# แนวทางการเตรียมความพร้อมและปัญหาทางกฎหมาย ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
# Compliance Guidelines for and Legal Issues under the Personal Data Protection Act B.E. 2562 (2019)

**อนุวัฒน์ งามประเสริฐกุล***

ทนายความหุ้นส่วน หัวหน้าส่วนงานระงับข้อพิพาท หัวหน้าร่วมส่วนงาน Tech-Media-Telecoms

บริษัท บลูเมนทอล ริชเตอร์ แอนด์ สุเมธ จำกัด

**Anuwat Ngamprasertkul**

Partner, Head of Litigation and Dispute Resolution, Co-Head of Tech-Media-Telecoms

Blumenthal Richter & Sumet Co., Ltd.

**พินิติ ชมสวัสดิ์****

ทนายความ ส่วนงานระงับข้อพิพาท และส่วนงาน Tech-Media-Telecoms

บริษัท บลูเมนทอล ริชเตอร์ แอนด์ สุเมธ จำกัด

**Piniti Chomsavas**

Lawyer, Litigation and Dispute Resolution, Tech-Media-Telecoms Departments

Blumenthal Richter & Sumet Co., Ltd.

วันที่รับบทความ ๒๕ กรกฎาคม ๒๕๖๕; วันที่แก้ไขบทความ ๓๐ กรกฎาคม ๒๕๖๕; วันที่ตอบรับบทความ ๕ สิงหาคม ๒๕๖๕

---

* น.บ. (เกียรตินิยม) (มหาวิทยาลัยธรรมศาสตร์), น.บ.ท., น.ม. (กฎหมายเอกชนและธุรกิจ) (จุฬาลงกรณ์มหาวิทยาลัย).

** น.บ. (เกียรตินิยม) (จุฬาลงกรณ์มหาวิทยาลัย).

## บทคัดย่อ

เป็นระยะเวลาประมาณ ๓ ปีที่ทั้งภาครัฐและเอกชนมีโอกาสในการศึกษา ตรวจสอบความพร้อมและปรับตัวเพื่อปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (**“พ.ร.บ. ข้อมูลส่วนบุคคลฯ”**) ตั้งแต่การประกาศใช้ในราชกิจจานุเบกษาเมื่อวันที่ ๒๗ พฤษภาคม ๒๕๖๒ จนถึงวันที่กฎหมายมีผลบังคับใช้อย่างเต็มรูปแบบในวันที่ ๑ มิถุนายน ๒๕๖๕ ที่ผ่านมา แต่เนื่องจาก พ.ร.บ. ข้อมูลส่วนบุคคลฯ เป็นกฎหมายใหม่ที่นำเสนอหลักการกฎหมายที่มุ่งเน้นการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล และควบคุมการเก็บ รวบรวม ประมวลข้อมูล หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่เกี่ยวข้อง ได้แก่ ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งหลักการดังกล่าวมีความแตกต่างกับกฎหมายฉบับอื่น ๆ ของประเทศไทย ด้วยเหตุดังกล่าว การบังคับใช้กฎหมายในช่วงแรกทั้งในส่วนของภาครัฐและภาคเอกชนจึงอาจมีอุปสรรคบางประการ และข้อจำกัดในการดำเนินการตามกฎหมาย ไม่ว่าจะเกิดจากความซับซ้อนของกฎหมาย ความไม่เข้าใจและขาดแนวทางในการเตรียมความพร้อม รวมทั้งการตระหนักรู้ถึงภาระและโทษตามกฎหมายของบุคคลที่เกี่ยวข้อง

จากประสบการณ์ที่ผู้เขียนได้ศึกษาข้อกฎหมายทั้ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ GENERAL DATA PROTECTION REGULATION หรือ GDPR รวมไปถึงแนวทางปฏิบัติตลอดจนแนวทางการตีความและตัดสินของหน่วยงานต่าง ๆ ในสหภาพยุโรป และได้มีโอกาสให้คำแนะนำกับองค์กรต่าง ๆ ในการเตรียมความพร้อมและการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลมาจำนวนหนึ่ง จึงขอนำเอาแนวทางวิธีในการดำเนินการเพื่อเตรียมความพร้อมและดำเนินการให้เป็นไปตามกฎหมาย โดยได้จัดลำดับขั้นตอนในการดำเนินการเพื่อปฏิบัติตาม พ.ร.บ. ข้อมูลส่วนบุคคลฯ เพื่อสร้างความตระหนักรู้และเสริมสร้างความเข้าใจให้กับบุคคลต่าง ๆ ที่เกี่ยวข้อง รวมถึงพิจารณาปัญหาทางกฎหมายที่เกี่ยวข้องเป็นลำดับขั้นตอนดังต่อไปนี้

๑. **การสำรวจข้อมูลภายในองค์กร (Data Discovery)** เพื่อตรวจสอบว่าหน่วยงานมีการเก็บ รวบรวม ประมวลผล หรือเปิดเผย “ข้อมูลส่วนบุคคล” หรือไม่ อย่างไร

รวมทั้งสามารถระบุสถานะและบทบาทของตนได้ว่าหน่วยงานของตนมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลส่วนบุคคลตามที่กฎหมายได้กำหนดนิยามไว้ เพื่อพิจารณาภาระหน้าที่และความรับผิดที่แตกต่างกันตามที่กฎหมายกำหนด

๒. **การจำแนกประเภทข้อมูลส่วนบุคคล (Data Classification)** โดยการแบ่งประเภทของข้อมูลส่วนบุคคลที่มีอยู่ว่าเข้าข่ายเป็นข้อมูลส่วนบุคคลอ่อนไหวตามที่กฎหมายกำหนด หรือมีข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงที่จะก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลได้หรือไม่

๓. **การระบุวัตถุประสงค์ (Purpose Identification)** โดยการประเมินและสอบทานวัตถุประสงค์ในการเก็บรวบรวม ประมวลผล หรือเปิดเผยข้อมูลส่วนบุคคลที่มีอยู่และพยายามลดการจัดเก็บข้อมูลส่วนบุคคลที่ไม่จำเป็น (Data Minimization)

๔. **การกำหนดฐานทางกฎหมาย (Lawful Basis)** โดยพิจารณาว่าในการประมวลผลข้อมูลส่วนบุคคลที่ระบุได้ข้างต้น จำต้องได้ความยินยอมจากเจ้าของข้อมูลส่วนบุคคลหรือมีฐานทางกฎหมายอื่นที่อนุญาตให้สามารถเก็บรวบรวม ประมวลผล หรือเปิดเผยข้อมูลส่วนบุคคลได้โดยไม่ต้องขอความยินยอมหรือไม่

๕. **การประเมินและวิเคราะห์ความเสี่ยง (Gap Analysis)** โดยประเมินว่าองค์กรได้ปฏิบัติหน้าที่ตามที่กฎหมายได้กำหนดไว้อย่างครบถ้วนหรือไม่ รวมทั้งประเมินว่ากิจกรรมที่เกี่ยวข้องกับข้อมูลส่วนบุคคลนั้นมีความเสี่ยงที่จะเกิดผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในระดับใด เพื่อที่จะได้จัดเตรียมแนวทางการป้องกันความเสี่ยงดังกล่าว

๖. **การจัดเตรียมเอกสาร นโยบาย ขั้นตอน และแนวทางที่เกี่ยวข้องเพื่อให้เป็นไปตามกฎหมาย (PDPA Compliance)** โดยจัดเตรียมให้มีรายละเอียดครบถ้วนตามที่กฎหมายกำหนด อาทิ ประกาศแจ้งการประมวลผลข้อมูลส่วนบุคคล แบบขอความยินยอมหรือสัญญากับผู้ประมวลผลข้อมูลส่วนบุคคล รวมถึงแนวทางการปฏิบัติเพื่อลดความเสี่ยง เช่น จัดทำนโยบาย ระเบียบ หรือแนวทางปฏิบัติภายในองค์กร และการจัดอบรมให้แก่พนักงานหรือบุคลากรที่เกี่ยวข้อง

ท้ายนี้ การทำความเข้าใจ พ.ร.บ. ข้อมูลส่วนบุคคลฯ การวิเคราะห์ปัญหาทางกฎหมายที่อาจเกิดขึ้น รวมไปถึงแนวทางการเตรียมความพร้อมในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้นมีความสำคัญและเป็นประโยชน์อย่างยิ่งกับทั้งนักกฎหมายและหน่วยงานที่ต้องบังคับใช้กฎหมายในการพิจารณาตรวจสอบความพร้อมขององค์กรและตัดสินโทษ รวมไปถึงสำหรับผู้ประกอบการซึ่งมีหน้าที่ต้องปฏิบัติตามกฎหมายไม่ว่าจะเป็นในฐานะผู้ควบคุมหรือผู้ประมวลผลข้อมูลส่วนบุคคล และที่สำคัญที่สุดคือประชาชนทั่วไปที่จะได้รับการคุ้มครองสิทธิต่าง ๆ ตามกฎหมายนี้

**คำสำคัญ :** พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล, ข้อมูลส่วนบุคคล, เจ้าของข้อมูลส่วนบุคคล, ผู้ควบคุมข้อมูลส่วนบุคคล, ผู้ประมวลผลข้อมูลส่วนบุคคล

## Abstract

The public and private sectors have had around three years to study, check their readiness and adapt to comply with the Personal Data Protection Act B.E. 2562 (2019) (“Personal Data Act”) from the date of publication in the Government Gazette on 27 May 2019 until the date the law was fully enforced on 1 June 2022. The Personal Data Act is a new law that introduces legal principles aimed at protecting the rights of personal data subjects and controlling the collection, processing or disclosure of personal data by data controllers or data processors. In the early stages of enforcement, there may be obstacles to compliance unless there are guidelines and awareness of the legal burdens and penalties in particular.

From the author’s experience of studying the law, the Personal Data Act and the General Data Protection Regulation, including guidelines for interpretation and judgments of various agencies in the European Union, have provided opportunities for organizations to prepare for and comply with

personal data protection laws. Therefore, the author would like to provide the steps to prepare for compliance with the Personal Data Act to create awareness, enhance understanding and identify related legal issues. The steps are as follows.

1. **Data Discovery** to determine whether the organization collects, processes or discloses “personal information”, and to be able to identify the status and roles of data controllers or data processors as defined under the law to determine different obligations and liabilities as required by the law.

2. **Data Classification** to categorize the types of personal data that exist, including sensitive personal data under the Personal Data Act, and determine whether personal data has a high risk of causing damage to data subjects.

3. **Purpose Identification** to evaluate and review the purposes for the collection, processing or disclosure of personal data, and attempt to reduce the unnecessary storage of personal data (data minimization).

4. **Legal Basis** by obtaining consent to process the personal data of the data subject above, or have other legal bases that allow the collection, processing or disclosure of personal data.

5. **GAP Analysis** by assessing whether the organization has performed its duties in full compliance with the law as well as the extent that activities related to personal data have exposed it and the impact on data subjects in order to determine the proper safeguards.

6. **PDPA Compliance** by preparing the relevant documents, policies, procedures and guidelines for compliance with the law by providing complete documentation and procedures as required by the law such as privacy notice, consent forms, data processing agreements with personal data processors and practice guidelines to reduce risks by establishing policies, regulations or guidelines within the organization and arranging training for employees or related personnel.

Understanding the Personal Data Act, analyzing potential legal issues and establishing guidelines for preparing to comply with personal data protection laws are important and useful to both lawyers and law enforcement agencies in reviewing the readiness of organizations and the award of penalties, including business operators who are obliged to comply with the law either as data controllers or data processors and most importantly all data subjects who are protected under the Personal Data Act.

**Keywords :** personal data protection act, personal data, data subject, data controller, data processor

## บทนำ

ตั้งแต่วันที่ ๑ มิถุนายน ๒๕๖๕ เป็นต้นมา พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (“พ.ร.บ. ข้อมูลส่วนบุคคลฯ”) ได้มีผลบังคับใช้เต็มรูปแบบหลังจากที่มีการประกาศเป็นกฎหมายมาเป็นระยะเวลากว่า ๓ ปี ตั้งแต่การประกาศใช้ในราชกิจจานุเบกษา เมื่อวันที่ ๒๗ พฤษภาคม ๒๕๖๒ และด้วยหลักการของกฎหมายที่แตกต่างไปจากกฎหมายทั่วไป จึงทำให้ พ.ร.บ. ข้อมูลส่วนบุคคลฯ เป็นกฎหมายที่ “ใหม่” ทั้งในมุมมองของประชาชนและบุคคลที่อยู่ในแวดวงของกฎหมาย ซึ่งบางครั้งทำให้เกิดความเข้าใจผิดว่ากฎหมายดังกล่าวจะเข้ามาจำกัดสิทธิเสรีภาพของประชาชนหรือไม่ หรือจะเป็นกฎหมายที่สร้างภาระ

เกินควรให้กับผู้ประกอบการ อย่างไรก็ตาม หากได้พิจารณาถึงเจตนารมณ์ของกฎหมายและบทบัญญัติที่เกี่ยวข้อง พ.ร.บ. ข้อมูลส่วนบุคคลฯ โดยละเอียด จะพบว่ากฎหมายนี้มีวัตถุประสงค์หลักที่ชัดเจนในการให้สิทธิแก่ประชาชนเหนือข้อมูลส่วนบุคคลของตนเองอย่างที่ไม่เคยมีอยู่ภายใต้กฎหมายอื่น รวมทั้งการให้หน่วยงานที่มีอำนาจมีสิทธิเข้ามากำกับตรวจสอบ และดูแลการเก็บ รวบรวม ประมวลผล หรือเปิดเผยข้อมูลส่วนบุคคลให้มีความถูกต้อง โปร่งใส และไม่ก่อให้เกิดความเดือดร้อนหรือสร้างความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล

พ.ร.บ. ข้อมูลส่วนบุคคลฯ นั้นมีต้นร่างมาจากกฎหมายคุ้มครองของข้อมูลส่วนบุคคลที่บังคับใช้อยู่ภายในสหภาพยุโรปชื่อ GENERAL DATA PROTECTION REGULATION หรือ GDPR ซึ่งมีผลบังคับใช้เต็มรูปแบบตั้งแต่วันที่ ๒๕ พฤษภาคม ๒๕๖๑[๑] ซึ่งเป็นกฎหมายที่มีจุดกำเนิดจากวัตถุประสงค์ในการปกป้องสิทธิขั้นพื้นฐาน[๒] เนื่องจากในปัจจุบันนั้นการประกอบธุรกิจของภาคเอกชน หรือแม้แต่การดำเนินงานของรัฐบาลในหลายประเทศมีการใช้ข้อมูลส่วนบุคคลมาเป็นส่วนประกอบสำคัญทั้งในการวิเคราะห์และสนับสนุนการตัดสินใจทางธุรกิจ การแก้ไขพัฒนาผลิตภัณฑ์หรือบริการ หรือการนำเสนอโฆษณาที่ปรับแต่งตามความสนใจของแต่ละบุคคล นั่นทำให้เกิดการจัดเก็บข้อมูลส่วนบุคคลในปริมาณมากและเกิดการซื้อขายแลกเปลี่ยนข้อมูลส่วนบุคคลกันเป็นวงกว้าง โดยที่ปัจเจกบุคคลซึ่งเป็นเจ้าของข้อมูลอาจไม่รู้ตัว รวมถึงมีผู้ที่ไม่หวังดีอาศัยช่องว่างทางกฎหมายและรอยรั่วทางเทคนิคในการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวมาใช้เพื่อวัตถุประสงค์ร้าย

โดยที่บทบัญญัติส่วนใหญ่ของ พ.ร.บ. ข้อมูลส่วนบุคคลฯ จะอ้างอิงมาจาก GDPR ซึ่งตั้งอยู่บนพื้นฐานที่เป็นหลักการสำคัญกล่าวคือข้อมูลส่วนบุคคลจะต้องตั้งอยู่บนพื้นฐานต่อไปนี้

---

[๑] **REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)** [Online], 25 July 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX% 3A02016R0679-20160504&qid=1532348683434.

[๒] Recital 1 Data Protection as a Fundamental Right.

๑. ถูกประมวลผลโดยชอบด้วยกฎหมาย เป็นธรรมและด้วยวิธีการอันโปร่งใสเมื่อสัมพันธ์กับผู้ถูกประมวลผล (“ความชอบด้วยกฎหมาย ความเป็นธรรมและความโปร่งใส” / “Lawfulness, fairness and transparency”)

๒. ถูกรวบรวมเพื่อวัตถุประสงค์ที่เฉพาะ ชัดเจนและชอบธรรมและไม่ถูกประมวลผลนอกเหนือไปจากที่ตกลงไว้แต่ต้น (“การกำหนดขอบเขตของวัตถุประสงค์” / “Purpose Limitation”)

๓. เพียงพอ เกี่ยวเนื่องและอยู่ในขอบเขตที่จำเป็นโดยสัมพันธ์กับวัตถุประสงค์ที่ข้อมูลถูกประมวลผล (“การใช้ข้อมูลให้น้อยที่สุด” / “Data Minimization”)

๔. แม่นยำและเป็นปัจจุบันเสมอหากจำเป็น ขั้นตอนที่จำเป็นทั้งหมดจะต้องถูกปฏิบัติเพื่อรับประกันว่าข้อมูลส่วนบุคคลที่ไม่แม่นยำจะถูกลบหรือแก้ไขโดยไม่ล่าช้า (“ความแม่นยำ” / “Accuracy”)

๕. คำนึงถึงวัตถุประสงค์ที่ข้อมูลถูกประมวลผลถูกเก็บรักษาในรูปแบบที่อนุญาตให้การระบุตัวตนของผู้ถูกประมวลผลข้อมูลไม่เป็นไปนานกว่าที่จำเป็นสำหรับวัตถุประสงค์ที่ข้อมูลส่วนบุคคลถูกประมวลผล (“การกำหนดขอบเขตการเก็บรักษา” / “Storage limitation”)

๖. ถูกประมวลผลด้วยวิธีการที่รับประกันความปลอดภัยของข้อมูลส่วนบุคคลตามสมควรอันรวมถึงการคุ้มครองจากการประมวลผลที่ไม่ได้รับอนุญาตหรือไม่ชอบด้วยกฎหมายและจากการสูญเสีย การถูกทำลายหรือความเสียหายโดยอุบัติเหตุ โดยใช้มาตรการทางเทคนิคหรือการจัดการองค์กรตามสมควร (“ความสมบูรณ์และเป็นความลับ” / “Integrity and confidentiality”)

๗. ผู้ควบคุมควรเป็นผู้รับผิดชอบต่อหลักการข้างต้นและสามารถแสดงว่าปฏิบัติตามได้ (“การถูกตรวจสอบได้” / “Accountability”)

กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลจึงเข้ามามีบทบาทสำคัญทั้งในด้านการคุ้มครองสิทธิของเจ้าของข้อมูล เพื่อให้เจ้าของข้อมูลมีสิทธิในการควบคุมและตรวจสอบการใช้ข้อมูลส่วนบุคคล รวมทั้งกำกับดูแลการใช้งานข้อมูลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลให้โปร่งใส และมีมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลที่ดีเพื่อป้องกันการรั่วไหล และการใช้ข้อมูลส่วนบุคคลโดยมิชอบ เนื่องจากปริมาณการใช้ข้อมูลส่วนบุคคลในปัจจุบัน โดยเฉพาะการวิเคราะห์ข้อมูลจำนวนมาก (Big Data Analytics) และการศึกษาข้อมูล (Data profiling) อาจก่อให้เกิดการละเมิด หรือรั่วไหลของข้อมูลส่วนบุคคลในแต่ละครั้งโดยเฉพาะในทางอิเล็กทรอนิกส์ย่อมมีผู้ได้รับผลกระทบเป็นวงกว้าง และโดยทั่วไปแล้วการรั่วไหลของข้อมูลนั้นมักไม่สามารถแก้ไขหรือทำให้ย้อนกลับได้ อีกทั้งทำให้เกิดความเสียหายร้ายแรงต่อเจ้าของข้อมูลส่วนบุคคล ทั้งในด้านที่อาจมีมูลค่าเป็นตัวเงิน อาทิ การรั่วไหลของข้อมูลเกี่ยวกับบัตรเครดิต หรือการหลอกลวงของมิจฉาชีพโดยอาศัยหมายเลขโทรศัพท์ หรืออาจส่งผลเสียต่อชื่อเสียงหรือการถูกเลือกปฏิบัติทางสังคมหากเกิดการรั่วไหลของข้อมูลส่วนบุคคลที่อ่อนไหวอีกด้วย

แต่ในทางกลับกันการรักษาสมดุลระหว่างการคุ้มครองสิทธิของเจ้าของข้อมูลกับมาตรการเชิงป้องกันและป้องปรามเพื่อมิให้เกิดเหตุทุจริต เช่น ในการที่หน่วยงานจะนำเอาข้อมูลส่วนบุคคลของพนักงาน หรือคู่ค้ามาใช้เพื่อตรวจสอบและวางนโยบายในการป้องกันปราบปราม ดำเนินคดี หรือควบคุมผลของเหตุทุจริตโดยนำเอาข้อมูลส่วนบุคคลมาวิเคราะห์ก็ยังสามารถทำได้ เพียงแต่ต้องกระทำโดยพิจารณาอย่างถี่ถ้วนเพื่อมิให้เกิดกรณีที่ผู้กระทำความผิดจะยกเอากฎหมายคุ้มครองข้อมูลส่วนบุคคลเพื่อฟ้องร้อง หรือดำเนินคดีโต้กลับบุคคลที่ฟ้องคดี[๓] รวมไปถึงความจำเป็นในการวิเคราะห์ข้อมูลส่วนบุคคลจะเป็นสิ่งสำคัญในการทำธุรกิจต่อไป ตามที่มีคนนิยามว่า “Data is the new Oil” หรือยุคที่ข้อมูลกลายเป็นสินทรัพย์ที่มีมูลค่ามหาศาล เปรียบเสมือนน้ำมันที่มีมูลค่ามากในอดีต บริษัทใดมีข้อมูลจำนวนมากยิ่งมีศักยภาพในการแข่งขันที่สูง

---

[๓] อนุวัฒน์ งามประเสริฐกุล, **อาชญากรรมคอปกขาว** : แนวทางการป้องกันและดำเนินคดีภายใต้ข้อจำกัดตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล, วารสารกฎหมาย นิติพัฒน์ นิด้า ปีที่ ๙ ฉบับที่ ๒ (กรกฎาคม - ธันวาคม) ๒๕๖๓.

บทความนี้จึงมีวัตถุประสงค์ในการสร้างความรู้ความเข้าใจในการตีความและบังคับใช้กฎหมายเพื่อที่จะได้วิเคราะห์ปัญหาทางกฎหมายที่มีให้ตรงตามเจตนารมณ์ของกฎหมายข้างต้นมากที่สุด รวมไปถึงการวางแนวทางในการเตรียมความพร้อม แนวทางการตรวจสอบและพิจารณาข้อพิพาทให้กับบุคคลและหน่วยงานต่าง ๆ ที่เกี่ยวข้อง โดยในบทความนี้ได้แบ่งการอธิบายในประเด็นที่สำคัญต่าง ๆ โดยผู้เขียนขอนำเสนอประเด็นที่สำคัญดังกล่าวในรูปแบบขั้นตอนการดำเนินการในการเตรียมความพร้อมให้เป็นไปตามกฎหมายซึ่งผู้เขียนได้นำมาปรับใช้ให้กับหลาย ๆ องค์กร โดยประกอบไปด้วยขั้นตอนต่าง ๆ ดังนี้

**แผนภาพที่ ๑ สรุปขั้นตอนการดำเนินการให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล**


**ขั้นตอนที่ ๑ การสำรวจข้อมูลส่วนบุคคลที่จัดเก็บและประมวลผล (Data Discovery)**

ขั้นตอนแรกคือการสร้างความรู้ ความเข้าใจ รวมทั้งเสริมการตระหนักรู้ เพื่อให้ทุกคนภายในองค์กรเห็นภาพกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นแบบเดียวกัน โดยมีนิยามและสถานะของบุคคลที่เกี่ยวข้อง ดังนี้

**นิยาม “ข้อมูลส่วนบุคคล”**

ความหมายและประเภทของ “ข้อมูลส่วนบุคคล” ที่จะได้รับความคุ้มครองตามกฎหมายนี้ โดยมาตรา ๖ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ ได้กำหนดนิยามของข้อมูลส่วนบุคคลไว้ว่า *“ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ”*

จากนิยามดังกล่าวจึงอาจกล่าวได้ว่า ข้อมูลส่วนบุคคลนั้น คือข้อมูลใด ๆ ที่เกี่ยวข้องหรือสามารถสื่อหรือเชื่อมโยงถึงบุคคลธรรมดาคนใดคนหนึ่ง โดยเฉพาะอย่างยิ่งด้วยการ

อ้างอิงจากสิ่งระบุอัตลักษณ์เป็นการเฉพาะ ด้วยเหตุนี้ ข้อมูลส่วนบุคคลจึงอาจแบ่งออกได้เป็น ๒ ประเภท ได้แก่

๑. ข้อมูลส่วนบุคคลที่สามารถระบุตัวของบุคคลได้โดยตรง กล่าวคือ เป็นข้อมูลที่สามารถสื่อถึงบุคคลใดบุคคลหนึ่งได้ในตัวเอง โดยไม่ต้องอาศัยข้อมูลอื่น ๆ ประกอบ เช่น ชื่อและนามสกุล หมายเลขบัตรประจำตัวประชาชน เป็นต้น

๒. ข้อมูลส่วนบุคคลที่สามารถระบุตัวของบุคคลได้โดยอ้อม กล่าวคือ เป็นข้อมูลซึ่งแม้ไม่สามารถระบุตัวบุคคลได้โดยตัวเอง แต่เมื่อประกอบกันเป็นชุดของข้อมูลแล้วสามารถใช้ระบุตัวบุคคลได้ ยกตัวอย่างเช่น ชื่อ หรือนามสกุลเพียงอย่างเดียว ที่อยู่ หมายเลขโทรศัพท์ วันเดือนปีเกิด อายุ เพศ เป็นต้น

นอกจากนี้ เมื่อพิจารณาถึงนิยามดังกล่าวจะพบว่า กฎหมายไม่ได้กำหนดเงื่อนไขของความเป็นข้อมูลส่วนบุคคลเกี่ยวข้องกับความเป็นความลับ การเปิดเผย หรือหน่วยงานที่เก็บข้อมูลดังกล่าว จึงกล่าวได้ว่าสถานะตามกฎหมายความเป็นข้อมูลส่วนบุคคลจะไม่เปลี่ยนแปลงไปแม้ว่าอาจมีการเปิดเผยข้อมูลดังกล่าวต่อสาธารณะ มีการเปิดเผยโดยเจ้าของข้อมูล หรือเป็นข้อมูลที่จัดเก็บโดยงานรัฐก็ตามตราบใดที่ข้อมูลดังกล่าวยังสามารถระบุตัวตนของบุคคลได้อยู่ ในทางกลับกันสิ่งที่จะทำให้สิ้นสภาพการเป็นข้อมูลส่วนบุคคล คือ การทำให้ข้อมูลนั้นไม่สามารถระบุตัวตนของบุคคลได้โดยถาวร ได้แก่ การลบทำลายข้อมูล หรือการจัดทำให้ข้อมูลส่วนบุคคลกลายเป็นข้อมูลนิรนาม (“Anonymization”) เท่านั้น

**สถานะความเป็น “เจ้าของข้อมูลส่วนบุคคล”**

แม้กฎหมายจะได้กำหนดนิยามของ “ข้อมูลส่วนบุคคล” ดังที่กล่าวไว้ข้างต้น แต่ไม่ได้มีการนิยามความหมายของ “เจ้าของข้อมูลส่วนบุคคล” ไว้โดยเฉพาะ จึงต้องตีความตามเจตนารมณ์ของกฎหมาย ประกอบกับนิยามของข้อมูลส่วนบุคคลที่กล่าวถึงก่อนหน้านี้ โดยเมื่อพิจารณาให้ลึกลงไปถึงลักษณะทางกายภาพ และความหมายของ “ข้อมูล” นั้น มีการให้นิยามไว้หลากหลาย อาทิ

- ข้อมูล หมายถึง ข้อเท็จจริงต่าง ๆ ซึ่งอาจแสดงเป็นตัวเลข ตัวหนังสือ หรือสัญลักษณ์[๔]

- ข้อมูล ได้แก่ ชื่อลูกค้า ตัวเลขเกี่ยวกับจำนวนชั่วโมงในการทำงานในแต่ละสัปดาห์ ตัวเลขเกี่ยวกับสินค้า[๕]

- ข้อมูล คือ คำอธิบายพื้นฐานเกี่ยวกับสิ่งของ เหตุการณ์ กิจกรรม และธุรกรรม ซึ่งได้รับการบันทึก จำแนกและจัดเก็บไว้[๖]

- ข้อมูลข่าวสาร หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริง ข้อมูล หรือสิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาดภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้[๗]

จากนิยามตามกฎหมายและลักษณะทางกายภาพของ “ข้อมูลส่วนบุคคล” จึงอาจสรุปได้ว่าความสัมพันธ์ระหว่างเจ้าของข้อมูลส่วนบุคคลและตัวข้อมูลส่วนบุคคลนั้น จึงไม่ใช่ลักษณะความเป็น “เจ้าของ” ตามความหมายทั่วไปในเชิงของกรรมสิทธิ์ หรือทรัพย์สินทางปัญญา แต่เจ้าของข้อมูลส่วนบุคคลนั้น หมายถึง บุคคลที่ถูกระบุตัวตนได้จากข้อมูลส่วนบุคคลนั่นเอง

---

[๔] สำนักงานทดสอบ, กรมวิชาการ, กระทรวงศึกษาธิการ, **แนวทางการจัดทำระบบสารสนเทศสถานศึกษา** (กรุงเทพฯ : โรงพิมพ์คุรุสภาลาดพร้าว, ๒๕๔๕), ๑๙.

[๕] Ralph M. Stair and George Reynold, **Fundamentals of information systems** (Cambridge, MA: Course Technology, 2001), 4.

[๖] Efraim Turban, Ephraim Mclean and James Wetherbe, **Information technology for management transforming business in the digital economy,** 3rd ed. (Toronto: John Wiley & Sons, 2001) 48.

[๗] มาตรา ๔ แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐.

ในประเด็นด้านกรรมสิทธิ์นั้น โดยสภาพของ “ข้อเท็จจริง” จึงไม่อาจถือเป็นทรัพย์หรือทรัพย์สินภายใต้ประมวลกฎหมายแพ่งและพาณิชย์ได้[๘] สิ่งที่อาจถือเป็นทรัพย์หรือทรัพย์สินได้เป็นเพียงแค่วัตถุหรือสื่อที่ใช้ในการบักทึกข้อมูลส่วนบุคคลเท่านั้น อาทิ บัตรประจำตัวประชาชน ทะเบียนบ้าน หรือการบันทึกในรูปแบบอิเล็กทรอนิกส์ เป็นต้น ซึ่งอาจส่งผลให้อาจมีบุคคลอื่นที่มีความเป็น “เจ้าของ” สื่อดังกล่าวนอกเหนือไปจากผู้เป็นเจ้าของข้อมูลส่วนบุคคล แต่รูปแบบในการจัดเก็บหรือบันทึกข้อมูลส่วนบุคคล หรือความเป็นเจ้าของกรรมสิทธิ์ในสื่อที่บันทึกข้อมูลส่วนบุคคลดังกล่าวไม่ได้ส่งผลต่อความเป็นเจ้าของข้อมูลส่วนบุคคลภายใต้กฎหมายข้อมูลส่วนบุคคลแต่อย่างใด และบุคคลที่สามารถถูกระบุตัวได้จากข้อมูลดังกล่าวยังคงมีฐานะเป็นเจ้าของข้อมูลส่วนบุคคลภายใต้กฎหมาย แม้ว่ารูปแบบการจัดเก็บข้อมูลจะได้เปลี่ยนแปลงหรือถูกทำลาย ยกตัวอย่างเช่น บุคคลได้ส่งมอบเอกสารเกี่ยวกับข้อมูลส่วนบุคคลของตนให้กับบริษัทแห่งหนึ่งเพื่อประกอบการสมัครงาน แม้บริษัทจะได้ไปซึ่งกรรมสิทธิ์ในเอกสารดังกล่าว โดยอาจนำไปใช้งานเพื่อประกอบการพิจารณาคุณสมบัติ นำไปแปลงเป็นข้อมูลทางอิเล็กทรอนิกส์เพื่อส่งต่อให้บุคคลที่เกี่ยวข้อง หรือทำลายทิ้งเมื่อใช้งานเสร็จแล้ว แต่บุคคลผู้สมัครงานนั้นยังคงมีฐานะเป็นเจ้าของข้อมูลส่วนบุคคลเหนือข้อมูลที่ปรากฏอยู่ในเอกสารดังกล่าว และสิทธิเรียกร้องต่อบริษัทภายใต้ พ.ร.บ. ข้อมูลส่วนบุคคลฯ หรือในกรณีที่บุคคลทำบัตรประจำตัวประชาชนสูญหายก็ไม่ได้ทำให้บุคคลนั้นสูญเสียชื่อหรือข้อมูลส่วนบุคคลที่ปรากฏในบัตรประชาชนแต่อย่างใด

หรือในอีกกรณีหนึ่ง การได้มาซึ่งข้อมูลส่วนบุคคลของบุคคลอื่นไม่จำเป็นต้องมีการส่งมอบสื่อจากเจ้าของข้อมูล ตามนัยของการส่งมอบทรัพย์ หรือทรัพย์สินตามกฎหมายแพ่ง เช่น การสัมภาษณ์บุคคลพร้อมจดบันทึกข้อมูลโดยผู้สัมภาษณ์ หรือการรวบรวมข้อมูลจากการสังเกตของผู้เก็บข้อมูลเอง

---

[๘] มาตรา ๑๓๗ ทรัพย์ หมายความว่า วัตถุมีรูปร่าง
มาตรา ๑๓๘ ทรัพย์สิน หมายความรวมทั้งทรัพย์และวัตถุไม่มีรูปร่าง ซึ่งอาจมีราคาและอาจถือเอาได้.

ในอีกแง่มุมหนึ่งข้อมูลส่วนบุคคลอาจเข้าไปเป็นส่วนหนึ่งของงานสร้างสรรค์อันมีลิขสิทธิ์ หรืออาจได้รับการคุ้มครองในฐานะทรัพย์สินทางปัญญารูปแบบหนึ่งได้ แต่สิทธิดังกล่าวไม่ได้มีเหนือกว่าสิทธิของเจ้าของข้อมูลส่วนบุคคลตาม พ.ร.บ. ข้อมูลส่วนบุคคลฯ ยกตัวอย่างเช่น ในการถ่ายภาพ หรือภาพเคลื่อนไหวซึ่งปรากฏภาพของบุคคลอื่น ซึ่งอาจเป็นงานอันมีลิขสิทธิ์ของผู้สร้างสรรค์[๙] และก่อสิทธิในการเผยแพร่ ทำซ้ำ หรือหาประโยชน์จากงานดังกล่าวได้ตามกฎหมายเกี่ยวกับทรัพย์สินทางปัญญา แต่การกระทำดังกล่าวอาจไม่ชอบด้วย พ.ร.บ. ข้อมูลส่วนบุคคลฯ ได้หากไม่ได้รับความยินยอมจากบุคคลในภาพ หรือไม่มีฐานทางกฎหมายรองรับการบันทึกภาพดังกล่าว

ดังนั้น พิจารณาถึงสถานะและสิทธิของเจ้าของข้อมูลส่วนบุคคลภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้น ต้องแยกประเด็นในการพิจารณาถึงสถานะความเป็นเจ้าของกรรมสิทธิ์เหนือทรัพย์ ทรัพย์สิน หรือทรัพย์สินทางปัญญา รวมถึงวิธีการได้มาซึ่งสื่อดังกล่าวว่าชอบด้วยกฎหมายที่เกี่ยวข้องกับทรัพย์หรือทรัพย์สินนั้น ๆ หรือไม่

**สถานะความเป็น “ผู้ควบคุมข้อมูลส่วนบุคคล”**

ตามมาตรา ๖ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ “ผู้ควบคุมข้อมูลส่วนบุคคล หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล”

จากนิยามข้างต้นความเป็นผู้ควบคุมข้อมูลส่วนบุคคลนั้นจึงพิจารณาจาก “อำนาจหน้าที่ตัดสินใจ” เกี่ยวกับการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล โดยไม่ได้พิจารณาความเป็นเจ้าของหรือการครอบครองในสื่อหรือวัตถุที่บันทึกข้อมูลส่วนบุคคล และในบางกรณีผู้ควบคุมข้อมูลส่วนบุคคลอาจไม่ได้ครอบครองหรือดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล

---

[๙] มาตรา ๔ แห่ง พ.ร.บ. ลิขสิทธิ์ พ.ศ. ๒๕๓๗

“ผู้สร้างสรรค์” หมายความว่า ผู้ทำหรือผู้ก่อให้เกิดงานสร้างสรรค์อย่างใดอย่างหนึ่งที่เป็นงานอันมีลิขสิทธิ์ตามพระราชบัญญัตินี้

“ลิขสิทธิ์” หมายความว่า สิทธิแต่ผู้เดียวที่จะทำการใด ๆ ตามพระราชบัญญัตินี้เกี่ยวกับงานที่ผู้สร้างสรรค์ได้ทำขึ้น.

ด้วยตนเองเลยก็ได้ โดยเฉพาะในกรณีที่การมอบหมายให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลแทน (โดยจะได้กล่าวโดยละเอียดต่อไป)

**สถานะความเป็น "ผู้ประมวลผลข้อมูลส่วนบุคคล"**

บุคคลอีกประเภทหนึ่งซึ่งมีความเกี่ยวข้องกับผู้ควบคุมข้อมูลส่วนบุคคลคือ "ผู้ประมวลผลข้อมูลส่วนบุคคล" ซึ่งกฎหมายให้นิยามไว้ว่า "บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล"

โดยทั่วไปนั้นผู้ประมวลผลข้อมูลส่วนบุคคลจึงพิจารณาจาก "การทำตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล" โดยการดำเนินการนั้นอาจเป็นเพียงกิจกรรมใดกิจกรรมหนึ่งที่ผู้ควบคุมข้อมูลส่วนบุคคลมอบหมาย เช่น การเก็บรวบรวมข้อมูลและส่งมอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล การประมวลผลข้อมูล หรือการจัดเก็บข้อมูล หรืออาจเป็นกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการทั้งหมดเลยก็ได้ เช่น การทำหน้าที่คำนวณและจ่ายเงินเดือนแทนบริษัทนายจ้าง หรือการรับมอบหมายให้รวบรวมข้อมูลส่วนบุคคลของผู้สนใจผลิตภัณฑ์ เป็นต้น

อย่างไรก็ตาม สถานะความเป็นผู้ประมวลผลข้อมูลส่วนบุคคลนั้นอาจเปลี่ยนแปลงไปได้ หากมีการประมวลผลข้อมูลส่วนบุคคลที่เกินขอบเขตของคำสั่งตามที่ได้รับมอบหมาย โดยเป็นตามบทบัญญัติมาตรา ๔๐ ความว่า

"มาตรา ๔๐ ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ดังต่อไปนี้

(๑) ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล**ตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น** เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้

.....

ผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งไม่ปฏิบัติตาม (๑) สำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลใด **ให้ถือว่าผู้ประมวลผลข้อมูลส่วนบุคคลเป็นผู้ควบคุมข้อมูลส่วนบุคคลสำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น**"

จากบทบัญญัติดังกล่าวจึงเห็นได้ว่า สถานะความเป็นผู้ประมวลผลข้อมูลส่วนบุคคลอาจมีสถานะเปลี่ยนแปลงไปได้ตามกิจกรรมและวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล โดยบุคคลซึ่งได้รับมอบหมายให้ปฏิบัติหน้าที่เป็นผู้ประมวลผลข้อมูลส่วนบุคคลนั้น อาจต้องมีความรับผิดเพิ่มเติมในฐานะผู้ควบคุมข้อมูลส่วนบุคคลสำหรับในกิจกรรมที่ได้ประมวลผลข้อมูลส่วนบุคคลเกินกว่าขอบเขตของคำสั่งที่ได้ตกลงไว้กับผู้ควบคุมข้อมูลส่วนบุคคลที่มอบหมาย ยกตัวอย่างเช่น

บริษัทจำหน่ายรถยนต์ได้จัดเก็บข้อมูลส่วนบุคคลของลูกค้าที่ซื้อรถ และส่งข้อมูลส่วนบุคลดังกล่าวพร้อมมอบหมายให้บริษัทที่ปรึกษาทางธุรกิจนำไปจัดเก็บ และวิเคราะห์ข้อมูลการตลาดตามคำสั่งของตน ซึ่งส่งผลให้บริษัทที่ปรึกษาเป็นผู้ประมวลผลข้อมูลส่วนบุคคลจากการประมวลผลข้อมูลตามคำสั่งของบริษัทจำหน่ายรถยนต์ อย่างไรก็ตาม หากมีข้อเท็จจริงว่าบริษัทที่ปรึกษาได้นำข้อมูลดังกล่าวไปวิเคราะห์รวมกับข้อมูลอื่น ๆ เพื่อประโยชน์ของตนเอง ซึ่งเป็นการกระทำที่นอกเหนือคำสั่ง กรณีดังกล่าวบริษัทที่ปรึกษาจึงมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลสำหรับการประมวลผลข้อมูลส่วนบุคคลที่นอกเหนือคำสั่งในส่วนนี้ และอาจมีความรับผิดหากมีการละเมิดข้อมูลส่วนบุคคล หรือไม่สามารถปฏิบัติหน้าที่ได้ครบถ้วนตามที่กฎหมายกำหนด

กรณีนี้จึงคล้ายคลึงกับหลักกฎหมายในเรื่องการกระทำนอกขอบอำนาจของตัวแทน ที่หากตัวแทนดำเนินการตามขอบอำนาจก็จะไม่ต้องรับผิดเป็นการส่วนตัว อย่างไรก็ตาม หากดำเนินการนอกขอบอำนาจ กิจการนั้นย่อมไม่ผูกพันตัวการ และตัวแทนจะต้องรับผิดเป็นการส่วนตัวด้วย

อย่างไรก็ตาม ความสัมพันธ์และสถานะของบุคคลสองบุคคลอันเกี่ยวข้องกับการใช้ประโยชน์ในข้อมูลส่วนบุคคลนั้นอาจมีความหลากหลายและซับซ้อนในทางปฏิบัติ โดยอีกนัยหนึ่งอาจมีกรณีในการแบ่งปันและประมวลผลข้อมูลส่วนบุคคลโดยที่ทั้งสองฝ่ายเป็นผู้ควบคุม

ข้อมูลส่วนบุคคลได้ หากทั้งสองฝ่ายต่างประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ของตนเองโดยไม่ต้องดำเนินการตามคำสั่งของอีกฝ่ายหนึ่ง ยกตัวอย่างในสถานการณ์ที่คล้ายคลึงกับตัวอย่างก่อนหน้านี้ บริษัทจำหน่ายรถยนต์ได้แบ่งปันข้อมูลส่วนบุคคลของลูกค้าที่ซื้อรถยนต์ให้กับบริษัทประกันภัยเพื่อใช้ประกอบการเสนอขายและทำสัญญาประกันภัยรถยนต์ ซึ่งแม้ว่าบริษัททั้งสองแห่งต่างมีวัตถุประสงค์ในการใช้ข้อมูลส่วนบุคคลเพื่อประโยชน์ในทางธุรกิจของตนโดยที่ไม่ได้มีอำนาจควบคุมการทำงานของอีกฝ่ายหนึ่ง ทั้งสองฝ่ายจึงมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลทั้งคู่ นอกจากนี้ อาจต้องรับผิดต่อเจ้าของข้อมูลส่วนบุคคลหากการส่งต่อข้อมูลนั้นไม่ได้เป็นไปโดยชอบด้วยกฎหมายตามมาตรา ๒๗ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ

ทั้งนี้ เมื่อทราบถึงนิยามต่าง ๆ ที่ปรากฏในกฎหมายแล้ว จึงเข้าสู่กระบวนการสำรวจตรวจสอบกิจการภายในของหน่วยงานว่าได้มีการเก็บ รวบรวม ประมวลผล หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลมาจากแหล่งใด มีรายละเอียดข้อมูลส่วนบุคคลอย่างไร และมีการไหลเวียนของข้อมูลส่วนบุคคลดังกล่าวภายในและออกสู่ภายนอกองค์กรอย่างไร

**ขั้นตอนที่ ๒ การจำแนกประเภทข้อมูล** (Data Classification)

ขั้นตอนนี้คือการนำเอาบันทึกรายการข้อมูลส่วนบุคคลที่ได้จากการสำรวจตรวจสอบภายในข้างต้นมาแยกประเภทว่าหน่วยงานของตนได้จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคลเชิงอ่อนไหวตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือเป็นข้อมูลที่มีความเสี่ยงสูงหากมีการรั่วไหลออกไปหรือไม่ ซึ่งข้อมูลเหล่านี้อาจจำเป็นต้องมีมาตรการในการดูแลรักษาความปลอดภัยมากกว่าข้อมูลส่วนบุคคลทั่วไป ดังมีรายละเอียดต่อไปนี้

**ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน** (Sensitive Personal Data)

เป็นข้อมูลที่กำหนดไว้ตามมาตรา ๒๖ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ ได้แก่ เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน

ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

**ข้อมูลที่มีความเสี่ยงสูง**

เป็นประเภทของข้อมูลที่กฎหมายไม่ได้กำหนดไว้โดยเฉพาะ แต่เป็นข้อมูลที่อาจส่งผลเสียหายต่อเจ้าของข้อมูลส่วนบุคคลได้มากหากเกิดการรั่วไหล เช่น ข้อมูลทางการเงิน (หมายเลขบัญชีธนาคาร หมายเลขบัตรเครดิต เป็นต้น) ข้อมูลเกี่ยวกับสำมะโนประชากรหรือที่สามารถใช้ยืนยันตัวตนได้ตามกฎหมาย (หมายเลขบัตรประจำตัวประชาชน หมายเลขหนังสือเดินทาง หรือสำเนาของเอกสารนั้น ๆ)

**ขั้นตอนที่ ๓ การระบุวัตถุประสงค์ (Identification Purpose)**

เมื่อหน่วยงานสามารถระบุรายการประมวลผลข้อมูลส่วนบุคคล และสามารถจำแนกลักษณะ ประเภท พร้อมทั้งความเสี่ยงเบื้องต้นของการเก็บ รวบรวม ประมวลผล หรือเปิดเผยข้อมูลส่วนบุคคลได้ ขั้นตอนต่อไปคือ การระบุวัตถุประสงค์ในการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ซึ่งมีความสำคัญในการปฏิบัติตาม พ.ร.บ. ข้อมูลส่วนบุคคลฯ อย่างมาก เนื่องจากผู้ควบคุมข้อมูลส่วนบุคคลนั้นจำเป็นต้องแจ้งวัตถุประสงค์แก่เจ้าของข้อมูลส่วนบุคคล[๑๐] และสามารถเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ได้เท่าที่จำเป็นตามวัตถุประสงค์ที่แจ้งเท่านั้น[๑๑] นอกจากนี้ การระบุวัตถุประสงค์ยังมีผลต่อการกำหนดฐานทางกฎหมาย ซึ่งจะส่งผลต่อความชอบด้วยกฎหมายในการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าวด้วย

ดังนั้น หากผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถระบุวัตถุประสงค์ในการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล หรือไม่สามารถตอบคำถามว่าเก็บข้อมูลมาเพื่อวัตถุประสงค์ใดหรือแจ้งว่าเก็บมาเผื่อเอาไว้ก่อน ย่อมเป็นกรณีการไม่ปฏิบัติตาม พ.ร.บ. ข้อมูลส่วนบุคคลฯ ซึ่งมีความเสี่ยงที่อาจได้รับโทษทางกฎหมายต่อไป

---

[๑๐] พ.ร.บ. ข้อมูลส่วนบุคคลฯ มาตรา ๒๓ (๑).

[๑๑] พ.ร.บ. ข้อมูลส่วนบุคคลฯ มาตรา ๒๑ และมาตรา ๒๒.

ในทางปฏิบัติ การระบุวัตถุประสงค์ของการใช้ข้อมูลนั้นสามารถทำได้หลายวิธี ไม่ว่าจะเป็นการทบทวนเอกสารที่เกี่ยวข้องกับการเก็บข้อมูลส่วนบุคคล เช่น ใบสมัครงาน ใบสมัครรับบริการ ว่ามีการเก็บข้อมูลที่ไม่จำเป็นหรือไม่ได้ใช้งานหรือไม่ โดยเฉพาะที่มีการใช้หรือจัดทำมาก่อนมีกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยข้อมูลที่ไม่จำเป็นที่พบได้บ่อยในประเทศไทย เช่น การเก็บข้อมูลเชื้อชาติ ศาสนา ซึ่งเป็นทั้งข้อมูลที่ไม่ได้ใช้งาน และยังเป็นข้อมูลอ่อนไหวตามกฎหมาย หรือในกรณีที่กำลังจะมีกิจกรรมที่ต้องใช้ข้อมูลส่วนบุคคลในอนาคต ควรมีการประเมินและกำหนดขอบเขตของข้อมูลส่วนบุคคลที่จำเป็นในการบรรลุวัตถุประสงค์นั้น ๆ

ทั้งนี้ หากสามารถระบุได้ว่าปัจจุบันมีข้อมูลบางส่วนที่ไม่สามารถระบุวัตถุประสงค์หรือเก็บมาโดยไม่มีความจำเป็น ควรหลีกเลี่ยงการเก็บข้อมูลดังกล่าว หรือลบทำลายข้อมูลประเภทนั้น ๆ ที่มีอยู่แล้วเพื่อลดความเสี่ยงจากการไม่ปฏิบัติตามกฎหมาย ทั้งนี้ เพื่อให้เป็นไปตามหลักการเพียงพอ เกี่ยวเนื่องและอยู่ในขอบเขตที่จำเป็นโดยสัมพันธ์กับวัตถุประสงค์ที่ข้อมูลถูกประมวลผล หรือที่เรียกว่าหลักการใช้ข้อมูลให้น้อยที่สุด (“Data Minimization”)

**ขั้นตอนที่ ๔ การกำหนดฐานตามกฎหมาย (Lawful Basis)**

เมื่อหน่วยงานได้ดำเนินการมาถึงขั้นตอนนี้ หน่วยงานจะสามารถบ่งบอกได้ว่า ปัจจุบันข้อมูลส่วนบุคคลที่ไหลเวียนอยู่นั้นมีประเภทใดบ้าง และเพื่อวัตถุประสงค์ใด หากว่าหน่วยงานไม่สามารถระบุถึงความจำเป็นหรือวัตถุประสงค์ในข้อมูลส่วนบุคคลชุดใดได้ หน่วยงานก็สมควรที่จะลบทำลาย หรือไม่จัดเก็บข้อมูลส่วนบุคคลนั้นมาเพื่อลดภาระ และลดความเสี่ยงขององค์กร

ต่อมาเป็นขั้นตอนที่นักกฎหมายจะเข้ามามีบทบาทสำคัญในการตรวจสอบความชอบด้วยกฎหมายของการประมวลผลข้อมูลส่วนบุคคลนั้น ๆ โดยทั่วไปการเก็บ รวบรวม ประมวลผล หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต้องมี “ฐานทางกฎหมาย” มารองรับ ได้แก่ ความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ซึ่งถือเป็นฐานทางกฎหมายฐานหนึ่ง อย่างไรก็ตามกฎหมายได้กำหนดเงื่อนไขในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลที่ต้องปฏิบัติตามโดยเคร่งครัดดังต่อไปนี้[๑๒]

[๑๒] พ.ร.บ. ข้อมูลส่วนบุคคลฯ มาตรา ๑๙.

๑. การขอความยินยอมต้องทำโดยชัดแจ้งเป็นหนังสือ หรือทำโดยผ่านระบบอิเล็กทรอนิกส์

๒. ต้องแจ้งวัตถุประสงค์ของการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย

๓. การขอความยินยอมนั้นต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน

๔. มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่ายและไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว

๕. ในการเข้าทำสัญญาซึ่งรวมถึงการให้บริการใด ๆ ต้องไม่มีเงื่อนไขในการให้ความยินยอมเพื่อเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่มีความจำเป็นหรือเกี่ยวข้องสำหรับการเข้าทำสัญญาซึ่งรวมถึงการให้บริการนั้น ๆ

๖. เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้โดยจะต้องถอนความยินยอมได้ง่ายเช่นเดียวกับการให้ความยินยอม

ทั้งนี้ ความยินยอมที่ไม่ได้ทำตามเงื่อนไขดังกล่าวจะไม่สามารถใช้อ้างได้ตามกฎหมาย

อย่างไรก็ตาม กฎหมายได้กำหนดข้อยกเว้นในการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล โดยข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลอ่อนไหวมีฐานทางกฎหมายที่แตกต่างกัน ดังนี้

**๑. ฐานทางกฎหมายสำหรับข้อมูลส่วนบุคคลทั่วไป (มาตรา ๒๔)**

๑. ฐานความยินยอม

๒. ฐานการจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ การศึกษาวิจัย หรือสถิติ

๓. ฐานเพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

๔. ฐานสัญญา - เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

๕. ฐานประโยชน์สาธารณะ - เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

๖. ฐานประโยชน์อันชอบธรรม - เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

๗. ฐานการปฏิบัติตามกฎหมาย - เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

**๒. ฐานทางกฎหมายสำหรับข้อมูลส่วนบุคคลอ่อนไหว (มาตรา ๒๖)**

เนื่องจากความแตกต่างของลักษณะและผลกระทบของข้อมูลส่วนบุคคลอ่อนไหวที่แตกต่างจากข้อมูลส่วนบุคคลทั่วไป กฎหมายจึงได้กำหนดฐานทางกฎหมายที่แตกต่างกันไว้โดยเฉพาะตามมาตรา ๒๖ ได้แก่

๑. ความยินยอมโดยชัดแจ้ง

๒. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม

๓. เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไร

๔. เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

๕. เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

๖. เป็นการจำเป็นในการปฏิบัติตามกฎหมาย เพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

(ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพหรือระบบและการให้บริการด้านสังคมสงเคราะห์

(ข) ประโยชน์สาธารณะด้านการสาธารณสุข

(ค) การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม

(ง) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น

(จ) ประโยชน์สาธารณะที่สำคัญ

ทั้งนี้ ฐานทางกฎหมายของข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลอ่อนไหวไม่สามารถใช้ปะปนหรือสลับกันได้

ทั้งนี้ เป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในการวิเคราะห์ และกำหนดฐานทางกฎหมายที่เหมาะสมกับวัตถุประสงค์ในการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

**ขั้นตอนที่ ๕ การประเมินและวิเคราะห์ความเสี่ยง (Gap Analysis)**

เมื่อหน่วยงานสามารถระบุฐานตามกฎหมายของการประมวลผลข้อมูลส่วนบุคคลได้อย่างชัดเจนแล้ว ประเด็นสำคัญต่อเนื่องคือการประเมินและวิเคราะห์ความเสี่ยงของการเก็บรวบรวม ประมวลผล หรือเปิดเผยข้อมูลส่วนบุคคล และหาแนวทางในการปิดความเสี่ยง

ต่าง ๆ ที่เกิดขึ้นรวมถึงการจำกัดผลเสียหายที่อาจเกิดขึ้นในอนาคต โดยหัวข้อในการพิจารณาจะมีความหลากหลายขึ้นอยู่กับลักษณะธุรกิจ และกิจกรรมที่ใช้ข้อมูลส่วนบุคคล โดยมีตัวอย่างในการพิจารณา ดังนี้

**สิทธิของเจ้าของข้อมูลส่วนบุคคล**

วัตถุประสงค์ที่สำคัญที่สุดของ พ.ร.บ. ข้อมูลส่วนบุคคลฯ คือการมุ่งปกป้องสิทธิของเจ้าของข้อมูลส่วนบุคคลจากการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่ชอบด้วยกฎหมาย โดยเป็นไปตามหมายเหตุท้ายพระราชบัญญัติ ความว่า

“เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าวทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้นเพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป จึงจำเป็นต้องตราพระราชบัญญัตินี้”[๑๓]

หลักการดังกล่าวสะท้อนกลับไปยังกฎหมายซึ่งเป็นต้นแบบของ พ.ร.บ. ข้อมูลส่วนบุคคลฯ GDPR มาตรา ๑ ความว่า

“มาตรา ๑ ประเด็นสำคัญและจุดมุ่งหมาย

๑. ข้อกำหนดนี้วางกฎที่สัมพันธ์กับการคุ้มครองบุคคลธรรมดาในประเด็นที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลและกฎที่สัมพันธ์กับการเคลื่อนย้ายข้อมูลส่วนบุคคลโดยเสรี

[๑๓] หมายเหตุท้ายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล.

๒. ข้อกำหนดนี้คุ้มครองสิทธิเสรีภาพขั้นพื้นฐานของบุคคลธรรมดาและโดยเฉพาะอย่างยิ่งสิทธิในการเข้าถึงการคุ้มครองข้อมูลส่วนบุคคล

๓. การเคลื่อนย้ายข้อมูลส่วนบุคคลโดยเสรีภายในสหภาพไม่ควรถูกจำกัดหรือห้ามด้วยเหตุผลที่เชื่อมโยงกับการคุ้มครองบุคคลธรรมดาในประเด็นที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล”[๑๔]

สิทธิลำดับแรกที่กฎหมายกำหนด คือสิทธิในการทราบรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล (Right to be informed) โดยสะท้อนมาจากเจตนารมณ์ของมาตรา ๒๓ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ ความว่า

“ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดดังต่อไปนี้ เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

(๑) วัตถุประสงค์ของการเก็บรวบรวมเพื่อการนำข้อมูลส่วนบุคคลไปใช้ หรือเปิดเผย ซึ่งรวมถึงวัตถุประสงค์ตามที่มาตรา ๒๔ ให้อำนาจในการเก็บรวบรวมได้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(๒) แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญาหรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล

(๓) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม

(๔) ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

---

[๑๔] นคร เสรีรักษ์ และคณะ ผู้แปล, GDPR ฉบับภาษาไทย, (กรุงเทพฯ : พี.เพรส, ๒๕๖๒), ๙๙.

(๕) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อ ในกรณีที่มีตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย

(๖) สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา ๑๙ วรรคห้า มาตรา ๓๐ วรรคหนึ่ง มาตรา ๓๑ วรรคหนึ่ง มาตรา ๓๒ วรรคหนึ่ง มาตรา ๓๓ วรรคหนึ่ง มาตรา ๓๔ วรรคหนึ่ง มาตรา ๓๖ วรรคหนึ่ง และมาตรา ๗๓ วรรคหนึ่ง”

จากตัวบทดังกล่าวนอกจากจะก่อหน้าที่ตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลในการแจ้งรายละเอียดของการเก็บ รวบรวม ใช้ หรือเปิดเผยให้แก่เจ้าของข้อมูลส่วนบุคคลทราบแล้ว ยังเป็นสิทธิของเจ้าของข้อมูลที่ต้องได้รับทราบถึงรายละเอียดดังกล่าวก่อนจะมีการให้ข้อมูลส่วนบุคคลของตนเอง และได้อ้างถึงสิทธิอื่น ๆ ของเจ้าของข้อมูลส่วนบุคคล ดังนี้

- สิทธิในการถอนความยินยอม[๑๕]
- สิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตน[๑๖]
- สิทธิขอรับและขอให้ส่งต่อข้อมูลส่วนบุคคล[๑๗]
- สิทธิคัดค้านการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล[๑๘]
- สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้[๑๙]
- สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคล[๒๐]

---

[๑๕] มาตรา ๑๙ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.
[๑๖] มาตรา ๓๐ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.
[๑๗] มาตรา ๓๑ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.
[๑๘] มาตรา ๓๒ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.
[๑๙] มาตรา ๓๓ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.
[๒๐] มาตรา ๓๔ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.

- สิทธิในการทำให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด[๒๑]

- สิทธิร้องเรียนการฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติหรือประกาศที่ออกตามพระราชบัญญัตินี้[๒๒]

ในขณะเดียวกันสิทธิดังกล่าวข้างต้นก็เป็นส่วนหนึ่งของหน้าที่ตามกฎหมายก่อหน้าที่ให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งจะกล่าวโดยละเอียดในส่วนถัดไป

**หน้าที่และความรับผิดของผู้ควบคุมข้อมูลส่วนบุคคล**

โดยทั่วไปผู้ควบคุมข้อมูลส่วนบุคคลจะเป็นบุคคลหลักที่กฎหมาย พ.ร.บ. ข้อมูลส่วนบุคคลฯ ได้กำหนดหน้าที่ความรับผิดชอบในการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ไม่ว่าจะเป็นก่อน ขณะ หรือภายหลังกิจกรรมดังกล่าว ยกตัวอย่างเช่น

- หน้าที่ในการขอความยินยอมในการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล[๒๓] หรือโดยมีฐานทางกฎหมายอนุญาตให้กระทำได้ [๒๔]

- หน้าที่ในการแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล[๒๕] และประมวลผลข้อมูลส่วนบุคคลเฉพาะตามที่ได้แจ้งรายละเอียดดังกล่าว[๒๖]

- ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจาก แหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่ได้รับความยินยอม หรือโดยมีฐานทางกฎหมายอนุญาตให้กระทำได้[๒๗]

---

[๒๑] มาตรา ๓๖ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.

[๒๒] มาตรา ๗๓ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.

[๒๓] มาตรา ๑๙ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.

[๒๔] มาตรา ๒๔ และ ๒๖ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.

[๒๕] มาตรา ๒๓ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.

[๒๖] มาตรา ๒๑ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.

[๒๗] มาตรา ๒๕ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.

- ห้ามเปิดเผยข้อมูลส่วนบุคคลเว้นแต่ได้รับความยินยอม หรือโดยมีฐานทางกฎหมายอนุญาตให้กระทำได้[๒๘]
- หน้าที่ในการดำเนินการกรณีการส่งข้อมูลไปยังต่างประเทศ[๒๙]
- หน้าที่ในการตอบสนองต่อการขอใช้สิทธิของเจ้าของข้อมูล[๓๐]
- หน้าที่ในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล[๓๑]
- หน้าที่ในการป้องกันการรั่วไหลของข้อมูลโดยบุคคลอื่น และหน้าที่ในการจัดทำสัญญาการประมวลผลข้อมูลกับผู้ประมวลผลข้อมูลส่วนบุคคล[๓๒]
- หน้าที่ในการจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล[๓๓]
- หน้าที่ในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่สำนักงาน หรือเจ้าของข้อมูลส่วนบุคคล[๓๔]
- หน้าที่ในการจัดทำบันทึกรายการการประมวลผลข้อมูลส่วนบุคคล[๓๕] เป็นต้น

จากตัวอย่างข้างต้น ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นผู้ที่ใช้ประโยชน์จากข้อมูลส่วนบุคคลนั้น จึงเป็นผู้ที่มีหน้าที่และความรับผิดหลักภายใต้กฎหมาย ไม่ว่าจะเป็นดำเนินการเพื่อให้การเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคลให้เป็นไปโดยชอบด้วยกฎหมาย

---

[๒๘] มาตรา ๒๗ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.

[๒๙] มาตรา ๒๘ - ๒๙ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.

[๓๐] มาตรา ๓๐ - ๓๖ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.

[๓๑] มาตรา ๒๗ (๑) แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.

[๓๒] มาตรา ๒๗ (๒) และมาตรา ๔๐ วรรคสาม แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.

[๓๓] มาตรา ๒๗ (๓) แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.

[๓๔] มาตรา ๒๗ (๔) แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.

[๓๕] มาตรา ๓๙ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.

การตอบสนองต่อการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล การดำเนินการให้การใช้ข้อมูลส่วนบุคคลมีมาตรฐาน โปร่งใส และสามารถตรวจสอบได้ตามที่กฎหมายกำหนด รวมถึงการควบคุมดูแลให้การประมวลผลข้อมูลส่วนบุคคลโดยบุคคลอื่นเป็นไปโดยชอบด้วยกฎหมาย

**หน้าที่และความรับผิดของผู้ประมวลผลข้อมูลส่วนบุคคล**

หน้าที่และความรับผิดของผู้ประมวลผลข้อมูลส่วนบุคคลนั้นมีน้อยกว่าผู้ควบคุมข้อมูลส่วนบุคคลมาก เนื่องจากไม่ได้เป็นผู้ตัดสินใจเกี่ยวกับวัตถุประสงค์และกิจกรรมในการประมวลผลข้อมูลส่วนส่วนบุคคล ยกตัวอย่างเช่น

- หน้าที่ดำเนินการเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น[๓๖]
- หน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม[๓๗]
- หน้าที่ในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อผู้ควบคุมข้อมูลส่วนบุคคล[๓๘]
- หน้าที่จัดทำบันทึกรายการการประมวลผลข้อมูลส่วนบุคคล[๓๙] เป็นต้น

จากมุมมองของบุคคลหรือหน่วยงานที่เกี่ยวข้องกับการใช้ข้อมูลส่วนบุคคล เนื่องจากการมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นส่งผลอย่างมากในการดำเนินการเพื่อปฏิบัติตาม พ.ร.บ. ข้อมูลส่วนบุคคลฯ เนื่องจากความแตกต่างของหน้าที่ความรับผิดตามกฎหมายข้างต้น

---

[๓๖] มาตรา ๔๐ (๑) แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.
[๓๗] มาตรา ๔๐ (๒) แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.
[๓๘] มาตรา ๔๐ (๒) แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.
[๓๙] มาตรา ๔๐ (๓) แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.

**บทลงโทษในการไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล**

ทั้งนี้ ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้กำหนดโทษสำหรับกรณีการละเมิดหรือไม่ปฏิบัติตามกฎหมายไว้ ดังนี้

**ก. โทษทางอาญา**

สิ่งหนึ่งที่ พ.ร.บ. ข้อมูลส่วนบุคคลฯ กำหนดไว้แตกต่างจากกฎหมายต้นแบบอย่าง GDPR นั้น คือได้มีการกำหนดโทษอาญาสำหรับกรณีการละเมิดกฎหมายในกรณีร้ายแรงไว้ ๒ กรณี ได้แก่

**๑. กรณีการเปิดเผยข้อมูลส่วนบุคคลอ่อนไหวโดยมิชอบ**

“มาตรา ๗๙ ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา ๒๗ วรรคหนึ่งหรือวรรคสอง หรือไม่ปฏิบัติตามมาตรา ๒๘ อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา ๒๖ โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา ๒๗ วรรคหนึ่งหรือวรรคสอง หรือไม่ปฏิบัติตามมาตรา ๒๘ อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา ๒๖ เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งล้านบาท หรือทั้งจำทั้งปรับ”

**๒. นำข้อมูลส่วนบุคคลที่ได้รับรู้มาจากการปฏิบัติหน้าที่ตามกฎหมายไปเปิดเผย**

“มาตรา ๘๐ ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

ความในวรรคหนึ่ง มิให้นำมาใช้บังคับแก่การเปิดเผย ในกรณีดังต่อไปนี้

(๑) การเปิดเผยตามหน้าที่

(๒) การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี

(๓) การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย

(๔) การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล

(๕) การเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่าง ๆ ที่เปิดเผยต่อสาธารณะ”

จากบทบัญญัติข้างต้นมีข้อสังเกตว่ากฎหมายใช้ถ้อยคำว่า “ผู้ใด” จึงทำให้ผู้กระทำผิดอาจเป็นบุคคลใดก็ได้ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล โดยไม่คำนึงถึงสถานะความเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล นอกจากนี้ หากกรณีเป็นการกระทำความผิดโดยนิติบุคคล ผู้แทนนิติบุคคล หรือผู้รับผิดชอบในการดำเนินการดังกล่าวอาจต้องร่วมรับผิดด้วย

“มาตรา ๘๑ ในกรณีที่ผู้กระทำความผิดตามพระราชบัญญัตินี้เป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย”

นอกจากนี้ สำหรับการกระทำความผิดที่มีองค์ประกอบด้านเจตนาพิเศษตามมาตรา ๗๙ วรรคสอง นั้น แม้ผู้กระทำจะไม่ได้มีเจตนาพิเศษตามที่กฎหมายกำหนด อันส่งให้การกระทำดังกล่าวไม่ครบองค์ประกอบความผิดและไม่ต้องรับโทษอาญา แต่ผู้ควบคุมข้อมูลส่วนบุคคลที่ละเมิดกฎหมายเกี่ยวกับการส่งต่อข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมายตามมาตรา ๒๗ - ๒๘ นั้น อาจยังต้องได้รับโทษทางปกครอง หรือรับผิดในความเสียหายทางแพ่งต่อเจ้าของข้อมูลส่วนบุคคล ซึ่งจะกล่าวถึงโดยละเอียดในหัวข้อถัดไป

อย่างไรก็ตาม การกระทำความผิดอาญาเกี่ยวกับ พ.ร.บ. ข้อมูลส่วนบุคคลฯ นั้น จะมีเพียง ๒ ฐานความผิดเท่านั้น แต่ในทางปฏิบัติ การกระทำที่เข้าข่ายการกระทำความผิดหรือไม่ปฏิบัติตาม พ.ร.บ. ข้อมูลส่วนบุคคลฯ นั้น อาจเป็นการกระทำที่ครบองค์ประกอบของกฎหมายที่มีโทษอาญาอื่นได้เช่นกัน อาทิ ความผิดฐานหมิ่นประมาท หรือหมิ่นประมาทโดยการโฆษณา หรือความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เป็นต้น

**ข. โทษทางปกครอง**

กรณีต่างจากโทษทางอาญาข้างต้น โทษทางปกครองนั้นเป็นโทษที่จะบังคับเฉพาะกับการไม่ปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล[๔๐] หรือผู้ประมวลผลข้อมูลส่วนบุคคล[๔๑] โดยเป็นโทษปรับที่พิจารณาโดยคณะกรรมการผู้เชี่ยวชาญซึ่งแต่งตั้งโดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยเป็นโทษที่เกิดจากการไม่ปฏิบัติตามหน้าที่ที่กฎหมายกำหนดเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล อาทิ การเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือไม่มีฐานทางกฎหมายรองรับ[๔๒] ไม่ได้แจ้งรายละเอียดในการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามรายละเอียดที่กำหนด[๔๓] ไม่ได้จัดให้มีบันทึกรายละเอียดการประมวลผลข้อมูลส่วนบุคคล[๔๔] หรือไม่ได้จัดให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอ[๔๕] เป็นต้น

ทั้งนี้ในการยื่นเรื่องร้องเรียนการไม่ปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลนั้น

---

[๔๐] มาตรา ๘๒ - ๘๔ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.

[๔๑] มาตรา ๘๕ - ๘๗ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.

[๔๒] มาตรา ๒๔ ประกอบมาตรา ๘๓ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.

[๔๓] มาตรา ๒๓ ประกอบมาตรา ๘๒ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.

[๔๔] มาตรา ๓๙ ประกอบมาตรา ๘๒ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.

[๔๕] มาตรา ๓๗ ประกอบมาตรา ๘๒ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.

ตามมาตรา ๗๓[๔๖] กำหนดให้เป็นสิทธิของเจ้าของข้อมูลส่วนบุคคล

อย่างไรก็ตาม ระเบียบคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ว่าด้วยการยื่น การไม่รับเรื่อง การยุติเรื่อง การพิจารณา และระยะเวลาในการพิจารณาคำร้องเรียน พ.ศ. ๒๕๖๕ ซึ่งออกภายใต้มาตรา ๗๓ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ ได้ใช้ถ้อยคำว่า “เจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง” เป็นผู้มีสิทธิในการยื่นคำร้องเรียนการไม่ปฏิบัติตาม พ.ร.บ. ข้อมูลส่วนบุคคลฯ ดังกล่าว

นอกจากนี้ ตามข้อ ๘ ของระเบียบดังกล่าวยังได้กำหนดว่าคำร้องเรียนนั้น ต้องประกอบด้วย “รายละเอียดความเดือดร้อนเสียหายหรือผลกระทบต่อผู้ร้องเรียน” อันถือเป็นองค์ประกอบสำคัญต่อความสมบูรณ์ของคำร้องเรียน[๔๗] และอาจไม่ได้รับการพิจารณาโดยคณะกรรมการผู้เชี่ยวชาญตามข้อ ๙ ของระเบียบ[๔๘]

จากระเบียบดังกล่าวจึงอาจตีความได้ว่าเจ้าของข้อมูลส่วนบุคคลที่มีสิทธิในการยื่นข้อร้องเรียนนั้น ต้องได้รับ “ความเดือดร้อนเสียหาย” หรือ “ผลกระทบ” แล้วเท่านั้น หรืออาจส่งผลให้เจ้าของข้อมูลส่วนบุคคลที่พบเห็นการไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูล

---

[๔๖] มาตรา ๗๓ เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติหรือประกาศที่ออกตามพระราชบัญญัตินี้

การยื่น การไม่รับเรื่อง การยุติเรื่อง การพิจารณา และระยะเวลาในการพิจารณาคำร้องเรียนให้เป็นไปตามระเบียบที่คณะกรรมการประกาศกำหนดโดยคำนึงถึงการกำหนดให้ไม่รับเรื่องร้องเรียนหรือยุติเรื่องในกรณีที่มีผู้มีอำนาจพิจารณาในเรื่องนั้นอยู่แล้วตามกฎหมายอื่นด้วย.

[๔๗] ข้อ ๘ คำร้องเรียนที่ยื่นต่อสำนักงาน ต้องมีความชัดเจน สามารถทำความเข้าใจได้ ใช้ถ้อยคำสุภาพ ไม่หยาบคาย ไม่มีลักษณะเป็นการกรรโชก ข่มขู่ ไม่ว่าจะโดยตรงหรือโดยอ้อม และต้องมีรายละเอียดและเอกสารหลักฐานอย่างน้อยดังต่อไปนี้ .....

(๓) รายละเอียดความเดือดร้อนเสียหายหรือผลกระทบต่อผู้ร้องเรียน.

[๔๘] ข้อ ๙ .....

“ในกรณีที่คำร้องเรียนมีลักษณะ รายละเอียด และเอกสารหลักฐานไม่ถูกต้องหรือไม่ครบถ้วน ให้พนักงานเจ้าหน้าที่แจ้งผู้ร้องเรียนหรือผู้รับมอบอำนาจทราบโดยเร็ว พร้อมทั้งให้คำแนะนำในการแก้ไขคำร้องเรียนและแจ้งให้ทราบว่า คำร้องเรียนดังกล่าวจะยังไม่มีผลสมบูรณ์และไม่ได้รับการพิจารณาจากคณะกรรมการผู้เชี่ยวชาญจนกว่าจะได้แก้ไขให้ถูกต้องครบถ้วนตามที่กำหนดในข้อ ๘”.

ส่วนบุคคลโดยที่ยังไม่มีความเสียหายหรือเกิดผลกระทบในเชิงลบนั้น อาจยังไม่สามารถใช้สิทธิตามกฎหมายได้ ซึ่งกรณีดังกล่าวอาจก่อให้เกิดปัญหาในการบังคับใช้กฎหมายได้ กรณีอาจเป็นการจำกัดสิทธิของเจ้าของข้อมูลส่วนบุคคลที่ขัดต่อ พ.ร.บ. ข้อมูลส่วนบุคคลฯ ซึ่งเป็นกฎหมายแม่บทได้ อย่างไรก็ตาม ต้องติดตามแนวทางการพิจารณาเรื่องร้องเรียนของคณะกรรมการผู้เชี่ยวชาญและคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลต่อไป

ในความเห็นของผู้เขียนนั้นมองว่า การกระทำความผิดหรือการไม่ปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นอาจไม่ได้ก่อให้เกิดความเสียหายที่เป็นรูปธรรมต่อเจ้าของข้อมูลส่วนบุคคลในขณะที่พบการไม่ปฏิบัติตามกฎหมายนั้น และกฎหมายควรให้สิทธิในการตรวจสอบรวมถึงให้อำนาจแก่หน่วยงานกำกับดูแลในการระงับการกระทำดังกล่าวเพื่อป้องกันไม่ให้เกิดเหตุการละเมิดหรือการรั่วไหลของข้อมูลที่จะส่งผลให้เกิดความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคลในที่สุดโดยมีเหตุผลสนับสนุนดังนี้

ประการแรก เมื่อพิจารณาถึงความเข้มข้นและปริมาณการใช้ข้อมูลส่วนบุคคลในปัจจุบัน การละเมิด หรือรั่วไหลของข้อมูลส่วนบุคคลในแต่ละครั้งโดยเฉพาะในทางอิเล็กทรอนิกส์ย่อมมีผู้ได้รับผลกระทบเป็นวงกว้าง และโดยทั่วไปแล้วการรั่วไหลของข้อมูลนั้นมักไม่สามารถแก้ไขหรือทำให้ย้อนกลับได้ อีกทั้งทำให้เกิดความเสียหายร้ายแรงต่อเจ้าของข้อมูลส่วนบุคคล ทั้งในด้านที่อาจมีมูลค่าเป็นตัวเงิน อาทิ การรั่วไหลของข้อมูลเกี่ยวกับบัตรเครดิต หรือการหลอกลวงของมิจฉาชีพโดยอาศัยหมายเลขโทรศัพท์ หรืออาจส่งผลเสียต่อชื่อเสียงหรือการถูกเลือกปฏิบัติทางสังคมหากเกิดการรั่วไหลของข้อมูลส่วนบุคคลที่อ่อนไหวอีกด้วย การกำหนดมาตรฐานและกวดขันการปฏิบัติตามกฎหมายย่อมมีประสิทธิภาพในการป้องกันเหตุการณ์ดังกล่าว มากกว่าการลงโทษหรือมีมาตรการเยียวยาความเสียหายภายหลังการเกิดเหตุการณ์ละเมิด ดังนั้น สิทธิในการร้องเรียนของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลที่พบเห็นการไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้นจึงไม่ควรต้องมีเงื่อนไขว่าต้องมีความเสียหายเกิดขึ้นก่อนจึงจะสามารถใช้สิทธิตามกฎหมายได้

ประการที่สอง ในส่วนของบทกำหนดโทษทางปกครองตามมาตรา ๘๒ - ๘๗ นั้น ได้ระบุองค์ประกอบของการกระทำความผิดไว้ว่าเป็นการไม่ปฏิบัติตามกฎหมายเท่านั้น โดยใช้ถ้อยคำ เช่น “ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา... ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท” หรือ “ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา... ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท” ซึ่งเห็นได้ว่ากฎหมายไม่ได้กำหนดให้ความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลเป็นองค์ประกอบในการกระทำความผิดแต่อย่างใด

นอกจากนี้ เมื่อพิจารณาแนวทางการวินิจฉัยของหน่วยงานกำกับดูแลด้านข้อมูลส่วนบุคคลของประเทศต่าง ๆ ในยุโรปนั้น พบว่ามีคำตัดสินจำนวนมากซึ่งได้มีคำสั่งลงโทษการไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล แม้ว่ายังไม่เกิดความเสียหายเป็นตัวเงินต่อเจ้าของข้อมูลส่วนบุคคล อาทิ

- **ประเทศเนเธอร์แลนด์** - ไม่ได้จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลอย่างเพียงพอ และไม่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลเกี่ยวกับรายละเอียดเกี่ยวกับการเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลภายนอก

๒๔ กุมภาพันธ์ ๒๕๖๕ - หน่วยงานกำกับดูแลด้านข้อมูลส่วนบุคคลของประเทศเนเธอร์แลนด์ (DPA) สั่งปรับกระทรวงการต่างประเทศของประเทศเนเธอร์แลนด์เป็นเงิน ๕๖๕,๐๐๐ ยูโร (ประมาณ ๒๐ ล้านบาท) จากการที่ไม่ได้จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลอย่างเพียงพอ และไม่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลเกี่ยวกับรายละเอียดเกี่ยวกับการเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลภายนอก[๔๙]

เกี่ยวกับการลงโทษในคดีนี้ กระทรวงการต่างประเทศของเนเธอร์แลนด์นั้นเป็นหน่วยงานที่ดูแลเกี่ยวกับการขอเข้าเมือง ซึ่งมีการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลจำนวนมาก และมีประชาชนยื่นเอกสารขอเข้าเมืองเฉลี่ยประมาณ ๕๓๐,๐๐๐ ครั้งต่อปี

---

[๔๙] **Boete voor Buitenlandse Zaken voor slechte beveiliging visumaanvragen** [Online], 14 July 2022. https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-voor-buitenlandse-zaken-visumaanvragen-slecht-beveiligd-en-informatie-over-delen.

อันประกอบไปด้วยข้อมูลส่วนบุคคลและข้อมูลส่วนบุคคลอ่อนไหวของผู้สมัครจำนวนมาก อาทิ ชื่อ - นามสกุล สัญชาติ ภาพถ่าย ลายนิ้วมือ เป็นต้น

ทาง DPA ได้ให้เหตุผลว่าทางกระทรวงนั้นเป็นหน่วยงานของรัฐที่ประชาชนจำเป็นต้องติดต่อและใช้บริการจำนวนมาก แต่ไม่ได้จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมทั้งทางด้านกายภาพและทางดิจิทัล ซึ่งเพิ่มโอกาสที่อาจทำให้ลูกจ้างซึ่งไม่เกี่ยวข้องสามารถเข้าถึงและเปลี่ยนแปลงข้อมูลส่วนบุคคลของผู้สมัครได้ และการกระทำนั้นอาจไม่ถูกตรวจพบได้เป็นเวลานานอันอาจทำให้เกิดผลกระทบที่ร้ายแรงต่อประชาชนได้ เช่น การถูกปฏิเสธ VISA หรือห้ามเดินทางเข้าออกประเทศ อีกทั้ง DPA ยังเชื่อว่าทางกระทรวงได้รับทราบถึงข้อบกพร่องดังกล่าวเป็นเวลานานแล้ว แต่ไม่ได้ดำเนินการอย่างเพียงพอที่จะแก้ไขให้ถูกต้อง

- **ฝรั่งเศส - การขอความยินยอมการใช้คุกกี้ในเว็บไซต์ที่ไม่ชอบด้วยกฎหมาย**

๓๑ ธันวาคม ๒๕๖๔ - หน่วยงานกำกับดูแลของฝรั่งเศส (CNIL) ได้สั่งปรับบริษัทผู้ให้บริการทางอินเทอร์เน็ต และบริษัทในกลุ่ม social media ในหลายคดีเป็นเงิน ๙๐ ล้านยูโร (ประมาณ ๓.๓ พันล้านบาท), เป็นเงิน ๖๐ ล้านยูโร (ประมาณ ๒.๒ พันล้านบาท),[๕๐] เป็นเงิน ๖๐ ล้านยูโร (ประมาณ ๒.๒ พันล้านบาท)[๕๑] จากกรณีการขอความยินยอมการใช้คุกกี้ในเว็บไซต์ที่ไม่ชอบด้วยกฎหมาย[๕๒] ทั้งนี้ แม้จะไม่ปรากฏข้อเท็จจริงว่ามีผู้ได้รับความเสียหายจากการใช้คุกกี้ดังกล่าวหรือไม่ อย่างไร

---

[๕๐] **Cookies : la CNIL sanctionne GOOGLE à hauteur de 150 millions d'euros** [Online], 14 July 2022. https://www.cnil.fr/fr/cookies-la-cnil-sanctionne-google-hauteur-de-150-millions-deuros.

[๕๑] **Cookies: €60 million penalty against FACEBOOK IRELAND LIMITED** [Online], 14 July 2022. https://www.cnil.fr/fr/cookies-sanction-de-60-millions-deuros-lencontre-de-facebook-ireland-limited.

[๕๒] **Cookies: the CNIL sanctions GOOGLE to the tune of 150 million euros and FACEBOOK to the tune of 60 million euros for non-compliance with the law** [Online], 14 July 2022 https://www.cnil.fr/fr/cookies-la-cnil-sanctionne-google-hauteur-de-150-millions-deuros-et-facebook-hauteur-de-60-millions.

กรณีข้างต้นเป็นกรณีตัวอย่างที่น่าสนใจอย่างยิ่ง โดยมีข้อเท็จจริงโดยสรุปว่า ทั้งบริษัทผู้ให้บริการทางอินเทอร์เน็ตและบริษัทในกลุ่ม social media นั้น มีการเก็บ “คุกกี้” อันเป็นรูปแบบหนึ่งของข้อมูลอิเล็กทรอนิกส์ที่ทำให้ตัวเว็บไซต์สามารถทราบรายละเอียดของผู้เข้าใช้บริการได้ กรณีจึงถือเป็นข้อมูลส่วนบุคคลตามกฎหมาย อย่างไรก็ดี คุกกี้นั้นสามารถแบ่งออกได้เป็นหลายประเภท ซึ่งมีทั้งแบบที่จำเป็นในการทำงานของเว็บไซต์และแบบที่จัดเก็บเพิ่มเติมเพื่อเป็นประโยชน์ในการให้บริการ เช่น ทำให้เว็บไซต์ทราบความชอบหรือข้อมูลจากประวัติการใช้งานบางส่วน อันช่วยให้เว็บไซต์หรือผู้ให้บริการเหล่านี้สามารถนำเสนอผลิตภัณฑ์ที่ตรงกับความต้องการของผู้ใช้งานได้ ทั้งนี้ การเก็บคุกกี้ในแบบหลังจึงจำเป็นต้องได้รับความยินยอมจากผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล

แม้ว่าเว็บไซต์ทั้งสองรายจะดำเนินการขอความยินยอมในการเก็บคุกกี้จากผู้ใช้งาน แต่หน่วยงานกำกับดูแลของฝรั่งเศส (CNIL) ได้วินิจฉัยว่า รูปแบบและการออกแบบการขอความยินยอมทางอิเล็กทรอนิกส์ของเว็บไซต์ดังกล่าวนั้นทำให้ผู้ใช้งานกดยินยอมให้เก็บคุกกี้ได้ง่าย และซับซ้อนน้อยกว่าการกดไม่ยินยอม รวมทั้งอาจทำให้เกิดความเข้าใจผิดว่าหากไม่ยินยอมให้เก็บคุกกี้นั้นจะไม่สามารถเข้าใช้งานเว็บไซต์ได้ กรณีจึงไม่เป็นความยินยอมที่ชอบด้วยกฎหมาย

จากตัวอย่างคำตัดสินของหน่วยงานกำกับดูแลภายใต้กฎหมาย GDPR ข้างต้น เหตุที่มีโทษปรับที่สูงมาก เนื่องจากกฎหมายได้กำหนดโทษทางปกครองไว้สูงสุดไม่เกิน ๒๐,๐๐๐,๐๐๐ ยูโร หรือไม่เกินร้อยละ ๒ ของผลประกอบการทั่วโลก อย่างไรก็ตาม พ.ร.บ. ข้อมูลส่วนบุคคลฯ ได้กำหนดโทษทางปกครองโดยให้อำนาจคณะกรรมการผู้เชี่ยวชาญมีอำนาจสั่งลงโทษผู้ที่ฝ่าฝืนกฎหมายได้ตั้งแต่ไม่เกิน ๕๐๐,๐๐๐ บาท[๕๓] ถึงไม่เกิน ๕,๐๐๐,๐๐๐ บาท[๕๔] หรือในกรณีที่ไม่ร้ายแรงอาจมีคำสั่งให้ตักเตือนหรือดำเนินการแก้ไข ดังนี้[๕๕]

---

[๕๓] มาตรา ๘๙ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.

[๕๔] มาตรา ๘๔ และ ๘๗ แห่ง พ.ร.บ. ข้อมูลส่วนบุคคลฯ.

[๕๕] ข้อ ๙ (๑) แห่งประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์การพิจารณาออกคำสั่งลงโทษปรับทางปกครองของคณะกรรมการผู้เชี่ยวชาญ พ.ศ. ๒๕๖๕.

(ก) ตักเตือนหรือสั่งให้ปฏิบัติหรือดำเนินการแก้ไข หยุด ระงับ ละเว้น หรืองดเว้นการกระทำที่ฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายให้ถูกต้องภายในระยะเวลาที่กำหนด โดยคำสั่งดังกล่าวต้องมีรายละเอียด เหตุผล และวัตถุประสงค์ของคำสั่งอย่างชัดเจนว่าจะต้องแก้ไขและดำเนินการให้ถูกต้องตามกฎหมายอย่างไร

(ข) สั่งห้ามกระทำการที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล หรือให้กระทำการใดเพื่อระงับความเสียหายนั้นภายในระยะเวลาที่กำหนด

(ค) สั่งจำกัดการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีการกระทำผิดไว้เพื่อระงับความเสียหายนั้นภายในระยะเวลาที่กำหนด

โดยในการพิจารณาคำสั่งลงโทษนั้น คณะกรรมการผู้เชี่ยวชาญจะต้องคำนึงถึงปัจจัยดังต่อไปนี้[๕๖]

(ก) รายละเอียดการกระทำผิดที่เกิดขึ้นโดยเฉพาะกรณีที่เป็นการกระทำผิดโดยเจตนาหรือจงใจ หรือประมาทเลินเล่ออย่างร้ายแรง หรือขาดความระมัดระวังตามสมควร

(ข) ความร้ายแรงของพฤติกรรมที่กระทำผิด

(ค) ขนาดกิจการของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

(ง) ผลของมาตรการลงโทษปรับทางปกครองที่จะบังคับว่าจะได้ช่วยบรรเทาความเสียหาย หรือความเดือดร้อนแก่เจ้าของข้อมูลส่วนบุคคลหรือไม่ เพียงใด

(จ) ประโยชน์ที่เจ้าของข้อมูลส่วนบุคคลจะได้รับจากมาตรการลงโทษปรับทางปกครอง และผลกระทบต่อผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลหรือบุคคลที่กระทำผิด และผลกระทบในวงกว้างต่อธุรกิจหรือกิจการอื่นที่เกี่ยวข้อง

---

[๕๖] ข้อ ๘ แห่งประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์การพิจารณาออกคำสั่งลงโทษปรับทางปกครองของคณะกรรมการผู้เชี่ยวชาญ พ.ศ. ๒๕๖๕.

(ฉ) มูลค่าความเสียหายและความร้ายแรงที่เกิดจากการกระทำผิดนั้น

(ช) ระดับโทษปรับทางปกครองและมาตรการบังคับทางปกครองที่เคยใช้กับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลรายอื่นในความผิดทำนองเดียวกัน (ถ้ามี)

(ซ) ประวัติการถูกลงโทษปรับทางปกครองและใช้มาตรการบังคับทางปกครองของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล และในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นนิติบุคคล ให้หมายความรวมถึงประวัติการถูกลงโทษปรับทางปกครองของบุคคลที่เกี่ยวข้องกับการกระทำของนิติบุคคลนั้นด้วย

(ฌ) ระดับความรับผิดชอบและมาตรฐานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในขณะที่มีการกระทำความผิด

(ญ) การดำเนินการตามประมวลจริยธรรม แนวปฏิบัติทางธุรกิจ หรือมาตรฐานในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในขณะที่มีการกระทำความผิด

(ฎ) การเยียวยาและบรรเทาความเสียหายของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเมื่อทราบเหตุที่กระทำความผิด

(ฏ) การชดใช้ค่าสินไหมทดแทนเพื่อเยียวยาความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ข้อเท็จจริงอื่น ๆ ที่เกี่ยวข้อง

**ค. สิทธิในการเรียกร้องค่าเสียหายอันเกิดจากการละเมิด หรือการไม่ปฏิบัติตาม พ.ร.บ. ข้อมูลส่วนบุคคลฯ ต่อศาล**

ในมุมของเจ้าของข้อมูลส่วนบุคคลนั้น หากการไม่ปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นสร้างความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคลสามารถเรียกร้องค่าเสียหายทางแพ่งได้ตามมาตรา ๗๗

ดังนี้

“มาตรา ๗๗ ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลอันเป็นการฝ่าฝืน หรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะพิสูจน์ได้ว่า

(๑) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง

(๒) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย

ค่าสินไหมทดแทนตามวรรคหนึ่ง ให้หมายความรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย”

ยิ่งไปกว่านั้น พ.ร.บ. ข้อมูลส่วนบุคคลฯ ยังให้อำนาจศาลในการกำหนดค่าสินไหมทดแทนเพื่อการลงโทษได้มากที่สุดถึง ๒ เท่าของค่าเสียหายที่แท้จริง

“มาตรา ๗๘ ให้ศาลมีอำนาจสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจ่ายค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มขึ้นจากจำนวนค่าสินไหมทดแทนที่แท้จริงที่**ศาลกำหนดได้ตามที่ศาลเห็นสมควร แต่ไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริงนั้น** ทั้งนี้ โดยคำนึงถึงพฤติการณ์ต่าง ๆ เช่น ความร้ายแรงของความเสียหายที่เจ้าของข้อมูลส่วนบุคคลได้รับ ผลประโยชน์ที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้รับ สถานะทางการเงินของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล การที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้บรรเทาความเสียหายที่เกิดขึ้น หรือการที่เจ้าของข้อมูลส่วนบุคคลมีส่วนในการก่อให้เกิดความเสียหายด้วย”

เมื่อพิจารณาจากตัวบทข้างต้น ในการเรียกร้องค่าเสียหายเจ้าของข้อมูลส่วนบุคคลจะมีภาระในการพิสูจน์ความเสียหายที่เกิดขึ้น หรือที่ตนได้รับจากการไม่ปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งสอดคล้องกับหลักเรียกร้องความเสียหายจากการละเมิดตามกฎหมายแพ่ง นอกจากนี้ ยังปรากฏแนวทางการตัดสินของศาลสูงภายใต้กฎหมายของสหภาพยุโรปว่าในการเรียกร้องค่าเสียหายจากการไม่ปฏิบัติตามกฎหมายนั้น จำเป็นต้องพิสูจน์ให้เห็นถึงความเสียหายดังกล่าว[๕๗] อย่างไรก็ตาม คำตัดสินของศาลดังกล่าวอยู่ภายใต้กฎหมาย Data Protection Act 1998 ของสหราชอาณาจักร ซึ่งมีการบังคับใช้ในช่วง European Union Data Protection Directive 1995 ในระยะเวลาก่อนที่กฎหมาย GDPR จะมีผลใช้บังคับ ซึ่งส่งผลให้คำตัดสินในอนาคตอาจเปลี่ยนแปลงไปได้ จากแนวทางดังกล่าวอาจทำให้เจ้าของข้อมูลส่วนบุคคลไม่สามารถเรียกร้องค่าเสียหายที่ไม่อาจคิดเป็นตัวเงินได้ ทั้งนี้ จากลักษณะของการขาดมาตรการรักษาความมั่นคงปลอดภัยในการรั่วไหลของข้อมูลส่วนบุคคลนั้นอาจไม่ส่งผลกระทบหรือก่อความเสียหายเป็นตัวเงินในทันที อย่างไรก็ตาม หากมีการรั่วไหลเกิดขึ้นอาจก่อให้เกิดภาระหรือความกังวล หรือความเสียหายในด้านอื่น ๆ ต่อเจ้าของข้อมูลส่วนบุคคลก็ได้ เช่น หากข้อมูลบัตรเครดิตรั่วไหล แม้จะยังไม่มีการใช้จ่ายที่ไม่ชอบด้วยกฎหมายเกิดขึ้น เจ้าของข้อมูลส่วนบุคคลก็ต้องดำเนินการยกเลิกหรือเปลี่ยนบัตรเพื่อความปลอดภัย หรือหากมีข้อมูลที่ใช้ประกอบการยืนยันตัวตนตามกฎหมายได้ เช่น สำเนาบัตรประชาชนรั่วไหล เจ้าของข้อมูลส่วนบุคคลย่อมเกิดความกังวลว่าอาจมีบุคคลนำข้อมูลดังกล่าวไปใช้โดยมิชอบในอนาคตหรือนำไปหลอกลวงบุคคลอื่น ๆ ต่อหรือไม่ ซึ่งแม้ยังไม่เกิดความเสียหายเป็นตัวเงินอย่างชัดเจน แต่เหตุการณ์ดังกล่าวย่อมส่งผลกระทบต่อการใช้ชีวิตของเจ้าของข้อมูลส่วนบุคคล อย่างไรก็ตาม ต้องติดตามแนวทางการตัดสินในอนาคตต่อไปว่ากฎหมายจะให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลในการเรียกร้องให้ชดใช้ความเสียหายในลักษณะนี้หรือไม่ และอย่างไร

[๕๗] **Lloyd v Google: No damages without proof of damage** [Online], 22 July 2022. https://www.shlegal.com/insights/lloyd-v-google-no-damages-without-proof-of-damage.

### ง. ผลกระทบในด้านอื่น ๆ

นอกเหนือไปจากโทษทางกฎหมายที่ได้กล่าวถึงข้างต้น การไม่ปฏิบัติตาม พ.ร.บ. ข้อมูลส่วนบุคคลฯ หรือการรั่วไหลของข้อมูลส่วนบุคคลนั้นย่อมส่งผลกระทบต่อประชาชนในวงกว้าง และตกเป็นที่สนใจของประชาชนที่เป็นเจ้าของข้อมูลส่วนบุคคล ซึ่งย่อมส่งผลต่อความเชื่อมั่นของลูกค้าในการซื้อสินค้าหรือใช้บริการ ซึ่งเป็นความเสียหายที่ไม่อาจแก้ไขเยียวยาได้โดยง่าย

## ขั้นตอนที่ ๖ การจัดเตรียมเอกสาร นโยบาย ขั้นตอน และแนวทางที่เกี่ยวข้องเพื่อให้เป็นไปตามกฎหมาย (PDPA Compliance)

ภายหลังจากการวิเคราะห์ระบุรายละเอียดต่าง ๆ เกี่ยวกับข้อมูลส่วนบุคคลในขั้นตอนที่ ๑ - ๕ ข้างต้น รวมถึงวิเคราะห์ความเสี่ยงที่อาจเกิดขึ้นจากกิจกรรมต่าง ๆ องค์กรจึงสามารถจัดทำเอกสารที่เกี่ยวข้องได้โดยมีรายละเอียดครบถ้วนตามที่กฎหมายกำหนด อาทิ

| ชื่อเอกสาร | มาตราอ้างอิง |
|---|---|
| หนังสือขอยินยอม (Consent Form) | ๑๙, ๒๔, ๒๖ |
| ประกาศแจ้งการประมวลผลข้อมูลส่วนบุคคล (Privacy Notice) | ๒๓ |
| แบบฟอร์มการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Right Form) | ๑๙ วรรคห้า, ๓๐ ถึง ๓๕, ๗๓ วรรคหนึ่ง |
| นโยบายการกำหนดระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคล และแนวทางการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา (Retention Policy) | ๓๗ (๓) |
| นโยบายและกระบวนการจัดการปัญหาเมื่อเกิดการละเมิด หรือการรั่วไหลของข้อมูลส่วนบุคคล (Personal Data Breach Procedure / Policy) | ๓๗ (๔) |
| แบบบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (Record of Data Processing Activities) | ๓๙ |
| สัญญาประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) | ๔๐ |
| หนังสือแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และสำนักงาน | ๔๑ |

นอกเหนือไปจากการดำเนินการเกี่ยวกับเอกสารที่เกี่ยวข้องข้างต้น ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลยังต้องให้ความสำคัญกับกระบวนการภายในต่าง ๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เช่น การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสม ทั้งในด้านมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย[๕๘]

นอกจากนี้ ยังต้องให้ความสำคัญกับการสร้างเสริมความตระหนักรู้ ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย และการแจ้งให้บุคลากร พนักงาน ลูกจ้าง หรือบุคคลอื่นที่เกี่ยวข้องทราบและถือปฏิบัติ ทั้งนี้ เนื่องจากผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นนิติบุคคลอาจต้องรับผิดจากการไม่ปฏิบัติตามกฎหมายของลูกจ้างหรือบุคลากรที่เกี่ยวข้องด้วย

ทั้งนี้ มีข้อควรระวังว่า การจัดให้มีเอกสารที่ครบถ้วนเพียงอย่างเดียว โดยเฉพาะการนำต้นแบบมาจากองค์กรอื่น ๆ นั้น ย่อมไม่เพียงพอต่อการดำเนินการเพื่อปฏิบัติตาม พ.ร.บ. ข้อมูลส่วนบุคคลฯ การจัดทำเอกสารต่าง ๆ นั้นเป็นเพียงผลลัพธ์ที่ต้องจัดทำขึ้นโดยอาศัยการระบุและทบทวนรายละเอียดของกิจกรรมที่เกี่ยวข้องกับการใช้ข้อมูลส่วนบุคคลขององค์กร ซึ่งเอกสารนั้นต้องมีองค์ประกอบตามที่กฎหมายกำหนดให้ครบถ้วน และมีรายละเอียดที่ถูกต้องตรงกับการดำเนินงานของแต่ละองค์กร ซึ่งเป็นสิ่งที่แต่ละองค์กรมีไม่เหมือนกันและไม่สามารถลอกเลียนกันได้ การศึกษาและเตรียมความพร้อมการปฏิบัติตามกฎหมาย โดยอย่างน้อยการดำเนินการตามขั้นตอนที่ผู้เขียนแจกแจงหรือการปรึกษาผู้เชี่ยวชาญนั้น ย่อมสามารถลดความเสี่ยงจากการละเมิดกฎหมายโดยไม่เจตนาที่อาจเกิดขึ้นได้

---

[๕๘] ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕.

## บทสรุปและข้อเสนอแนะ

ในมุมมองของนักกฎหมายหรือผู้ใช้กฎหมาย พ.ร.บ. ข้อมูลส่วนบุคคลฯ เป็นกฎหมายเฉพาะที่มีวัตถุประสงค์เฉพาะเรื่องอย่างชัดเจน จึงทำให้ตัวบทกฎหมายมีหลายส่วนที่ใช้ถ้อยคำที่ไม่ตรงกับกฎหมายอื่น ๆ หรือไม่ตรงกับความหมายทั่วไป ด้วยเหตุนี้ การตีความตามความหมายของกฎหมายอื่นอาจทำให้ไม่สามารถบรรลุถึงเจตนารมณ์ของกฎหมายได้อย่างครบถ้วน นักกฎหมายจึงต้องอาศัยความเข้าใจถึงรากฐานและเจตนารมณ์ของ พ.ร.บ. ข้อมูลส่วนบุคคลฯ เป็นสำคัญ

เนื่องด้วย พ.ร.บ. ข้อมูลส่วนบุคคลฯ ได้รับหลักการและนำบทบัญญัติส่วนใหญ่มาจากกฎหมาย GDPR ซึ่งมีการบังคับใช้มาก่อนแล้ว การศึกษาแนวการวินิจฉัยของหน่วยงานกำกับดูแล และกรณีศึกษาในต่างประเทศจะเป็นส่วนช่วยในการทำความเข้าใจการตีความและบังคับใช้กฎหมายได้ดีมากยิ่งขึ้น และอาจนำมาเป็นรากฐานในการให้คำแนะนำ หรือปรับกับการบังคับใช้กฎหมายในประเทศไทยต่อไป

ในมุมมองของผู้ประกอบการ การใช้ข้อมูลส่วนบุคคลในปัจจุบันมีส่วนเพิ่มโอกาสในการต่อยอดทางธุรกิจอย่างมีนัยสำคัญ ผู้ประกอบการจำนวนมากจึงมีโอกาสที่จะเป็นผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล หรือมีโอกาสที่จะดำเนินการประมวลผลเกี่ยวกับข้อมูลส่วนบุคคลในอนาคต การศึกษาและปฏิบัติตาม พ.ร.บ. ข้อมูลส่วนบุคคลฯ จึงเป็นสิ่งที่ไม่อาจหลีกเลี่ยงได้

และในลำดับสุดท้าย เจตนารมณ์ที่สำคัญที่สุดของ พ.ร.บ. ข้อมูลส่วนบุคคลฯ คือการมุ่งปกป้องสิทธิของประชาชนทุกคนในฐานะเจ้าของข้อมูลส่วนบุคคลจากการสูญเสียการควบคุมเหนือข้อมูลส่วนบุคคลของตนเอง หรือจากการถูกเอาข้อมูลส่วนบุคคลไปใช้หาประโยชน์โดยไม่ชอบด้วยกฎหมาย การศึกษากฎหมายฉบับนี้จะทำให้เจ้าของข้อมูลส่วนบุคคลรับรู้ถึงสิทธิของตนเอง และเป็นประโยชน์ในการป้องกันตนเองจากการถูกเอาเปรียบหรือป้องกันผลกระทบจากการถูกนำข้อมูลส่วนบุคคลของตนเองไปใช้โดยที่ไม่ต้องการได้