจากข้อมูลหรือขั้นตอนที่อยู่ภายใต้การยกเว้นของสิ่งระบุตัวตนชีวภาพ[343]

3.3 หลักการคุ้มครองข้อมูลส่วนบุคคล

ภายใต้ข้อบังคับของ BIPA นั้นได้มีการกำหนดหลักการในการประมวลผลข้อมูลส่วนบุคคลชีวภาพไว้ดังนี้

3.3.1 หลักความชอบด้วยกฎหมาย เป็นธรรม และโปร่งใส (Lawfully, fairly and in a transparent manner)

การประมวลผลข้อมูลส่วนบุคคลชีวภาพนั้นจะต้องกระทำโดยชอบด้วยกฎหมาย เป็นธรรมและมีความโปร่งใสต่อเจ้าของข้อมูลส่วนบุคคล โดย BIPA ได้บัญญัติหลักการประมวลผลข้อมูลชีวภาพโดยชอบด้วยกฎหมายไว้ใน มาตรา 15 (b) นอกจากนี้ยังมีการกำหนดให้ต้องมีการจัดทำนโยบายการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลชีวภาพเป็นลายลักษณ์อักษรและเปิดเผยต่อสาธารณชน โดยในนโยบายนั้นต้องกำหนดตารางการเก็บรักษา และแนวทางสำหรับการทำลายสิ่งระบุตัวตน หรือข้อมูลส่วนบุคคลประเภทชีวภาพอย่างถาวร[344] นอกจากนี้ ยังต้องมีการแจ้งให้เจ้าของข้อมูลได้รับทราบเป็นลายลักษณ์อักษรก่อนการเก็บรวบรวมข้อมูลส่วนบุคคลชีวภาพ ทั้งนี้ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงวัตถุประสงค์ และระยะเวลาการจัดเก็บอีกด้วย[345]

3.3.2 หลักจำกัดวัตถุประสงค์ (Purpose Limitation)

ข้อมูลส่วนบุคคลชีวภาพและสิ่งระบุตัวตนชีวภาพจะต้องใช้ภายใต้วัตถุประสงค์ที่กำหนด โดย BIPA ไม่อนุญาตให้ขาย เช่า แลกเปลี่ยน หรือทำกำไรจากสิ่งระบุตัวตนชีวภาพ หรือข้อมูลส่วนบุคคลชีวภาพและต้องทำการลบข้อมูลชีวภาพและสิ่งระบุตัวตนชีวภาพเมื่อบรรลุวัตถุประสงค์ในการจัดเก็บ[346]

3.3.3 หลักข้อจำกัดในการจัดเก็บ (Storage Limitation)

เมื่อบรรลุวัตถุประสงค์ในการจัดเก็บข้อมูลส่วนบุคคลชีวภาพ และสิ่งระบุตัวตนชีวภาพแล้ว หรือครบ 3 ปีนับจากวันสุดท้ายที่ผู้ควบคุมข้อมูลส่วนบุคคลประเภทชีวภาพได้ติดต่อกับเจ้าของข้อมูลส่วนบุคคลผู้ควบคุมข้อมูลส่วนบุคคลจะต้องทำการลบข้อมูลชีวภาพ และสิ่งระบุตัวตนชีวภาพเสีย[347]

3.3.4 หลักการรักษาความลับ (Confidentiality)

การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลชีวภาพและสิ่งระบุตัวตนชีวภาพนั้นจะต้องมีมาตรการในการรักษาความปลอดภัยที่เหมาะสม โดยมาตรการการรักษาความปลอดภัยนั้นจะต้องมีมาตรฐานในระดับเดียวกับองค์กรในกลุ่มอุตสาหกรรมของตน และต้องมีการ

---

[343] 740 ILCS 14/10.

[344] 740 ILCS 14/15(a).

[345] 740 ILCS 14/15(b).

[346] 740 ILCS 14/15(a).

[347] 740 ILCS 14/15(a).

รักษาความปลอดภัยที่เท่ากันหรือมากกว่าการรักษาความปลอดภัยของข้อมูลที่เป็นความลับและข้อมูลที่มีความอ่อนไหวอื่น ๆ[348]

3.3.5 หลักความรับผิดชอบ (Accountability)

ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องมีความรับผิดชอบในการเก็บรวบรวม ใช้และเปิดเผยข้อมูลส่วนบุคคลชีวภาพ โดยมีการดำเนินการตามหลักมาตรฐานการรักษาความปลอดภัยของกลุ่มอุตสาหกรรมของตน โดยเฉพาะอย่างยิ่งต้องมีความรับผิดชอบต่อข้อมูลส่วนบุคคลชีวภาพในอัตราที่เท่ากันหรือมากกว่าข้อมูลที่เป็นความลับหรือข้อมูลที่มีความอ่อนไหวอื่น ๆ[349]

3.4 การประมวลผลข้อมูลส่วนบุคคลที่ชอบด้วยกฎหมาย

ภายใต้ข้อบังคับของ BIPA การประมวลผลข้อมูลส่วนบุคคลประเภทชีวภาพนั้นจะสามารถทำได้หากผู้ควบคุมข้อมูลส่วนบุคคลได้รับความยินยอมเป็นลายลักษณ์อักษร (written consent) จากเจ้าของข้อมูลส่วนบุคคล โดยในการขอความยินยอมนั้นผู้ควบคุมข้อมูลส่วนบุคคลจะต้องระบุวัตถุประสงค์และระยะเวลาที่มีการรวบรวม จัดเก็บ และใช้

ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวม ซื้อ หรือรับโดยทางการค้า สิ่งระบุตัวตนทางชีวภาพ หรือข้อมูลส่วนบุคคลประเภทชีวภาพ เว้นแต่[350]

1) ได้ทำการแจ้งเจ้าของข้อมูลส่วนบุคคล หรือตัวแทนที่ได้รับอนุญาตตามกฎหมาย เป็นลายลักษณ์อักษรว่ามีการรวบรวม หรือเก็บสิ่งระบุตัวตนทางชีวภาพ หรือข้อมูลส่วนบุคคลประเภทชีวภาพ

2) ได้ทำการแจ้งเจ้าของข้อมูลส่วนบุคคล หรือตัวแทนที่ได้รับอนุญาตตามกฎหมายเป็นลายลักษณ์อักษร เกี่ยวกับวัตถุประสงค์และระยะเวลาที่มีการรวบรวม จัดเก็บ และใช้สิ่งระบุตัวตนทางชีวภาพ หรือข้อมูลส่วนบุคคลประเภทชีวภาพ

3) ได้รับอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลส่วนบุคคล หรือตัวแทนที่ได้รับอนุญาตตามกฎหมาย

BIPA ไม่อนุญาตให้ผู้ควบคุมข้อมูลส่วนบุคคลประเภทชีวภาพขาย เช่า แลกเปลี่ยน หรือทำกำไรจากสิ่งระบุตัวตนทางชีวภาพ หรือข้อมูลส่วนบุคคลประเภทชีวภาพกับบุคคลที่สาม และต้องปฏิบัติต่อข้อมูลชีวภาพเสมือนเป็นข้อมูลที่ละเอียดอ่อนและเป็นความลับ[351]

ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลที่ครอบครองสิ่งระบุตัวตนทางชีวภาพ หรือข้อมูลส่วนบุคคลประเภทชีวภาพเปิดเผยหรือเปิดเผยซ้ำ เว้นแต่[352]

1) เจ้าของข้อมูลส่วนบุคคล หรือตัวแทนที่ได้รับอนุญาตตามกฎหมายยินยอมให้มีการเปิดเผยหรือการเปิดเผยซ้ำ

---

[348] 740 ILCS 14/15(e).

[349] 740 ILCS 14/15(e).

[350] 740 ILCS 14/15(b).

[351] 740 ILCS 14/15(c).

[352] 740 ILCS 14/15(d).

2) การเปิดเผยข้อมูลหรือการเปิดเผยข้อมูลซ้ำเป็นการทำให้ธุรกรรมทางการเงินที่เจ้าของข้อมูลส่วนบุคคล หรือตัวแทนที่ได้รับอนุญาตตามกฎหมายได้ทำการร้องขอ หรืออนุญาตให้ดำเนินการเสร็จสมบูรณ์

3) การเปิดเผยหรือการเปิดเผยซ้ำเป็นสิ่งที่ต้องกระทำภายใต้กฎหมายของรัฐหรือรัฐบาลกลาง หรือกฎหมายเทศบาล หรือ

4) การเปิดเผยข้อมูลตามคำสั่งของศาล หรือหมายศาลที่ออกโดยศาลที่มีอำนาจ

3.5 สิทธิของเจ้าของข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการได้รับทราบ (The right to be informed) ถึงรายละเอียดในการเก็บรวบรวม การนำไปใช้ หรือการเปิดเผย สิ่งระบุตัวตน หรือข้อมูลชีวภาพของตน โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงรายละเอียด เช่น วัตถุประสงค์ในการเก็บข้อมูล ระยะเวลาที่ข้อมูลส่วนบุคคลดังกล่าวจะถูกจัดเก็บ โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบเป็นลายลักษณ์อักษรและเจ้าของข้อมูลส่วนบุคคลต้องให้อนุญาตเป็นลายลักษณ์อักษรด้วยเช่นกัน[353]

3.6 การรักษาความปลอดภัยของข้อมูลส่วนบุคคล

BIPA ควบคุมข้อมูลส่วนบุคคลประเภทชีวภาพตั้งแต่ขั้นตอนของการเก็บรวบรวมและการเก็บรักษาก่อนที่จะมีการละเมิดหรือการเข้าถึงที่ไม่ได้รับอนุญาต โดย BIPA กำหนดให้ผู้ที่มีข้อมูลส่วนบุคคลประเภทชีวภาพอยู่ในครอบครองพัฒนานโยบายที่เป็นลายลักษณ์อักษรและเปิดเผยต่อสาธารณชน โดยในนโยบายนั้นต้องกำหนดตารางการเก็บรักษา และแนวทางสำหรับการทำลายสิ่งระบุตัวตน หรือข้อมูลส่วนบุคคลประเภทชีวภาพอย่างถาวรเมื่อวัตถุประสงค์ในการเก็บ รวบรวม สิ่งระบุตัวตนหรือข้อมูลดังกล่าวได้สำเร็จลุล่วงหรือภายใน 3 ปี นับจากวันสุดท้ายที่ผู้ควบคุมข้อมูลส่วนบุคคลประเภทชีวภาพได้ติดต่อกับเจ้าของข้อมูลส่วนบุคคล แล้วแต่วันใดจะถึงก่อน[354]

นอกจากนี้ การจัดเก็บ ส่ง และคุ้มครองสิ่งระบุตัวตนทางชีวภาพ หรือข้อมูลส่วนบุคคลประเภทชีวภาพต้องเป็นไปโดยใช้มาตรฐานการดูแลที่เหมาะสมในลักษณะที่เหมือนกับ หรือมากกว่าการคุ้มครองที่ใช้ในการจัดเก็บ ส่ง และปกป้องข้อมูลที่เป็นความลับและละเอียดอ่อนอื่น ๆ ที่ใช้ภายในอุตสาหกรรมของผู้ควบคุมข้อมูลส่วนบุคคล[355]

3.7 การร้องเรียน

3.7.1 หน่วยงานกำกับดูแล

BIPA มิได้กำหนดให้มีการจัดตั้งหน่วยงานกำกับดูแลการประมวลผลข้อมูลส่วนบุคคลดังเช่น GDPR หรือ DPA แต่ BIPA นั้นบัญญัติให้เจ้าของข้อมูลส่วนบุคคลสามารถยื่นฟ้องผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลได้หากเจ้าของข้อมูลส่วนบุคคลเห็นว่าผู้

---

[353] 740 ILCS 14/15.

[354] 740 ILCS 14/15(a).

[355] 740 ILCS 14/15(e).

ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นได้กระทำการละเมิดสิทธิของตนโดยสามารถยื่นฟ้องคดีต่อศาลได้

3.7.2 กระบวนการร้องเรียน

เมื่อเจ้าของข้อมูลส่วนบุคคลพิจารณาแล้วเห็นว่าการประมวลผลข้อมูลส่วนบุคคลของตนโดยผู้ควบคุมข้อมูลส่วนบุคคล และ/หรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นเป็นการละเมิดข้อกำหนดของ BIPA เจ้าของข้อมูลส่วนบุคคลมีสิทธิยื่นฟ้องคดีต่อศาลได้ โดยสามารถยื่นฟ้องคดีต่อศาลของรัฐ (State Circuit Court) หรือ ศาลแขวงของรัฐบาลกลาง (Federal State Court) ได้ ทั้งนี้ในการยื่นฟ้องคดีสามารถยื่นฟ้องคดีแบบกลุ่ม (Class Action) ได้ เนื่องจากลักษณะของการละเมิดมักมีผู้เสียหายเป็นจำนวนมาก

นอกจากนี้ BIPA ยังไม่มีบทบัญญัติในเรื่องของอายุความ ซึ่งทำให้เจ้าของข้อมูลส่วนบุคคลสามารถยื่นฟ้องคดีต่อศาลเมื่อใดก็ได้ และจนถึงปัจจุบันยังไม่มีการฟ้องเรื่องของอายุความต่อศาลจึงยังไม่มีการตีความเรื่องของอายุความสำหรับการดำเนินคดีเรื่องการละเมิดข้อกำหนดของ BIPA

3.8 การเยียวยา และบทลงโทษ

3.8.1 การเยียวยา

ภายใต้ข้อกำหนดของ BIPA ไม่ได้กำหนดให้มีหน่วยงานกำกับดูแล ดังนั้นบุคคลที่ได้รับความเดือดร้อน (aggrieved) มีสิทธิยื่นฟ้องต่อศาล ไม่ว่าจะเป็นระดับ ศาลของรัฐ (State Circuit Court) หรือ ศาลแขวงของรัฐบาลกลาง (Federal State Court) ได้

ขณะนี้ศาลอุทธรณ์ของรัฐบาลกลางมีความเห็นที่ไม่สอดคล้องกันในเรื่องความเสียหายที่โจทก์ต้องแสดงต่อศาล ในคดี Patel v. Facebook นั้น Nine Circuit Court มีความเห็นว่าความเสียหายที่จับต้องไม่ได้นั้นเพียงพอสำหรับการฟ้องคดีละเมิดข้อกำหนดของ BIPA แต่ในคดี Vigil v. Take-Two Interactive Software, Inc. นั้น Second Circuit Court มีความเห็นว่าโจทก์จะต้องแสดงให้เห็นถึงความเสียหายทางการเงิน ทางอารมณ์ หรือชื่อเสียง หรือความเสียหายอื่นอันเป็นรูปธรรม

อย่างไรก็ดี เมื่อวันที่ 25 มกราคม พ.ศ. 2562 ศาลฎีกาของรัฐอิลลินอยส์พิพากษาในคดีของ Rosenbach v. Six Flags ว่าบุคคลธรรมดาสามารถฟ้องคดีได้แม้ว่าความเดือดร้อนเพียงอย่างเดียวที่ได้รับคือการถูกละเมิดสิทธิตามกฎหมาย ทั้งนี้ศาลพิพากษาว่าผู้ที่ถูกละเมิดสิทธิภายใต้ BIPA ถือเป็นผู้ที่ได้รับความเดือดร้อนซึ่งสามารถยื่นฟ้องคดีต่อศาลได้แม้ไม่ได้รับความเสียหายเป็นรูปธรรมจากการละเมิด เนื่องจากสภานิติบัญญัติแห่งรัฐอิลลินอยส์มิได้ให้นิยามคำว่า “เดือดร้อน (aggrieved)” ไว้ และศาลได้ให้เหตุผลว่าคำดังกล่าวควรมีความหมายตามปกติซึ่งรวมถึงการถูกปฏิเสธสิทธิตามกฎหมาย และโดยการบัญญัติ BIPA นั้นสภานิติบัญญัติแห่งรัฐอิลลินอยส์ได้ตัดสินใจแล้วว่าบุคคลควรมีสิทธิในความเป็นส่วนตัวและมีสิทธิควบคุมข้อมูลชีวภาพของตนเองได้ ดังนั้นเมื่อมีการละเมิดสิทธิ BIPA ของเจ้าของข้อมูลส่วนบุคคลจะทำให้เจ้าของข้อมูลส่วนบุคคลได้รับความ “เดือดร้อน” ตามความหมายทั่วไป[356]

---

[356] Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186.

3.8.2 บทลงโทษ

บุคคลที่ได้รับความเสียหายจากการละเมิด BIPA มีสิทธิดำเนินการในทางศาล โดยสามารถยื่นฟ้องต่อศาลของรัฐ หรือศาลแขวงของรัฐบาลกลาง โดยสามารถฟ้องคดีต่อนิติบุคคลที่กระทำการละเมิดได้ โดยบทลงโทษสำหรับการละเมิดบทบัญญัติ มีดังนี้[357]

1) สำหรับการฝ่าฝืนบทบัญญัติของ BIPA โดยประมาท ผู้กระทำการละเมิดจะต้องจ่ายค่าสินไหม 1,000 เหรียญสหรัฐ หรือค่าเสียหายตามจริง แล้วแต่จำนวนใดจะสูงกว่า

2) สำหรับการฝ่าฝืนบทบัญญัติของ BIPA โดยเจตนา หรือโดยปราศจากความระมัดระวัง ผู้กระทำการละเมิดจะต้องจ่ายค่าสินไหม 5,000 เหรียญสหรัฐ หรือค่าเสียหายตามจริง แล้วแต่จำนวนใดจะสูงกว่า

3) ค่าฤชาธรรมเนียม และค่าใช้จ่ายของทนายที่สมเหตุสมผล รวมถึงค่าธรรมเนียมพยานผู้เชี่ยวชาญ และค่าใช้จ่ายในการดำเนินคดีอื่น ๆ และ

4) การชดเชยอื่นใดตามแต่ศาลของรัฐหรือศาลรัฐบาลกลางเห็นสมควร

ทั้งนี้บทลงโทษดังกล่าวเป็นบทลงโทษสำหรับการละเมิดต่อเจ้าของข้อมูลส่วนบุคคล 1 ราย หากการทำละเมิดต่อเจ้าของข้อมูลส่วนบุคคลเป็นจำนวนมากเท่าไหร่ จำนวนค่าปรับจะสูงขึ้นเป็นทวีคูณตามจำนวนเจ้าของข้อมูลส่วนบุคคลที่ถูกละเมิด

เนื่องจากผู้เสียหายสามารถยื่นฟ้องดำเนินคดีแบบกลุ่ม และวิธีการคำนวณค่าปรับเป็นทวีคูณตามจำนวนเจ้าของข้อมูลส่วนบุคคลที่ถูกละเมิด ทำให้ผู้ถูกฟ้องร้องอาจต้องจ่ายค่าสินไหมเป็นจำนวนมหาศาลหากศาลพิพากษาให้ชดใช้ค่าเสียหายต่อผู้เสียหาย ดังนั้นในบางกรณีจึงอาจมีการประนีประนอมยอมความ เมื่อเดือนกุมภาพันธ์ พ.ศ. 2563 Facebook ยอมจ่ายค่าเสียหายเป็นจำนวนมากถึง 550 ล้านเหรียญสหรัฐ ในการประนีประนอมยอมความในคดี Patel v. Facebook คดีดังกล่าวเริ่มต้นขึ้นในปี พ.ศ. 2558 เมื่อโจทก์ยื่นฟ้อง Facebook ในการใช้ "คำแนะนำแท็ก" ของ Facebook ว่าเป็นการเก็บรวบรวมข้อมูลใบหน้าของผู้ใช้จากภาพถ่ายโดยไม่ได้รับอนุญาต หรือแจ้งให้ทราบล่วงหน้า[358] รวมถึงไม่แจ้งให้ทราบถึงระยะเวลาในการเก็บข้อมูลไว้ในฐานข้อมูล ซึ่งถือเป็นการละเมิดบทบัญญัติของ BIPA คดีนี้เกิดจากกรณีการฟ้องคดีที่แยกกันสามคดี โดยมีคดีที่ยื่นฟ้องต่อศาลของรัฐบาลกลางสองคดี และคดีที่สามฟ้องต่อศาลของรัฐอิลลินอยส์ โดย Facebook ได้ร้องต่อศาลให้นำคดีที่สามไปฟ้องต่อศาลรัฐบาลกลางภายใต้บทบัญญัติของ Class Action Fairness Act และได้มีการรวมคดีทั้งสามเข้าเป็นคดีเดียวกันในที่สุด[359] มีการคาดการณ์ว่าผู้ใช้ Facebook ที่อาศัยอยู่ในรัฐอิลลินอยส์อาจได้รับค่าเสียหายรายละประมาณ 200 ถึง 400 เหรียญสหรัฐ[360] ซึ่งน้อยมากหาก

---

[357] 740 ILCS 14/15(.20).

[358] Pester, R. (2020). Patel v. Facebook: Facebook Settles Illinois Biometric Information Privacy Act ("BIPA") Violation Suit. *JOLT Digest*. สืบค้นจาก https://jolt.law.harvard.edu/digest/patel-v-facebook-facebook-settles-illinois-biometric-information-privacy-act-bipa-violation-suit

[359] Patel v. Facebook Inc. - 290 F. Supp. 3d 948 (N.D. Cal. 2018). *LexisNexis*. สืบค้นจาก https://www.lexisnexis.com/community/casebrief/p/casebrief-patel-v-facebook-inc-2133717695

[360] Morrison, S. (2020). Facebook's sad summer continues with a $650 million settlement. สืบค้นจาก https://www.vox.com/recode/2020/7/23/21335806/facebook-settlement-illinois-facial-recognition-photo-tagging

เปรียบเทียบกับค่าปรับที่ BIPA กำหนดไว้ที่ 1,000 เหรียญสหรัฐหากศาลตัดสินว่าเป็นการกระทำโดยประมาท และที่ 5,000 เหรียญสหรัฐ หากศาลตัดสินว่าเป็นการกระทำโดยเจตนา หรือปราศจากความระมัดระวัง

บทที่ 4
การคุ้มครองข้อมูลส่วนบุคคลประเภทชีวภาพตามกฎหมายไทย กับการศึกษา วิเคราะห์ และเปรียบเทียบกับการคุ้มครองข้อมูลส่วนบุคคลประเภทชีวภาพของ สหภาพยุโรป สหราชอาณาจักร และรัฐอิลลินอยส์ สหรัฐอเมริกา

1. การคุ้มครองข้อมูลส่วนบุคคลประเภทชีวภาพตามกฎหมายไทย

ความพยายามในการออกกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยเริ่มต้นตั้งแต่ปี พ.ศ. 2540 ในระหว่างนั้นมีการจัดทำร่างกฎหมายหลายฉบับ จนเมื่อวันที่ 28 พฤษภาคม พ.ศ. 2562 ได้มีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ราชกิจจานุเบกษาได้ประกาศ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เมื่อวันที่ 27 พฤษภาคม พ.ศ. 2562 ทั้งนี้ให้มีผลบังคับใช้เฉพาะบางส่วนในวันที่ 28 พฤษภาคม พ.ศ. 2562 คือ 1) หมวด 1 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และ 2) หมวด 4 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล สำหรับส่วนที่จะมีผลบังคับใช้ใน 1 ปีนับจากวันที่ประกาศในราชกิจจานุเบกษาซึ่งคือวันที่ 27 พฤษภาคม พ.ศ. 2563 คือ 1) หมวด 2 การคุ้มครองข้อมูลส่วนบุคคล 2) หมวด 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล 3) หมวด 5 การร้องเรียน 4) หมวด 6 ความรับผิดทางแพ่ง 5) หมวด 7 บทกำหนดโทษ และ 6) มาตรา 95 และ 7) มาตรา 96

อย่างไรก็ดีแม้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะมีผลบังคับใช้แล้ว แต่ต่อมาได้มีการประกาศใช้พระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563 ทำให้หน่วยงานและกิจการ 22 กิจการมิอยู่ภายใต้บังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลจนกว่าจะถึงวันที่ 31 พฤษภาคม พ.ศ. 2564 โดยหน่วยงาน และกิจการที่ได้รับการยกเว้น มีดังต่อไปนี้

1) หน่วยงานของรัฐ
2) หน่วยงานของรัฐต่างประเทศและองค์การระหว่างประเทศ
3) มูลนิธิ สมาคม องค์กรศาสนา และองค์กรไม่แสวงหากำไร
4) กิจการด้านเกษตรกรรม
5) กิจการด้านอุตสาหกรรม
6) กิจการด้านพาณิชยกรรม
7) กิจการด้านการแพทย์และสาธารณสุข
8) กิจการด้านพลังงาน ไอน้ำ น้ำ และการกำจัดของเสีย รวมทั้งกิจการที่เกี่ยวข้อง
9) กิจการด้านการก่อสร้าง
10) กิจการด้านการซ่อมและการบำรุงรักษา
11) กิจการด้านการคมนาคม ขนส่ง และการเก็บสินค้า

12) กิจการด้านการท่องเที่ยว

13) กิจการด้านการสื่อสาร โทรคมนาคม คอมพิวเตอร์ และดิจิทัล

14) กิจการด้านการเงิน การธนาคาร และการประกันภัย

15) กิจการด้านอสังหาริมทรัพย์

16) กิจการด้านการประกอบวิชาชีพ

17) กิจการด้านการบริหารและบริการสนับสนุน

18) กิจการด้านวิทยาศาสตร์และเทคโนโลยี วิชาการ สังคมสงเคราะห์ และศิลปะ

19) กิจการด้านการศึกษา

20) กิจการด้านความบันเทิงและนันทนาการ

21) กิจการด้านการรักษาความปลอดภัย

22) กิจการในครัวเรือนและวิสาหกิจชุมชน ซึ่งไม่สามารถจำแนกกิจกรรมได้อย่างชัดเจน[361]

1.1 ขอบเขตการบังคับใช้

ขอบเขตของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ครอบคลุมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลทั้งในภาครัฐและภาคเอกชน แต่กระนั้นก็มีข้อยกเว้นไม่ใช้บังคับแก่

1) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลธรรมดาเพื่อกิจกรรมส่วนตัวหรือกิจกรรมในครัวเรือน

2) การดำเนินการของหน่วยงานราชการที่เกี่ยวกับการรักษาความมั่นคง เช่น การรักษาความปลอดภัยของประชาชน การป้องกันและปราบปรามการฟอกเงิน เป็นต้น

3) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่องานสื่อมวลชน หรือเพื่องานด้านศิลปกรรมและวรรณกรรม ทั้งนี้ต้องเป็นประโยชน์ต่อสังคมโดยรวม และกระทำภายใต้จริยธรรมของวิชาชีพ

4) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยสภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการต่าง ๆ เพื่อใช้ในกิจการตามอำนาจหน้าที่ของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ

5) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาพิพากษาคดีของศาล การดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี การวางทรัพย์ และการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

6) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อการดำเนินการตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต[362]

---

[361] พระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563

[362] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 4.

อย่างไรก็ดี พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ใช้บังคับสำหรับ กรณีดังต่อไปนี้

1) ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่มีสถานประกอบการอยู่ในประเทศไทย ไม่ว่าการเก็บรวบรวม ใช้หรือเปิดเผยจะทำอยู่ในประเทศหรือนอกประเทศ

2) ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ไม่มีสถานประกอบการอยู่ในประเทศไทยแต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลอยู่ในประเทศไทย เพื่อวัตถุประสงค์ดังต่อไปนี้

(1) การนำเสนอสินค้าหรือบริการแก่เจ้าของข้อมูลส่วนบุคคล โดยไม่คำนึงว่ามีการซื้อสินค้าและบริการโดยเจ้าของข้อมูลส่วนบุคคลหรือไม่

(2) การติดตามตรวจสอบพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในประเทศไทย[363]

ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ไม่มีสถานประกอบการในประเทศไทยต้องทำการแต่งตั้งตัวแทนในประเทศไทย และตัวแทนต้องได้รับมอบอำนาจให้กระทำการแทนผู้ควบคุมข้อมูลส่วนบุคคลได้โดยไม่มีการจำกัดความรับผิดแต่อย่างใด[364]

1.2 ความหมายของข้อมูลส่วนบุคคล

1.2.1 ความหมายของข้อมูลส่วนบุคคล

คำจำกัดความของคำว่า “ข้อมูลส่วนบุคคล” ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หมายความถึง “ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ”[365]

1.2.2 ความหมายของข้อมูลส่วนบุคคลประเภทชีวภาพ

ข้อมูลส่วนบุคคลประเภทชีวภาพนั้นถือเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวตามมาตรา 26 ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่กำหนดให้ข้อมูลดังต่อไปนี้เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว

> *“...ข้อมูลส่วนบุคคลที่เกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด...”*[366]

นอกจากนี้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ให้คำจำกัดความว่า “ข้อมูลชีวภาพ” หมายความถึง “ข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่

---

[363] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 5.

[364] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (5).

[365] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 6.

[366] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26.

เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือข้อมูลจำลองลายนิ้วมือ”[367]

1.3 หลักการคุ้มครองข้อมูลส่วนบุคคล

ในปี พ.ศ. 2523 (ค.ศ. 1980) องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organization for Economic Cooperation and Development - OECD) ได้วางแนวทางในการคุ้มครองข้อมูลส่วนบุคคลขึ้นอย่างเป็นรูปธรรม และเป็นหลักเกณฑ์ที่ประเทศส่วนใหญ่ให้การยอมรับ หลักเกณฑ์นี้คือ Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data โดยเอกสารฉบับนี้ได้รับการยอมรับโดยทั่วไปว่าเป็นหลักเกณฑ์พื้นฐานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่สำคัญ และหลายประเทศได้นำไปบัญญัติเป็นกฎหมายภายในของตน[368] ทั้งนี้ประเทศไทยได้นำหลักการสำคัญ 8 ประการตามแนวทางดังกล่าวมาบัญญัติไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล[369] โดยหลักการในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล มีดังนี้

1.3.1 หลักการเก็บรวบรวมข้อมูลอย่างจำกัด (Collection Limitation Principle)

OECD ได้ให้แนวทางว่าควรมีการจำกัดการรวบรวมข้อมูลส่วนบุคคลและข้อมูลดังกล่าวควรได้มาโดยวิธีการที่ชอบด้วยกฎหมาย เป็นธรรม และตามความเหมาะสมด้วยความรู้หรือความยินยอมของเจ้าของข้อมูล[370] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีหลักการเก็บรวมรวมข้อมูลอย่างจำกัด ดังนี้

1) การเก็บรวบรวมข้อมูลส่วนบุคคลให้เก็บรวบรวมได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล[371]

2) หากไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถทำการเก็บรวบรวมข้อมูลส่วนบุคคล นอกจาก

(1) เพื่อวัตถุประสงค์ด้านการการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์โดยรวมของสาธารณะ หรือเป็นการศึกษาวิจัยหรือสถิติ ทั้งนี้ต้องมีมาตรการคุ้มครองปกป้องสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

---

[367] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 วรรค 2.

[368] สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์. (2558). รายงานฉบับสมบูรณ์ โครงการศึกษาและพัฒนาแนวทางการคุ้มครองข้อมูลส่วนบุคคลภายใต้ประชาคมอาเซียน

Retrieved from

http://www.oic.go.th/FILEWEB/CABIWEBSITE/DRAWER01/GENERAL/DATA0007/00007559.PDF น.14.

[369] สราวุธ ปิติยาศักดิ์. (2561). โครงการวิจัย นโยบายคลาวด์และการคุ้มครองข้อมูลส่วนบุคคลในระบบคลาวด์ระหว่างสหภาพยุโรป สหรัฐอเมริกา ออสเตรเลียและอาเซียน: มุมมองของไทย (รายงานฉบับสมบูรณ์). สำนักงานสนับสนุนกองทุนการวิจัย (สกว.), น. 294.

[370] OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188. p 6.

[371] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 22.

(2) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

(3) เพื่อการปฏิบัติตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับเจ้าของข้อมูลส่วนบุคคลหรือใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา

(4) เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ผู้ควบคุมข้อมูลส่วนบุคคลได้รับมอบหมาย

(5) เพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้อื่น เว้นเสียแต่สิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคลมีความสำคัญเหนือประโยชน์ดังกล่าว

(6) เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิบัติตามกฎหมาย[372]

3) การเก็บรวบรวมข้อมูลส่วนบุคคลต้องเก็บจากเจ้าของข้อมูลส่วนบุคคลโดยตรงเท่านั้น หากมีการเก็บจากแหล่งอื่นจะต้องทำการแจ้งเจ้าของข้อมูลส่วนบุคคลภายใน 30 วัน และต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล นอกเสียจากข้อมูลส่วนบุคคลที่ไม่ได้เก็บจากเจ้าของข้อมูลส่วนบุคคลโดยตรงนั้นได้รับการยกเว้นไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามมาตรา 24 หรือ มาตรา 26[373]

4) การเก็บข้อมูลส่วนบุคคลที่มีความอ่อนไหวต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลเสมอ เว้นแต่

(1) ในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ แต่ต้องกระทำเพื่อเป็นการป้องกันอันตรายที่อาจเกิดต่อสุขภาพ ร่างกาย หรือชีวิตของบุคคล

(2) เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลของสมาชิก อดีตสมาชิก หรือผู้ที่มีการติดต่ออย่างสม่ำเสมอกับสมาคม มูลนิธิ หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์ด้านการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงาน โดยเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยกันภายในองค์กรเท่านั้น

(3) เป็นข้อมูลที่เจ้าของข้อมูลส่วนบุคคลเปิดเผยต่อสาธารณะด้วยความยินยอมอย่างชัดแจ้ง

(4) ข้อมูลส่วนบุคคลนั้นมีความจำเป็นสำหรับการใช้สิทธิเรียกร้องตามกฎหมาย ไม่ว่าจะเป็นการก่อตั้งสิทธิ การปฏิบัติตามหรือการใช้สิทธิ หรือยกขึ้นต่อสู้สิทธิ

(5) การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลจำเป็นสำหรับการปฏิบัติตามกฎหมาย เพื่อให้บรรลุวัตถุประสงค์ดังต่อไปนี้

ก. ประโยชน์ด้านเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคและการรักษาทางการแพทย์ การบริการด้านสุขภาพหรือสังคม การจัดการด้านสุขภาพหรือการบริการด้านสังคมสงเคราะห์ อนึ่ง หากข้อมูลส่วนบุคคลอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วน

---

[372] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24.

[373] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 25.

บุคคลให้เป็นความลับตามกฎหมายผู้นั้นต้องปฏิบัติตามสัญญาที่มีอยู่ระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์หากผู้นั้นมิได้มีข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการปฏิบัติตามกฎหมาย

ข. ประโยชน์สาธารณะด้านการสาธารณสุข ไม่ว่าจะเป็นการป้องกันโรคติดต่ออันตรายหรือโรคระบาดที่อาจเข้ามาในประเทศ หรือการควบคุมมาตรฐานและคุณภาพของยา และเครื่องมือเครื่องใช้ในทางการแพทย์ ทั้งนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะอย่างยิ่งการรักษาความลับตามหลักวิชาชีพหรือตามจริยธรรม

ค. การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับคุ้มครองทางสังคม เช่น การคุ้มครองแรงงาน การประกันสังคม การประกันสุขภาพ สวัสดิการในการรักษาพยาบาล ที่จำเป็นเพื่อการปฏิบัติตามสิทธิหรือหน้าที่ไม่ว่าจะเป็นของเจ้าของข้อมูลส่วนบุคคลหรือผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการในการคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลให้เหมาะสม

ง. การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือเพื่อประโยชน์สาธารณะอื่น[374]

1.3.2 หลักคุณภาพของข้อมูล (Data Quality Principle)

แนวทางของ OECD สำหรับหลักคุณภาพของข้อมูล คือ ต้องมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเท่าที่เหมาะสมและเกี่ยวข้องกับวัตถุประสงค์ที่จะนำไปใช้เท่านั้น นอกจากนี้ข้อมูลส่วนบุคคลดังกล่าวยังควรถูกต้อง ครบถ้วนและทันสมัยอยู่เสมอ[375]

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดให้มีการเก็บรวบรวมข้อมูลส่วนบุคคลได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล[376] และกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด[377] ทั้งนี้เพื่อให้เป็นไปตามแนวทางหลักคุณภาพของข้อมูล

1.3.3 หลักการระบุวัตถุประสงค์ (Purpose Specification Principle)

แนวทางของ OECD สำหรับหลักการระบุวัตถุประสงค์ คือควรระบุวัตถุประสงค์ในการรวบรวมข้อมูลส่วนบุคคลอย่างช้าที่สุดคือ ณ เวลาที่รวบรวมข้อมูลส่วนบุคคล และการนำข้อมูลส่วนบุคคลมาใช้งานในภายหลังต้องจำกัดเฉพาะเพื่อให้บรรลุวัตถุประสงค์ดังกล่าว หรือ

---

[374] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26.

[375] OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188. p 6.

[376] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 22.

[377] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 35.

บรรลุวัตถุประสงค์อื่นที่สอดคล้องกับวัตถุประสงค์ที่ได้ระบุไว้ หรือตามวัตถุประสงค์ที่ได้ระบุไว้ในแต่ละครั้งที่มีการเปลี่ยนแปลงวัตถุประสงค์[378]

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวมเท่านั้น ไม่สามารถกระทำเพื่อวัตถุประสงค์อื่นนอกเหนือจากที่ได้แจ้งไว้ได้ หากมีวัตถุประสงค์ใหม่จะต้องแจ้งและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนเก็บรวบรวม ใช้ หรือเปิดเผยเสมอ นอกจากกรณีที่ข้อกำหนดของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือกฎหมายอื่นอนุญาตให้ทำได้[379]

1.3.4 หลักการใช้ข้อมูลอย่างจำกัด (Use Limitation Principle)

แนวทางของ OECD ระบุว่าการเปิดเผยข้อมูลส่วนบุคคลหรือใช้ข้อมูลส่วนบุคคลต้องเป็นไปเพื่อวัตถุประสงค์ที่ได้ระบุไว้เท่านั้น ไม่สามารถกระทำเพื่อวัตถุประสงค์อื่นใดได้ยกเว้นเจ้าของข้อมูลส่วนบุคคลจะให้ความยินยอม หรือสามารถทำได้โดยอำนาจของกฎหมาย[380]

สำหรับหลักการใช้ข้อมูลอย่างจำกัด พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดไม่ให้มีการใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล นอกเสียจากเป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมโดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26 สำหรับข้อมูลส่วนบุคคลที่ได้รับการยกเว้นไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลผู้ที่ได้รับข้อมูลดังกล่าวจากผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบและต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าวเพื่อวัตถุประสงค์อื่นนอกเหนือจากที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้หากมีการใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับการยกเว้นไม่ต้องขอความยินยอมผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการบันทึกการใช้หรือเปิดเผยข้อมูลส่วนบุคคลนั้นไว้ในรายการกิจกรรม[381]

นอกจากนี้ หากมีการส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ ผู้ควบคุมข้อมูลส่วนบุคคลต้องแน่ใจว่าผู้ที่รับข้อมูลส่วนบุคคลมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมและเพียงพอ ทั้งนี้ได้มีการกำหนดมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลไว้ในหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลตามประกาศคณะกรรมการตามมาตรา 16(5) ซึ่งการส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศต้องเป็นไปตามกฎเกณฑ์ดังกล่าว เว้นเสียแต่

---

[378] OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188. p 6.

[379] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 21.

[380] OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188. p 6.

[381] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 27.

1) การส่งหรือโอนข้อมูลส่วนบุคคลนั้นเป็นการปฏิบัติตามกฎหมาย

2) ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลในการส่งหรือโอนข้อมูลส่วนบุคคลนั้น รวมถึงได้มีการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบว่ามาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ปลายทางที่รับข้อมูลส่วนบุคคลนั้นต่ำกว่ามาตรฐาน

3) การส่งหรือโอนข้อมูลส่วนบุคคลมีความจำเป็นเพื่อการปฏิบัติตามสัญญาที่เจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา

4) การส่งหรือโอนข้อมูลส่วนบุคคลนั้นกระทำเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับผู้อื่น

5) เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ และการส่งหรือโอนข้อมูลส่วนบุคคลนั้นเป็นการกระทำเพื่อป้องกันอันตรายต่อชีวิต หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น

6) การส่งหรือโอนข้อมูลส่วนบุคคลนั้นเป็นการจำเป็นเพื่อภารกิจเพื่อประโยชน์สาธารณะที่มีความสำคัญ[382]

อนึ่ง ให้มีการเสนอต่อคณะกรรมการเป็นผู้วินิจฉัยในกรณีที่มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของปลายทางที่รับข้อมูลส่วนบุคคลไม่เพียงพอหรือมีปัญหา และเมื่อมีหลักฐานใหม่ที่สามารถทำให้เชื่อได้ว่าปลายทางที่รับข้อมูลส่วนบุคคลได้มีการปรับปรุงจนได้มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลคณะกรรมการอาจทบทวนคำวินิจฉัยได้[383]

1.3.5 หลักการรักษาความปลอดภัยของข้อมูล (Security Safeguards Principle)

แนวทางของ OECD ระบุว่าข้อมูลส่วนบุคคลควรได้รับการปกป้องโดยการรักษาความปลอดภัยที่เหมาะสมเพื่อป้องกันความเสี่ยง เช่น การสูญเสีย หรือการเข้าถึง การทำลาย การใช้ การแก้ไข หรือเปิดเผยโดยไม่ได้รับอนุญาต[384]

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสมเพื่อป้องกันการสูญหาย การเข้าถึง หรือเปิดเผยข้อมูลส่วนบุคคลโดยผู้ที่ไม่มีอำนาจหน้าที่ในการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลนั้น ทั้งนี้เพื่อให้การรักษาความปลอดภัยมีประสิทธิภาพต้องกำหนดให้มีการทบทวนมาตรการการรักษาความปลอดภัยเป็นประจำเมื่อมีความจำเป็นหรือเมื่อมีการเปลี่ยนแปลงของเทคโนโลยี นอกจากนี้มาตรฐานนั้นยังต้องเป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการได้กำหนดไว้อีกด้วย[385]

---

[382] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 16(5).

[383] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28.

[384] OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188. p 6.

[385] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 38(1).

1.3.6 หลักการเปิดเผย (Openness Principle)

หลักการเปิดเผยตามแนวทางของ OECD คือ ผู้ควบคุมข้อมูลส่วนบุคคลควรมีนโยบายซึ่งระบุถึงการเปิดเผยการพัฒนา แนวปฏิบัติ และนโยบายเกี่ยวกับข้อมูลส่วนบุคคล อีกทั้งควรมีวิธีการในการกำหนดลักษณะของข้อมูลส่วนบุคคล วัตถุประสงค์หลักของการนำข้อมูลส่วนบุคคลไปใช้งานตลอดจนข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล และสถานที่อยู่อาศัยของผู้ควบคุมข้อมูลส่วนบุคคล[386]

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีการกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลด้วยความโปร่งใส โดยก่อนหรือในขณะที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยให้เจ้าของข้อมูลส่วนบุคคลทราบ โดยมีรายละเอียดดังต่อไปนี้

1) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อการนำไปใช้หรือเปิดเผย ไม่ว่าจะเป็นการเก็บรวบรวมที่ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลหรือได้รับการยกเว้นตามมาตรา 24

2) ในกรณีเป็นการปฏิบัติตามกฎหมายหรือสัญญาแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงเหตุผลและความจำเป็นที่ต้องให้ข้อมูลส่วนบุคคล รวมทั้งต้องแจ้งผลกระทบที่อาจเกิดขึ้นจากการไม่ให้ข้อมูลส่วนบุคคลอีกด้วย

3) ข้อมูลส่วนบุคคลที่เก็บรวบรวม เช่น ชื่อ นามสกุล ที่อยู่ อายุ อาชีพ และระยะเวลาที่ผู้ควบคุมข้อมูลส่วนบุคคลจะจัดเก็บข้อมูลดังกล่าว หากไม่สามารถกำหนดระยะเวลาที่ชัดเจนได้ให้ใช้ระยะเวลาที่สามารถคาดหมายได้ตามมาตรฐานของการเก็บรวบรวมข้อมูล

4) ข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจถูกนำไปเปิดเผยให้บุคคลหรือหน่วยงานประเภทใดบ้าง

5) ข้อมูลติดต่อของผู้ควบคุมข้อมูลส่วนบุคคล และตัวแทนผู้ควบคุมข้อมูลส่วนบุคคลหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (ถ้ามี)

6) สิทธิของเจ้าของข้อมูลส่วนบุคคลตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เช่น สิทธิในการถอนความยินยอม สิทธิขอเข้าถึง สิทธิขอรับข้อมูลส่วนบุคคล และ สิทธิในการคัดค้าน เป็นต้น[387]

การเก็บข้อมูลส่วนบุคคลต้องกระทำด้วยความเป็นธรรม โดยมิได้มีการหลอกลวงเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคล โดย พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติว่าการขอความยินยอมต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่าย[388] ทั้งนี้องค์กรที่ทำการประมวลข้อมูลส่วนบุคคลจะต้องมี

---

[386] OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188. p 6.

[387] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23.

[388] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 วรรค 2.

ความชัดเจนและซื่อสัตย์โดยต้องแจ้งเหตุผลของการรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบ อีกทั้งไม่ทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว

1.3.7 หลักการมีส่วนร่วมของเจ้าของข้อมูลส่วนบุคคล (Individual Participation Principle)

ตามแนวทางในการคุ้มครองข้อมูลส่วนบุคคล ของ OECD บุคคลควรมีสิทธิ

1) ได้รับจากการยืนยันจากผู้ควบคุมข้อมูลส่วนบุคคลหรือจากผู้อื่นว่าผู้ควบคุมข้อมูลส่วนบุคคลนั้นมีข้อมูลที่เกี่ยวข้องกับตนหรือไม่

2) ได้รับการสื่อสาร หรือได้รับข้อมูลที่เกี่ยวข้องกับตน ภายในเวลาอันสมควร โดยหากมีค่าใช้จ่ายจะต้องไม่มากเกินไป อีกทั้งการสื่อสารและข้อมูลต้องมีความชัดเจนสามารถเข้าใจได้ง่าย

3) ได้รับเหตุผลหากคำขอภายใต้ 1) หรือ 2) ได้ถูกปฏิเสธและสามารถโต้แย้งคัดค้านการปฏิเสธดังกล่าว และ

4) สามารถโต้แย้งคัดค้านได้ในกรณีที่เห็นว่าข้อมูลที่เกี่ยวกับตนไม่ถูกต้องหรือไม่สมบูรณ์ และหากการโต้แย้งคัดค้านสำเร็จเจ้าของข้อมูลส่วนบุคคลสามารถขอให้ลบ แก้ไขข้อมูล หรือทำให้ข้อมูลสมบูรณ์ได้[389]

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคลไว้ ดังนี้

1) เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล[390]

2) เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอรับข้อมูลส่วนบุคคลที่เกี่ยวกับตนจากผู้ควบคุมข้อมูลส่วนบุคคลได้ หากผู้ควบคุมข้อมูลส่วนบุคคลได้ทำให้ข้อมูลส่วนบุคคลอยู่ในรูปแบบที่สามารถอ่านหรือใช้งานได้โดยอัตโนมัติและสามารถใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ[391]

3) เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนเมื่อใดก็ได้[392]

4) เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้[393]

---

[389] OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188. p 6.

[390] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 30.

[391] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 31.

[392] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 32.

[393] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 33.

5) เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลหยุดนำข้อมูลส่วนบุคคลของตนไปใช้ได้[394]

6) เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลแก้ไขข้อมูลให้ถูกต้อง ทันสมัย สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด[395]

1.3.8 หลักความรับผิดชอบ(Accountability Principle)

ตามแนวทางในการคุ้มครองข้อมูลส่วนบุคคล ของ OECD ผู้ควบคุมข้อมูลควรรับผิดชอบในการปฏิบัติตามมาตรการที่สอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคล[396]

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ได้กล่าวถึงความรับผิดชอบในการปฏิบัติตามมาตรการอย่างชัดเจน แต่มีบทบัญญัติหลายมาตราที่เกี่ยวข้องกับการใช้มาตรการรักษาความปลอดภัยเพื่อป้องกันการสูญเสีย การเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต นอกจากนี้ยังมีการกำหนดหน้าที่สำหรับผู้ควบคุมข้อมูลส่วนบุคคลในการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer – DPO) และการประเมินผลกระทบความเสี่ยงข้อมูลส่วนบุคคล (Data Protection Impact Assessment – DPIA) อีกด้วย

1.4 การประมวลผลข้อมูลส่วนบุคคลที่ชอบด้วยกฎหมาย

1.4.1 ข้อมูลส่วนบุคคลธรรมดา

ฐานที่ชอบด้วยกฎหมายในการประมวลผลข้อมูลส่วนบุคคลตามบทบัญญัติของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีดังต่อไปนี้

1) ฐานความยินยอม (Consent)

ตามบทบัญญัติของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่สามารถทำได้หากมิได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ทั้งนี้การขอความยินยอมต้องทำก่อนหรือในขณะที่ทำการเก็บรวบรวมข้อมูล และต้องทำให้ชัดแจ้งโดยสามารถทำเป็นลายลักษณ์อักษร หรือทำผ่านระบบอิเล็กทรอนิกส์ เว้นแต่ในกรณีที่ไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้ ทั้งนี้ต้องมีการแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเสมอ โดยต้องแยกส่วนออกมาจากข้อความอื่นอย่างชัดเจน มีแบบและข้อความที่สามารถเข้าถึงได้ง่าย ใช้ภาษาที่อ่านง่าย ไม่หลอกลวงหรือใช้ภาษาหรือวิธีอื่นใดที่จะทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิด

นอกจากนี้ การขอความยินยอมยังต้องคำนึงถึงอิสระในการให้ความยินยอมของเจ้าของข้อมูลส่วนบุคคลเสมอ โดยการเข้าทำสัญญาต้องไม่มีเงื่อนไขในการให้ความยินยอมเพื่อเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลใด ๆ ที่ไม่มีความจำเป็นหรือเกี่ยวข้องกับการปฏิบัติตามสัญญาหรือการให้บริการ เมื่อให้ความยินยอมแล้วเจ้าของข้อมูลส่วนบุคคลสามารถถอนความยินยอมเมื่อใดก็ได้ การถอนความยินยอมนั้นจะต้องสามารถกระทำได้โดยง่ายเช่นเดียวกับ

---

[394] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 34.

[395] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 35.

[396] OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188. p 7.

การให้ความยินยอม โดยการถอนความยินยอมนั้นย่อมไม่มีผลกระทบต่อการประมวลผลที่ชอบด้วยกฎหมายที่เกิดขึ้นก่อนการถอนความยินยอมนั้น นอกจากนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบที่อาจเกิดจากการถอนความยินยอมอีกด้วย[397]

สำหรับความยินยอมที่เจ้าของข้อมูลส่วนบุคคลได้ให้ไว้ก่อนพระราชบัญญัติมีผลบังคับใช้ยังมีผลบังคับใช้โดยผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวม และใช้ข้อมูลส่วนบุคคลต่อไปได้ภายใต้ขอบเขตวัตถุประสงค์เดิม ทั้งนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องกำหนดวิธียกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวม และใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย[398]

2) ฐานสัญญา (Contract)

การเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลสามารถทำได้หากข้อมูลส่วนบุคคลนั้นเป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา[399] ดังนั้นหากข้อมูลส่วนบุคคลนั้นไม่มีความจำเป็นในการปฏิบัติตามสัญญา หรือข้อมูลส่วนบุคคลนั้นมิได้เป็นของคู่สัญญาผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจะไม่สามารถเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลภายใต้เงื่อนไขนี้ได้ ในกรณีก่อนเข้าทำสัญญาการเก็บรวบรวมข้อมูลส่วนบุคคลสำหรับการปฏิบัติตามสัญญาใช้ได้ต่อเมื่อเป็นการดำเนินตามคำขอของเจ้าของข้อมูลส่วนบุคคลเท่านั้น ไม่สามารถใช้ในกรณีที่ผู้อื่นนอกเหนือจากเจ้าของข้อมูลส่วนบุคคลเป็นผู้ร้องขอได้

3) ฐานการปฏิบัติหน้าที่ตามกฎหมาย (Legal Obligation)

การเก็บรวบรวมข้อมูลส่วนบุคคลภายใต้การปฏิบัติหน้าที่ตามกฎหมายเป็นการเก็บรวบรวมโดยผู้ควบคุมข้อมูลส่วนบุคคลเนื่องจากความจำเป็นที่จะต้องปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล[400] โดยความจำเป็นดังกล่าวจะต้องเป็นหลักเกณฑ์ที่ถูกกำหนดโดยกฎหมายไทย

ตัวอย่าง ธนาคารพาณิชย์ต้องรายงานพฤติกรรมทางการเงินที่น่าสงสัยให้กับธนาคารแห่งประเทศไทย ตามประกาศธนาคารแห่งประเทศไทย

ทั้งนี้การเก็บรวบรวมข้อมูลส่วนบุคคลภายใต้ฐานการปฏิบัติตามกฎหมายจะต้องมีความเหมาะสม และเป็นสัดส่วนกันกับวัตถุประสงค์ การเก็บรวบรวมข้อมูลส่วนบุคคลภายใต้หลักเกณฑ์นี้ไม่สามารถใช้อ้างได้หากมีวิธีอื่นที่สามารถปฏิบัติตามกฎหมายได้โดยมิต้องมีการเก็บรวบรวมข้อมูลส่วนบุคคล

---

[397] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19.

[398] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 95.

[399] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(3).

[400] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(6).

การเก็บรวบรวมผลโดยใช้ฐานการปฏิบัติตามกฎหมายมีผลทำให้เจ้าของข้อมูลส่วนบุคคลถูกจำกัดสิทธิในการเรียกให้ผู้ควบคุมข้อมูลส่วนบุคคลลบข้อมูลส่วนบุคคลของตน และเนื่องจากถูกจำกัดสิทธิดังกล่าวจึงไม่สามารถใช้สิทธิในการย้ายข้อมูลส่วนบุคคลของตนไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยเสรีได้ นอกจากนี้เจ้าของข้อมูลส่วนบุคคลอาจไม่สามารถใช้สิทธิในการโต้แย้งคัดค้านได้หากประโยชน์จากการประมวลผลข้อมูลส่วนบุคคลเพื่อการปฏิบัติตามกฎหมายนั้นเหนือกว่าประโยชน์หรือสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล

4) ฐานประโยชน์สำคัญต่อชีวิต (Vital Interest)

การเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์สำคัญต่อชีวิต คือการเก็บรวบรวมข้อมูลส่วนบุคคลที่จำเป็นเพื่อปกป้องผลประโยชน์ที่สำคัญของเจ้าของข้อมูลส่วนบุคคลหรือของบุคคลอื่น ซึ่งเป็นการกระทำเพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล[401] ทั้งนี้การเก็บรวบรวมข้อมูลส่วนบุคคลด้วยหลักเกณฑ์นี้จะต้องกระทำเนื่องจากมีความจำเป็นเท่านั้น ดังนั้นหากมีวิธีอื่นที่จะกระทำเพื่อปกป้องผลประโยชน์ที่สำคัญของเจ้าของข้อมูลส่วนบุคคลหรือของบุคคลอื่นจะไม่สามารถใช้หลักเกณฑ์นี้ได้

กรณีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อประโยชน์สำคัญต่อชีวิตของบุคคลอื่นอาจนำไปใช้กับการเก็บรวบรวมที่จำเป็นสำหรับวัตถุประสงค์ด้านมนุษยธรรม เช่น การตรวจสอบการระบาดของโรค หรือสำหรับเหตุฉุกเฉินด้านมนุษยธรรม เช่น การตอบสนองภัยพิบัติ กรณีที่มีการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อผลประโยชน์ที่สำคัญของบุคคลอื่นควรใช้เฉพาะในกรณีที่ไม่มีพื้นฐานทางกฎหมายอื่น ๆ รองรับเท่านั้น

สำหรับข้อมูลที่เกี่ยวกับสุขภาพ หากเจ้าของข้อมูลส่วนบุคคลสามารถให้ความยินยอมได้ ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถอ้างหลักเกณฑ์ประโยชน์สำคัญต่อชีวิตได้ และจะต้องใช้หลักเกณฑ์การขอความยินยอมแทน

ตัวอย่าง เมื่อมีผู้ประสบอุบัติเหตุได้รับบาดเจ็บสาหัสและหมดสติ มีความจำเป็นต้องได้รับการผ่าตัดเพื่อรักษาชีวิต เนื่องจากผู้ประสบอุบัติเหตุไม่มีสติสัมปชัญญะ ผู้ควบคุมข้อมูลส่วนบุคคลจึงไม่สามารถขอความยินยอมในการเก็บรวบรวมข้อมูลส่วนบุคคลได้ ดังนั้นจึงต้องใช้ฐานเพื่อประโยชน์สำคัญต่อชีวิต แต่หากผู้ประสบอุบัติเหตุมีสติสัมปชัญญะ รู้สึกตัวดี การเก็บรวบรวมข้อมูลส่วนบุคคลด้วยหลักเกณฑ์เพื่อประโยชน์สำคัญต่อชีวิตก็ไม่สามารถใช้ได้

ตัวอย่าง เมื่อเด็กป่วยหนักเป็นอันตรายถึงชีวิต และต้องได้รับการรักษาโดยทันที อาจมีความจำเป็นต้องใช้หลักเกณฑ์การเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์สำคัญต่อชีวิตผู้อื่นในการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับสุขภาพของบิดาและมารดา

การเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์สำคัญต่อชีวิตมักเกี่ยวข้องกับข้อมูลด้านสุขภาพ ซึ่งเป็นข้อมูลส่วนบุคคลที่ละเอียดอ่อน การเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์สำคัญต่อชีวิตจึงต้องคำนึงถึงบทบัญญัติเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคลที่ละเอียดอ่อนภายใต้มาตรา 26 ด้วย

---

[401] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(2).

5) ฐานภารกิจสาธารณะ หรืออำนาจของรัฐ (Public Task)

การเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะ หรือเพื่อปฏิบัติหน้าที่ในการใช้อำนาจของรัฐ คือการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็นการจำเป็นต่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือในการใช้อำนาจรัฐของผู้ควบคุมข้อมูลส่วนบุคคล[402] โดยความจำเป็นดังกล่าวจะต้องเป็นหลักเกณฑ์ที่ถูกกำหนดภายใต้กฎหมายไทย การเก็บรวบรวมข้อมูลส่วนบุคคลด้วยหลักเกณฑ์ภารกิจของรัฐต้องกระทำด้วยความจำเป็นและต้องเหมาะสมเป็นสัดส่วนกับวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล หากมีวิธีอื่นที่สามารถกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวได้ผู้ควบคุมข้อมูลส่วนบุคคลจะไม่สามารถใช้หลักเกณฑ์นี้ในการเก็บรวบรวมข้อมูลส่วนบุคคลได้ นอกจากนี้การเก็บรวบรวมข้อมูลส่วนบุคคลโดยใช้หลักเกณฑ์ประโยชน์สาธารณะและอำนาจของรัฐทำให้เจ้าของข้อมูลส่วนบุคคลถูกจำกัดสิทธิในการขอให้ผู้ควบคุมข้อมูลส่วนบุคคลลบข้อมูลส่วนบุคคลของตน รวมทั้งไม่สามารถใช้สิทธิในการย้ายข้อมูลส่วนบุคคลของตนไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยเสรีได้

6) ฐานประโยชน์อันชอบธรรม (Legitimate Interest)

การเก็บรวบรวมข้อมูลส่วนบุคคลภายใต้ฐานประโยชน์อันชอบธรรม คือการเก็บรวบรวมข้อมูลส่วนบุคคลเมื่อมีความจำเป็นเพื่อประโยชน์ที่ชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของผู้อื่น แต่หากสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลมีความสำคัญมากกว่าประโยชน์ดังกล่าวการเก็บรวบรวมข้อมูลส่วนบุคคลภายใต้ฐานนี้ก็จะไม่สามารถกระทำได้[403] หลักเกณฑ์ข้อนี้นับได้ว่าเป็นหลักเกณฑ์ที่มีความยืดหยุ่นมากกว่าฐานการเก็บรวบรวมข้อมูลส่วนบุคคลอื่น ๆ ที่ได้กล่าวมาข้างต้น แต่อาจมิใช่ฐานที่เหมาะสมที่สุดในการเก็บรวบรวมข้อมูลส่วนบุคคล

ฐานประโยชน์อันชอบธรรมเหมาะแก่การใช้สำหรับกรณีการเก็บรวบรวมข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลทั่วไปสามารถคาดเดาได้ และมีผลกระทบต่อความเป็นส่วนตัวน้อย หรือมีเหตุผลอันไม่อาจหลีกเลี่ยงได้ เช่น การเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อป้องกันการฉ้อโกง หากต้องการใช้ฐานประโยชน์อันชอบธรรมนี้ในการเก็บรวบรวมข้อมูลส่วนบุคคลผู้ควบคุมข้อมูลส่วนบุคคลจะต้องคำนึงถึงสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลให้มากเนื่องจากมีโอกาสเกิดการละเมิดสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลได้ง่าย

อย่างไรก็ดีการเก็บรวบรวมข้อมูลส่วนบุคคลภายใต้ฐานประโยชน์อันชอบธรรมไม่ว่าจะเป็นประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูล หรือของผู้อื่น และไม่ว่าจะเป็นความชอบธรรมเพื่อผลประโยชน์เชิงพาณิชย์ ผลประโยชน์ส่วนตัว หรือผลประโยชน์ของสังคมโดยรวม จะต้องมีความจำเป็นเช่นเดียวกับการเก็บรวบรวมข้อมูลส่วนบุคคลภายใต้ฐานอื่น ๆ หากสามารถได้ผลลัพธ์ที่คล้ายกันโดยมิต้องใช้ข้อมูลส่วนบุคคล ให้ถือว่ามิได้มีความจำเป็นต้องใช้ข้อมูลส่วนบุคคลและไม่สามารถอ้างหลักเกณฑ์ประโยชน์อันชอบธรรมได้

---

[402] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(5).

[403] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(5).

7) ฐานเอกสารประวัติศาสตร์ จดหมายเหตุ และการศึกษาวิจัยหรือสถิติ

การเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลสามารถทำได้หากวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลคือเพื่อวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ เพื่อประโยชน์สาธารณะ หรือวัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ ทั้งนี้เพื่อเป็นการคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีการมาตรการการคุ้มครองที่เหมาะสมและเป็นไปตามประกาศคณะกรรมการ[404]

1.4.2 ข้อมูลส่วนบุคคลประเภทชีวภาพ

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลได้บัญญัติให้ข้อมูลชีวภาพเป็นข้อมูลส่วนบุคคลชนิดพิเศษ[405] ซึ่งถือว่าเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว (sensitive data) และห้ามมิให้ประมวลผลข้อมูลชนิดนี้โดยมิได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล ยกเว้นกรณีดังต่อไปนี้

1) ประโยชน์สำคัญต่อชีวิต (Vital interests)

การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวโดยไม่ได้รับความยินยอมสามารถทำได้หากมีความจำเป็นเพื่อเป็นการป้องกันหรือระงับอันตรายที่มีต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล และเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ไม่ว่าด้วยเหตุใด[406]

การเก็บรวบรวมข้อมูลส่วนบุคคลภายใต้หลักเกณฑ์นี้มีไว้เพื่อปกป้องประโยชน์สำคัญที่จำเป็นต่อชีวิต ไม่ว่าจะเป็นชีวิตของเจ้าของข้อมูลส่วนบุคคลหรือของบุคคลอื่น จึงควรมีขอบเขตการใช้ที่จำกัดและใช้สำหรับกรณีที่เป็นเรื่องของความเป็นความตาย การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวภายใต้หลักเกณฑ์นี้จะไม่สามารถทำได้หากเจ้าของข้อมูลส่วนบุคคลสามารถให้ความยินยอมได้

2) กิจกรรมโดยชอบขององค์กรไม่แสวงหาผลกำไร (Not-for-profit bodies)

การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวโดยไม่ได้รับความยินยอมสามารถทำได้สำหรับการดำเนินการกิจกรรมที่ชอบด้วยกฎหมายของ มูลนิธิ สมาคม หรือองค์กรไม่แสวงหาผลกำไรอื่นที่มีวัตถุประสงค์เกี่ยวกับการเมือง ปรัชญา หรือสหภาพแรงงาน โดยมีเงื่อนไขว่าการเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวนั้นจะต้องเกี่ยวข้องเฉพาะสมาชิก หรือผู้เคยเป็นสมาชิกขององค์กร หรือผู้ซึ่งมีการติดต่อกับองค์กรอย่างสม่ำเสมอ ภายใต้วัตถุประสงค์ขององค์กร และข้อมูลส่วนบุคคลที่มีความอ่อนไหวต้องไม่ถูกเปิดเผยออกไปภายนอกองค์กร[407]

---

[404] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(1).

[405] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 วรรคหนึ่ง.

[406] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26(1).

[407] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26(2).

3) เปิดเผยข้อมูลต่อสาธารณชน (Made public by the data subject)

การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวสามารถทำได้โดยชอบด้วยกฎหมายหากเจ้าของข้อมูลส่วนบุคคลนั้นได้เปิดเผยข้อมูลส่วนบุคคลดังกล่าวต่อสาธารณชนด้วยความยินยอมโดยชัดแจ้งของตนเอง[408] ซึ่งการเปิดเผยนั้นต้องเป็นการเปิดเผยที่เจ้าของข้อมูลส่วนบุคคลกระทำไปโดยมีความตั้งใจที่จะเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวต่อสาธารณชน การรั่วไหลของข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่ทำให้สาธารณชนได้ทราบข้อมูลดังกล่าวไม่ถือว่าเป็นการเปิดเผยข้อมูลต่อสาธารณชนด้วยตนเองของเจ้าของข้อมูลส่วนบุคคล

ทั้งนี้ เจ้าของข้อมูลส่วนบุคคลบางคนอาจเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหว เช่น ความคิดเห็นทางการเมือง หรือศาสนาต่อสาธารณชนด้วยตนเอง อย่างไรก็ดีการนำข้อมูลส่วนบุคคลที่มีความอ่อนไหวไปใช้ภายใต้ฐานเปิดเผยข้อมูลต่อสาธารณชนควรกระทำด้วยความระมัดระวัง เนื่องจากต้องดูพื้นฐานในการเปิดเผยข้อมูลว่าเจ้าของข้อมูลต้องการเปิดเผยให้แค่คนใกล้ชิดทราบ เช่น เพื่อนในโซเชียลมีเดีย หรือต้องการเปิดเผยให้สาธารณชนทราบ

การเปิดเผยให้สาธารณชนทราบ หมายถึง การเปิดเผยที่บุคคลทั่วไปสามารถเข้าถึงได้ มิใช่เข้าถึงได้แค่เฉพาะกลุ่ม การที่บุคคลใดบุคคลหนึ่งสามารถเข้าถึงข้อมูลได้มิได้หมายความว่าทุกคนสามารถเข้าถึงข้อมูลดังกล่าวได้ ดังนั้นการที่บุคคลใดบุคคลหนึ่ง หรือกลุ่มใดกลุ่มหนึ่งสามารถเข้าถึงข้อมูลได้มิได้หมายความว่าข้อมูลดังกล่าวเป็นข้อมูลที่เปิดเผยให้สาธารณชนทราบ

4) สิทธิเรียกร้องตามกฎหมาย (Legal claims or judicial acts)

การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวสามารถกระทำได้โดยชอบด้วยกฎหมายหากเป็นการจำเป็นสำหรับสิทธิเรียกร้องตามกฎหมาย ไม่ว่าจะเป็นการก่อให้เกิดสิทธิ การปฏิบัติตามหรือการใช้สิทธิ หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย[409]

ตัวอย่าง นายจ้างกำลังถูกลูกจ้างฟ้องร้องในคดีที่เกี่ยวกับอุบัติเหตุที่เกิดขึ้นในสถานที่ทำการของนายจ้าง นายจ้างต้องปรึกษาทนายเพื่อขอคำแนะนำ การนำข้อมูลที่เกี่ยวข้องกับอุบัติเหตุรวมถึงข้อมูลการบาดเจ็บของลูกจ้างซึ่งเป็นข้อมูลสุขภาพที่เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวไปเปิดเผยกับทนายของนายจ้าง ถือว่าเป็นการกระทำโดยชอบด้วยกฎหมายเนื่องจากเป็นการจำเป็นภายใต้หลักเกณฑ์สิทธิเรียกร้องตามกฎหมาย

ตัวอย่าง การที่ผู้อนุบาลทำนิติกรรมแทนผู้ไร้ความสามารถอาจต้องมีการเปิดเผยข้อมูลให้ผู้ที่เข้าทำนิติกรรมด้วยทราบว่าเป็นการกระทำการแทนผู้ไร้ความสามารถ ซึ่งถือว่าเป็นการเปิดเผยข้อมูลสุขภาพซึ่งเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว การเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวในกรณีนี้สามารถทำได้โดยชอบด้วยกฎหมาย

5) วัตถุประสงค์ทางเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ (Preventive or Occupational Medicine)

การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวสามารถทำได้หากมีความจำเป็นเพื่อปฏิบัติตามกฎหมายสำหรับวัตถุประสงค์ด้านเวชศาสตร์ป้องกัน หรืออาชีวเวชศาสตร์

---

[408] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26(3).

[409] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26(4).

เพื่อการประเมินความสามารถในการทำงานของพนักงาน การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลให้เป็นความลับตามกฎหมายสามารถมีข้อมูลส่วนบุคคลอยู่ในความรับผิดชอบได้เพียงสองกรณี คือ เป็นการปฏิบัติตามกฎหมาย หรือเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์เท่านั้น[410]

6) ประโยชน์ด้านสาธารณสุข (Public health)

การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวโดยไม่ได้รับความยินยอมอย่างชัดแจ้งสามารถทำได้หากเป็นการจำเป็นเพื่อปฏิบัติตามกฎหมายสำหรับวัตถุประสงค์เพื่อประโยชน์ด้านสาธารณสุข ทั้งนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการที่เหมาะสมในการคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะในการเก็บรักษาความลับตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ[411] การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวภายใต้หลักเกณฑ์ของประโยชน์ด้านสาธารณสุขมีวัตถุประสงค์เพื่อป้องกันและควบคุมโรคติดต่อ รวมถึงภัยคุกคามอื่นซึ่งอาจเป็นอันตรายต่อสุขภาพโดยเน้นไปที่โรคติดต่อซึ่งอาจแพร่เข้ามาในราชอาณาจักร ทั้งนี้แม้การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวเพื่อความจำเป็นทางสาธารณะประโยชน์ในด้านสาธารณสุขไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูล แต่การประมวลผลดังกล่าวควรอยู่ภายใต้มาตรการที่เหมาะสมและเฉพาะเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

ตัวอย่าง การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวด้านสุขภาพ เช่น ประวัติการติดเชื้อโควิด-19 สามารถทำได้โดยชอบด้วยกฎหมายภายใต้หลักเกณฑ์เพื่อปฏิบัติตามกฎหมายสำหรับประโยชน์ด้านสาธารณสุข ทั้งนี้ข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมนั้นจะต้องจำเป็นและเกี่ยวข้องกับการติดเชื้อโควิด-19 เท่านั้น การเก็บข้อมูลส่วนบุคคลที่ไม่เกี่ยวข้องและไม่จำเป็นจะไม่สามารถทำได้

7) ประโยชน์สาธารณะด้านการคุ้มครองและประกันสังคม (Health or Social Care System)

การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวในกรณีที่เป็นการจำเป็นสำหรับการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะในด้านการคุ้มครองทางสังคม เช่น การคุ้มครองแรงงาน การประกันสังคม และสวัสดิการการรักษาพยาบาล โดยการเก็บรวบรวมนั้นต้องจัดให้มีมาตรการการปกป้องสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลที่เหมาะสม[412]

8) การวิจัยหรือทางสถิติ (Scientific or historical research)

การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวเพื่อวัตถุประสงค์ในการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือทางสถิติสามารถทำได้หากเป็นการจำเป็นเพื่อการปฏิบัติตามกฎหมาย การเก็บรวบรวมดังกล่าวต้องกระทำเพียงเท่าที่จำเป็น อีกทั้งยังต้องจัดให้มี

---

[410] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26(5)(ก).

[411] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26(5)(ข).

[412] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26(5)(ค).

มาตรการการปกป้องสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลที่เหมาะสมตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด[413] ดังนั้นการวิจัยที่มิได้เป็นการวิจัยทางวิทยาศาสตร์หรือประวัติศาสตร์จึงไม่สามารถอ้างหลักเกณฑ์นี้ในการเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวได้

9) ประโยชน์สาธารณะที่สำคัญ (Reasons of substantial public interest)

การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวในกรณีที่เป็นการจำเป็นเพื่อปฏิบัติตามกฎหมายสำหรับประโยชน์สาธารณะที่สำคัญ โดยการเก็บรวบรวมข้อมูลดังกล่าวจะต้องจัดให้มีมาตรการการปกป้องสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลที่เหมาะสม[414]

ตัวอย่างของประโยชน์สาธารณะที่สำคัญ เช่น การปฏิบัติหน้าที่ของสภานิติบัญญัติ การปฏิบัติงานตามอำนาจหน้าที่ของหน่วยงานรัฐ การดำเนินการเพื่อสร้างความเท่าเทียม การป้องกันการฉ้อโกง การต้องสงสัยเกี่ยวกับการสนับสนุนทางการเงินสำหรับการก่อการร้าย หรือการฟอกเงิน การเผยแพร่คำพิพากษา และ การป้องกันการใช้สารต้องห้ามในการแข่งกีฬา[415] เป็นต้น

1.5 สิทธิของเจ้าของข้อมูลส่วนบุคคล

ภายใต้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เจ้าของข้อมูลส่วนบุคคลมีสิทธิดังต่อไปนี้

1) สิทธิในการถอนความยินยอมที่ได้เคยให้กับผู้ควบคุมข้อมูลส่วนบุคคล โดยจะถอนเมื่อใดก็ได้ และเช่นเดียวกับการให้ความยินยอมการถอนความยินยอมนั้นต้องสามารถทำได้โดยง่าย นอกเสียจากจะมีข้อจำกัดสิทธิในการถอนความยินยอมตามกฎหมายหรือสัญญาอันเป็นประโยชน์ต่อเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอม[416]

2) เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม ทั้งนี้เมื่อได้รับคำร้องแล้วผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการภายในสามสิบวันนับแต่วันที่ได้รับคำขอ[417]

3) เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอรับข้อมูลส่วนบุคคลที่เกี่ยวกับตนหากผู้ควบคุมข้อมูลส่วนบุคคลได้ทำให้ข้อมูลส่วนบุคคลนั้นอยู่ในรูปแบบที่สามารถอ่านได้ด้วยเครื่องมือหรือ

---

[413] พ.ร.บ. คมครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26(5)(ง).

[414] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26(5)(จ).

[415] คณะนิติศาสตร์, ศ. (2562). แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล *Thailand Data Protection Guidelines 2.0*. Retrieved from https://www.law.chula.ac.th/wp-content/uploads/2019/10/TDPG2.0-C5-20191009.pdf น. 49-50.

[416] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 วรรค 5 และ 6.

[417] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 30.

อุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้วิธีการอัตโนมัติในการนำข้อมูลส่วนบุคคลนั้นไปใช้หรือเปิดเผยได้[418]

4) เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนเมื่อใดก็ได้ ในกรณีดังต่อไปนี้

(1) ข้อมูลส่วนบุคคลนั้นได้มีการเก็บรวบรวมไว้โดยได้รับการยกเว้นไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลมีเหตุอันชอบด้วยกฎหมายที่สำคัญกว่าสิทธิของเจ้าของข้อมูลส่วนบุคคลและสามารถแสดงให้เห็นถึงเหตุนั้นได้ หรือการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อสิทธิเรียกร้องตามกฎหมาย เช่น การก่อตั้งสิทธิ หรือการยกขึ้นต่อสู้สิทธิ เป็นต้น

(2) ข้อมูลส่วนบุคคลนั้นได้เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ทางด้านการตลาดแบบตรง

(3) ข้อมูลส่วนบุคคลนั้นเก็บรวบรวม ใช้ หรือเปิดเผยเพื่อวัตถุประสงค์ด้านการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ยกเว้นเป็นการจำเป็นเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล[419]

5) เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ในกรณีดังต่อไปนี้

(1) เมื่อหมดความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้ให้ไว้ ณ ขณะที่ทำการเก็บรวบรวม

(2) หากเจ้าของข้อมูลส่วนบุคคลต้องการถอนความยินยอมและผู้ควบคุมข้อมูลส่วนบุคคลไม่มีอำนาจตามกฎหมายที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น

(3) เมื่อเจ้าของข้อมูลส่วนบุคคลต้องการคัดค้านกรณีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อการตลาดแบบตรง หรือคัดค้านกรณีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ต้องขอความยินยอมเพื่อความจำเป็นในการปฏิบัติหน้าที่ หรือการใช้อำนาจรัฐตามมาตรา 24 (4) หรือเพื่อประโยชน์โดยชอบด้วยกฎหมายตามมาตรา 24 (5) และผู้ควบคุมข้อมูลส่วนบุคคลไม่อาจปฏิเสธคำขอตามมาตรา 32 (1) (ก) หรือ (ข) ได้

(4) เมื่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นไปโดยไม่ชอบด้วยกฎหมาย[420]

6) เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคลได้ ในกรณีดังต่อไปนี้

---

[418] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 31.

[419] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 32.

[420] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 33.

(1) หากเจ้าของข้อมูลส่วนบุคคลได้ร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิด และผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในระหว่างการตรวจสอบตามคำร้องของเจ้าของข้อมูลส่วนบุคคล

(2) เมื่อข้อมูลส่วนบุคคลนั้นได้มาจากการเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมายจึงเป็นข้อมูลที่ต้องลบหรือทำลาย แต่เจ้าของข้อมูลส่วนบุคคลขอให้ระงับการใช้แทนการลบทำลาย

(3) เมื่อหมดความจำเป็นตามวัตถุประสงค์ที่ได้เก็บรวบรวมข้อมูลส่วนบุคคล แต่เจ้าของข้อมูลส่วนบุคคลอาจมีความจำเป็นต้องขอให้เก็บรักษาไว้เพื่อใช้สำหรับสิทธิเรียกร้องตามกฎหมาย

(4) เมื่อผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในขั้นตอนการพิสูจน์วัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลหรือตรวจสอบวัตถุประสงค์เพื่อปฏิเสธการคัดค้านของเจ้าของข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล[421]

7) เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลแก้ไขให้ข้อมูลส่วนบุคคลของตนนั้นถูกต้องเป็นปัจจุบัน ทั้งนี้หากผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามคำร้องของเจ้าของข้อมูลส่วนบุคคลไม่ว่าจะด้วยเหตุใดก็ตามผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกคำร้องขอพร้อมด้วยเหตุผลในการไม่ดำเนินการตามคำร้องไว้ในบันทึกรายการกิจกรรมตามมาตรา 39[422]

8) ในกรณีที่มีการฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือประกาศที่ออกภายใต้พระราชบัญญัตินี้ เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างได้[423]

1.6 การรักษาความปลอดภัยของข้อมูลส่วนบุคคล

การรักษาความปลอดภัยของข้อมูลส่วนบุคคลนั้นเป็นหน้าที่สำคัญของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติไว้ว่า “ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า “บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล” และ “ผู้ประมวลผลข้อมูลส่วนบุคคล”หมายถึง “บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล”[424]

สำหรับในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ไม่มีสถานประกอบการอยู่ในประเทศไทย (ดูรายละเอียด 1.1ขอบเขตการบังคับใช้) ต้องแต่งตั้งตัวแทนใน

---

[421] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 34.

[422] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 36.

[423] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 73.

[424] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 6.

ประเทศโดยตัวแทนต้องได้รับมอบอำนาจให้กระทำการแทนผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่มีข้อจำกัดความรับผิดที่เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคล[425]

1.6.1 ใช้มาตรการที่เหมาะสมเพื่อรักษาความปลอดภัยของข้อมูลส่วนบุคคล (Data Security)

ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสมเพื่อป้องกันความเสียหายหรืออันตรายอันอาจเกิดขึ้นกับข้อมูลส่วนบุคคลจากการกระทำของผู้ที่ไม่มีอำนาจหรือผู้ไม่ประสงค์ดี และมาตรการเหล่านั้นต้องได้รับการทบทวนและปรับปรุงโดยผู้ควบคุมข้อมูลส่วนบุคคลเมื่อมีความจำเป็น หรือเมื่อเทคโนโลยีเปลี่ยนแปลง เพื่อให้การรักษาความมั่นคงปลอดภัยมีประสิทธิภาพและเหมาะสม[426] และหากต้องให้ข้อมูลส่วนบุคคลแก่ผู้อื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องมีการดำเนินการเพื่อป้องกันมิให้ผู้นั้นนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยโดยปราศจากอำนาจหรือโดยมิชอบ[427]

สำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยผู้ประมวลผลข้อมูลส่วนบุคคลสามารถกระทำได้ในขอบเขตเท่าที่ผู้ควบคุมข้อมูลส่วนบุคคลมีคำสั่งเท่านั้น[428] หากผู้ประมวลผลข้อมูลส่วนบุคคลไม่ปฏิบัติตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลให้ถือว่าผู้ประมวลผลข้อมูลส่วนบุคคลนั้นกลายเป็นผู้ควบคุมข้อมูลส่วนบุคคล[429]

นอกจากนี้ผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสมเพื่อป้องกันข้อมูลส่วนบุคคลจากอันตรายต่าง ๆ อันอาจเกิดขึ้นกับข้อมูลส่วนบุคคลจากการกระทำของผู้ที่ไม่มีอำนาจหรือผู้ไม่ประสงค์ดี และมีการแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการรั่วไหลของข้อมูลส่วนบุคคลที่เกิดขึ้น[430]

อนึ่ง ขณะนี้มีประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ.2563 ซึ่งกำหนดมาตรฐานขั้นต่ำสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลสำหรับหน่วยงานและกิจการตามบัญชีท้ายแนบของพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563 ซึ่งกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องมีมาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard) มาตรการป้องกันด้านเทคนิค (technical safeguard) และมาตรการป้องกันทางกายภาพ (physical safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control) โดยอย่างน้อยต้องประกอบด้วย

---

[425] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (5).

[426] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1).

[427] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (2).

[428] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 40 (1).

[429] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 40 วรรคสอง.

[430] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 40 (2).

1) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

2) การกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล

3) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว

4) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

5) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล[431]

ทั้งนี้ผู้ควบคุมข้อมูลส่วนบุคคลอาจเลือกใช้มาตรฐานการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่แตกต่างไปจากประกาศฉบับนี้ได้หากมาตรฐานดังกล่าวมีมาตรการรักษาความปลอดภัยมากกว่า หรือเท่ากับที่กำหนดในประกาศ

สำหรับหน่วยงานและกิจการที่อยู่ในบัญชีท้ายแนบของพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563 นั้นหากพ้นระยะการบังคับใช้พระราชกฤษฎีกาฉบับดังกล่าวในวันที่ 31 พฤษภาคม พ.ศ. 2564 แล้วและมิได้มีการต่ออายุพระราชกฤษฎีกาฯ มาตรฐานการรักษาความปลอดภัยต้องเป็นไปตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลว่าด้วยมาตรฐานขั้นต่ำเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลซึ่งในขณะนี้ยังมิได้มีการประกาศใช้แต่อย่างใด

1.6.2 แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

สำหรับการจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลภายใต้บทบัญญัติของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องมีการดำเนินการดังกล่าว ในกรณีต่อไปนี้

1) หากผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นหน่วยงานของรัฐ

2) มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นจำนวนมากจึงต้องมีการตรวจสอบการเก็บรวบรวม ใช้ หรือเปิดเผยอย่างสม่ำเสมอ

3) กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหว

---

[431] ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563 ข้อ 5

อนึ่ง ธุรกิจหรือกิจการที่อยู่ในเครือเดียวกันสามารถใช้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลร่วมกันได้ นอกจากนี้หน่วยงานของรัฐที่มีขนาดใหญ่หรือมีสถานที่ทำการหลายแห่งก็สามารถใช้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลร่วมกันได้เช่นกัน[432]

1.6.3 จัดให้มีการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อหมดความจำเป็น

เมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือข้อมูลส่วนบุคคลนั้นไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ที่ใช้ในการเก็บรวบรวม หรือเมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอให้ลบ หรือถอนความยินยอม ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการลบ หรือทำลายข้อมูลส่วนบุคคล โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบ หรือทำลายข้อมูลส่วนบุคคลดังกล่าวนั้น เว้นแต่เก็บรักษานั้นมีวัตถุประสงค์ในการใช้เพื่อเสรีภาพในการแสดงความคิดเห็น การใช้เพื่อสิทธิเรียกร้องตามกฎหมาย ในกรณีดังต่อไปนี้[433]

1) เก็บรักษาเพื่อการศึกษาวิจัยหรือสถิติ หรือการจัดทำเอกสารด้านประวัติศาสตร์หรือจดหมายเหตุอันเป็นประโยชน์สาธารณะ[434]

2) การเก็บรักษาจำเป็นสำหรับการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล[435]

3) การเก็บรักษาจำเป็นในการปฏิบัติตามกฎหมายเพื่อวัตถุประสงค์ด้านเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรค การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพหรือระบบและการให้บริการด้านสังคมสงเคราะห์[436]

4) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เพื่อประโยชน์สาธารณะด้านการสาธารณสุข[437]

1.6.4 การแจ้งถึงการรั่วไหลของข้อมูลส่วนบุคคล (Data Breach Notification)

ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเหตุการณ์รั่วไหลของข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมงนับแต่ทราบเหตุ เว้นแต่การรั่วไหลดังกล่าวไม่มีความเสี่ยงที่กระทบต่อสิทธิและเสรีภาพของผู้ใด สำหรับกรณีที่การรั่วไหลของข้อมูลมีความเสี่ยงสูงที่จะกระทบต่อสิทธิและเสรีภาพเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วน

---

[432] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 41.

[433] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (3).

[434] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24 (1).

[435] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24 (4).

[436] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 (5) (ก).

[437] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 (5) (ข).

บุคคลต้องแจ้งเหตุการรั่วไหลให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแจ้งแนวทางในการเยียวยาโดยไม่ชักช้า[438]

1.6.5 การบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดทำการบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคลเพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้ โดยการบันทึกจะทำเป็นหนังสือหรือด้วยระบบอิเล็กทรอนิกส์ก็ได้และต้องมีรายการอย่างน้อยดังต่อไปนี้

1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขที่เกี่ยวข้อง

6) การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่ต้องขอความยินยอมตามข้อยกเว้น

7) การปฏิเสธหรือการคัดค้านคำร้องขอของเจ้าของข้อมูลส่วนบุคคลในการขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล การขอรับข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลส่วนบุคคล การคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผย การขอให้ดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

8) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย[439]

นอกจากผู้ควบคุมข้อมูลส่วนบุคคลจะมีหน้าที่ในการบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคลดังที่กล่าวมาแล้ว ผู้ประมวลผลข้อมูลส่วนบุคคลเองก็มีหน้าที่ต้องจัดทำและเก็บบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคลตามหลักเกณฑ์และวิธีการตามประกาศคณะกรรมการเช่นกัน[440] ยกเว้นในกรณีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่กระทำเป็นครั้งคราวโดยผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นกิจการขนาดเล็ก แต่หากการกระทำนั้นมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมีการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหว แม้ผู้ประมวลผลข้อมูลส่วนบุคคลจะเป็นกิจการขนาดเล็กหรือกระทำเป็นครั้งคราวก็จำต้องมีการบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคลเช่นกัน[441]

1.7 การร้องเรียน

1.7.1 หน่วยงานกำกับดูแล

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติให้มีการจัดตั้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ซึ่งมีอำนาจหน้าที่ในการจัดทำแผนแม่บทการดำเนินงานด้าน

---

[438] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (4).

[439] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 39.

[440] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 40 (3).

[441] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 40 วรรคสี่.

การส่งเสริมและการคุ้มครองข้อมูลส่วนบุคคล ส่งเสริมและสนับสนุนหน่วยงานของรัฐและภาคเอกชนให้ดำเนินการตามแผนแม่บทดังกล่าว รวมทั้งประเมินผลการดำเนินงานตามแผนแม่บท นอกจากนี้ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลยังมีหน้าที่ในการกำหนดมาตรการหรือแนวทางการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ออกประกาศหรือระเบียบเพื่อให้การดำเนินการเป็นไปตามพระราชบัญญัติ รวมทั้งประกาศกำหนดหลักเกณฑ์และข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล หน้าที่สำคัญอีกอย่างหนึ่งของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลคือหน้าที่ในการตีความและวินิจฉัยชี้ขาดปัญหาที่เกิดจากการบังคับใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562[442]

นอกจากนี้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแต่งตั้งคณะกรรมการผู้เชี่ยวชาญในแต่ละสาขาตามความเชี่ยวชาญในแต่ละเรื่องหรือตามที่คณะกรรมการเห็นสมควร[443] คณะกรรมการผู้เชี่ยวชาญ มีหน้าที่ดังต่อไปนี้

1) พิจารณาเรื่องร้องเรียนตามข้อกำหนดในพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2) ตรวจสอบการกระทำของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล

3) ไกล่เกลี่ยข้อพิพาทที่เกี่ยวกับข้อมูลส่วนบุคคล

4) ปฏิบัติการอื่น ๆ ตามที่กำหนดใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และตามที่คณะกรรมการมอบหมาย[444]

1.7.2 กระบวนการร้องเรียน

ในกรณีที่มีการฝ่าฝืนหรือไม่ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือประกาศที่ออกตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ว่าจะเป็นการกระทำของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญโดยตรง[445] นอกจากนี้หากผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลไม่ดำเนินตามคำร้องของเจ้าของข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคลสามารถยื่นคำร้องเพื่อให้คณะกรรมการผู้เชี่ยวชาญสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้ ในกรณีดังต่อไปนี้

1) ไม่ดำเนินการลบ หรือทำลายข้อมูลส่วนบุคคล[446]

2) ไม่ดำเนินการระงับการใช้ข้อมูลส่วนบุคคล[447]

ทั้งนี้คณะกรรมการผู้เชี่ยวชาญมีอำนาจ ดังต่อไปนี้

---

[442] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 16.

[443] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 71.

[444] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 72.

[445] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 73.

[446] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 33 วรรคสี่.

[447] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 34 วรรคสอง.

1) หากผู้ร้องเรียนไม่ได้ปฏิบัติให้ถูกต้องตามระเบียบที่กำหนดไว้ หรือเป็นเรื่องร้องเรียนที่ระเบียบนั้นได้กำหนดไม่ให้รับพิจารณา คณะกรรมการมีอำนาจไม่รับเรื่องร้องเรียน[448]

2) สั่งยุติเรื่องหากพิจารณาหรือตรวจสอบแล้วว่าเรื่องร้องเรียนหรือการกระทำนั้นไม่มีมูล[449]

3) ดำเนินการไกล่เกลี่ยในกรณีที่พิจารณาหรือตรวจสอบแล้วว่าเรื่องที่ร้องเรียนหรือการกระทำนั้นเป็นกรณีซึ่งอาจไกล่เกลี่ยได้และคู่กรณีประสงค์จะให้ไกล่เกลี่ย แต่หากไม่อาจไกล่เกลี่ยได้หรือการไกล่เกลี่ยไม่เป็นผลคณะกรรมการผู้เชี่ยวชาญมีอำนาจ ดังต่อไปนี้

(1) ออกคำสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการแก้ไขให้ถูกต้องหรือให้ปฏิบัติตามภายในระยะเวลาที่กำหนด

(2) ออกคำสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลกระทำการเพื่อระงับความเสียหาย หรือห้ามมิให้กระทำการอันอาจก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลภายในระยะเวลาที่กำหนด[450]

ทั้งนี้หากเจ้าของข้อมูลส่วนบุคคลเห็นว่าผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการใด ๆ อันเป็นการฝ่าฝืนบทบัญญัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แล้วก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคลสามารถยื่นฟ้องคดีต่อศาลได้[451]

1.8 การเยียวยา และบทลงโทษ

1.8.1 การเยียวยา

บุคคลที่ได้รับความเสียหายอันเป็นผลจากการละเมิดพระราชบัญญัตินี้มีสิทธิได้รับค่าสินไหมทดแทนจากสำหรับความเสียหายที่เกิดขึ้นโดยที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องเป็นผู้รับผิดชอบ เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจะพิสูจน์ได้ว่า ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง หรือเป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจของกฎหมาย โดยค่าสินไหมทดแทนดังกล่าวรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย[452]

นอกจากนี้ศาลมีอำนาจสั่งให้มีการจ่ายค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มเติมจากจำนวนค่าสินไหมทดแทนที่แท้จริงได้ตามที่เห็นสมควร ทั้งนี้ไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริง โดยการกำหนดจำนวนค่าสินไหมทดแทนเพื่อการลงโทษศาลจะคำนึงถึงความร้ายแรงของความเสียหายที่เกิดกับเจ้าของข้อมูลส่วนบุคคล สถานะทางการเงินของผู้ควบคุมข้อมูล

---

[448] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 74 วรรคหนึ่ง.

[449] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 74 วรรคสอง.

[450] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 74 วรรคสาม.

[451] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 77 วรรคหนึ่ง.

[452] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 77.

ส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งผลประโยชน์ที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้รับจากการละเมิดนั้น นอกจากนี้ยังคำนึงถึงการช่วยบรรเทาความเสียหายโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล หรือส่วนร่วมของเจ้าของข้อมูลส่วนบุคคลในการก่อให้เกิดความเสียหายอีกด้วย[453]

1.8.2 บทลงโทษ

สำหรับบทลงโทษในกรณีฝ่าฝืนบทบัญญัติของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีทั้งบทลงโทษทางแพ่ง ทางอาญา และทางปกครอง

1) โทษทางแพ่ง

ดังที่กล่าวมาแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องจ่ายค่าสินไหมทดแทนให้กับเจ้าของข้อมูลส่วนบุคคลที่ได้รับความเสียหายอันเป็นผลจากการละเมิดพระราชบัญญัตินี้ โดยได้กำหนดให้ใช้หลักความรับผิดเด็ดขาด (strict liability) ดังนั้นการกระทำใด ๆ ที่เป็นการฝ่าฝืนบทบัญญัติตามพระราชบัญญัติฉบับนี้ไม่ว่าจะเป็นการกระทำโดยจงใจหรือโดยประมาทเลินเล่อหากก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลแล้วจะต้องชดใช้ค่าสินไหมทดแทน ทั้งนี้ค่าสินไหมทดแทนดังกล่าวรวมถึงค่าใช้จ่ายที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปทั้งหมดไม่ว่าจะเป็นการใช้จ่ายเพื่อระงับความเสียหายที่เกิดขึ้นแล้วหรือเพื่อป้องกันความเสียหายที่กำลังจะเกิดขึ้นก็ตาม[454] นอกจากนี้ศาลยังมีอำนาจสั่งให้จ่ายค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มขึ้นจากจำนวนค่าสินไหมทดแทนที่แท้จริงได้ตามสมควรแต่ทั้งนี้ต้องไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริง[455]

2) โทษทางอาญา

กรณีผู้ควบคุมข้อมูลส่วนบุคคลมิได้ดำเนินการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนหรือระหว่างการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือผู้ที่ได้รับการเปิดเผยข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลส่วนบุคคลได้ทำการใช้หรือเปิดเผยข้อมูลส่วนบุคคลนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งผู้ควบคุมข้อมูลส่วนบุคคลไว้ หรือผู้ควบคุมข้อมูลส่วนบุคคลทำการส่งหรือโอนข้อมูลส่วนบุคคลที่มีความอ่อนไหวไปยังต่างประเทศโดยที่ปลายทางที่รับข้อมูลส่วนบุคคลขาดมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคล หากการทำละเมิดดังกล่าวทำให้เจ้าของข้อมูลส่วนบุคคลเสียหาย เสียชื่อเสียง หรือถูกดูหมิ่นเกลียดชัง มีโทษจำคุกไม่เกิน 6 เดือนหรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ แต่หากการละเมิดดังกล่าวเป็นไปเพื่อแสวงหาประโยชน์อันมิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่นมี โทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ เนื่องจากความผิดนี้มิได้เป็นความผิดต่อรัฐหรือสังคมโดยรวมจึงเป็นความผิดอันยอมความได้[456] ทั้งนี้ความรุนแรงของการลงโทษทางอาญานั้นขึ้นอยู่กับความร้ายแรงของการกระทำผิด และในกรณีที่ผู้ประกอบธุรกิจเป็นนิติ

---

[453] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 78.

[454] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 77.

[455] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 78.

[456] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 79.

บุคคล กรรมการ ผู้จัดการ หรือผู้ที่รับผิดชอบการดำเนินงานของนิติบุคคลนั้นอาจจะต้องรับผิดเป็นส่วนตัวสำหรับการกระทำความผิดนั้น ๆ ด้วย[457]

3) โทษทางปกครอง

สำหรับโทษปรับทางปกครองนั้น มีอัตราโทษปรับขั้นต่ำอยู่ที่ 500,000 บาท และโทษสูงสุดอยู่ที่ 5,000,000 บาท[458] โดยคณะกรรมการผู้เชี่ยวชาญมีอำนาจในการสั่งปรับผู้ทำการละเมิด พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ตามขนาดกิจการของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลและความร้ายแรงของการกระทำความผิด ทั้งนี้คณะกรรมการผู้เชี่ยวชาญอาจตักเตือนหรือสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่กระทำความผิดแก้ไขก่อนที่จะมีคำสั่งปรับได้[459]

2. ศึกษา วิเคราะห์ เปรียบเทียบการคุ้มครองข้อมูลส่วนบุคคลระหว่างสหภาพยุโรป สหราชอาณาจักร รัฐอิลลินอยส์ สหรัฐอเมริกา และไทย

2.1 คำจำกัดความ

การให้คำจำกัดความของคำว่า “ข้อมูลชีวภาพ” นั้นมีความสำคัญ เนื่องจากคำจำกัดความที่ไม่ครอบคลุมอาจทำให้ต้องมีการตีความ หรืออาจทำให้เกิดความเข้าใจที่ไม่ถูกต้อง ทำให้การนำกฎหมายไปปฏิบัตินั้นอาจเกิดปัญหาได้

2.1.1 ผลจากการศึกษาข้อมูลเอกสาร

ผลจากการศึกษาข้อมูลจากเอกสารต่าง ๆ สามารถสรุปได้ว่า คำจำกัดความของ “ข้อมูลชีวภาพ” ที่ได้บัญญัติไว้ในกฎหมายของสหภาพยุโรป สหราชอาณาจักร รัฐอิลลินอยส์ สหรัฐอเมริกา และไทย มีดังต่อไปนี้

สหภาพยุโรป	- “ข้อมูลชีวภาพ” หมายถึง “ข้อมูลส่วนบุคคลที่เกิดจากการประมวลผลโดยใช้เทคนิคพิเศษที่เกี่ยวกับลักษณะทางกายภาพ ทางสรีรวิทยาหรือพฤติกรรมของบุคคลซึ่งสามารถนำไปใช้เพื่อระบุตัวตน หรือใช้เพื่อยืนยันตัวตนของบุคคล เช่น ภาพใบหน้า หรือลายนิ้วมือ”
สหราชอาณาจักร	- “ข้อมูลชีวภาพ” หมายถึง “ข้อมูลส่วนบุคคลที่เกิดจากการประมวลผลโดยใช้เทคนิคพิเศษที่เกี่ยวกับลักษณะทางกายภาพ ทางสรีรวิทยาหรือพฤติกรรมของบุคคลซึ่งสามารถนำไปใช้เพื่อระบุตัวตน หรือใช้เพื่อยืนยันตัวตนของบุคคล เช่น ภาพใบหน้า หรือลายนิ้วมือ”
รัฐอิลลินอยส์ สหรัฐอเมริกา	- “สิ่งระบุตัวตนชีวภาพ (Biometrics Identifier)” หมายถึง “การสแกนม่านตาหรือจอประสาทตา ลายนิ้วมือ เสียง หรือการสแกนมือ หรือใบหน้า ทั้งนี้สิ่งระบุตัวตนชีวภาพ ไม่รวมถึงตัวอย่างลายมือ ลายเซ็น ภาพถ่าย

[457] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 81.

[458] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 82 ถึง 89.

[459] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 90.

	ตัวอย่างทางชีวภาพของมนุษย์ที่ใช้สำหรับการทดสอบหรือการคัดกรองทางวิทยาศาสตร์ ข้อมูลประชากร คำอธิบายรอยสัก คำอธิบายทางกายภาพ เช่น ส่วนสูง น้ำหนัก สีผม หรือสีตา นอกจากนี้ สิ่งระบุตัวตนชีวภาพยังไม่รวมถึง อวัยวะ เนื้อเยื่อ หรือชิ้นส่วนที่ได้จากการบริจาคตามที่กำหนดไว้ในพระราชบัญญัติการบริจาคอวัยวะ (Illinois Anatomical Gift Act - 755 ILCS 50/) หรือ เลือด หรือเซรุ่ม ที่เก็บไว้ในนามของผู้รับหรือผู้ที่อาจได้รับการปลูกถ่ายอวัยวะ ไม่ว่าอวัยวะนั้นจะมาจากผู้ที่ยังมีชีวิตอยู่ หรือมาจากผู้ที่เสียชีวิตไปแล้ว และได้รับหรือเก็บรักษาโดยหน่วยงานจัดหาอวัยวะที่ได้รับมอบหมายจากรัฐบาลกลาง สิ่งระบุตัวตนชีวภาพไม่รวมถึงวัสดุชีวภาพที่มีการควบคุมภายใต้พระราชบัญญัติความเป็นส่วนตัวข้อมูลทางพันธุกรรม (Genetic Information Privacy Act) สิ่งระบุตัวตนชีวภาพไม่รวมถึงข้อมูลที่ได้จากผู้ป่วยในการดูแลสุขภาพหรือข้อมูลที่รวบรวมใช้หรือเก็บรักษาเพื่อการรักษาพยาบาล การชำระเงิน หรือการดำเนินงานภายใต้พระราชบัญญัติประกันสุขภาพและความรับผิดชอบต่อหน้าที่ 1996 (Health Insurance Portability and Accountability Act 1996) ของรัฐบาลกลาง สิ่งระบุตัวตนชีวภาพไม่รวมถึงการเอกซเรย์ ไม่ว่าจะเป็นการเอกซเรย์รังสีเอกซเรย์คอมพิวเตอร์ (ซีทีสแกน) เอ็มอาร์ไอ PET/CT สแกน หรือการเอกซเรย์เต้านม (mammography) หรือ ภาพของกายวิภาคของมนุษย์ที่ใช้ในการวินิจฉัยพยากรณ์โรคหรือรักษาโรค หรือสภาวะด้านสุขภาพอื่น ๆ หรือเพื่อตรวจสอบเพิ่มเติมการทดสอบหรือการคัดกรองทางวิทยาศาสตร์” - "ข้อมูลชีวภาพ (Biometric Information)" หมายถึง “ข้อมูลสิ่งระบุตัวตนชีวภาพใด ๆ โดยไม่คำนึงถึงวิธีการที่ถูกบันทึก แปลง จัดเก็บ หรือใช้ ที่นำไปใช้ในการระบุตัวบุคคล ทั้งนี้ ข้อมูลชีวภาพ ไม่รวมถึงข้อมูลที่ได้มาจากข้อมูลหรือขั้นตอนที่อยู่ภายใต้การยกเว้นของสิ่งระบุตัวตนชีวภาพ”
ไทย	- “ข้อมูลส่วนบุคคลประเภทชีวภาพ” หมายถึง “ข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือข้อมูลจำลองลายนิ้วมือ”

2.1.2 อภิปรายผลการศึกษา

สหภาพยุโรปได้ให้คำจำกัดความของ “ข้อมูลชีวภาพ” ว่าหมายถึง “ข้อมูลส่วนบุคคลที่เกิดจากการประมวลผลโดยใช้เทคนิคพิเศษที่เกี่ยวกับลักษณะทางกายภาพ ทางสรีรวิทยา

หรือพฤติกรรมของบุคคลซึ่งสามารถนำไปใช้เพื่อระบุตัวตน หรือใช้เพื่อระบุตัวตนของบุคคล เช่น ภาพใบหน้า หรือลายนิ้วมือ” สำหรับสหราชอาณาจักรคำจำกัดความของ “ข้อมูลชีวภาพ” DPA เหมือนกันกับของสหภาพยุโรป เนื่องจากเมื่อ GDPR มีผลบังคับในปี พ.ศ. 2561 (ค.ศ. 2018) สหราชอาณาจักรยังมีสถานภาพเป็นหนึ่งในประเทศสมาชิกของสหภาพยุโรป เมื่อถึงกำหนดที่สหราชอาณาจักรพ้นจากการเป็นสมาชิกสหภาพยุโรปแล้วสหราชอาณาจักรจะใช้เพียง DPA และจะทำการแปลง GDPR มาเป็นกฎหมายภายในของสหราชอาณาจักรต่อไป ดังนั้นการที่คำจำกัดความของความว่า “ข้อมูลชีวภาพ” ของ GDPR และ DPA เหมือนกันนั้นจึงถือได้ว่าเหมาะสมแล้ว เมื่อทำการวิเคราะห์แล้ว ข้อมูลชีวภาพภายใต้คำจำกัดความของ GDPR และ DPA นั้นประกอบด้วย 4 ส่วน คือ 1) ต้องเป็นข้อมูลส่วนบุคคล 2) ต้องเป็นข้อมูลที่ได้จากการประมวลผลโดยใช้เทคนิคพิเศษ 3) ต้องเกี่ยวกับลักษณะทางกายภาพ หรือทางสรีรวิทยา หรือพฤติกรรมของบุคคล และ 4) ต้องสามารถนำไปใช้ระบุตัวตน หรือใช้เพื่อระบุตัวตนได้

สำหรับ BIPA ของรัฐอิลลินอยส์ สหรัฐอเมริกานั้น “ข้อมูลชีวภาพ” ว่าคือ “ข้อมูลสิ่งระบุตัวตนชีวภาพ ที่ไม่ว่าจะมีวิธีการบันทึก แปลง จัดเก็บ หรือใช้อย่างไร แต่หากมีการนำไปใช้ในการระบุตัวบุคคลล้วนแล้วแต่ถือว่าเป็นข้อมูลชีวภาพ” อย่างไรก็ดี BIPA ได้มีการกำหนดไว้อย่างชัดเจนว่าสิ่งใดมิถือว่าเป็นข้อมูลสิ่งระบุตัวตนชีวภาพ คือ ตัวอย่างลายมือ ลายเซ็น ภาพถ่าย ตัวอย่างทางชีวภาพของมนุษย์ที่ใช้สำหรับการทดสอบหรือการคัดกรองทางวิทยาศาสตร์ ข้อมูลประชากร คำอธิบายรอยสัก คำอธิบายทางกายภาพ เช่น ส่วนสูง น้ำหนัก สีผม หรือสีตา เป็นต้น นอกจากนี้ยังได้มีการระบุอย่างชัดเจนว่าสิ่งระบุตัวตนชีวภาพนั้นไม่รวมถึงวัสดุหรือสิ่งอื่นใดที่เกี่ยวกับชีวภาพซึ่งอยู่ภายใต้กฎหมายอื่น เช่น พระราชบัญญัติการบริจาคอวัยวะ (Illinois Anatomical Gift Act - 755 ILCS 50/) พระราชบัญญัติความเป็นส่วนตัวข้อมูลทางพันธุกรรม (Genetic Information Privacy Act) พระราชบัญญัติประกันสุขภาพและความรับผิดชอบต่อหน้าที่ 1996 (Health Insurance Portability and Accountability Act 1996) เป็นต้น ทั้งนี้เพื่อให้มีความชัดเจนว่าสิ่งใดบ้างถือเป็นข้อมูลชีวภาพ และเนื่องจากมีบางสิ่งสามารถนำไปใช้ในการระบุตัวตน หรือยืนยันตัวตนได้ เช่น ลายเซ็น ลายสัก หรือ ดีเอ็นเอ เป็นต้น การระบุอย่างชัดเจนเช่นนี้ทำให้ความจำเป็นในการตีความว่าสิ่งใดคือข้อมูลชีวภาพนั้นลดน้อยลง

สำหรับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้มีการบัญญัติไว้ตามแนวทางเดียวกับ GDPR หากแต่มีข้อปลีกย่อยที่ต่างกัน โดย พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ระบุว่า “เป็นการนำลักษณะเด่นทางกายภาพ หรือทางพฤติกรรมของบุคคลมาใช้” ในขณะที่ GDPR และ DPA ระบุว่า “ต้องเกี่ยวกับลักษณะทางกายภาพ หรือทางสรีรวิทยา หรือพฤติกรรมของบุคคล” ดังนั้นข้อมูลชีวภาพตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงประกอบไปด้วย 4 ส่วน คือ 1) เป็นข้อมูลส่วนบุคคล 2) เกิดจากการใช้เทคนิคหรือเทคโนโลยี 3) เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ 4) ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้

ในขณะที่ GDPR และ DPA กำหนดว่าข้อมูลทางสรีรวิทยานั้นหากมีการนำมาใช้เพื่อระบุตัวตนหรือยืนยันตัวตนแล้วจะถือว่าเป็นข้อมูลชีวภาพ แต่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นกำหนดให้เฉพาะข้อมูลทางกายภาพและพฤติกรรมที่นำมาใช้เพื่อระบุตัวตนหรือ

ยืนยันตัวตนเป็นข้อมูลชีวภาพ คำว่า “สรีรวิทยา” นั้นหมายถึงหน้าที่การทำงานของส่วนหรืออวัยวะต่างๆ ของร่างกาย ดังนั้นการที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มิได้กำหนดให้ข้อมูลทางสรีรวิทยาเป็นข้อมูลชีวภาพอาจทำให้ข้อมูลชีวภาพบางอย่าง เช่น คลื่นสมอง หรือจังหวะการเต้นของหัวใจ ซึ่งสามารถนำมาใช้ในการระบุตัวตนและยืนยันตัวตนได้นั้นมิได้เป็นข้อมูลชีวภาพภายใต้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

การให้คำจำกัดความของ “ข้อมูลชีวภาพ” ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อาจก่อให้เกิดคำถามว่าสิ่งใดบ้างที่ถือว่าเป็นข้อมูลชีวภาพ ส่วนหนึ่งเนื่องมาจาก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังมิได้มีผลบังคับใช้อย่างเต็มรูปแบบจึงยังไม่มีคำพิพากษาของศาลฎีกาที่จะสามารถใช้ยึดเป็นแนวทางได้ นอกจากนั้นการพัฒนาของเทคโนโลยีแบบก้าวกระโดดนั้นอาจทำให้สิ่งที่ไม่ได้เป็นข้อมูลชีวภาพในปัจจุบันกลายเป็นข้อมูลชีวภาพได้ในอนาคต ดังที่เราทราบดีว่าในอดีตภาพถ่ายไม่สามารถนำไปใช้เพื่อวัตถุประสงค์ในการระบุตัวตนหรือยืนยันตัวตนได้เนื่องจากไม่มีความคมชัดเพียงพอ หรือไม่ได้อยู่ในรูปแบบที่สามารถนำไปใช้สำหรับการระบุตัวตนหรือยืนยันตัวตนได้ แต่ด้วยเทคโนโลยีในปัจจุบันไม่เพียงแต่จะสามารถนำภาพถ่ายไปใช้ในการระบุตัวตน หรือยืนยันตัวตนได้ แต่ลายนิ้วมือจากภาพถ่ายที่ถ่ายในระยะไกลยังสามารถนำไปใช้สร้างลายนิ้วมือด้วยปริ้นเตอร์ 3 มิติเพื่อปลดล็อกไอโฟนได้อีกด้วย[460]

เนื่องจากใช้ข้อมูลชีวภาพนั้นเป็นการใช้ในลักษณะอัตโนมัติ (automated) และทันทีทันใด (real-time) ในปัจจุบันสารพันธุกรรมหรือดีเอ็นเอ อาจนำไปใช้ยืนยันตัวตน หรือระบุตัวตน แต่ไม่อาจถือว่าเป็นข้อมูลชีวภาพได้เนื่องจากไม่สามารถใช้ในการยืนยันตัวตนหรือระบุตัวตนในลักษณะอัตโนมัติในทันทีทันใดได้ การตรวจพิสูจน์ดีเอ็นเอนั้นมีหลายขั้นตอนและใช้เวลานานอีกทั้งบางขั้นตอนมิใช่วิธีการอัตโนมัติ[461] จึงยังไม่สามารถใช้ดีเอ็นเอในลักษณะเดียวกับข้อมูลชีวภาพได้ อย่างไรก็ดีในอนาคตเราอาจสามารถใช้ดีเอ็นเอในการยืนยันตัวตน หรือระบุตัวตนได้แบบอัตโนมัติในทันทีทันใดได้ หรือแม้กระทั่งข้อมูลอื่น ๆ ที่เราคาดไม่ถึงในปัจจุบันอาจถูกนำมาใช้ในการยืนยันตัวตนหรือระบุตัวตนในลักษณะดังกล่าวได้ ดังนั้นการให้คำจำกัดความของคำว่า “ข้อมูลชีวภาพ” จึงควรเปิดกว้างเพื่อรองรับเทคโนโลยีในอนาคต

นอกจากนี้แล้วคำจำกัดความที่บัญญัติไว้ใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นข้อมูลชีวภาพตั้งต้นที่นำไปใช้ในการสร้างแม่แบบ เช่น ภาพถ่ายใบหน้า หรือภาพถ่ายลายนิ้วมือนั้นไม่ถือว่าเป็นข้อมูลชีวภาพ เนื่องจากไม่ได้เป็นข้อมูลที่ได้มาจากการใช้เทคนิคหรือเทคโนโลยี แต่ข้อมูลเหล่านี้ล้วนมีความสำคัญที่ต้องได้รับการคุ้มครองเท่าเทียมกับข้อมูลแม่แบบ เนื่องจากสามารถนำไปใช้สร้างข้อมูลแม่แบบเพื่อนำไปใช้ในการยืนยันตัวตนหรือระบุตัวตนต่อไปได้

ทั้งนี้ Els J. Kindt ผู้เขียนหนังสือ Privacy and Data Protection Issues of Biometrics Applications ได้เสนอคำจำกัดความของ “ข้อมูลชีวภาพ” ไว้อย่างน่าสนใจดังนี้

---

[460] Scharr, J. (2014). iPhone Hack Fools Touch ID with Hand Photos. *Tom's Guide*. สืบค้นจาก https://www.tomsguide.com/us/iphone-touch-id-hack,news-20066.html

[461] Kindt, E. J. (2013). *Privacy and Data Protection Issues of Biometrics Applications*. New York: Springer. p.171.

"ข้อมูลชีวภาพ คือ ข้อมูลส่วนบุคคลทั้งหมดซึ่ง (ก) เกี่ยวข้องโดยตรงหรือโดยอ้อมกับลักษณะทางชีววิทยาหรือพฤติกรรมที่เป็นเอกลักษณ์เฉพาะของมนุษย์และ (ข) ถูกใช้หรือเหมาะสมที่จะใช้โดยวิธีอัตโนมัติ (ค) เพื่อวัตถุประสงค์ในการระบุตัวตน การยืนยันตัวตนหรือการตรวจสอบการเรียกร้องสิทธิของบุคคลธรรมดา"[462]

คำจำกัดความนี้ระบุให้ถือว่าข้อมูลที่เกี่ยวข้องกับลักษณะทางชีววิทยาหรือพฤติกรรมที่เป็นเอกลักษณ์เฉพาะของมนุษย์ไม่ว่าจะโดยตรงหรือโดยอ้อมเป็นข้อมูลชีวภาพทั้งหมด ดังนั้น ข้อมูลชีวภาพตั้งต้นจึงถือว่าเป็นข้อมูลชีวภาพตามคำจำกัดความของ Kindt แต่กฎหมายภายใต้การวิจัยนี้ไม่ว่าจะเป็น GDPR, DPA, BIPA และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ถือว่าข้อมูลชีวภาพตั้งต้นคือข้อมูลชีวภาพ นอกจากนี้แล้ว คำจำกัดความนี้ยังครอบคลุมถึงข้อมูลชีวภาพที่ยังไม่ถูกใช้เป็นข้อมูลชีวภาพ แต่มีความเหมาะสมที่จะถูกนำไปใช้เป็นข้อมูลชีวภาพในอนาคตอีกด้วย กล่าวคือข้อมูลชีวภาพบางอย่าง เช่น ข้อมูลดีเอ็นเอ ซึ่งสามารถนำไปใช้ระบุตัวตน หรือยืนยันตัวตนได้ แต่ยังไม่สามารถนำไปใช้แบบอัตโนมัติในทันทีทันใดได้นั้นไม่ถือว่าเป็นข้อมูลชีวภาพตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือแม้กระทั่ง GDPR และ DPA แต่ตามคำจำกัดความของ Kindt นั้นถือว่าเป็นข้อมูลชีวภาพซึ่งเป็นการเปิดกว้างสำหรับรองรับวิวัฒนาการทางเทคโนโลยีในอนาคต

2.2 การประมวลผลข้อมูลชีวภาพที่ชอบด้วยกฎหมาย

2.2.1 ผลจากการศึกษาข้อมูลเอกสาร

สำหรับการประมวลผลข้อมูลส่วนบุคคลชีวภาพนั้น สามารถกระทำได้ภายใต้หลักเกณฑ์ดังต่อไปนี้

สหภาพยุโรป	- ความยินยอมโดยชัดแจ้ง - ความจำเป็นสำหรับการปฏิบัติหน้าที่ - ประโยชน์สำคัญต่อชีวิต - กิจกรรมโดยชอบขององค์กรไม่แสวงหาผลกำไร - เปิดเผยข้อมูลต่อสาธารณชน - สิทธิเรียกร้องตามกฎหมาย - ประโยชน์สาธารณะที่สำคัญ - ประโยชน์สาธารณะด้านการคุ้มครองและประกันสังคม - ประโยชน์ด้านสาธารณสุข - จดหมายเหตุ การวิจัยหรือทางสถิติ
สหราชอาณาจักร	- ความยินยอมโดยชัดแจ้ง - ความจำเป็นสำหรับการปฏิบัติหน้าที่ - ประโยชน์สำคัญต่อชีวิต - กิจกรรมโดยชอบขององค์กรไม่แสวงหาผลกำไร

[462] Kindt, E. J. (2013). Privacy and Data Protection Issues of Biometrics Applications. New York: Springer. p.149.

	- เปิดเผยข้อมูลต่อสาธารณชน - สิทธิเรียกร้องตามกฎหมาย - ประโยชน์สาธารณะที่สำคัญ - ประโยชน์สาธารณะด้านการคุ้มครองและประกันสังคม - ประโยชน์ด้านสาธารณสุข - จดหมายเหตุ การวิจัยหรือทางสถิติ
รัฐอิลลินอยส์ สหรัฐอเมริกา	- ความยินยอมเป็นลายลักษณ์อักษร - ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวม ซื้อ หรือรับโดยทางการค้าสิ่งระบุตัวตนทางชีวภาพ หรือข้อมูลส่วนบุคคลประเภทชีวภาพ ยกเว้นจะได้แจ้งให้เจ้าของข้อมูลชีวภาพทราบเป็นลายลักษณ์อักษร และได้รับอนุญาตจากเจ้าของข้อมูลชีวภาพเป็นลายลักษณ์อักษร - ห้ามมิให้ขาย เช่า แลกเปลี่ยน หรือทำกำไรจากสิ่งระบุตัวตนทางชีวภาพหรือข้อมูลส่วนบุคคลประเภทชีวภาพกับบุคคลที่สาม และต้องปฏิบัติต่อข้อมูลชีวภาพเสมือนเป็นข้อมูลที่ละเอียดอ่อนและเป็นความลับ - ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลที่ครอบครองสิ่งระบุตัวตนทางชีวภาพหรือข้อมูลส่วนบุคคลประเภทชีวภาพเปิดเผยหรือเปิดเผยซ้ำ ยกเว้นได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือการเปิดเผยหรือเปิดเผยซ้ำนั้นทำให้ธุรกรรมทางการเงินของเจ้าของข้อมูลส่วนบุคคลเสร็จสมบูรณ์ หรือ เป็นสิ่งที่ต้องกระทำภายใต้กฎหมายของรัฐ หรือรัฐบาลกลาง หรือกฎหมายเทศบาล หรือเป็นการเปิดเผยข้อมูลตามคำสั่งของศาล หรือหมายศาลที่ออกโดยศาลที่มีอำนาจ

ไทย	การประมวลผลข้อมูลชีวภาพ ซึ่งเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวนั้นต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลเสมอ ยกเว้นในกรณีดังต่อไปนี้
	- ประโยชน์สำคัญต่อชีวิต
	- กิจกรรมโดยชอบขององค์กรไม่แสวงหาผลกำไร
	- เปิดเผยข้อมูลต่อสาธารณชน
	- สิทธิเรียกร้องตามกฎหมาย
	- การปฏิบัติตามกฎหมาย
	  - วัตถุประสงค์ทางเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์
	  - ประโยชน์ด้านสาธารณสุข
	  - ประโยชน์สาธารณะด้านการคุ้มครองและประกันสังคม
	  - การวิจัยหรือทางสถิติ
	  - ประโยชน์สาธารณะที่สำคัญ

2.2.2 อภิปรายผลการศึกษา

หลักเกณฑ์การประมวลผลข้อมูลส่วนบุคคลประเภทชีวภาพที่สามารถทำได้ภายใต้กฎหมายของ GDPR และ DPA นั้นมีความเหมือนกันเนื่องจากเมื่อ GDPR มีผลบังคับในปี พ.ศ. 2561 (ค.ศ. 2018) ในขณะที่สหราชอาณาจักรยังมีสถานภาพเป็นหนึ่งในประเทศสมาชิกของสหภาพยุโรป สหราชอาณาจักรจึงบัญญัติให้ DPA นั้นล้อกันกับ GDPR ให้มากที่สุด เพื่อหลีกเลี่ยงปัญหาที่อาจจะเกิดขึ้นได้ ดังนั้นการที่หลักเกณฑ์ในการประมวลผลข้อมูลส่วนบุคคลประเภทชีวภาพของ GDPR และ DPA เหมือนกันนั้นจึงถือได้ว่าเหมาะสมแล้ว

เมื่อเปรียบเทียบหลักเกณฑ์ในการประมวลผลข้อมูลส่วนบุคคลประเภทชีวภาพที่ถูกต้องตามกฎหมายระหว่าง GDPR, DPA และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในด้านของการให้ความยินยอมแล้ว ผู้วิจัยพบว่าการประมวลผลข้อมูลส่วนบุคคลประเภทชีวภาพที่ถูกต้องตามกฎหมายต้องได้รับความยินยอมอย่างชัดแจ้งทั้งหมด นอกจากนั้นสำหรับรัฐอิลลินอยส์สหรัฐอเมริกาแม้มิได้ระบุว่าต้องได้รับความยินยอมอย่างชัดแจ้ง แต่ในตัวบทกฎหมายได้มีการบัญญัติข้อแม้ในการได้รับความยินยอมไว้ว่าต้องได้รับความยินยอมเป็นลายลักษณ์อักษร ซึ่งถือว่าต้องได้รับความยินยอมอย่างชัดแจ้ง ดังนั้นการได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลจึงทำให้การประมวลผลข้อมูลส่วนบุคคลชีวภาพนั้นถูกต้องตามกฎหมายทั้งในสหภาพยุโรป สหราชอาณาจักร รัฐอิลลินอยส์ สหรัฐอเมริกา และไทย

นอกจากการประมวลผลที่ชอบด้วยกฎหมายโดยได้รับความยินยอมโดยชัดแจ้งแล้ว GDPR, DPA และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังได้บัญญัติหลักเกณฑ์อันชอบด้วยกฎหมายสำหรับการประมวลผลข้อมูลส่วนบุคคลประเภทชีวภาพไว้เหมือนกันในหัวข้อต่อไปนี้ 1) ประโยชน์สำคัญต่อชีวิต 2) กิจกรรมโดยชอบขององค์กรไม่แสวงหาผลกำไร 3) เปิดเผยข้อมูลต่อสาธารณชน 4) สิทธิเรียกร้องตามกฎหมาย 5) ประโยชน์ด้านสาธารณสุข 6) ประโยชน์สาธารณะด้านการคุ้มครองและประกันสังคม 7) การวิจัยหรือทางสถิติ และ 8) ประโยชน์สาธารณะที่สำคัญ สำหรับหลักเกณฑ์วัตถุประสงค์ทางเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ที่มีการบัญญัติไว้ใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แยกออกมานั้น GDPR และ DPA ได้บัญญัติไว้เป็นส่วนหนึ่งภายใต้หลักเกณฑ์ประโยชน์สาธารณะด้านการคุ้มครองและประกันสังคมแล้ว นอกจากนี้ ในกรณีการประมวลผลเพื่อการวิจัยหรือทางสถิตินั้น GDPR และ DPA ได้บัญญัติว่าสามารถทำได้หากเป็นการจำเป็นสำหรับวัตถุประสงค์ในการจัดเก็บในลักษณะจดหมายเหตุเพื่อประโยชน์สาธารณะ เพื่อการวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือเพื่อวัตถุประสงค์ทางสถิติ ในขณะที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้สามารถทำได้หากเป็นการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น โดยมิได้ระบุเจาะจงว่าต้องเป็นการเก็บในลักษณะจดหมายเหตุ

อนึ่ง GDPR และ DPA มีการบัญญัติหลักเกณฑ์ความจำเป็นสำหรับการปฏิบัติหน้าที่เป็นหนึ่งในหลักเกณฑ์การประมวลผลข้อมูลส่วนบุคคลชีวภาพที่ชอบด้วยกฎหมาย ซึ่งใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มิได้มีการบัญญัติไว้ ซึ่งหลักเกณฑ์ความจำเป็นสำหรับการปฏิบัติหน้าที่ตาม GDPR และ DPA นั้นครอบคลุมการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่มีความจำเป็นสำหรับการปฏิบัติหน้าที่ รวมถึงการใช้สิทธิเฉพาะของผู้ควบคุมข้อมูลส่วนบุคคล หรือเจ้าของข้อมูลส่วนบุคคลตามกฎหมายแรงงาน กฎหมายประกันสังคม หรือกฎหมายคุ้มครองสังคม ซึ่ง

ในกรณีการปฏิบัติตามกฎหมาย พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้มีการกำหนดหลักเกณฑ์การจำเป็นสำหรับการปฏิบัติตามกฎหมายไว้แล้ว แต่หากเป็นการใช้สิทธิตามกฎหมายสามารถใช้หลักเกณฑ์สิทธิเรียกร้องตามกฎหมายภายใต้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้

ทั้งนี้ การประมวลผลข้อมูลส่วนบุคคลประเภทชีวภาพที่ถูกต้องตามกฎหมาย BIPA รัฐอิลลินอยส์ สหรัฐอเมริกานั้นมีเพียงหลักเกณฑ์เดียว คือหลักเกณฑ์การได้รับความยินยอมโดยชัดแจ้ง อย่างไรก็ตามสิ่งที่ BIPA บัญญัติไว้ต่างไปจาก GDPR, DPA และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 คือ BIPA ได้มีการกำหนดข้อห้ามมิให้นำข้อมูลชีวภาพไปใช้ในทางการค้า โดยห้ามมิให้มีการซื้อขายโดยมิได้รับอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลส่วนบุคคลชีวภาพ นอกจากนี้ยังมีข้อห้ามมิให้ขาย เช่า แลกเปลี่ยน หรือทำกำไรจากข้อมูลส่วนบุคคลประเภทชีวภาพ อีกทั้งยังห้ามมิให้มีการเปิดเผย หรือเปิดเผยซ้ำโดยมิได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลชีวภาพอีกด้วย

2.3 การรักษาความปลอดภัยของข้อมูลส่วนบุคคล

2.3.1 ผลจากการศึกษาข้อมูลเอกสาร

ผลจากการศึกษาข้อมูลจากเอกสารต่าง ๆ สามารถสรุปได้ว่าการรักษาความปลอดภัยของข้อมูลส่วนบุคคลชีวภาพ มีดังต่อไปนี้

สหภาพยุโรป	- ใช้มาตรการทางด้านเทคนิค และทางด้านองค์กรที่เหมาะสมเพื่อรักษาความปลอดภัยของการประมวลผลข้อมูลส่วนบุคคล โดยมีการกำหนดมาตรการไว้เช่น ต้องมีการเข้ารหัสหรือทำให้เป็นข้อมูลแฝง ระบบงานต้องมีความสามารถในการเก็บรักษาความลับ ความสมบูรณ์ การเข้าถึงได้ มีความสามารถในการกู้คืนการเข้าถึงระบบ มีกระบวนการทดสอบและประเมินประสิทธิภาพอย่างสม่ำเสมอ เป็นต้น - กำหนดแนวทางในการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล - ในการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงให้มีการประเมินผลกระทบการคุ้มครองข้อมูลส่วนบุคคลเสมอ - ให้มีการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อหมดความจำเป็น หรือเจ้าของข้อมูลส่วนบุคคลร้องขอให้ลบหรือถอนความยินยอม - ให้มีการแจ้งการรั่วไหลของข้อมูลส่วนบุคคลแก่หน่วยงานกำกับดูแลภายใน 72 ชั่วโมง - ให้มีการบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล
สหราชอาณาจักร	- สำหรับการรักษาความปลอดภัยของข้อมูลส่วนบุคคลนั้น DPA ไม่ได้มีบทบัญญัติเพิ่มเติมจาก GDPR หากแต่มีบทยกเว้นสำหรับการแจ้งถึงการละเมิดข้อมูลส่วนบุคคล (Data Breach Notification) ซึ่งบัญญัติให้มีการยกเว้นมิต้องแจ้งการละเมิดข้อมูลส่วนบุคคลหากการประมวลผลข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อการหลีกเลี่ยงการละเมิดสิทธิของสภา

	ผู้แทนราษฎร และเพื่อวัตถุประสงค์ด้านการสื่อสารมวลชน ด้านวิชาการ ด้านศิลปะ ด้านวรรณกรรม
รัฐอิลลินอยส์ สหรัฐอเมริกา	- ต้องมีการพัฒนานโยบายที่เป็นลายลักษณ์อักษรและเปิดเผยต่อสาธารณชน โดยในนโยบายนั้นต้องกำหนดตารางการเก็บรักษา และแนวทางสำหรับการทำลายสิ่งระบุตัวตน หรือข้อมูลส่วนบุคคลประเภทชีวภาพอย่างถาวรเมื่อวัตถุประสงค์ในการเก็บ รวบรวม สิ่งระบุตัวตนหรือข้อมูลดังกล่าวได้สำเร็จลุล่วงหรือภายใน 3 ปี นับจากวันสุดท้ายที่ผู้ควบคุมข้อมูลส่วนบุคคลประเภทชีวภาพได้ติดต่อกับเจ้าของข้อมูลส่วนบุคคล แล้วแต่วันใดจะถึงก่อน
ไทย	สำหรับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้มีการกำหนดให้ - ผู้ควบคุมข้อมูลส่วนบุคคลต้องใช้มาตรการที่เหมาะสมเพื่อรักษาความปลอดภัยของข้อมูลส่วนบุคคล โดยต้องมีการทบทวน และปรับปรุงให้มีประสิทธิภาพอยู่เสมอ โดยมีการกำหนดมาตรฐานขั้นต่ำสำหรับหน่วยงานและกิจการที่ยังไม่อยู่ภายใต้บังคับของพระราชบัญญัติฉบับนี้ - ให้มีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สำหรับผู้ควบคุมข้อมูลส่วนบุคคลที่เป็นหน่วยงานของรัฐ หรือกรณีที่มีการใช้ข้อมูลส่วนบุคคลเป็นจำนวนมาก หรือหากกิจกรรมหลักเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหว - ให้มีการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อหมดความจำเป็น เช่น เจ้าของข้อมูลส่วนบุคคลร้องขอให้ลบหรือถอนความยินยอม หรือเมื่อพ้นระยะเวลาการเก็บรักษาหรือข้อมูลส่วนบุคคลนั้นไม่มีความเกี่ยวข้อง หรือเกินความจำเป็นตามวัตถุประสงค์ - ต้องแจ้งเหตุการณ์รั่วไหลของข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง - ต้องมีการบันทึกรายการเพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้

2.3.2 อภิปรายผลการศึกษา

สำหรับการรักษาความปลอดภัยของข้อมูลส่วนบุคคลตามบทบัญญัติของ GDPR และ DPA มีการกำหนดให้การประมวลผลข้อมูลส่วนบุคคลต้องมีมาตรการทั้งด้านเทคนิคและทางด้านองค์กรที่เหมาะสม รวมถึงนโยบายคุ้มครองข้อมูลส่วนบุคคลต้องเป็นไปตามหลักการคุ้มครองข้อมูลส่วนบุคคลด้วยการออกแบบ (data protection by design) และการคุ้มครองข้อมูลส่วนบุคคลขั้นพื้นฐาน (data protection by default) ทางด้าน BIPA ของอิลลินอยส์ สหรัฐอเมริกาแม้มิได้มีการกำหนดหลักเกณฑ์ในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลไว้ หากแต่ได้กำหนดว่าต้องมีนโยบายในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่เป็นลายลักษณ์อักษร และต้องเปิดเผยต่อสาธารณชน สำหรับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นกำหนดให้ผู้ควบคุมข้อมูลส่วน

บุคคลต้องใช้มาตรการที่เหมาะสมเพื่อรักษาความปลอดภัยของข้อมูลส่วนบุคคล อีกทั้งยังต้องมีการทบทวน และปรับปรุงให้มีประสิทธิภาพอยู่เสมอโดยจะมีการกำหนดมาตรฐานขั้นต่ำไว้ แต่ในขณะที่ยังมีการยกเว้นการบังคับใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และยังมิได้มีการประกาศใช้ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลว่าด้วยมาตรฐานขั้นต่ำเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล เพื่อให้องค์กรต่าง ๆ สามารถดำเนินการปรับปรุงมาตรการการรักษาความปลอดภัยของข้อมูลส่วนบุคคลให้รองรับข้อกำหนดตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายลำดับรองได้นั้นองค์กรเอกชนหลายแห่งในประเทศไทยจึงให้ความสนใจไปที่การจัดทำมาตรฐานความปลอดภัยให้แก่ข้อมูลหรือ ISO 27001 (Information Security Standard) ซึ่งเป็นมาตรฐานที่เป็นที่ยอมรับในระดับสากลสำหรับการวางมาตรการความปลอดภัยของข้อมูล[463] ซึ่งคาดว่าน่าจะเพียงพอสำหรับการรักษาความปลอดภัยของข้อมูลส่วนบุคคล

นอกจาก ISO 27001 Information Security Standard ซึ่งเป็นมาตรฐานสำหรับการวางมาตรการความปลอดภัยของข้อมูลแล้ว มาตรฐานการรักษาความปลอดภัยของข้อมูลชีวภาพที่เป็นที่ยอมรับในระดับสากลยังมีอยู่อีกหลายฉบับ เช่น ISO/IEC 24745:2011 - Information Technology – Security Techniques – Biometric Information Protection นอกจากนี้ยังมี ISO 19092:2008 Financial services — Biometrics — Security framework ซึ่งเป็นมาตรฐานระดับสากลของการรักษาความปลอดภัยของข้อมูลชีวภาพสำหรับการให้บริการด้านการเงิน รวมทั้งมาตรฐานสำหรับการพัฒนาระบบงานข้อมูลชีวภาพตามที่คณะทำงาน ISO/IEC JTC 1/SC 37 Biometrics ได้กำหนดไว้เพื่อเป็นมาตรฐานในการพัฒนาระบบข้อมูลชีวภาพ ทั้งนี้ธนาคารแห่งประเทศไทยได้มีการพัฒนาแนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในการให้บริการทางการเงินเพื่อใช้อ้างอิงเป็นมาตรฐานเพื่อให้มั่นใจว่าการให้บริการทางการเงินที่เกี่ยวข้องกับเทคโนโลยีชีวภาพนั้นมีความมั่นคงปลอดภัย โดยแนวปฏิบัติดังกล่าวสอดคล้องกับมาตรฐานสากลและครอบคลุมตั้งแต่ระดับนโยบายขององค์กรไปจนถึงแนวทางการดำเนินการและการบริหารความเสี่ยง[464]

GDPR และ DPA กำหนดให้มีการประเมินผลกระทบการคุ้มครองข้อมูลส่วนบุคคลสำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูง ดังนั้นการประมวลผลข้อมูลชีวภาพจึงต้องมีการประเมินผลกระทบก่อนเสมอ ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลจำเป็นต้องวิเคราะห์ผลกระทบที่อาจเกิดต่อเจ้าของข้อมูลส่วนบุคคลเสียก่อน และหากผลกระทบที่อาจเกิดต่อเจ้าของข้อมูลส่วนบุคคลสูงจึงจำเป็นจะต้องมีการรักษาความปลอดภัยที่สูงตามไปด้วย ด้าน BIPA ของอิลลินอยส์สหรัฐอเมริกา และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ได้มีการกำหนดให้มีการประเมินผลกระทบการคุ้มครองข้อมูลส่วนบุคคลไว้แต่อย่างใด

---

[463] ศุภวัชร์ มาลานนท์, & ชิโนภาส อุดมผล. (2020). มาตรฐาน ISO 27001 และกฎหมายคุ้มครองข้อมูลส่วนบุคคล. ข่าวหุ้นธุรกิจออนไลน์. สืบค้นจาก ข่าวหุ้นธุรกิจออนไลน์ website: https://www.kaohoon.com/content/379182.

[464] หนังสือเวียน ธนาคารแห่งประเทศไทย เลขที่ ธปท.ฝทง. ว. 760/2563. นำส่งแนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในการให้บริการทางการเงิน

ทั้งนี้ได้มีการกำหนดแนวทางในการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไว้ใน GDPR, DPA และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แต่สำหรับ BIPA นั้นไม่ได้มีการกำหนดแนวทางในการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

อนึ่ง การลบหรือทำลายข้อมูลส่วนบุคคล GDPR ได้กำหนดให้ลบข้อมูลส่วนบุคคลเมื่อหมดความจำเป็น หรือเมื่อเจ้าของข้อมูลส่วนบุคคลขอร้องให้ลบ เช่นเดียวกันกับ DPA และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แต่สำหรับ BIPA ได้กำหนดไว้อย่างชัดเจน กล่าวคือ ต้องลบเมื่อวัตถุประสงค์สำเร็จลุล่วง หรือภายใน 3 ปี นับจากวันสุดท้ายที่ผู้ควบคุมข้อมูลส่วนบุคคลประเภทชีวภาพได้ติดต่อกับเจ้าของข้อมูลส่วนบุคคล แล้วแต่วันใดจะถึงก่อน

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้มีการกำหนดข้อยกเว้นสำหรับการลบข้อมูลส่วนบุคคลไว้ว่า ไม่ต้องลบหากการเก็บรักษานั้นมีวัตถุประสงค์ในการใช้เพื่อเสรีภาพในการแสดงความคิดเห็น หรือการใช้เพื่อสิทธิเรียกร้องตามกฎหมาย เช่น การเก็บรักษาเพื่อการศึกษาวิจัยหรือสถิติ หรือการเก็บรักษาเป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เพื่อประโยชน์สาธารณะด้านการสาธารณสุข เป็นต้น สำหรับ GDPR และ DPA นั้น มีข้อกำหนดว่าไม่ต้องลบข้อมูลส่วนบุคคลในกรณีที่การประมวลผล 1) มีความจำเป็นเพื่อการใช้สิทธิเสรีภาพในการแสดงออกและการเข้าถึงข้อมูล 2) การปฏิบัติตามกฎหมาย 3) เพื่อประโยชน์สาธารณะเกี่ยวกับสุขภาพของประชาชน และ 4) วัตถุประสงค์ในการเก็บรวบรวมเพื่อประโยชน์สาธารณะ เพื่อการวิจัยทางวิทยาศาสตร์ หรือประวัติศาสตร์ หรือวัตถุประสงค์ทางสถิติ

สำหรับการรั่วไหลของข้อมูลส่วนบุคคลนั้น สหภาพยุโรป สหราชอาณาจักร และไทย ได้กำหนดให้ต้องมีการแจ้งหน่วยงานกำกับดูแลในกรณีที่มีการรั่วไหลของข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง อย่างไรก็ดี สหราชอาณาจักรมีข้อยกเว้นสำหรับการรั่วไหลของข้อมูลส่วนบุคคลในกรณีที่การประมวลผลข้อมูลส่วนบุคคลเป็นไปเพื่อวัตถุประสงค์ในการหลีกเลี่ยงการละเมิดสิทธิของสภาผู้แทนราษฎร หรือเพื่อวัตถุประสงค์ด้านการสื่อสารมวลชน ด้านวิชาการ ด้านศิลปะ และด้านวรรณกรรมว่ามิต้องแจ้งให้หน่วยงานกำกับดูแลทราบถึงการรั่วไหลของข้อมูลส่วนบุคคล

อนึ่ง การบันทึกรายการการประมวลผลข้อมูลส่วนบุคคลนั้นได้มีการกำหนดไว้ใน GDPR, DPA และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้มีการบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ แต่สำหรับ BIPA ไม่มีข้อกำหนดเกี่ยวกับการบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้แต่อย่างใด

2.4 การร้องเรียน

2.4.1 ผลจากการศึกษาข้อมูลเอกสาร

ผลจากการศึกษาข้อมูลจากเอกสารต่าง ๆ สามารถสรุปได้ว่าการร้องเรียนสำหรับการละเมิดข้อมูลส่วนบุคคลชีวภาพ มีดังต่อไปนี้

สหภาพยุโรป	- เจ้าของข้อมูลส่วนบุคคลต้องได้รับความเดือดร้อน หรือความเสียหายแก่ทรัพย์สิน หรือสิ่งอื่นใดอันเป็นผลจากการละเมิดข้อกำหนดจึงจะมีสิทธิได้รับค่าสินไหมทดแทน - เจ้าของข้อมูลส่วนบุคคลมีสิทธิยื่นฟ้องหน่วยงานกำกับดูแลในกรณีที่หน่วยงานกำกับดูแลไม่ดำเนินการจัดการกับคำร้อง หรือไม่แจ้งเจ้าของ

	ข้อมูลส่วนบุคคลให้ทราบถึงความคืบหน้าหรือผลของคำร้องภายใน 3 เดือน หรือเจ้าของข้อมูลส่วนบุคคลต้องการอุทธรณ์คำตัดสินของหน่วยงานกำกับดูแล - เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการฟ้องคดีต่อผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลหากเห็นว่าผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลกระทำการละเมิดสิทธิของตนภายใต้ข้อกำหนด GDPR
สหราชอาณาจักร	- เมื่อพิจารณาแล้วเห็นว่าผู้ควบคุมข้อมูลประมวลผลข้อมูลส่วนบุคคลของตนละเมิดข้อกำหนดตาม GDPR เจ้าของข้อมูลส่วนบุคคลมีสิทธิยื่นคำร้องต่อ ICO ได้ - หากเจ้าของข้อมูลส่วนบุคคลเห็นว่าผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลกระทำการอันเป็นการละเมิดสิทธิของตนภายใต้ข้อกำหนด GDPR และ DPA เจ้าของข้อมูลส่วนบุคคลมีสิทธิยื่นฟ้องผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลต่อศาล
รัฐอิลลินอยส์ สหรัฐอเมริกา	- เมื่อเห็นว่าการประมวลผลข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นการละเมิดข้อกำหนดของ BIPA เจ้าของข้อมูลส่วนบุคคลมีสิทธิยื่นฟ้องคดีต่อศาลได้ โดยสามารถยื่นฟ้องคดีต่อศาลของรัฐ (State Circuit Court) หรือ ศาลแขวงของรัฐบาลกลาง (Federal State Court) ได้ ทั้งนี้ในการยื่นฟ้องคดีสามารถยื่นฟ้องคดีแบบกลุ่ม (Class Action) ได้ เนื่องจากลักษณะของการละเมิดมักมีผู้เสียหายเป็นจำนวนมาก ทั้งนี้ BIPA ไม่ได้มีการกำหนดอายุความสำหรับการฟ้องคดี - เจ้าของข้อมูลส่วนบุคคลสามารถยื่นฟ้องได้แม้ยังไม่ได้รับความเสียหายจากการละเมิด
ไทย	- เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้าง ฝ่าฝืนหรือไม่ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือประกาศของคณะกรรมการ - หากเจ้าของข้อมูลส่วนบุคคลเห็นว่าผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลกระทำการละเมิดบทบัญญัติของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แล้วก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคลสามารถยื่นฟ้องคดีต่อศาลได้

2.4.2 อภิปรายผลการศึกษา

เจ้าของข้อมูลส่วนบุคคลสามารถร้องเรียนต่อหน่วยงานกำกับดูแลได้หากได้รับความเดือดร้อน หรือเกิดความเสียหายแก่ทรัพย์สินอันเป็นผลจากการละเมิดข้อกำหนดใน GDPR และ DPA รวมถึงมีสิทธิยื่นฟ้องหน่วยงานกำกับดูแล และมีสิทธิในการฟ้องคดีต่อผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้อีกด้วย ทั้งนี้ในตัวบทกฎหมายของทั้ง GDPR และ DPA ได้มีการบัญญัติไว้ว่าเจ้าของข้อมูลส่วนบุคคลสามารถร้องเรียนได้หากเกิดความเสียหาย แต่อย่างไรก็ดีศาลในสหราชอาณาจักรได้มีคำพิพากษาว่าการที่เจ้าของข้อมูลส่วนบุคคลสูญเสียการควบคุมข้อมูลส่วนบุคคลของตนนั้นถือเป็นความเสียหายซึ่งต้องได้รับการเยียวยา ซึ่งเป็นไปในแนวทางเดียวกันกับ BIPA ซึ่งศาลฎีกาของรัฐอิลลินอยส์ได้พิพากษาว่าเจ้าของข้อมูลส่วนบุคคลสามารถฟ้องคดีได้แม้ว่าความเดือดร้อนเพียงอย่างเดียวที่ได้รับคือการถูกละเมิดสิทธิตามกฎหมาย สำหรับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดว่าหากมีการฝ่าฝืน หรือไม่ปฏิบัติตามข้อกำหนดในพระราชบัญญัตินี้เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อหน่วยงานกำกับดูแลเช่นกัน และหากการละเมิดนั้นทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคลสามารถยื่นฟ้องคดีต่อศาลได้ อย่างไรก็ดี เนื่องจาก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังไม่มีการบังคับใช้อย่างเต็มรูปแบบ จึงยังไม่มีการร้องเรียน ไม่มีการฟ้องคดีต่อศาล ดังนั้นจึงไม่มีคำพิพากษาศาลฎีกาอันสามารถจะนำมาเป็นแนวทางได้

ด้านการดำเนินคดีแบบกลุ่ม (class action) นั้นสามารถทำได้ในสหราชอาณาจักรตามคำพิพากษาของศาลอุทธรณ์ในคดี Lloyd v Google LLC [2019] EWCA Civ 1599 ที่ให้ถือว่า Richard Lloyd เป็นตัวแทนของผู้ใช้ไอโฟนที่ใช้เว็บเบราว์เซอร์ซาฟารีทั้งหมดในประเทศอังกฤษและเวลส์[465] แต่ GDPR ไม่มีบทบัญญัติเกี่ยวกับการดำเนินคดีแบบกลุ่ม ทางด้านรัฐอิลลินอยส์การดำเนินคดีแบบกลุ่มโดยถือว่าโจทก์เป็นตัวแทนของเจ้าของข้อมูลส่วนบุคคลที่ถูกละเมิดทั้งหมดสามารถทำได้เช่นเดียวกันตามกฎหมายของสหรัฐอเมริกาเนื่องจากลักษณะของการละเมิดมักมีผู้เสียหายเป็นจำนวนมาก

นอกจากนี้คดีละเมิดข้อมูลส่วนบุคคลในรัฐอิลลินอยส์ยังไม่มีอายุความอีกด้วย เนื่องจากไม่ได้มีการกำหนดอายุความไว้แต่อย่างใด สำหรับ GDPR และ DPA มิได้มีการกำหนดอายุความไว้เช่นเดียวกัน แต่สำหรับการละเมิดข้อมูลส่วนบุคคลตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นมีอายุความ 3 ปี นับแต่วันที่ผู้เสียหายได้รับรู้ถึงความเสียหายและรู้ตัวผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องรับผิด หรือ 10 ปีนับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล[466]

---

[465] Covington & Burling LLP. (2019). Landmark Case Opens the Door to UK Data Protection Consumer Class Actions. สืบค้นจาก https://www.cov.com/en/news-and-insights/insights/2019/10/landmark-case-opens-the-door-to-uk-data-protection-consumer-class-actions

[466] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 78 วรรค 2.

2.5 บทลงโทษ

2.5.1 ผลจากการศึกษาข้อมูลเอกสาร

ผลจากการศึกษาข้อมูลจากเอกสารต่าง ๆ สามารถสรุปได้ว่าบทลงโทษสำหรับการละเมิดข้อมูลส่วนบุคคลชีวภาพ มีดังต่อไปนี้

สหภาพยุโรป	- การฝ่าฝืนข้อกำหนด GDPR ต้องระวางโทษทางปกครองไม่เกิน 10,000,000 ยูโร หรือ 20,000,000 ยูโร หรือในกรณีขององค์กรธุรกิจ (undertakings) ต้องระวางค่าปรับทางปกครองไม่เกินร้อยละ 2 หรือร้อยละ 4 ของมูลค่ายอดขายทั่วโลกของปีงบประมาณก่อนหน้า แล้วแต่จำนวนใดจะสูงกว่า ทั้งนี้ขึ้นอยู่กับฐานความผิด - ประเภทของข้อมูลส่วนบุคคลที่ได้รับผลกระทบจากการละเมิดอาจทำให้จำนวนค่าปรับสูงขึ้น ทั้งนี้ขึ้นอยู่กับการพิจารณาของหน่วยงานกำกับดูแล
สหราชอาณาจักร	- บทลงโทษสำหรับผู้ฝ่าฝืนข้อกำหนดของ DPA อยู่ในรูปของค่าปรับทางปกครอง โดย ICO หน่วยงานผู้มีหน้าที่กำกับดูแลเป็นผู้มีอำนาจในการลงโทษ โดยอัตราค่าปรับของการละเมิดบทบัญญัติของ DPA นั้นมี 2 ระดับ 1) ระดับสูงสุด คือ ไม่เกิน 20,000,000 ยูโร หรือในกรณีขององค์กรธุรกิจ (undertakings) ต้องระวางค่าปรับทางปกครองไม่เกินร้อยละ 4 ของมูลค่ายอดขายทั่วโลกของปีงบประมาณก่อนหน้า แล้วแต่จำนวนใดจะสูงกว่า หรือ 2) ระดับทั่วไป ต้องระวางโทษทางปกครองไม่เกิน 10,000,000 ยูโร หรือในกรณีขององค์กรธุรกิจ (undertakings) ต้องระวางค่าปรับทางปกครองไม่เกินร้อยละ 2 ของมูลค่ายอดขายทั่วโลกของปีงบประมาณก่อนหน้า แล้วแต่จำนวนใดจะสูงกว่า
รัฐอิลลินอยส์ สหรัฐอเมริกา	- สำหรับการฝ่าฝืนบทบัญญัติของ BIPA โดยประมาท ผู้กระทำการละเมิดจะต้องจ่ายค่าสินไหม 1,000 เหรียญสหรัฐ หรือค่าเสียหายตามจริง แล้วแต่จำนวนใดจะสูงกว่า - สำหรับการฝ่าฝืนบทบัญญัติของ BIPA โดยเจตนา หรือโดยปราศจากความระมัดระวัง ผู้กระทำการละเมิดจะต้องจ่ายค่าสินไหม 5,000 เหรียญสหรัฐ หรือค่าเสียหายตามจริง แล้วแต่จำนวนใดจะสูงกว่า - นอกจากนี้ผู้ละเมิดยังต้องจ่ายค่าฤชาธรรมเนียมและค่าใช้จ่ายของทนายที่สมเหตุสมผล รวมถึงค่าธรรมเนียมพยานผู้เชี่ยวชาญและค่าใช้จ่ายในการดำเนินคดีอื่น ๆ และ การชดเชยอื่นใดตามแต่ศาลของรัฐหรือศาลรัฐบาลกลางเห็นสมควร
ไทย	- โทษทางแพ่ง – ค่าสินไหมทดแทนสำหรับความเสียหายที่เกิดขึ้นภายใต้หลักความรับผิดเด็ดขาด (strict liability) ซึ่งรวมค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้ว และศาล

	อาจสั่งให้จ่ายค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มได้ ทั้งนี้ต้องไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริง - โทษทางอาญา - หากการละเมิดทำให้เกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย มีโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ และหากการละเมิดดังกล่าวเป็นไปเพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น อาจถูกลงโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ เนื่องจากความผิดนี้มิได้เป็นความผิดต่อรัฐหรือสังคมโดยรวมจึงเป็นความผิดอันยอมความได้ ในกรณีที่ผู้ประกอบธุรกิจเป็นนิติบุคคล กรรมการ ผู้จัดการ หรือผู้ที่รับผิดชอบการดำเนินงานของนิติบุคคลนั้นอาจจะต้องรับผิดเป็นส่วนตัวสำหรับการกระทำความผิดนั้น ๆ ด้วย - โทษทางปกครอง – มีโทษขั้นต่ำอยู่ที่ 500,000 บาท และโทษสูงสุดอยู่ที่ 5,000,000 บาท ขึ้นอยู่กับความร้ายแรงของการกระทำความผิดและขนาดของกิจการของผู้ที่กระทำผิด

2.5.2 อภิปรายผลการศึกษา

บทลงโทษของ DPA นั้นเหมือนกับของ GDPR โดยเป็นบทลงโทษทางปกครองไม่เกิน 10,000,000 ยูโร หรือ 20,000,000 ยูโร หรือในกรณีขององค์กรธุรกิจค่าปรับทางปกครองไม่เกินร้อยละ 2 หรือร้อยละ 4 ของมูลค่ายอดขายทั่วโลกของปีงบประมาณก่อนหน้า แล้วแต่จำนวนใดจะสูงกว่า ทั้งนี้ขึ้นอยู่กับฐานความผิดและประเภทของข้อมูลส่วนบุคคลที่ถูกละเมิด สำหรับ BIPA นั้นเป็นบทลงโทษทางปกครองเช่นเดียวกัน สำหรับการกระทำโดยประมาทต้องจ่ายค่าสินไหม 1,000 เหรียญสหรัฐ หรือค่าเสียหายตามจริง แล้วแต่จำนวนใดจะสูงกว่า แต่หากเป็นการกระทำโดยเจตนาค่าปรับจะสูงถึง 5,000 เหรียญสหรัฐ หรือค่าเสียหายตามจริง แล้วแต่จำนวนใดจะสูงกว่า ทั้งนี้การคำนวณค่าปรับสำหรับ BIPA นั้นอัตราบทลงโทษเป็นค่าเสียหายต่อราย ซึ่งหากมีจำนวนผู้เสียหายมากเท่าใดค่าเสียหายก็มากขึ้นเท่านั้น ดังเช่นกรณี Patel v. Facebook ซึ่ง Facebook ยินยอมจ่ายค่าเสียหายให้ 550 ล้านเหรียญสหรัฐในการไกล่เกลี่ย และในเวลาต่อมายอมเพิ่มเป็น 650 ล้านเหรียญสหรัฐ ซึ่งเจ้าของข้อมูลส่วนบุคคลจะได้รับค่าสินไหมเฉลี่ยที่ 200-400 เหรียญต่อคน[467] ยังถือได้ว่าน้อยกว่าบทปรับขั้นต่ำที่กำหนดไว้ที่ 1,000 เหรียญสหรัฐอยู่มาก

อนึ่ง ประเทศไทยเป็นประเทศเดียวภายใต้ขอบเขตการวิจัยที่มีทั้งโทษทางแพ่ง โทษทางอาญา และโทษทางปกครอง สำหรับโทษทางอาญาที่บัญญัติไว้ใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นอ้างอิงมาจากการกระทำผิดโดยการหมิ่นประมาท และการกระทำผิดโดยการทุจริต กล่าวคือ หากผู้ควบคุมข้อมูลส่วนบุคคลทำผิดบทบัญญัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วน

[467] Morrison, S. (2020). Facebook's sad summer continues with a $650 million settlement. สืบค้นจาก https://www.vox.com/recode/2020/7/23/21335806/facebook-settlement-illinois-facial-recognition-photo-tagging

บุคคล พ.ศ. 2562 หากมีคนนำข้อมูลนั้นไปใช้แล้วทำให้เจ้าของข้อมูลส่วนบุคคลได้รับความเสียหาย เสื่อมเสียชื่อเสียง ถูกดูหมิ่นเกลียดชัง หรือได้รับความอับอาย ซึ่งถือเป็นการกระทำหมิ่นประมาทตามประมวลกฎหมายอาญา มาตรา 326 จะต้องได้รับโทษทางอาญา เช่นเดียวกันกับการกระทำละเมิด พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมาย ซึ่งการแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายถือเป็นการทุจริต สำหรับโทษทางแพ่งนั้นได้กำหนดให้ใช้หลักความรับผิดเด็ดขาด (strict liability) โดยจะต้องชดใช้ค่าสินไหมทดแทนไม่ว่าจะจงใจหรือประมาทเลินเล่อ ทั้งนี้ได้กำหนดให้ค่าสินไหมทดแทนขึ้นอยู่กับความเสียหายที่เกิดขึ้นตามจริง รวมถึงค่าใช้จ่ายที่ได้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้ว นอกจากค่าสินไหมทดแทนที่แท้จริงแล้วศาลอาจสั่งให้จ่ายค่าสินไหมทดแทนเพื่อการลงโทษได้ไม่เกินสองเท่าของค่าสินไหมทดแทนที่ได้จ่ายไปตามจริง สำหรับโทษทางปกครองนั้นขึ้นอยู่กับความร้ายแรงของการกระทำความผิด และขนาดของกิจการของผู้กระทำความผิด

บทที่ 5
บทสรุป และข้อเสนอแนะ

1. บทสรุป

เมื่อการพัฒนาของเทคโนโลยีทำให้โอกาสการรั่วไหลของข้อมูลส่วนบุคคลมีมากขึ้น ผู้ไม่หวังดีสามารถเจาะระบบได้ง่ายขึ้น สามารถล้วงเอาข้อมูลส่วนบุคคลและรหัสผ่านไปได้ง่ายขึ้น สร้างความเสียหายให้กับเจ้าของข้อมูลอย่างมาก จึงมีแนวคิดในการนำข้อมูลอัตลักษณ์บุคคล หรือข้อมูลชีวภาพ (biometric) มาใช้ในการยืนยันตัวตน เพื่อเป็นการยกระดับการรักษาความปลอดภัยของข้อมูล เนื่องจากมีความเชื่อว่าข้อมูลชีวภาพนั้นไม่สามารถลอกเลียนได้ แต่อย่างไรก็ดีในความเป็นจริงมีการยืนยันจากหลาย ๆ แหล่งว่าการลอกเลียนข้อมูลชีวภาพมิได้ยากจนเกินไป

มีการเริ่มนำข้อมูลชีวภาพมาใช้ในการทำธุรกิจต่าง ๆ เช่น การใช้ facial recognition ในการเปิดบัญชีธนาคาร การใช้ลายนิ้วมือในการลงเวลาทำงาน เป็นต้น ข้อมูลส่วนบุคคลสามารถแบ่งออกได้เป็นสองประเภท คือ ข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลที่มีความอ่อนไหว สำหรับข้อมูลชีวภาพนั้นถือว่าเป็นข้อมูลที่มีความอ่อนไหวสูง และด้วยลักษณะของข้อมูลชีวภาพ ซึ่งเป็นข้อมูลเฉพาะตัวของเจ้าของข้อมูลที่มีความเป็นเอกลักษณ์ เป็นสากล และเป็นถาวรแล้ว หากมีการรั่วไหลแล้วอาจสร้างความเสียหายให้กับเจ้าของข้อมูลอย่างไม่สามารถแก้ไขให้กลับมาเหมือนเดิมได้อีก ดังนั้นเมื่อมีการนำข้อมูลชีวภาพไปใช้ในการดำเนินธุรกิจจึงควรมีกฎหมายคุ้มครองมากกว่าข้อมูลส่วนบุคคลทั่วไป

เดิมทีสิทธิส่วนบุคคลสามารถแบ่งออกได้เป็น 4 ประเภท คือ 1) ความเป็นส่วนตัวของบุคคล (Privacy of the person) 2) ความเป็นส่วนตัวของพฤติกรรมของบุคคล (Privacy of personal behavior) 3) ความเป็นส่วนตัวของข้อมูลส่วนบุคคล (Privacy of personal data) และ 4) ความเป็นส่วนตัวของการสื่อสารของบุคคล (Privacy of personal communication) ซึ่งต่อมาการพัฒนาอย่างก้าวกระโดดของเทคโนโลยีทำให้มีการปรับเปลี่ยนสิทธิส่วนบุคคลออกเป็น 7 ประเภท คือ 1) ความเป็นส่วนตัวของบุคคล (Privacy of the person) 2) ความเป็นส่วนตัวด้านพฤติกรรมและการกระทำ (Privacy of behavior and action 3) ความเป็นส่วนตัวด้านการสื่อสาร (Privacy of communication) 4) ความเป็นส่วนตัวด้านข้อมูลและรูปถ่าย (Privacy of data and image) 5) ความเป็นส่วนตัวด้านความคิดและความรู้สึก (Privacy of thoughts and feelings) 6) ความเป็นส่วนตัวด้านที่ตั้งและพื้นที่ (Privacy of location and space) และ 7) ความเป็นส่วนตัวด้านการสมาคม (Privacy of association) เนื่องจากเทคโนโลยีได้พัฒนาจนเข้ามาเป็นส่วนหนึ่งของชีวิตเรามากขึ้น เทคโนโลยีมีความสามารถในการนำรูปถ่าย ความคิดและความรู้สึก รวมถึงตำแหน่งที่ตั้งและพื้นที่ของเราไปใช้ได้อย่างง่ายดาย นอกจากนี้ เทคโนโลยีทำให้สามารถมีการบันทึกข้อมูลทุกอย่างของเราไว้ได้ ไม่ว่าจะเป็นปุ่มทุกปุ่มที่เรากด เว็บทุกเว็บที่เราเข้าไปดู การเคลื่อนหรือคลิกเม้าส์ของเราไปตำแหน่งต่าง ๆ อาจมีการบันทึกไว้ได้เสมอโดยที่เราไม่รู้ตัว

ดังนั้นองค์การเพื่อความร่วมมือและการพัฒนาทางเศรษฐกิจ (The Organization for Economic Cooperation and Development หรือ OECD) จึงได้กำหนดกรอบในการคุ้มครองข้อมูลส่วนบุคคลที่เรียกว่า “ข้อแนะนำเกี่ยวกับแนวทางการคุ้มครองความเป็นส่วนตัวและการส่งผ่านข้อมูลส่วนบุคคลระหว่างประเทศ (Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data)” ซึ่งกำหนดหลักเกณฑ์ไว้ว่า การเก็บข้อมูลส่วนบุคคลนั้นจะต้องเก็บเท่าที่จำเป็น อย่างถูกต้องด้วยกฎหมาย และต้องได้รับความยินยอมจากเจ้าของข้อมูล ข้อมูลที่ทำการเก็บต้องเกี่ยวข้องกับวัตถุประสงค์ในการเก็บข้อมูล และต้องมีความถูกต้องและเป็นปัจจุบัน โดยจะต้องมีการระบุวัตถุประสงค์อย่างชัดเจนและใช้ภายในวัตถุประสงค์ที่ได้ระบุไว้เท่านั้น รวมทั้งยังต้องมีการดูแลรักษาความปลอดภัยอย่างเหมาะสม นอกจากนี้ ผู้รวบรวมข้อมูลส่วนบุคคลยังต้องมีนโยบายการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่มีความโปร่งใสโดยให้เจ้าของข้อมูลมีส่วนร่วมในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลด้วย

ข้อมูลส่วนบุคคลชีวภาพอาจเป็นข้อมูลลักษณะทางสรีระหรือลักษณะทางพฤติกรรมก็ได้ แต่ต้องมีความเป็นเอกลักษณ์ เป็นสากล และเป็นถาวรจึงจะสามารถนำมาใช้ในการยืนยันตัวตนได้ นอกจากนี้ ยังควรมีความง่ายในการเก็บตัวอย่าง เป็นที่ยอมรับว่าสามารถนำไปใช้เพื่อยืนยันตัวตนหรือระบุตัวตนได้ โดยสามารถปลอมหรือหลอกระบบได้ยาก อีกทั้งยังต้องมีความแม่นยำในการนำไปใช้อีกด้วย

ขั้นตอนในการทำงานของระบบยืนยันตัวตนชีวภาพ เริ่มจากการลงทะเบียนโดยเก็บข้อมูลของเจ้าของข้อมูลส่วนบุคคลเข้าระบบ เช่น การถ่ายรูป การสแกนลายนิ้วมือ เป็นต้น จากนั้นระบบจะนำข้อมูลที่ได้ไปทำให้ปรกติ คือกำจัดข้อมูลไม่พึงประสงค์ออก แล้วจึงนำไปสกัดคุณลักษณะและสร้างแม่แบบไว้ในระบบ เมื่อเจ้าของข้อมูลส่วนบุคคลต้องการยืนยันตัวตน เช่น ต้องการเข้าถึงข้อมูลในบัญชีเงินฝากของตนเอง ระบบจะเก็บข้อมูลชีวภาพจากเจ้าของข้อมูลส่วนบุคคลอีกครั้ง กำจัดข้อมูลไม่พึงประสงค์ออก นำไปสกัดคุณลักษณะ และนำไปเทียบกับแม่แบบที่ได้สร้างไว้ในขั้นตอนลงทะเบียน และหากเป็นขั้นตอนการระบุตัวตนระบบจะนำข้อมูลที่เก็บจากเจ้าของข้อมูลส่วนบุคคลที่ได้กำจัดข้อมูลไม่พึงประสงค์ออก และสกัดคุณลักษณะแล้ว ไปเปรียบเทียบกับข้อมูลทั้งหมดที่ระบบเก็บไว้ในฐานข้อมูล

หลักการคุ้มครองข้อมูลส่วนบุคคลชีวภาพที่เหมาะสมควรประกอบไปด้วย 1) ความยินยอมของเจ้าของข้อมูล 2) เจ้าของข้อมูลได้รับการแจ้งข้อมูลที่ชัดเจน และโปร่งใสจากผู้ควบคุมข้อมูลส่วนบุคคล รวมถึงรายละเอียดต่าง ๆ ที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล 3) มีการเก็บข้อมูลชีวภาพเท่าที่จำเป็น ใช้ภายใต้วัตถุประสงค์ที่กำหนด 4) ข้อมูลส่วนบุคคลต้องมีความถูกต้อง และเป็นปัจจุบันเสมอ 5) มีการกำหนดจำนวนและขอบเขตของการใช้งานข้อมูลส่วนบุคคลชีวภาพ โดยใช้เฉพาะที่จำเป็น มีวัตถุประสงค์ที่ชัดเจน และถูกต้องตามกฎหมาย 6) ใช้หลักการไม่เปิดเผยตัวตน เพื่อลดปัญหาการละเมิดความเป็นส่วนตัว โดยการรวมแนวทางการปฏิบัติด้านการรักษาด้านความปลอดภัยที่เกี่ยวกับการทำให้ย้อนกลับไม่ได้ (non-invertibility) การทำให้เชื่อมโยงไม่ได้ (un-linkability) การยกเลิก (cancelability) และการต่ออายุ (renewability)

การนำข้อมูลส่วนบุคคลประเภทชีวภาพมาใช้นั้นมีความเสี่ยง ทั้งความเสี่ยงที่เกิดจากธรรมชาติของข้อมูลชีวภาพเอง และความเสี่ยงที่เกิดจากความผิดพลาดของระบบข้อมูลชีวภาพซึ่งอาจ

เกิดจากวิธีการทำงานของระบบ หรือเกิดจากการโจมตีจากภายนอก การนำข้อมูลชีวภาพมาใช้มากขึ้น ทำให้เกิดความเสี่ยงมากขึ้นตามไปด้วย เนื่องจากการปลอมแปลงข้อมูลชีวภาพบางชนิดสามารถทำได้อย่างง่ายดาย เช่น การปลอมลายนิ้วมือ แม้แต่การปลอมม่านตาจากรูปถ่ายก็สามารถทำได้ ดังนั้น การใช้ข้อมูลชีวภาพอาจทำให้ผู้สุจริตกลายเป็นผู้ต้องหา หรืออาจเพิ่มอัตราการเกิดอาชญากรรม ซึ่งความเสี่ยงเหล่านี้ล้วนเกิดจากธรรมชาติของข้อมูลชีวภาพ นอกจากนี้ความผิดพลาดของระบบข้อมูลชีวภาพอาจเกิดขึ้นได้ซึ่งส่วนหนึ่งเป็นความผิดพลาดที่เกิดจากธรรมชาติของวิธีการทำงานของระบบเอง อันอาจทำให้เจ้าของข้อมูลส่วนบุคคลไม่สามารถใช้บริการหรือซื้อสินค้าที่ใช้ระบบข้อมูลชีวภาพได้ หรือไม่สามารถกระทำการยืนยันตัวตนได้ และเมื่อมีการใช้ข้อมูลชีวภาพมากขึ้นย่อมทำให้ข้อมูลชีวภาพนั้นตกเป็นเป้าหมายของการโจมตีอย่างหลีกเลี่ยงมิได้

เนื่องจากข้อมูลส่วนบุคคลประเภทชีวภาพเป็นข้อมูลที่อ่อนไหว ข้อมูลชีวภาพบางชนิดอาจทำให้ผู้เก็บรวบรวมได้รู้ข้อมูลเกี่ยวกับเจ้าของข้อมูลที่เจ้าของข้อมูลไม่ต้องการให้ผู้อื่นทราบ ดังนั้น การเก็บข้อมูลชีวภาพจึงทำให้เกิดความเสี่ยงต่อการละเมิดความเป็นส่วนตัวของเจ้าของข้อมูลอีกด้วย

สำหรับการวิเคราะห์กฎหมายคุ้มครองส่วนบุคคลชีวภาพของสหภาพยุโรป สหราชอาณาจักร รัฐอิลลินอยส์ สหรัฐอเมริกา และไทย สามารถสรุปได้ดังต่อไปนี้

1.1 คำจำกัดความ

สำหรับคำจำกัดความของคำว่า “ข้อมูลชีวภาพ” หรือ “ข้อมูลส่วนบุคคลประเภทชีวภาพ” นั้น GDPR และ DPA ได้ให้คำจำกัดความที่เหมือนกัน และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้มีการบัญญัติไว้ใกล้เคียงกับ GDPR และ DPA โดยต่างกันที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ระบุว่า “เป็นการนำลักษณะเด่นทางกายภาพ หรือทางพฤติกรรมของบุคคลมาใช้” ในขณะที่ GDPR และ DPA ระบุว่า “ต้องเกี่ยวกับลักษณะทางกายภาพ หรือทางสรีรวิทยา หรือพฤติกรรมของบุคคล” ซึ่งหมายความว่าลักษณะทางสรีรวิทยาไม่ถือว่าเป็นข้อมูลส่วนบุคคลชีวภาพตามความหมายของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ดังนั้นจึงอาจตีความได้ว่าข้อมูลชีวภาพ เช่น คลื่นสมอง (brain pattern) หรือ การเต้นของหัวใจ (heart rhythms) นั้นไม่ถือว่าเป็นข้อมูลชีวภาพเนื่องจากเป็นลักษณะทางสรีรวิทยา สำหรับ BIPA นั้นได้มีกำหนดไว้ค่อนข้างชัดเจนว่าสิ่งใดถือเป็นข้อมูลส่วนบุคคลชีวภาพ สิ่งใดไม่ถือเป็นข้อมูลส่วนบุคคลชีวภาพ และยังมีการระบุอีกด้วยว่าหากสิ่งนั้นอยู่ภายใต้การคุ้มครองของกฎหมายอื่น เช่น พระราชบัญญัติการบริจาคอวัยวะ (Illinois Anatomical Gift Act - 755 ILCS 50/) พระราชบัญญัติความเป็นส่วนตัวข้อมูลทางพันธุกรรม (Genetic Information Privacy Act) พระราชบัญญัติประกันสุขภาพและความรับผิดชอบต่อหน้าที่ 1996 (Health Insurance Portability and Accountability Act 1996) แล้ว สิ่งนั้นมิได้อยู่ภายใต้การคุ้มครองของ BIPA ทั้งนี้เพื่อหลีกเลี่ยงการขัดกันของกฎหมายนั่นเอง

นอกจากนี้ข้อมูลตั้งต้นที่นำไปสร้างแม่แบบเพื่อใช้ในการเปรียบเทียบนั้น เช่น ภาพถ่าย ภาพลายนิ้วมือ เป็นต้น ไม่ได้ถือว่าเป็นข้อมูลส่วนบุคคลชีวภาพตามคำจำกัดความของ GDPR, DPA และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แต่สำหรับ BIPA ดังที่กล่าวมาแล้วได้มีการกำหนดชัดเจนว่าสิ่งใดรวม หรือไม่รวมอยู่ในความหมายของคำว่า “ข้อมูลส่วนบุคคลประเภทชีวภาพ”

อย่างไรก็ดี การให้คำจำกัดความที่เหมาะสมมีความสำคัญและจำเป็นที่จะต้องครอบคลุมสิ่งที่ควรได้รับความคุ้มครอง ผู้วิจัยจึงเห็นสมควรให้มีการปรับคำจำกัดความให้เหมาะสมต่อไป

1.2 หลักเกณฑ์การประมวลผลข้อมูลชีวภาพ

การได้รับความยินยอมโดยชัดแจ้งเป็นหนึ่งในหลักเกณฑ์การประมวลผลข้อมูลส่วนบุคคลประเภทชีวภาพที่ชอบด้วยกฎหมายภายใต้ GDPR, DPA BIPA และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทั้งนี้การได้รับความยินยอมโดยชัดแจ้งเป็นหลักเกณฑ์การประมวลผลข้อมูลส่วนบุคคลประเภทชีวภาพที่ชอบด้วยกฎหมายเพียงหลักเกณฑ์เดียวสำหรับ BIPA แต่สำหรับ GDPR, DPA และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แล้วการประมวลผลข้อมูลส่วนบุคคลประเภทชีวภาพที่ชอบด้วยกฎหมายสามารถทำได้ภายใต้ 1) ประโยชน์สำคัญต่อชีวิต 2) กิจกรรมโดยชอบขององค์กรไม่แสวงหาผลกำไร 3) เปิดเผยข้อมูลต่อสาธารณชน 4) สิทธิเรียกร้องตามกฎหมาย 5) ประโยชน์สาธารณะที่สำคัญ 6) ประโยชน์สาธารณะด้านการคุ้มครองและประกันสังคม 7) ประโยชน์ด้านสาธารณสุข และ 8) การวิจัยหรือทางสถิติ นอกจากนี้ GDPR และ DPA ยังมีการบัญญัติว่าความจำเป็นสำหรับการปฏิบัติหน้าที่ถือเป็นหลักเกณฑ์การประมวลผลข้อมูลส่วนบุคคลชีวภาพที่ชอบด้วยกฎหมายอีกด้วย แต่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มิได้มีการบัญญัติหลักเกณฑ์ความจำเป็นสำหรับการปฏิบัติหน้าที่ไว้

โดยรวมแล้วหลักเกณฑ์ในการประมวลผลข้อมูลส่วนบุคคลประเภทชีวภาพตาม GDPR, DPA และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นเหมือนกันกับหลักเกณฑ์การประมวลผลที่ชอบด้วยกฎหมายสำหรับข้อมูลส่วนบุคคลอ่อนไหวอื่น ๆ เช่น เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน และข้อมูลพันธุกรรม เป็นต้น

อย่างไรก็ตาม สำหรับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลภายใต้หลักเกณฑ์1) ประโยชน์สาธารณะที่สำคัญ 2) ประโยชน์สาธารณะด้านการคุ้มครองและประกันสังคม 3) ประโยชน์ด้านสาธารณสุข และ 4) การวิจัยหรือทางสถิติ นั้นต้องยึดหลักการว่าวัตถุประสงค์นั้นจำเป็นในการปฏิบัติตามกฎหมายด้วย หากวัตถุประสงค์ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลนั้นมิได้จำเป็นในการปฏิบัติตามกฎหมายก็มิสามารถใช้หลักเกณฑ์เหล่านี้ได้

1.3 การรักษาความปลอดภัย

การรักษาความปลอดภัยของข้อมูลส่วนบุคคลประเภทชีวภาพนั้นสามารถทำได้ทั้งทางด้านเทคนิคและด้านองค์กร ทั้งนี้ GDPR และ DPA ได้กำหนดให้การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลนั้นต้องมีมาตรการทั้งสองด้าน อีกทั้งยังต้องมีการคุ้มครองข้อมูลส่วนบุคคลด้วยการออกแบบ (data protection by design) และการคุ้มครองข้อมูลส่วนบุคคลขั้นพื้นฐาน (data protection by default) อีกด้วย สำหรับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นมีการกำหนดให้ใช้มาตรการที่เหมาะสม อย่างไรก็ดีในขณะนี้ยังไม่มีการประกาศใช้กฎหมายลำดับรองอย่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลว่าด้วยมาตรฐานขั้นต่ำเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล

นอกจากมาตรการรักษาความปลอดภัยแล้ว การประเมินผลกระทบการคุ้มครองข้อมูลส่วนบุคคลสำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงยังเป็นมาตรการส่วนหนึ่งในการรักษาความปลอดภัยของข้อมูลได้อีกด้วย เนื่องจากข้อมูลที่มีความเสี่ยงสูงจะต้องได้รับการรักษาความปลอดภัยที่สูงขึ้นตามไปด้วย ทั้งนี้ GDPR และ DPA ได้กำหนดให้มีการประเมินผลกระทบการคุ้มครองข้อมูลส่วนบุคคลสำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูง แต่ BIPA และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ได้มีการกำหนดให้มีการประเมินผลกระทบการคุ้มครองข้อมูลส่วนบุคคลไว้แต่อย่างใด

การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลก็เป็นอีกมาตรการหนึ่งซึ่งสามารถช่วยให้มั่นใจว่าข้อมูลส่วนบุคคลได้รับการรักษาความปลอดภัยที่เหมาะสมได้ เนื่องจากหน้าที่ส่วนหนึ่งของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลคือให้คำแนะนำเกี่ยวกับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าจะเป็น GDPR, DPA หรือ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แต่ BIPA นั้นมิได้มีการกำหนดให้มีการจัดตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ทั้ง GDPR, DPA และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้มีการกำหนดให้มีการแจ้งการรั่วไหลของข้อมูลส่วนบุคคลให้หน่วยงานกำกับดูแลทราบภายใน 72 ชั่วโมง สำหรับ BIPA นั้นมิได้มีการกำหนดเงื่อนไขสำหรับการแจ้งการรั่วไหลของข้อมูลไว้แต่อย่างใด

นอกจากนี้ GDPR, DPA และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังกำหนดให้มีการบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้เพื่อให้มีการตรวจสอบได้ แต่ BIPA มิได้มีการกำหนดเงื่อนไขสำหรับการบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้

1.4 การร้องเรียน

หากเจ้าของข้อมูลส่วนบุคคลได้รับความเดือดร้อน หรือเกิดความเสียหายแก่ทรัพย์สินอันเป็นผลจากการละเมิดข้อกำหนด GDPR, DPA และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เจ้าของข้อมูลส่วนบุคคลสามารถร้องเรียนต่อหน่วยงานกำกับดูแลได้ นอกจากนี้ยังสามารถยื่นฟ้องคดีต่อหน่วยงานกำกับดูแล ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลอีกด้วย

ทั้งนี้ศาลในสหราชอาณาจักร และศาลฎีกาในรัฐอิลลินอยส์ได้พิพากษาว่าความเสียหาย หรือเดือดร้อนนั้น ไม่จำเป็นต้องเป็นความเสียหายทางด้านการเงิน หรือความเดือดร้อนอันสามารถกำหนดมูลค่าได้ เพียงสูญเสียการควบคุมข้อมูลส่วนบุคคล หรือถูกละเมิดสิทธิตามกฎหมายก็สามารถถือได้ว่าเจ้าของข้อมูลส่วนบุคคลได้รับความเสียหายที่ต้องได้รับการเยียวยาแล้ว

เนื่องจากลักษณะของการละเมิดข้อมูลส่วนบุคคลมักมีผู้เสียหายจำนวนมาก ดังนั้นกฎหมายคุ้มครองข้อมูลส่วนบุคคล DPA และ BIPA จึงกำหนดให้สามารถดำเนินคดีแบบกลุ่มโดยให้โจทก์เป็นตัวแทนผู้เสียหายทั้งหมดอีกด้วย ทั้งนี้ไม่ว่าในคดี Lloyd v Google ในสหราชอาณาจักร หรือคดี Rosenbach v. Six Flags ในรัฐอิลลินอยส์ สหรัฐอเมริกาล้วนแล้วแต่เป็นการดำเนินคดีแบบ

กลุ่มทั้งสิ้น โดยศาลพิพากษาว่า Richard Lloyd ถือเป็นตัวแทนของผู้ใช้ไอโฟนที่ใช้เว็บเบราว์เซอร์ซาฟารีทั้งหมดในประเทศอังกฤษและเวลส์[468]

นอกจากนี้ในสหรัฐอเมริกามี Class Action Fairness Act ซึ่งทำให้สามารถดำเนินคดีแบบกลุ่มสำหรับการละเมิด BIPA ได้ เช่น คดี Patel v. Facebook ที่ได้รวมสามคดีเข้าด้วยกันและกำหนดให้ผู้เสียหายเป็นผู้ที่ใช้ Facebook ในรัฐอิลลินอยส์ที่มีอายุมากกว่า 18 ปีซึ่งมีภาพที่ Facebook ใช้สร้างแม่แบบที่เก็บไว้หลังจากวันที่ 7 มิถุนายน พ.ศ. 2554 ซึ่งเป็นวันที่ Facebook ชี้แจงว่ามีการเริ่มให้บริการแนะนำแท็กในประเทศส่วนใหญ่และผู้เสียหายต้องอาศัยอยู่ในรัฐอิลลินอยส์เป็นเวลาอย่างน้อยหกเดือน[469]

ใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มิได้มีการกล่าวถึงการดำเนินคดีแบบกลุ่ม ดังนั้นจึงต้องยึดหลักการดำเนินคดีแบบกลุ่มตามประมวลกฎหมายวิธีพิจารณาความแพ่ง พ.ศ. 2563 ซึ่งสามารถดำเนินคดีแบบกลุ่มได้ ทั้งนี้ ประมวลกฎหมายวิธีพิจารณาความแพ่ง พ.ศ. 2563 มาตรา 222/1 ถึง 222/49 ได้บัญญัติให้สามารถมีการดำเนินคดีแบบกลุ่มได้สำหรับคดีละเมิด คดีผิดสัญญา และคดีเรียกร้องสิทธิตามกฎหมายต่าง ๆ เช่น กฎหมายเกี่ยวกับสิ่งแวดล้อม การคุ้มครองผู้บริโภค แรงงาน หลักทรัพย์และตลาดหลักทรัพย์ การแข่งขันทางการค้า[470] แต่อย่างไรก็ดี ในการฟ้องคดีอาจต้องคำนึงถึงอำนาจพิจารณาพิพากษาของศาลและข้อเท็จจริงในคดีเป็นกรณี ๆ ไป เช่น กรณีนายจ้างเก็บรวบรวมข้อมูลส่วนบุคคลของลูกจ้างโดยความยินยอมของลูกจ้างแต่นำไปใช้โดยขัดกับวัตถุประสงค์ในการเก็บรวบรวม ลูกจ้างไม่สามารถยื่นฟ้องเป็นคดีแรงงานได้ และต้องยื่นฟ้องเป็นคดีแพ่งสามัญจึงจะสามารถดำเนินคดีแบบกลุ่มได้

ในด้านของอายุความนั้น ทั้ง GDPR, DPA และ BIPA มิได้มีการกำหนดอายุความ แต่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นคดีมีอายุความ 3 ปี นับแต่วันที่ผู้เสียหายรู้ถึงความเสียหายและรู้ตัวผู้ควบคุมข้อมูลส่วนบุคคลหรือ ผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องรับผิด หรือเมื่อพ้นสิบปีนับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล

1.5 บทลงโทษ

บทลงโทษของ GDPR และ DPA นั้นมีเพียงโทษทางปกครอง โดยกำหนดบทลงโทษตามผลกระทบที่เกิดจากการละเมิด หากการละเมิดนั้นมีผลกระทบสูงบทลงโทษจะสูงตามไปด้วย โดยมีอัตราค่าปรับสูงสุดอยู่ที่ ร้อยละ 4 ของมูลค่ายอดขายทั่วโลก หรือ 20 ล้านยูโร แล้วแต่จำนวนใดจะสูงกว่า และจำนวนค่าปรับขึ้นอยู่กับฐานความผิดและประเภทของข้อมูลส่วนบุคคลที่ถูกละเมิด สำหรับ BIPA นั้นมีเพียงโทษปรับทางปกครองเช่นเดียวกัน แต่กำหนดโทษรุนแรงตามการกระทำ หากกระทำโดยเจตนาหรือปราศจากความระมัดระวังต้องได้รับโทษสูงกว่า นอกจากนี้ยังกำหนดโทษต่อ

---

[468] Covington & Burling LLP. (2019). Landmark Case Opens the Door to UK Data Protection Consumer Class Actions. สืบค้นจาก https://www.cov.com/en/news-and-insights/insights/2019/10/landmark-case-opens-the-door-to-uk-data-protection-consumer-class-actions

[469] Marotti, A. (2020). Some Illinois Facebook users could get $300 under massive biometric privacy settlement. *Chicago Tribune*. สืบค้นจาก https://www.chicagotribune.com/business/ct-biz-facebook-biometric-privacy-class-action-settlement-20200514-b53gxxmyhfezzl7hlh32777dlq-story.html

[470] ประมวลกฎหมายวิธีพิจารณาความแพ่ง พ.ศ. 2563, มาตรา 222/8.

จำนวนผู้เสียหายโดยมีค่าสินไหมสูงสุดที่ 5,000 เหรียญสหรัฐต่อราย สำหรับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นบทลงโทษมีทั้งทางแพ่ง ทางอาญา และทางปกครอง โดยบทลงโทษทางอาญานั้นมีความคล้ายคลึงกับมาตรา 326 ตามประมวลกฎหมายอาญา[471] ซึ่งเป็นความผิดฐานหมิ่นประมาท แม้ระวางโทษจำคุกขั้นสูงสุดใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 น้อยกว่าความผิดฐานหมิ่นประมาท แต่อัตราค่าปรับขั้นสูงสุดที่บัญญัติไว้ใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นสูงกว่าความผิดฐานหมิ่นประมาท อย่างไรก็ดี พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นยังได้กำหนดโทษทางอาญาสำหรับการแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายอีกด้วย นอกจากนี้สำหรับผู้ประกอบธุรกิจที่เป็นนิติบุคคล กรรมการ ผู้จัดการ หรือผู้ที่รับผิดชอบการดำเนินงานของนิติบุคคลนั้นอาจจะต้องรับผิดเป็นส่วนตัวสำหรับการกระทำความผิดนั้น ๆ อีกด้วย ส่วนโทษทางปกครองมีโทษปรับสูงสุดอยู่ที่ 5,000,000 บาท ทั้งนี้ค่าปรับขึ้นอยู่กับความร้ายแรงของการกระทำความผิดและขนาดกิจการของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล โดยเป็นบทปรับสำหรับการไม่ปฏิบัติตามข้อกำหนดในพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับโทษทางแพ่งได้กำหนดให้จ่ายค่าสินไหมทดแทนความเสียหายที่เกิดขึ้นภายใต้หลักความรับผิดเด็ดขาด ค่าใช้จ่ายที่ได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้น หรือระงับความเสียหายที่เกิดขึ้นแล้ว นอกจากนี้ศาลอาจสั่งให้จ่ายค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มได้แต่ไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริง อย่างไรก็ดีไม่ได้มีการกำหนดว่าอัตราการลงโทษนั้นขึ้นอยู่กับประเภทของข้อมูลส่วนบุคคลที่ถูกละเมิด

2. ข้อเสนอแนะ

หลังจากการศึกษาวิจัยข้อมูลต่าง ๆ แล้ว ผู้วิจัยมีข้อเสนอแนะดังต่อไปนี้

2.1 คำจำกัดความ

เนื่องจากคำว่า “ข้อมูลชีวภาพ” ตามความหมายที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้บัญญัติไว้ อาจทำให้เกิดความเข้าใจคลาดเคลื่อนได้ เนื่องจากคำว่า “ชีวภาพ” ที่คนทั่วไปคุ้นเคยกัน และตามความหมายในพจนานุกรม ฉบับราชบัณฑิตยสถานนั้น หมายถึง “1) น. ความเป็นสิ่งมีชีวิต 2) ว. เกี่ยวกับสิ่งที่มีชีวิตและสิ่งที่สืบเนื่องมาจากสิ่งมีชีวิต เช่น วิทยาศาสตร์ชีวภาพ ปุ๋ยชีวภาพ” นอกจากนี้ สำนักงานราชบัณฑิตยสภา ยังได้ให้ความหมายของคำว่า “ชีวภาพ” ว่าหมายถึง

“ชีวิต เกี่ยวกับสิ่งมีชีวิต เช่น ความหลากหลายทางชีวภาพทำให้เกิดความสมดุลของธรรมชาติ หมายถึง สิ่งที่จำเป็นสำหรับการดำรงชีวิต เช่น ภาวะซึมเศร้าอาจเกิดจากความไม่สมดุลของสารชีวภาพในสมอง บางครั้งคำว่า ชีวภาพ ใช้เกี่ยวกับจุลินทรีย์และกระบวนการผลิตสิ่งที่ได้และเกิดจากสิ่งมีชีวิต เช่น เกษตรกรมักใช้วิธีการทางชีวภาพทำปุ๋ยหมัก การกำจัดน้ำเสีย ด้วยน้ำหมักชีวภาพซึ่งมีจุลินทรีย์นับว่าได้ผลเป็นที่พอใจ ในการทำสงครามนอกจากจะใช้ชีปนาวุธและยุทโธปกรณ์

---

[471] ประมวลกฎหมายอาญา มาตรา 326 ผู้ใดใส่ความผู้อื่นต่อบุคคลที่สาม โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง ผู้นั้นกระทำความผิดฐานหมิ่นประมาท ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

ต่าง ๆ ยังพบการใช้อาวุธนิวเคลียร์ อาวุธเคมี และอาวุธชีวภาพอีกด้วย นอกจากนั้นคำว่า ชีวภาพ ยังมีความหมายตรงข้ามกับคำว่า กายภาพ ในความหมายว่า สิ่งมีชีวิต ตรงข้ามกับ สิ่งไม่มีชีวิต เช่น เพื่อการพัฒนาที่ยั่งยืน ครัวเรือนของเกษตรกรต้องมีทรัพยากรทางกายภาพ และชีวภาพเพียงพอต่อการดำรงชีพ บุคลากรที่ทำงานเสี่ยงภัยต้องสวมใส่อุปกรณ์เพื่อป้องกันตนเองจากอันตรายทางกายภาพและอันตรายทางชีวภาพ"[472]

ดังนั้น ความหมายของคำว่า "ชีวภาพ" จึงตรงกับคำว่า "biological" มากกว่า "biometrics" และเนื่องจากข้อมูลชีวภาพตามความหมายของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นจะต้องเกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพ หรือพฤติกรรมของบุคคลมาใช้ในการยืนยันตัวตน ผู้วิจัยจึงขอเสนอให้เปลี่ยนคำว่า "ข้อมูลชีวภาพ" เป็น "ข้อมูลชีวมาตร" ตามพจนานุกรม ราชบัณฑิตยสถาน ศัพท์คอมพิวเตอร์และเทคโนโลยีสารสนเทศ (พิมพ์ครั้งที่ 7 พ.ศ. 2549) ซึ่งจะทำให้ได้ความหมายชัดเจนและสามารถเข้าใจได้ง่ายขึ้น

สำหรับคำจำกัดความนั้น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้บัญญัติไว้สอดคล้องกับหลักที่ GDPR ได้วางไว้ว่า "ข้อมูลชีวภาพ" หมายความว่า ข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือข้อมูลจำลองลายนิ้วมือ[473] อย่างไรก็ดีผู้วิจัยเสนอว่าเนื่องจากการพัฒนาอย่างรวดเร็วของเทคโนโลยีคำจำกัดความของ "ข้อมูลชีวภาพ" จึงควรเปิดกว้างไว้เพื่อให้รองรับข้อมูลที่อาจเป็นข้อมูลชีวภาพได้ในอนาคต อีกทั้งยังควรครอบคลุมข้อมูลชีวภาพตั้งต้นเนื่องจากข้อมูลชีวภาพตั้งต้นสามารถนำไปใช้สร้างข้อมูลชีวภาพแม่แบบได้ และมีความชัดเจนมากขึ้นว่าสิ่งใดคือข้อมูลชีวภาพ โดยผู้วิจัยเสนอให้ปรับคำจำกัดความ ดังต่อไปนี้

"ข้อมูลชีวมาตร" หมายถึง "ข้อมูลส่วนบุคคลที่เกิดจากการใช้หรือเหมาะสมที่จะใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องโดยตรงหรือโดยอ้อมกับการนำลักษณะเด่นทางกายภาพ ทางสรีรวิทยาหรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือข้อมูลจำลองลายนิ้วมือ ทั้งนี้ไม่รวมถึง ตัวอย่างทางชีวภาพของมนุษย์ที่ใช้สำหรับการทดสอบหรือการคัดกรองทางวิทยาศาสตร์ ข้อมูลประชากร คำอธิบายรอยสัก คำอธิบายทางกายภาพ เช่น ส่วนสูง น้ำหนัก สีผม หรือสีตา นอกจากนี้ ข้อมูลชีวมาตรยังไม่รวมถึง อวัยวะ เนื้อเยื่อ หรือชิ้นส่วนที่ได้จากการบริจาค หรือ เลือด หรือเซรุ่ม ที่เก็บไว้ในนามของผู้รับหรือผู้ที่อาจได้รับการปลูกถ่ายอวัยวะ ไม่ว่าอวัยวะนั้นจะมาจากผู้ที่ยังมีชีวิตอยู่ หรือมาจากผู้ที่เสียชีวิตไปแล้ว และไม่รวมถึงการเอกซเรย์ ไม่ว่าจะเป็นการเอกซเรย์รังสีเอกซเรย์คอมพิวเตอร์ ซีทีสแกน เอ็มอาร์ไอ เพ็ทสแกน หรือการเอกซเรย์เต้านม หรือ ภาพของกายวิภาคของมนุษย์ที่ใช้ในการวินิจฉัยพยากรณ์โรคหรือรักษาโรค หรือสภาวะด้านสุขภาพอื่น ๆ หรือเพื่อตรวจสอบเพิ่มเติมการทดสอบหรือการคัดกรองทางวิทยาศาสตร์"

---

[472] http://www.royin.go.th/?knowledges=ชีวภาพ-๘-ธันวาคม-๒๕๕๕

[473] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 26 วรรค 2.

คำจำกัดความนี้ครอบคลุมถึงข้อมูลชีวภาพตั้งต้น และข้อมูลที่อาจเป็นข้อมูลชีวภาพได้ในอนาคต อีกทั้งยังมีการกำหนดชัดเจนว่าสิ่งใดไม่ถือเป็นข้อมูลชีวภาพเพื่อลดความจำเป็นในการตีความ

2.2 หลักเกณฑ์การประมวลผลข้อมูลชีวภาพ

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้บัญญัติว่าข้อมูลส่วนบุคคลที่มีความอ่อนไหว คือ เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ข้อมูลชีวภาพ ความพิการ ข้อมูลสหภาพแรงงาน และข้อมูลพันธุกรรม เป็นต้น จากการวิจัยพบว่าข้อมูลส่วนบุคคลประเภทชีวภาพมีลักษณะไม่เหมือนกับข้อมูลส่วนบุคคลที่มีความอ่อนไหวอื่น ๆ และการรั่วไหลหรือการนำข้อมูลส่วนบุคคลชีวภาพไปใช้ในทางที่ไม่ควรนั้นอาจทำให้เกิดผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลซึ่งมีความรุนแรงอันไม่อาจระงับได้ และในปัจจุบันองค์กรเอกชนต่าง ๆ เริ่มมีการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลชีวภาพมากขึ้น ดังนั้นผู้วิจัยเห็นว่าควรพิจารณาหลักเกณฑ์ในการประมวลผลข้อมูลส่วนบุคคลชีวภาพให้เหมาะสม

ดังที่กล่าวมาแล้ว การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลชีวภาพกระทำเพื่อวัตถุประสงค์ในการยืนยันตัวตน (authentication) และการระบุตัวตน (identification) ดังนั้นจึงต้องพิจารณาว่าหลักเกณฑ์การประมวลผลสำหรับข้อมูลส่วนบุคคลชีวภาพในภาคเอกชนโดยมิได้รับความยินยอมอย่างชัดแจ้งนั้นมีความจำเป็นมากน้อยเพียงใด และควรใช้เพื่อวัตถุประสงค์ใดบ้าง การใช้ข้อมูลชีวภาพเพื่อระบุตัวตนคือการกระทำเพื่อระบุว่าบุคคลนั้นคือใครซึ่งมักใช้ในการรักษาความปลอดภัย เช่น การรักษาความปลอดภัยของสนามบิน การตรวจคนเข้าเมืองและการจับคนร้าย ซึ่งเป็นการกระทำที่ควรจำกัดสำหรับภาครัฐเท่านั้น ในภาคเอกชนการระบุตัวตนมักจะถูกนำมาใช้ในการทำโปรไฟลิ่ง (profiling) เช่น การทำโฆษณาแบบเจาะจงซึ่งใช้การวิเคราะห์กริยาท่าทาง ความรู้สึก อายุหรือเพศ แล้วทำการแสดงโฆษณาให้ตรงกับเป้าหมาย ซึ่งการกระทำดังกล่าวอาจเป็นการละเมิดความเป็นส่วนตัวอย่างรุนแรงและเปิดเผยข้อมูลซึ่งเจ้าของข้อมูลอาจไม่ต้องการให้เปิดเผย เช่น การทำโปรไฟลิ่งสำหรับโฆษณาแบบเจาะจงสำหรับผู้หญิงที่กำลังตั้งครรภ์ทำให้สามารถคาดเดาได้ว่าเป้าหมายกำลังตั้งครรภ์หรือไม่และทำการแสดงโฆษณาสินค้าแม่และเด็กให้กับเป้าหมายนั้น ซึ่งเจ้าของข้อมูลส่วนบุคคลผู้ตกเป็นเป้าหมายอาจมีเหตุผลส่วนตัวที่ไม่ต้องการเปิดเผยการตั้งครรภ์ให้ผู้อื่นแม้กระทั่งคนในครอบครัวทราบ ดังนั้นการใช้ข้อมูลชีวภาพเพื่อการระบุตัวตนในภาคเอกชนโดยมิได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลจึงเป็นสิ่งที่ไม่ควรกระทำเนื่องจากเป็นการเปิดโอกาสให้มีการละเมิดสิทธิส่วนบุคคลโดยไม่มีความจำเป็น และผู้วิจัยมีความเห็นว่าในภาคเอกชนควรกำหนดให้มีการใช้ข้อมูลส่วนบุคคลชีวภาพเพียงเพื่อการยืนยันตัวตนเท่านั้น

สำหรับภาครัฐนั้น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีบทบัญญัติยกเว้นมิให้มีการบังคับใช้ พ.ร.บ. ฉบับนี้กับ “การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการ

รักษาความมั่นคงปลอดภัยไซเบอร์”[474] และ “การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา”[475] ดังนั้นการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลใด ๆ รวมถึงข้อมูลชีวภาพเพื่อการรักษาความปลอดภัยโดยภาครัฐในการรักษาความมั่นคงของรัฐ และความปลอดภัยของประชาชนจึงสามารถทำได้โดยมิต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลหรืออ้างฐานการประมวลผลที่ชอบด้วยกฎหมายอื่น ๆ แต่อย่างใด

อย่างไรก็ดี เมื่อพิจารณาแล้วผู้วิจัยเห็นว่าหลักเกณฑ์ในการประมวลผลข้อมูลชีวภาพตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นมีความเหมาะสมอยู่แล้ว เนื่องจากการเก็บเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลชีวภาพโดยไม่ได้รับความยินยอมโดยชัดแจ้งสามารถกระทำได้ภายใต้หลักเกณฑ์ที่จำกัด เช่น 1) ประโยชน์สำคัญต่อชีวิต 2) กิจกรรมโดยชอบขององค์กรไม่แสวงหาผลกำไร ซึ่งไม่อนุญาตให้เปิดเผยข้อมูลส่วนบุคคลออกไปภายนอก 3) เปิดเผยข้อมูลต่อสาธารณชนด้วยความยินยอมโดยชัดแจ้ง 4) สิทธิเรียกร้องตามกฎหมาย และ 5) จำเป็นในการปฏิบัติตามกฎหมาย

2.3 การรักษาความปลอดภัย

ข้อมูลส่วนบุคคลประเภทชีวภาพนั้นต้องได้รับการรักษาความปลอดภัยในระดับสูง เนื่องจากการรั่วไหลของข้อมูลส่วนบุคคลประเภทดังกล่าวอาจก่อให้เกิดความเสียหายร้ายแรงได้ ดังนั้นผู้วิจัยมีความเห็นว่า พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ควรมีการคุ้มครองข้อมูลส่วนบุคคลด้วยการออกแบบ (data protection by design) และการคุ้มครองข้อมูลส่วนบุคคลขั้นพื้นฐาน (data protection by default) ตามแนวทางของ GDPR และ DPA และควรมีการกำหนดมาตรการต่างๆ ตามความเหมาะสม เช่น การเข้ารหัสลับข้อมูล (encrypt) การทำให้เป็นข้อมูลแฝงที่ไม่สามารถระบุตัวตนได้ (Pseudonymized) หรือการมีกระบวนการในการทดสอบ ประเมินประสิทธิภาพของมาตรการด้านเทคนิคและมาตรการด้านองค์กรอย่างสม่ำเสมอ นอกจากนี้ การรักษาความปลอดภัยของข้อมูลส่วนบุคคลประเภทชีวภาพควรใช้เทคโนโลยีที่ทันสมัยที่ยึดแนวทางการปฏิบัติด้านการรักษาความปลอดภัยที่เหมาะสมกับการรักษาความปลอดภัยข้อมูลส่วนบุคคลชีวภาพ ไม่ว่าจะเป็นการทำให้ย้อนกลับไม่ได้ (non-invertibility) การทำให้เชื่อมโยงไม่ได้ (un-linkability) การยกเลิก (cancelability) และการต่ออายุ (renewability) เช่น Cancelable Biometric เป็นต้น ซึ่งสิ่งเหล่านี้นับเป็นการคุ้มครองข้อมูลส่วนบุคคลด้วยการออกแบบ (privacy by design)

อนึ่ง การรักษาความปลอดภัยของข้อมูลชีวภาพควรยึดหลักมาตรฐานที่เป็นที่ยอมรับในระดับสากลในการรักษาความปลอดภัยของระบบข้อมูลชีวภาพ ไม่ว่าจะเป็น ISO 27001 Information Security Standard ซึ่งเป็นมาตรฐานที่เป็นที่ยอมรับสำหรับการวางมาตรการความปลอดภัยของข้อมูล และ ISO/IEC 24745:2011 - Information Technology – Security Techniques – Biometric Information Protection หรือ ISO 19092:2008 Financial services — Biometrics — Security framework ซึ่งเป็นมาตรฐานระดับสากลของการรักษาความปลอดภัย

---

[474] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 4 (2).

[475] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 4 (5).

ของข้อมูลชีวภาพ รวมทั้งมาตรฐานสำหรับการพัฒนาระบบงานข้อมูลชีวภาพตามที่คณะทำงาน ISO/IEC JTC 1/SC 37 Biometrics ได้กำหนดไว้เพื่อเป็นมาตรฐานในการพัฒนาระบบข้อมูลชีวภาพ

นอกจากนี้ ผู้วิจัยเสนอว่าในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลประเภทชีวภาพนั้นควรมีการประเมินผลกระทบและความจำเป็นในการเก็บข้อมูลเสียก่อน และไม่ควรมีการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลชีวภาพที่ไม่จำเป็น ดังนั้นหากจะมีการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลประเภทชีวภาพ หากทำการประเมินผลกระทบแล้วผลที่ได้คือมีความเสี่ยงสูงควรได้รับการอนุมัติจากคณะกรรมการคุ้มครองส่วนบุคคลเสียก่อนเช่นเดียวกันกับ GDPR และ DPA

ตัวอย่าง ในปัจจุบันการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลชีวภาพที่ใช้กันอย่างแพร่หลายคือการสแกนลายนิ้วมือ ไม่ว่าจะเป็นเพื่อการบันทึกเวลาเข้า-ออกสำหรับพนักงานหรือนักเรียน นักศึกษา ซึ่งเป็นการใช้ “สิ่งที่คุณเป็น (what you are)” เพื่อการยืนยันตัวตน ทั้งนี้เพื่อป้องกันการรูดบัตรแทนกัน แต่อย่างไรก็ดี เนื่องจากความเสี่ยงของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลชีวภาพนั้นมีสูง ไม่ว่าลายนิ้วมือตั้งต้น หรือลายนิ้วมือแม่แบบ ไม่ควรถูกเก็บอยู่บนเซิฟเวอร์ จึงควรหาวิธีที่เหมาะสมในการยืนยันตัวตนโดยลดความเสี่ยงให้กับเจ้าของข้อมูลส่วนบุคคล เช่น การเก็บลายนิ้วมือไว้ในบัตรประจำตัวพนักงาน (what you have) และเปรียบเทียบกับลายนิ้วมือ (what you are) ที่สแกนขณะที่เข้า-ออก หรือหลีกเลี่ยงการใช้ลายนิ้วมือโดยการรูดบัตร (what you have) และให้ระบบส่ง one-time-password (OTP) ไปยังมือถือของพนักงานเพื่อป้อนเข้าสู่ระบบ (what you know) เห็นได้ว่ามีวิธีอีกมากมายที่จะหลีกเลี่ยงการใช้ข้อมูลส่วนบุคคลชีวภาพ ทั้งนี้สังคมต้องตระหนักถึงความรุนแรงของความเสียหายอันอาจเกิดขึ้นได้ และใช้ข้อมูลส่วนบุคคลชีวภาพด้วยความระมัดระวังอย่างสูงสุด

ปรกติแล้วระบบการรักษาความปลอดภัยทางเทคโนโลยีของผู้ให้บริการทางการเงินอยู่ในระดับที่สูงกว่าองค์กรเอกชนในธุรกิจอื่น เนื่องจากผู้ให้บริการทางการเงินมักตกเป็นเป้าหมายของการโจมตีมากกว่าธุรกิจอื่นทำให้มีความเสี่ยงสูง ความเสียหายที่อาจเกิดขึ้นมักมีความรุนแรงและกระทบทุกภาคส่วน ทำให้ผู้ให้บริการทางการเงินต้องมีการรักษาความปลอดภัยทางเทคโนโลยีสูงกว่าธุรกิจอื่น เมื่อวันที่ 22 กรกฎาคม พ.ศ. 2563 ธนาคารแห่งประเทศไทยได้ออกแนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometric Technology) เพื่อให้ผู้ให้บริการทางการเงินใช้อ้างอิงเป็นมาตรฐานเพื่อให้การบริการที่เกี่ยวข้องกับเทคโนโลยีชีวมิติมีความมั่นคงปลอดภัย โดยแนวปฏิบัตินั้นครอบคลุมหลักการ 6 ด้าน ดังต่อไปนี้ 1) การกำหนดนโยบายและการกำกับดูแลการใช้เทคโนโลยีชีวมิติ 2) การรวบรวมข้อมูลชีวมิติของผู้ใช้บริการอย่างมีคุณภาพ ปลอดภัย 3) การประมวลผลข้อมูลชีวมิติของผู้ใช้บริการอย่างแม่นยำ 4) การรักษาความปลอดภัยข้อมูลของผู้ใช้บริการอย่างเข้มงวดและรัดกุมตามมาตรฐานสากล 5) การคุ้มครองผู้ใช้บริการและให้ความรู้เกี่ยวกับการทำธุรกรรมด้วยเทคโนโลยีชีวมิติอย่างเหมาะสมเพียงพอ และ 6) การควบคุมความเสี่ยงด้านปฏิบัติการและรองรับการให้บริการอย่างต่อเนื่อง ซึ่งหลักการทั้ง 6 ครอบคลุมกระบวนการตั้งแต่ต้นจนจบ ทั้งนี้แนวปฏิบัติดังกล่าวกำหนดให้มีการประเมินการนำข้อมูลชีวภาพมาใช้ในการให้บริการอย่างรอบด้านเสียก่อน ไม่ว่าจะเป็นการประเมินประโยชน์ ความเหมาะสมกับรูปแบบในการให้บริการ ผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล ความเสี่ยงของเทคโนโลยีชีวมิติ และแนวทางในการจัดการความเสี่ยงด้านต่าง ๆ

นอกจากนี้แล้ว ยังกำหนดแนวทางไม่เก็บข้อมูลชีวมิติตั้งต้น[476] โดยให้เก็บเป็นข้อมูลแม่แบบ รวมทั้งต้องทำให้ไม่สามารถแปลงย้อนกลับเป็นข้อมูลชีวมิติตั้งต้นได้อีกด้วย[477]

ทั้งนี้ผู้วิจัยเห็นว่าแนวปฏิบัติของธนาคารแห่งประเทศไทยในการใช้เทคโนโลยีชีวมิตินั้นมีความเหมาะสมที่จะนำมาใช้เป็นแนวปฏิบัติสำหรับองค์กรธุรกิจที่มิใช่การให้บริการทางการเงิน แม้ว่าแนวปฏิบัติในการรักษาความปลอดภัยสำหรับองค์กรที่ให้บริการทางการเงินจะเข้มงวดรัดกุมกว่าองค์กรในภาคธุรกิจอื่น แต่ข้อมูลส่วนบุคคลประเภทชีวภาพนั้นมีความสำคัญและหากมีการรั่วไหลหรือถูกนำไปใช้ในทางไม่เหมาะสม อาจสร้างความเสียหายให้กับเจ้าของข้อมูลส่วนบุคคลได้อย่างมหาศาล

2.4 การร้องเรียน

ด้วยลักษณะพิเศษของข้อมูลส่วนบุคคลประเภทชีวภาพ ทำให้ความเสียหายที่อาจเกิดขึ้นจากการละเมิด หรือการรั่วไหลของข้อมูลส่วนบุคคลประเภทชีวภาพนั้นไม่อาจระงับได้ ดังนั้นจึงไม่สามารถประเมินความเสียหายอันอาจเกิดขึ้นได้ ผู้วิจัยจึงเสนอแนะว่าในการยื่นคำร้องต่อหน่วยงานกำกับดูแล หรือฟ้องคดีต่อศาลนั้นเจ้าของข้อมูลส่วนบุคคลเพียงสูญเสียการควบคุมข้อมูลส่วนบุคคล หรือถูกละเมิดสิทธิตามกฎหมายก็เพียงพอที่จะยื่นคำร้องได้แล้ว มิจำเป็นต้องได้รับความเสียหายด้านการเงิน หรือความเดือดร้อนอันสามารถกำหนดมูลค่าได้ ทั้งนี้เป็นไปตามแนวทางที่ศาลอุทธรณ์ในสหราชอาณาจักรได้พิพากษาไว้ในคดี Lloyd v Google และศาลฎีกาในรัฐอิลลินอยส์ได้พิพากษาไว้ในคดี Rosenbach v. Six Flags ว่าความเสียหาย หรือเดือดร้อนนั้น ไม่จำเป็นต้องเป็นความเสียหายทางด้านการเงิน หรือความเดือดร้อนอันสามารถกำหนดมูลค่าได้ เพียงสูญเสียการควบคุมข้อมูลส่วนบุคคล หรือถูกละเมิดสิทธิตามกฎหมายก็สามารถถือได้ว่าเจ้าของข้อมูลส่วนบุคคลได้รับความเสียหายที่ต้องได้รับการเยียวยาแล้ว

2.5 บทลงโทษ

เนื่องจากการรั่วไหลของข้อมูลส่วนบุคคลประเภทชีวภาพอาจทำให้เจ้าของข้อมูลส่วนบุคคลได้รับความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอายดังนั้นผู้วิจัยจึงเห็นสมควรที่จะคงโทษทางอาญาไว้ทั้งนี้เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลใช้ความระมัดระวัง เพื่อป้องกันมิให้เกิดการกระทำผิดตามทฤษฎีของการลงโทษเพื่อข่มขู่ยับยั้ง

สำหรับโทษทางปกครอง ผู้วิจัยเสนอว่าให้คงไว้เนื่องจากโทษทางปกครองเป็นการปรับสำหรับการกระทำความผิดที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติของกฎหมายหรือคำสั่งของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เช่น ไม่แจ้งวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบ ไม่เก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งไว้กับเจ้าของข้อมูลส่วนบุคคล ไม่แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เป็น

---

[476] ข้อมูลชีวมิติตั้งต้น (Biometric Sample) หมายถึง ข้อมูลชีวมิติที่เกิดจากการรวบรวมอัตลักษณ์ของบุคคลและแปลงให้อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์ โดยข้อมูลดังกล่าวยังไม่ถูกประมวลให้เป็นเทมเพลตชีวมิติ ตัวอย่างเช่น ภาพใบหน้าที่ถูกถ่ายเพื่อนำไปใช้กับเทคโนโลยีการเปรียบเทียบใบหน้า

[477] ธนาคารแห่งประเทศไทย. แนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในการให้บริการทางการเงิน, (2563).สืบค้นจาก https://www.bot.or.th/Thai/FIPCS/Documents/FOG/2563/ThaiPDF/25630177.pdf.

ต้น แต่ให้ปรับอัตราโทษเป็นต่อรายเช่นเดียวกันกับบทลงโทษของรัฐอิลลินอยส์ สหรัฐอเมริกา ทั้งนี้เพื่อเป็นการป้องปรามมิให้มีการละเมิดและให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้ความระมัดระวังและมาตรการในการรักษาความปลอดภัยที่เหมาะสม นอกจากนี้ยังทำให้อัตราบทลงโทษนั้นได้สัดส่วนกับจำนวนข้อมูลส่วนบุคคลชีวภาพที่ได้รับผลกระทบอีกด้วย

อนึ่ง ผู้วิจัยเสนอให้คงบทลงโทษทางแพ่งไว้ อย่างไรก็ดี เนื่องจากการละเมิดข้อมูลส่วนบุคคลประเภทชีวภาพนั้นไม่สามารถรอให้เกิดความเสียหายที่มีมูลค่าแล้วจึงทำการฟ้องคดี ทำให้อาจไม่สามารถประเมินความเสียหายเป็นจำนวนเงินได้ แต่จากแนวทางการพิพากษาของศาลฎีกาของรัฐอิลลินอยส์พิพากษาในคดีของ Rosenbach v. Six Flags ว่าแม้ว่าความเดือดร้อนเพียงอย่างเดียวที่ได้รับคือการถูกละเมิดสิทธิตามกฎหมายบุคคลธรรมดาก็สามารถฟ้องคดีได้ และคำพิพากษาของศาลอุทธรณ์อังกฤษในคดี Lloyd v. Google ที่พิพากษาว่าการสูญเสียการควบคุมข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลนั้นเป็นถือเป็นความเสียหายซึ่งต้องได้รับการเยียวยา ดังนั้นความเสียหายจากการละเมิดการประมวลผลข้อมูลส่วนบุคคลแม้ยังไม่เกิดความเสียหายที่สามารถจับต้องได้ก็ถือว่าเป็นความเสียหายที่เกิดขึ้นจริงแล้ว ซึ่งค่าเสียหายให้เป็นไปตามดุลพินิจของศาล

บรรณานุกรม

บรรณานุกรม

จันทจิรา เอี่ยมมยุรา. (2547). การคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย. *วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 34*(4), 627-652.

ชุลีพร น่วมทนง. (2557). *หลักสิทธิมนุษยชน : สิทธิมนุษยชนกับการคุ้มครองข้อมูลส่วนบุคคล.* (หลักสูตรนิติธรรมเพื่อประชาธิปไตย รุ่นที่ 2), วิทยาลัยรัฐธรรมนูญ สถาบันรัฐธรรมนูญศึกษา สำนักงานศาลรัฐธรรมนูญ.

ซิตี้ ยกระดับการเงิน ใช้นวัตกรรม "Voice Biometrics" ยืนยันตัวตนด้วย "เสียงพูด". (2559, 10 พฤศจิกายน 2559). *สยามรัฐออนไลน์*. สืบค้นจาก https://siamrath.co.th/n/5050

ธนาคารแห่งประเทศไทย. *แนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในการให้บริการทางการเงิน*, (2563). สืบค้นจาก https://www.bot.or.th/Thai/FIPCS/Documents/FOG/2563/ThaiPDF/25630177.pdf

นคร เสรีรักษ์, ณรงค์ ใจหาญ, ประสิทธิ์ ปิวาวัฒนพานิช, ศุภเกียรติ ศุภศักดิ์ศึกษากร, & นิชานันท์ นันทศิริศรณ์. (2563). *General Data Protection Regulation ฉบับภาษาไทย*. กรุงเทพฯ: P.Press.

นัยนา มาแสง. (2551). เทคโนโลยีไบโอเมตริก. *วารสารวิชาการ มหาวิทยาลัยธนบุรี*. 2551;2(1):1-4.

ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พุทธศักราช 2563. (2563, 17 กรกฎาคม). *ราชกิจจานุเบกษา.* เล่ม 137 ตอนพิเศษ 164 ง. หน้า 12-13.

ประกาศธนาคารแห่งประเทศไทย เรื่อง หลักเกณฑ์การรู้จักลูกค้า (Know Your Customer: KYC) สำหรับการเปิดบัญชีเงินฝากของสถาบันการเงิน พุทธศักราช 2562. (2562, 2 กันยายน). *ราชกิจจานุเบกษา.* เล่ม 136 ตอนพิเศษ 219 ง. หน้า 8-16.

พระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายวิธีพิจารณาความแพ่ง (ฉบับที่ 26) พุทธศักราช 2558. (2558, 8 เมษายน). ราชกิจจานุเบกษา. เล่ม 132 ตอนที่ 28 ก. หน้า 1-18.

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562. (2562, 27 พฤษภาคม). *ราชกิจจานุเบกษา*. เล่ม 136 ตอนที่ 69 ก. หน้า 52-95.

วาทิณี คำดี. (2561). *ปัญหากฎหมายเกี่ยวกับการดำเนินคดีเพื่อเรียกร้องค่าเสียหายกรณีร่วมกันกำหนดราคาอันเป็นการผูกขาดหรือลดการแข่งขันหรือจำกัดการแข่งขัน.* (นิติศาสตรมหาบัณฑิต กลุ่มวิชากฎหมายธุรกิจ), มหาวิทยาลัยศรีปทุม, กรุงเทพฯ.

ศุภวัชร์ มาลานนท์, & ชิโนภาส อุดมผล. (2562). มาตรฐาน ISO 27001 และกฎหมายคุ้มครองข้อมูลส่วนบุคคล. *ข่าวหุ้นธุรกิจออนไลน์*. สืบค้นจาก https://www.kaohoon.com/content/379182

ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. (2562). *แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล Thailand Data Protection Guidelines 2.0*.

สกู๊ปข่าวหน้า 1 นสพ.มติชนรายวัน 21 กันยายน 2562. (2562). *เทคโนโลยีระบุตัวตน "ชีวมาตร" น่ากลัวหรือไม่*. สืบค้นจาก https://www.matichon.co.th/news-monitor/news_1679649

สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์. (2558). *รายงานฉบับสมบูรณ์ โครงการศึกษาและพัฒนาแนวทางการคุ้มครองข้อมูลส่วนบุคคลภายใต้ประชาคมอาเซียน*.

สราวุธ ปิติยาศักดิ์. (2561). *โครงการวิจัย นโยบายคลาวด์และการคุ้มครองข้อมูลส่วนบุคคลในระบบคลาวด์ระหว่างสหภาพยุโรป สหรัฐอเมริกา ออสเตรเลียและอาเซียน: มุมมองของไทย (รายงานฉบับสมบูรณ์).* สำนักงานสนับสนุนกองทุนการวิจัย (สกว.), กรุงเทพฯ.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2561). *ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์*.

สุขวสา ถมังรักษ์สัตว์. (2562). การคุ้มครองข้อมูลส่วนบุคคลของเด็กบนสื่ออิเล็กทรอนิกส์. *วารสารเกษมบัณฑิต, 20*(1), 131-145.

อธิพร สิทธิธีรรัตน์. (2558). *ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็กทรอนิกส์.* (นิติศาสตร์มหาบัณฑิต), มหาวิทยาลัยธรรมศาสตร์

อนงค์รัตน์ คงลาภ. (2553). *ค่าเสียหายเชิงลงโทษความท้าทายใหม่ในระบบกฎหมายของประเทศไทย*. สืบค้นจาก https://oia.coj.go.th/th/content/category/detail/id/8/cid/129/iid/120294

'เอสซีบี'ยืนยันตัวตนลูกค้าสายคอลเซนเตอร์ด้วยเสียง. (2561). เดลินิวส์. สืบค้นจาก https://www.dailynews.co.th/economic/636183

"SCB EASY" เดินหน้าพัฒนาเทคโนโลยีเจาะกลุ่มลูกค้าใหม่ เปิดตัว "EASY E-KYC" ธนาคารแรกที่ให้บริการเปิดบัญชีลูกค้าใหม่โดยไม่ต้องมาธนาคาร 2561. สืบค้นจาก https://www.scb.co.th/th/about-us/news/jul-2561/nws-easy-e-kyc.html

740 ILCS 14/ Biometric Information Privacy Act. (2008). IL. United States of America.

755 ILCS 50/Illinois Anatomical Gift Act. (2006). IL. United States of America.

Adams, D. (2019). *Five of the Biggest Data Breach Fines Issued by the ICO*. Retrieved from https://digit.fyi/five-of-the-biggest-data-breach-fines-issued-by-the-ico/

Alcohol's Effects on Eye Health. Retrieved from https://guardionhealth.com/alcohols-effect-eye-health/

Allan, K. (2020). *Why deepfakes could threaten everything from biometrics to democracy.* Retrieved from https://www.itpro.co.uk/security/357591/why-deepfakes-could-threaten-everything-from-biometrics-to-democracy

AP imposes GDPR fine for processing biometric data without a demonstrated authentication or security need. (2020). *Insights*. Retrieved from https://www.osborneclarke.com/insights/ap-imposes-gdpr-fine-processing-biometric-data-without-demonstrated-authentication-security-need/

Bergsman, J. (2016). Biometrics are less secure than passwords -- this is why. *Betanews*. Retrieved from https://betanews.com/2016/08/24/unsafe-biometrics/

Bromba, M. (2006, 23/12/2006). *On the reconstruction of biometric raw data from template data*. Retrieved from https://www.bromba.com/knowhow/temppriv.htm

Cellan-Jones, R. (2019). *British Airways faces record £183m fine for data breach*. Retrieved from https://www.bbc.com/news/business-48905907

Clarke, R. (1997). *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*. In X. Consultancy (Ed.). Retrieved from http://www.rogerclarke.com/DV/Intro.html

CNIL. (2019). *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC*. Retrieved from https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

Coseraru, R. (2017). *Facial Recognition Systems and their Data Protection Risks Under the GDPR*. (Master Thesis), Tilburg University, Retrieved from http://arno.uvt.nl/show.cgi?fid=143731

Covington & Burling LLP. (2019). *Landmark Case Opens the Door to UK Data Protection Consumer Class Actions*. Retrieved from https://www.cov.com/en/news-and-insights/insights/2019/10/landmark-case-opens-the-door-to-uk-data-protection-consumer-class-actions

Data Protection Act 2018, United Kingdom.

Dunham A. (2016). *Dubai buses get safer thanks to facial recognition technology: Timeout Dubai*; 2016. Retrieved from https://www.timeoutdubai.com/aroundtown/news/74054-dubai-buses-get-safer-thanks-to-facial-recognition-technology.

Fadi Aloul, Syed Zahidi, & El-Hajj, W. (2009). *Two Factor Authentication Using Mobile Phones*. Paper presented at the The 7th IEEE/ACS International Conference on Computer Systems and Applications, AICCSA 2009 Rabat, Morocco.

Friedewald, M., Finn, R., & Wright, D. (2013). *Seven Types of Privacy*. Retrieved from https://www.researchgate.net/publication/258892458_Seven_Types_of_Privacy

Fruhlinger, J. (2020). The OPM hack explained: Bad security practices meet China's Captain America. *CSO ASEAN*. Retrieved from https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

Gemalto. (2018). *Data Breaches Compromised 3.3 Billion Records in First Half of 2018*. Retrieved from https://www.gemalto.com/press/Pages/Data-Breaches-Compromised-3-3-Billion-Records-in-First-Half-of-2018.aspx

General Data Protection Regulation (GDPR), The European Union.

Gocheva, V. (2017). *Challenges For The Business When Complying With The General Data Protection Regulation.* (L.L.M.), Tilburg University,

Hall, J. A., & Kimura, D. (1994). Dermatoglyphic Asymmetry and Sexual Orientation in Men. *Behavioral Neuroscience, 108*(6), 1203-1206.

Hallinan, D., Schuetz, P., Friedewald, M., & Hert, P. d. (2012). *Neurodata and Neuroprivacy: Data Protection Outdated?* Retrieved from https://www.researchgate.net/publication/265048889_Neurodata_and_Neuroprivacy_Data_Protection_Outdated

Houser, K. (2019). After Bone Marrow Tranplant, Man's Semen Contains Only Donor's DNA. *Neoscope*, 2019.

Information Commissioner's Office. (2019). *Guide to the General Data Protection Regulation (GDPR)*. In Information Commissioner's Office (Ed.).

Information Commissioner's Office. *An overview of the Data Protection Act 2018*. In. Retrieved from https://ico.org.uk/media/for-organisations/documents/2614158/ico-introduction-to-the-data-protection-bill.pdf

Insler, C. N. (2018). How to ride the litigation rollercoaster driven by the Biometric Information Privacy Act. *Southern Illinois University Law Journal, 43*, 819-826.

International Data Corporation. (2019). *2019 Thales Data Threat Report – Global Edition*. Retrieved from https://www.thalesesecurity.com/2019/data-threat-report

Jian, A. K., Ross, A., & Prabhakar, S. (2004). *An Introduction to Biometric Recognition*. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4-20.

Kent, J. (2005). *Malaysia car thieves steal finger*. Retrieved from http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm

Kindt, E. J. (2009). The Use of Privacy Enhancing Technologies for Biometric Systems Analysed from a Legal Perspective. *Privacy and Identity Management for Life,*

5th IFIP WG 9.2, 9.6/11.4, 11.6, 11.7/ PrimeLife International Summer School (PRIMELIFE), 134-145.

Kindt, E. J. (2013). *Privacy and Data Protection Issues of Biometrics Applications*. New York: Springer.

Latham & Watkins LLP. *GDPR Resource Center - Derogations Tracker*. Retrieved from https://gdpr.lw.com/Home/Derogations

Mai, G., Cao, K., Yuen, P. C., & Jain, A. K. (2018). *On the Reconstruction of Face Images from Deep Face Templates*. Retrieved from https://arxiv.org/pdf/1703.00832.pdf

Marcus Smith, Monique Mann, & Urbas, G. (2018). *Biometrics, Crime and Security*. New York: Routledge.

Marotti, A. (2020). Some Illinois Facebook users could get $300 under massive biometric privacy settlement. *Chicago Tribune*. Retrieved from https://www.chicagotribune.com/business/ct-biz-facebook-biometric-privacy-class-action-settlement-20200514-b53gxxmyhfezzl7hlh32777dlq-story.html

Mayhew, S. (2016). *Fingerprint and Passport Data Leaked in Philippines Voter Database Breach*. Retrieved from https://www.biometricupdate.com/201604/fingerprint-and-passport-data-leaked-in-philippines-voter-database-breach

Moloi S. (2018). *Opening a new bank account as easy as taking a selfie*. iAfrikan. Retrieved from: https://www.iafrikan.com/2018/05/18/open-a-new-bank/

Morrison, S. (2020). *Facebook's sad summer continues with a $650 million settlement*. Retrieved from https://www.vox.com/recode/2020/7/23/21335806/facebook-settlement-illinois-facial-recognition-photo-tagging

Nixon, J. (2010). No anonymity on future web says Google CEO. *Thinq.co.uk*. Retrieved from http://www.thinq.co.uk/2010/8/5/no-anonymity-future-web-says-google-ceo/

Patel v. Facebook Inc. - 290 F. Supp. 3d 948 (N.D. Cal. 2018). *LexisNexis*. Retrieved from https://www.lexisnexis.com/community/casebrief/p/casebrief-patel-v-facebook-inc-2133717695

Personal Data Protection Act 2010 (PDPA), Malaysia.

Personal Data Protection Act 2012 (PDPA), Singapore.

Pester, R. (2020). Patel v. Facebook: Facebook Settles Illinois Biometric Information Privacy Act ("BIPA") Violation Suit. *JOLT Digest*. Retrieved from

https://jolt.law.harvard.edu/digest/patel-v-facebook-facebook-settles-illinois-biometric-information-privacy-act-bipa-violation-suit

Pfitzmann, A. (2008). Biometrics - How to Put to Use and How Not at All? ใน S. Furnell, S. K. Katsikas, & A. Lioy (Eds.), *Trust, Privacy and Security in Digital Business, LNCS* (Vol. 5185, pp. 3-5). Springer-Verlag Berlin Heidelberg: TrustBus 2008.

Pope, C. (2018). Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data. *Journal of Law and Policy, 26*(2), 769-803. Retrieved from https://brooklynworks.brooklaw.edu/jlp/vol26/iss2/7/

Rutkowska J, Interewiczi B, Rydzewski A, Swietek M, Dominiak A, Durlik M, Olszewski WL. Donor DNA is detected in recipient blood for years after kidney transplantation using sensitive forensic medicine methods. *Ann Transplant*. 2007;12(3):12-4.

Scharr, J. (2014). iPhone Hack Fools Touch ID with Hand Photos. *Tom's Guide*. Retrieved from https://www.tomsguide.com/us/iphone-touch-id-hack,news-20066.html

Singer, N., & Isaac, M. (2020). Facebook to Pay $550 Million to Settle Facial Recognition Suit. *The New York Times*. Retrieved from https://www.nytimes.com/2020/01/29/technology/facebook-privacy-lawsuit-earnings.html

Smith, M., Mann, M., & Urbas, G. (2018). *Biometrics, Crime and Security*. New York: Routledge.

Temperton, J. (2016). The Philippines Election Hack is 'Freaking Huge'. *Wired.* Retrieved from https://www.wired.co.uk/article/philippines-data-breach-fingerprint-data

Thakkar D. U.S. States Enact Biometric Information Privacy. *Bayometric*. Retrieved from https://www.bayometric.com/u-s-states-enact-bipa/

The Organization for Economic Cooperation and Development. (2013). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.

The Organization for Economic Cooperation and Development. (2013). *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD/LEGAL/0188.

The Organization for Economic Cooperation and Development. (2013). *The OECD Privacy Framework*, Retrieved from http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Toli, C.-A. (2018). *Secure and Privacy-Preserving Biometric Systems.* (Doctor of Engineering Science (PhD)), Katholieke Universiteit Leuven, Retrieved from https://www.esat.kuleuven.be/cosic/publications/thesis-308.pdf

Vielhauer, C. (2018). *User-Centric Privacy and Security in Biometrics*. United Kingdom: The Institution of Engineering and Technology.

vpnMentor. (2019). *Report: Data Breach in Biometric Security Platform Affecting Millions of Users*. Retrieved from https://www.vpnmentor.com/blog/report-biostar2-leak/

ประวัติผู้วิจัย

ชื่อ	นางสาวแสงระวี วิปุลาคม
ประวัติการศึกษา	Bachelor of Applied Science (Computing), Monash University, Australia. 1986 Master of Science (Computer Science), University of Miami, U.S.A. 1989 ปริญญาโท บริหารธุรกิจสถาบันบัณฑิตบริหารธุรกิจศศินทร์ จุฬาลงกรณ์มหาวิทยาลัย ปีการศึกษา 2540 ปริญญาตรี นิติศาสตรบัณฑิต มหาวิทยาลัยสุโขทัยธรรมาธิราช ปีการศึกษา 2559
สถานที่ทำงาน	ธนาคารไทยพาณิชย์ จำกัด (มหาชน)
ตำแหน่ง	ผู้จัดการโครงการ สารสนเทศ พ.ศ 2560-ปัจจุบัน