# ข้อมูลเบื้องต้นเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (the General Data Protection Regulation (GDPR))

*นายรักไท เทพปัญญา*[†]

**๑. ความนำ**

ในช่วงปลายเดือนพฤษภาคมที่ผ่านมา หลายท่านอาจได้รับอีเมล์ซึ่งมีเนื้อหาทำนองว่า “เราได้ทำการปรับปรุงนโยบายเกี่ยวกับความเป็นส่วนตัวของบริษัทเพื่อให้เป็นไปโดยสอดคล้องกับ the EU General Data Protection Regulation (GDPR)” หรือ “หากท่านประสงค์ที่จะได้รับจดหมายข่าวจากเราต่อไป ขอให้ท่านตอบตกลงโดยคลิกที่แถบด้านล่างนี้” (ผู้เขียนบทความก็ได้รับอีเมล์ในลักษณะดังกล่าวเช่นเดียวกันจากบริษัทซอฟต์แวร์แอนตี้ไวรัส บริษัทดาวน์โหลดเกมส์ในรูปแบบดิจิทัล และจากผู้ให้คำแนะนำการเล่นกีตาร์ทางออนไลน์) และหากท่านผู้อ่านได้สังเกตในระยะสองถึงสามเดือนที่ผ่านมาอาจพบว่ามีการกล่าวถึงสิ่งที่เรียกว่า GDPR ในสังคมออนไลน์อยู่บ่อยครั้งโดยเฉพาะเพจบนโซเชียลเน็ตเวิร์คของสื่อชื่อดังต่างประเทศ และแม้กระทั่งในประเทศไทยเองก็ปรากฏว่ามีการลงบทความเกี่ยวกับ GDPR หลายบทความ ไม่ว่าจะในสื่อกระแสหลักอย่างมติชน ไทยรัฐ หรือเนชั่นมัลติมีเดีย หรือสื่อทางเลือกอย่าง the Standard หรือ Blognone ก็ตาม นอกจากนี้ ในวงวิชาการเองก็มีความตื่นตัวต่อ GDPR เช่นเดียวกัน โดยผู้เขียนบทความได้มีโอกาสเข้าร่วมรับฟังการเสวนาในเรื่องนี้ที่จัดขึ้นโดยมหาวิทยาลัยชั้นนำของประเทศถึงสามครั้งในช่วงหนึ่งเดือนที่ผ่านมา ซึ่งก่อนที่จะกล่าวไปถึงว่าเหตุใด GDPR จึงได้รับความสนใจมากในระยะหลัง ผู้เขียนบทความจะขอกล่าวในเบื้องต้นเสียก่อนว่าอะไรคือ GDPR

GDPR นั้นเป็นชื่อที่ย่อมาจาก “the General Data Protection Regulation” ซึ่งเป็นกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ทั้งนี้ ก่อนหน้าที่จะมี GDPR หลักเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปจะเป็นไปตาม EU Directive 95/46/ec ซึ่งความแตกต่างระหว่าง Directive กับ Regulation ก็คือ กรณีแรกนั้น ประเทศสมาชิกจะต้องนำมาตรการต่าง ๆ ที่ Directive กำหนดไว้มาบรรจุในกฎหมายภายในของรัฐเพื่อให้บรรลุตามวัตถุประสงค์ของ Directive นั้น ๆ แต่สำหรับกรณีของ Regulation เมื่อมีผลใช้บังคับแล้วจะมีผลบังคับทางกฎหมายต่อทุกประเทศสมาชิกโดยทันที ไม่จำต้องมีการนำไปบัญญัติไว้ในกฎหมายภายในของรัฐแต่อย่างใด[๑] สำหรับวัตถุประสงค์ของ GDPR นั้น ก็เพื่อให้ความคุ้มครองบุคคลธรรมดาในเรื่องเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล ตลอดจนเพื่อการเคลื่อนไหวโดยเสรีของข้อมูล ซึ่งมีการกล่าวว่า กฎหมายนี้เป็นก้าวย่างสำคัญที่จะเสริมสร้างความแข็งแกร่งให้แก่สิทธิขั้นพื้นฐานของ

---

[†]นักกฎหมายกฤษฎีกาชำนาญการ ฝ่ายกฎหมายการศึกษาขั้นพื้นฐานและการกีฬา สำนักงานคณะกรรมการกฤษฎีกา (กรกฎาคม ๒๕๖๑)

[๑]เว็บไซต์คณะกรรมาธิการยุโรป https://ec.europa.eu/info/law/law-making-process/types-eu-law_en

พลเมืองในยุคดิจิทัลและเอื้ออำนวยความสะดวกให้แก่ภาคธุรกิจโดยทำให้กฎเกณฑ์ต่าง ๆ ง่ายขึ้นสำหรับบริษัทในตลาดร่วมด้านดิจิทัล (digital single market)[๒]

อนึ่ง ในปัจจุบันกฎหมายฉบับนี้มีผลใช้บังคับแล้วเมื่อวันที่ ๒๕ พฤษภาคม ๒๕๖๑ ที่ผ่านมา

**๒. ผลบังคับใช้นอกเขตแดนและค่าปรับทางปกครอง "เหตุแห่งความตื่นตัว"**

ขณะนี้เราทราบแล้วว่า GDPR คือกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป แต่ผู้อ่านบทความก็อาจตั้งคำถามในใจว่า ในเมื่อ GDPR เป็นกฎหมายของสหภาพยุโรปไม่ใช่กฎหมายไทยแล้วเหตุใดเราถึงต้องให้ความสนใจ GDPR ด้วย ซึ่งเหตุที่ทั่วโลกรวมทั้งในประเทศไทยเองให้ความสนใจกับ GDPR นั้นก็เพราะว่า แม้ GDPR จะเป็นกฎหมายของสหภาพยุโรปก็ตาม แต่สภาพบังคับของ GDPR ไม่ได้จำกัดอยู่แค่ภายในสหภาพยุโรปเท่านั้น โดยหากเราพิจารณา Article 3 ของ GDPR ซึ่งเป็นบทบัญญัติที่กำหนดขอบเขตการบังคับใช้เชิงพื้นที่ของ GDPR เอาไว้ก็จะพบว่า GDPR จะนำมาใช้บังคับกับ

(๑) การประมวลผลข้อมูลส่วนบุคคลที่อยู่ในบริบทของกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ในสหภาพยุโรป ไม่ว่าการประมวลผลดังกล่าวจะเกิดขึ้นในสหภาพยุโรปหรือไม่ (Art. 3 1.) และ

(๒) การประมวลผลข้อมูลส่วนบุคคลที่กระทำโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่นอกสหภาพยุโรป แต่เจ้าของข้อมูลส่วนบุคคลที่ข้อมูลของตนถูกประมวลผลนั้นอยู่ในสหภาพยุโรป และการประมวลผลนั้นเป็นการ ๑) เสนอสินค้าหรือบริการโดยมิพักต้องคำนึงว่าจะมีการชำระราคากันหรือไม่ หรือ ๒) เป็นการเฝ้าสังเกตพฤติกรรมของเจ้าของข้อมูลที่เกิดขึ้นในสหภาพยุโรป (Art. 3 2.)[๓]

จากขอบเขตการบังคับใช้เชิงพื้นที่ข้างต้น จะเห็นได้ว่า ผู้ที่ทำการประมวลผลข้อมูลส่วนบุคคลที่แม้ว่าตัวจะตั้งอยู่ในประเทศไทย แต่ก็อาจจะต้องตกอยู่ภายใต้บังคับของ GDPR ด้วย จากบทบัญญัติดังกล่าวแล้ว หากเราพิจารณากรณีตัวอย่างดังต่อไปนี้

*<u>กรณีตัวอย่างที่ ๑</u> บริษัทผู้ให้บริการสายการบินที่มีสำนักงานสาขาตั้งอยู่ในประเทศที่เป็นสมาชิกสหภาพยุโรป จะตกอยู่ภายใต้บังคับของ GDPR หรือไม่*

กรณีตามตัวอย่างที่ ๑ หากพิจารณาตาม (๑) ข้างต้นแล้ว ย่อมถือได้ว่าบริษัทผู้ให้บริการสายการบินดังกล่าวเป็นผู้ที่ทำการประมวลผลข้อมูลส่วนบุคคลที่ตั้งอยู่ในสหภาพยุโรปและต้องอยู่ภายใต้บังคับของ GDPR

---

[๒] เว็บไซต์คณะกรรมาธิการยุโรป https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

[๓] นอกจากนี้ GDPR ยังใช้บังคับกับการประมวลผลข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ไม่ได้ตั้งอยู่ในสหภาพยุโรป แต่อยู่ในสถานที่ซึ่งกฎหมายของประเทศสมาชิกจะต้องนำมาใช้ด้วยโดยผลของกฎหมายมหาชนระหว่างประเทศ (Art. 3 3.)

*<u>กรณีตัวอย่างที่ ๒</u> ผู้ประกอบกิจการร้านค้าออนไลน์ที่ตั้งอยู่ในประเทศไทยชื่อว่า "Ultimativ Thaiboxen" ซึ่งขายสินค้าเกี่ยวกับมวยไทย เช่น กางเกงมวยไทย และคลิปวีดีโอสอนแม่ไม้มวยไทยที่ผู้รับชมสามารถเลือกซับไตเติ้ลได้สามภาษาระหว่างภาษาอังกฤษ เยอรมัน และ ฝรั่งเศส โดยภาษาที่ใช้ในร้านค้าออนไลน์ดังกล่าวมีทั้งภาษาอังกฤษ เยอรมัน และฝรั่งเศส เช่นกัน และในร้านค้ามีการระบุข้อมูลเกี่ยวกับการจัดส่งสินค้าไปยังประเทศในสหภาพยุโรป และใช้เงินสกุลยูโรในการทำธุรกรรม นอกจากนี้ ทางร้านค้าได้เก็บรวบรวมข้อมูลชื่อ ที่อยู่ อายุ ตลอดจนประวัติสินค้าที่สั่งซื้อของลูกค้าเพื่อใช้ในการเสนอขายสินค้าใหม่ ๆ ต่อไป เช่นนี้ ร้านค้าออนไลน์นี้จะต้องปฏิบัติตาม GDPR หรือไม่*

สำหรับกรณีตามตัวอย่างที่ ๒ นั้น หากพิจารณาตาม (๒) แล้ว ก็อาจถือได้ว่าร้านค้าออนไลน์ "Ultimativ Thaiboxen" ได้ทำการประมวลผลข้อมูลส่วนบุคคลที่เป็นการเสนอสินค้าให้กับผู้ที่อยู่ในสหภาพยุโรปแล้วและย่อมต้องอยู่ในบังคับของ GDPR

ลำพังผลบังคับใช้นอกเขตพื้นที่ของ GDPR เพียงอย่างเดียวอาจยังไม่สามารถสร้างความตื่นตระหนกกังวลให้แก่หน่วยธุรกิจต่าง ๆ ทั้งในประเทศไทยและประเทศนอกสหภาพยุโรปได้ อย่างไรก็ตาม GDPR ได้มีการกำหนดความรับผิดสำหรับการฝ่าฝืนบทบัญญัติของ GDPR เอาไว้ปรากฏอยู่ในหมวด ๘ การเยียวยา ความรับผิด และโทษ (Remedies, liability and penalties) ซึ่งมาตรการบังคับสำหรับการฝ่าฝืน GDPR นั้นมีทั้งกรณีที่ผู้ฝ่าฝืนจะต้องชดใช้ค่าสินไหมทดแทนสำหรับความเสียหายที่เจ้าของข้อมูลส่วนบุคคลได้รับ (Art. 82 1.) และกรณีที่ผู้ฝ่าฝืนจะต้องชำระค่าปรับทางปกครอง (administrative fine) **ซึ่งการฝ่าฝืนบทบัญญัติบางกรณีมีโทษปรับทางปกครองสูงสุดเป็นจำนวนเงินสูงถึงไม่เกิน ๑๐ ล้านยูโร หรือไม่เกินร้อยละ ๒ ของรายได้รวมจากทั่วโลกในรอบปี (worldwide annual turnover) แล้วแต่ว่าจำนวนใดจะสูงกว่ากัน (Art. 83 4.) และบางกรณีมีโทษปรับทางปกครองสูงสุดเป็นจำนวนเงินถึงไม่เกิน ๒๐ ล้านยูโร หรือไม่เกินร้อยละ ๔ ของรายได้รวมจากทั่วโลกในรอบปี แล้วแต่ว่าจำนวนใดจะสูงกว่ากัน (Article 83 5.)** อย่างไรก็ดี ในทางปฏิบัติก็ยังมีข้อน่าพิจารณาว่าสำหรับกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลอยู่นอกสหภาพยุโรปแล้วจะทำการบังคับตามค่าปรับดังกล่าวอย่างไร

ด้วยผลบังคับใช้นอกเขตพื้นที่และโทษปรับทางปกครองที่มีเพดานค่าปรับเป็นจำนวนที่สูงเป็นอย่างมาก จึงทำให้เกิดข้อกังวลอย่างมากแก่ผู้ที่อยู่ในขอบข่ายอาจต้องอยู่ในบังคับของ GDPR ถึงขนาดที่ในช่วงระยะเวลาก่อนที่ GDPR จะมีผลบังคับ ปรากฏว่ามีเว็บไซต์หลายแห่งระงับการให้บริการแก่ผู้ที่อยู่ในสหภาพยุโรป[๔] ซึ่งมีตัวอย่างของข้อความที่แสดงบนเว็บไซต์บางแห่งสำหรับผู้ใช้บริการที่อยู่ในสหภาพยุโรปว่า[๕]

*"เป็นที่น่าเสียดายว่าในขณะนี้เว็บไซต์ของพวกเราไม่สามารถเข้าอ่านได้สำหรับประเทศส่วนใหญ่ในทวีปยุโรป เรากำลังเผชิญหน้ากับปัญหาและมีความมุ่งมั่นที่จะพิจารณาทางเลือกเพื่อสนับสนุนการให้บริการในรูปแบบดิจิทัลอย่างเต็มรูปแบบในตลาดสหภาพยุโรปได้ เราจะหาหนทางดำเนินการให้*

[๔] ข้อมูลจากเว็บไซต์สำนักข่าว the Guardian https://www.theguardian.com/technology/2018/may/24/sites-block-eu-users-before-gdpr-takes-effect

[๕] ข้อมูลจากเว็บไซต์สำนักข่าว the Guardian https://www.theguardian.com/technology/2018/may/25/gdpr-us-based-news-websites-eu-internet-users-la-times

*สอดคล้องกับกฎเกณฑ์ทางเทคนิคต่อไปเพื่อที่จะให้บริการแก่ผู้อ่านทุกท่าน ด้วยความเป็นสื่อมวลชนระดับชนะรางวัลของเรา”*

อย่างไรก็ดี แม้ GDPR จะมีขอบเขตการบังคับใช้ขยายออกไปนอกพื้นที่สหภาพยุโรป และมีการกำหนดโทษปรับทางปกครองที่มีโทษสูงสุดเป็นจำนวนที่สูงมาก แต่สำหรับบุคคลธรรมดาที่ใช้ข้อมูลส่วนบุคคลตามปกติชีวิตประจำวันก็ไม่จำต้องเป็นกังวลกับการปฏิบัติตาม GDPR แต่อย่างใด เนื่องจากกฎหมายนี้ไม่นำมาใช้กับการประมวลผลข้อมูลส่วนบุคคลที่กระทำโดยบุคคลธรรมดาที่เป็นกิจกรรมส่วนตัวหรือเป็นกิจกรรมภายในครัวเรือนโดยแท้ ซึ่งกิจกรรมดังกล่าวอาจรวมไปถึงการติดต่อกันทางจดหมาย การเก็บข้อมูลที่อยู่ หรือการใช้โซเชียลเนทเวิร์คและกิจกรรมออนไลน์ต่าง ๆ ที่อยู่ในบริบทของกิจกรรมดังกล่าว[๖] นอกจากนี้ GDPR ยังไม่นำมาบังคับใช้กับการดำเนินการโดยเจ้าหน้าที่ของรัฐซึ่งมีอำนาจหน้าที่เพื่อการป้องกัน สอบสวน (investigation) สืบสวน (detection) การดำเนินคดีอาญา การบังคับใช้โทษอาญา รวมทั้งการป้องกันภัยคุกคามต่อความปลอดภัยสาธารณะอีกด้วย (Art. 2)

**๓. เนื้อหาโดยสังเขปของ GDPR**

หากกล่าวถึงสาระสำคัญของ GDPR แบบกว้าง ๆ แล้ว อาจกล่าวได้ว่า GDPR เป็นกฎหมายที่คุ้มครองบุคคลธรรมดาเกี่ยวกับการที่ข้อมูลส่วนบุคคลของตนจะถูกประมวลผล ทั้งนี้หากพิจารณาจาก GDPR ทั้งฉบับแล้วจะพบว่ากฎหมายนี้มีเนื้อหาค่อนข้างยาว ลำพังเพียงแค่บทนำ (recital) ก่อนที่จะถึงบทบัญญัติของ GDPR ก็มีจำนวนถึง ๑๗๓ ข้อ สำหรับในส่วนบทบัญญัติของ GDPR เองก็มีความยาวถึง ๙๙ มาตรา แบ่งออกเป็น ๑๑ หมวด ซึ่งมีเนื้อหาต่าง ๆ เช่น

- หมวด ๒ หลักการทั่วไป ซึ่งกำหนดเรื่องต่าง ๆ เช่น หลักการในการประมวลผลข้อมูลส่วนบุคคล (Art. 5) ฐานที่ทำให้การประมวลผลชอบด้วยกฎหมาย (Art. 6) เงื่อนไขในการขอความยินยอม (Art. 7) การประมวลผลข้อมูลส่วนบุคคลที่มีลักษณะพิเศษ (Art. 9) เป็นต้น
- หมวด ๓ สิทธิของเจ้าของข้อมูลส่วนบุคคล ซึ่งกำหนดสิทธิต่าง ๆ ของเจ้าของข้อมูลส่วนบุคคลเอาไว้ เช่น สิทธิที่จะลบ (หรือสิทธิที่จะถูกลืม) (right to erasure (right to be forgotten)) (Art. 17) หรือสิทธิที่จะโอนย้ายข้อมูล (data portability) (Art. 18) เป็นต้น
- หมวด ๔ ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งกำหนดเรื่องต่าง ๆ เกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล เช่น ภาระหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (Section 1) ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (Section 2) การประเมินผลกระทบต่อความเป็นส่วนตัว (Section 3) หรือการจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data protection officer หรือ DPO) (Section 4) เป็นต้น
- หมวด ๕ การโอนข้อมูลส่วนบุคคลไปยังประเทศที่สามหรือองค์การระหว่างประเทศ ซึ่งกำหนดหลักเกณฑ์เกี่ยวกับการโอนข้อมูลส่วนบุคคลข้ามดินแดน

[๖] Recital 18

ออกไปนอกสหภาพยุโรปว่าจะสามารถทำได้ในกรณีใดบ้าง และภายใต้เงื่อนไขอย่างไร

- หมวด ๖ หน่วยงานอิสระที่ทำหน้าที่กำกับดูแล (Independent supervisory authorities) หรือ
- หมวด ๘ การเยียวยา ความรับผิด และโทษ (Remedies, liability and penalties) เป็นต้น

ที่กล่าวมาข้างต้นเป็นเพียงบางหมวดของ GDPR เท่านั้น และเนื่องจากเนื้อหาของ GDPR นั้นยาวและมีรายละเอียดมาก ในบทความนี้จึงจะกล่าวถึงเนื้อหาเพียงบางเรื่องพอสังเขป ได้แก่ (๑) นิยามศัพท์ที่สำคัญ (๒) หลักการในการประมวลผลข้อมูลส่วนบุคคล (๓) ฐานที่ทำให้การประมวลผลชอบด้วยกฎหมาย (๔) สิทธิของเจ้าของข้อมูลส่วนบุคคล และ (๕) การโอนข้อมูลไปยังประเทศที่สาม ทั้งนี้ นอกจากเรื่องต่าง ๆ เหล่านี้แล้ว GDPR ก็ยังกำหนดหลักเกณฑ์ในเรื่องอื่น ๆ ที่มีความสำคัญเช่นเดียวกัน เช่น การประมวลผลข้อมูลส่วนบุคคลที่มีลักษณะพิเศษเฉพาะซึ่งการประมวลผลข้อมูลเหล่านี้จะมีหลักเกณฑ์เพิ่มเติม หรือการจัดตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data protection officer (DPO)) ในองค์กรเพื่อทำหน้าที่ต่าง ๆ เช่น ดูแลการดำเนินการขององค์กรนั้นให้สอดคล้องกับ GDPR มีบทบาทในการช่วยเหลือผู้ควบคุมข้อมูลส่วนบุคคลในการประเมินความเสี่ยงผลกระทบต่อข้อมูลส่วนบุคคล (Data protection impact assessment) หรือให้ความร่วมมือและประสานกับหน่วยงานผู้กำกับดูแล เป็นต้น[๗] ซึ่งผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลบางจำพวก เช่น หน่วยงานของรัฐ (public authorities) องค์กรที่กิจกรรมหลักเป็นการเฝ้าติดตามพฤติกรรมของบุคคลเป็นจำนวนมากอย่างเป็นระบบ หรือองค์กรที่ทำการประมวลผลข้อมูลส่วนบุคคลที่มีลักษณะพิเศษเป็นจำนวนมาก จะต้องจัดตั้ง DPO ขึ้นในองค์กรของตนด้วย เป็นต้น[๘]

**(๓.๑) นิยามศัพท์ที่สำคัญ**

บทนิยามของ GDPR ปรากฏอยู่ใน Article 4 ซึ่งมีการกำหนดนิยามไว้ถึง ๒๖ คำ แต่โดยที่วัตถุประสงค์ของบทความนี้คือเพื่อให้ผู้อ่านได้ทราบข้อมูลเบื้องต้นของ GDPR เท่านั้น ในที่นี้จึงจะขอกล่าวถึงแต่เพียงความหมายของ “ข้อมูลส่วนบุคคล” เพื่อให้ทราบว่าข้อมูลประเภทใดบ้างที่จะอยู่ภายใต้ GDPR “การประมวลผลข้อมูลส่วนบุคคล” เพื่อให้ทราบว่าการดำเนินการอย่างไรกับข้อมูลส่วนบุคคลที่จะต้องเป็นไปตามกฎเกณฑ์ของกฎหมายนี้ และความหมายของตัวละครที่สำคัญใน GDPR ซึ่งได้แก่ “ผู้ควบคุมข้อมูลส่วนบุคคล” และ “ผู้ประมวลผลข้อมูลส่วนบุคคล” ดังนี้

<u>๑) ข้อมูลส่วนบุคคล (personal data)</u>

ตาม Article 4 (1) ได้ให้ความหมายของ “ข้อมูลส่วนบุคคล” เอาไว้ได้แก่ ข้อมูลใด ๆ ก็ตามที่เกี่ยวข้องกับบุคคลธรรมดาที่ระบุตัว หรืออาจถูกระบุตัวบุคคลผู้นั้นได้ ซึ่งการที่ข้อมูลนั้น “อาจระบุตัวบุคคลได้” จะเป็นโดยทางตรงหรือทางอ้อมก็ได้ โดยอาศัยสิ่งบ่งชี้ (identifier) ต่าง ๆ ซึ่งอาจเป็น ชื่อ หมายเลขประจำตัวประชาชน ที่อยู่ เอกลักษณ์ออนไลน์ (online

---

[๗] Article 29 Data Protection Working Party, Guidelines on Data Protection Officers (DPO), p. 17-18.

[๘] เพิ่งอ้าง, หน้า ๔.

identifier) หรือเอกลักษณ์ทางร่างกายอย่างใดอย่างหนึ่ง ลักษณะทางกายภาพ พันธุกรรม จิตใจ เศรษฐกิจ วัฒนธรรม หรือสังคมของบุคคล นั้น เป็นต้น

การที่จะพิจารณาว่าข้อมูลนั้นสามารถบ่งชี้หรือระบุตัวบุคคลได้หรือไม่ จะต้องพิจารณาว่าข้อมูลดังกล่าวทำให้สามารถบรรยายถึงบุคคลนั้นในประการที่จะแบ่งแยกบุคคลนั้นออกจากบุคคลอื่น ๆ และสามารถจดจำบุคคลนั้นในฐานะปัจเจกบุคคลได้หรือไม่ ตัวอย่างที่สำคัญของสิ่งบ่งชี้อย่างหนึ่งคือชื่อของบุคคล ซึ่งชื่อนั้นเป็นสิ่งที่สามารถระบุตัวบุคคลได้โดยตรง[๙] นอกจากนี้ หมายเลข IP address หรือการใช้คุกกี้บนเว็บไซต์[๑๐] ก็เป็นสิ่งที่สามารถบ่งชี้ตัวบุคคลได้เช่นเดียวกัน[๑๑] แต่สำหรับข้อมูลที่ไม่ระบุชื่อเจ้าของข้อมูล (anonymous information) ซึ่งเป็นข้อมูลที่ไม่เกี่ยวข้องกับบุคคลที่ถูกระบุตัวหรือที่อาจระบุตัวบุคคลได้ หรือข้อมูลไม่ระบุชื่อที่ไม่สามารถระบุตัวเจ้าของข้อมูลได้อีกต่อไป ก็จะไม่อยู่ภายใต้ของหลักการตามกฎหมายนี้[๑๒] นอกจากนี้ กฎหมายนี้ยังไม่นำมาใช้บังคับกับข้อมูลของบุคคลที่ถึงแก่กรรมแล้วด้วย[๑๓]

๒) <u>การประมวลผล (processing)</u>

ความหมายของถ้อยคำนี้ปรากฏอยู่ใน Article 4 (2) ซึ่งได้กำหนดความหมายเอาไว้โดยมีขอบเขตที่กว้างมาก โดยหมายความว่า การดำเนินการหรือชุดของการดำเนินการที่ทำต่อข้อมูลส่วนบุคคลหรือชุดของข้อมูลส่วนบุคคล ทั้งนี้ ไม่ว่าการดำเนินการดังกล่าวจะอาศัยวิธีการอัตโนมัติ (automated mean) หรือวิธีการไม่อัตโนมัติ (manual) ก็ตาม เช่น การเก็บรวบรวม บันทึก จัดกลุ่ม จัดวางโครงสร้าง เก็บ ปรับปรุงหรือเปลี่ยนแปลง การกู้คืน ค้นหา (consultation) ใช้ เปิดเผยโดยการโอน (disclosure by transmission) เผยแพร่หรือทำให้เข้าถึงได้ จัดเรียงหรือควบรวม (alignment or combination) จำกัด (restriction) ลบ (erasure) หรือทำลาย (destruction) เป็นต้น ซึ่งหากพิจารณาจากนิยามนี้แล้ว กรณีที่บริษัทได้ทำการเก็บรวบรวมข้อมูลต่าง ๆ ของลูกค้า เช่น ชื่อ เพศ อายุ และรายการสินค้าที่เคยสั่งซื้อไว้ในระบบคอมพิวเตอร์ และนำข้อมูลดังกล่าวมาจัดกลุ่มลูกค้าตามความสนใจในสินค้าแต่ละประเภท ก็ถือได้ว่าบริษัทนั้นทำการประมวลผลข้อมูลส่วนบุคคลแล้ว

<u>๓) ผู้ควบคุมข้อมูลส่วนบุคคล (controller) และผู้ประมวลผลข้อมูลส่วนบุคคล (processor)</u>

การพิจารณาว่าผู้ใดเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นมีความสำคัญ เนื่องจากบุคคลดังกล่าวมีหน้าที่ตาม GDPR ที่จะต้องปฏิบัติแตกต่างกัน เช่น ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่จะต้องเก็บบันทึกกิจกรรมการประมวลผลข้อมูลของตนเพื่อแสดงว่าตนได้ปฏิบัติตามหน้าที่ที่กำหนดใน GDPR แล้ว (Art. 30 (2)) เป็นต้น

ทั้งนี้ Article 4 (7) ได้กำหนดความหมายของ *“ผู้ควบคุมข้อมูลส่วนบุคคล”* เอาไว้หมายความถึง **ผู้ที่ทำการตัดสินใจเกี่ยวกับวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล** โดยผู้นี้จะเป็นบุคคลธรรมดาหรือนิติบุคคลก็ได้ และอาจเป็นหน่วยงานของรัฐ

---

[๙]European Union Agency for Fundamental Rights (FRA), Handbook on European data protection law, 2018 edition, p. 89.

[๑๐]หมายความถึงข้อมูลขนาดเล็กบนเว็บไซต์ที่ส่งเข้ามาเก็บไว้ในเครื่องคอมพิวเตอร์ของผู้ที่เข้าชมเว็บไซต์นั้น

[๑๑]ICO. Information Commissioner’s Office, Guide to the General Data Protection Regulation (GDPR), p. 11.

[๑๒]Recital 26

[๑๓]Recital 27

(public authority) เจ้าหน้าที่ (agency) หรือองค์กรอื่น ๆ (other body) ก็ได้ ในขณะที่ *"ผู้ประมวลผลข้อมูลส่วนบุคคล"* มีการกำหนดความหมายเอาไว้ใน Article 4 (8) ว่า บุคคลธรรมดา หรือนิติบุคคล หน่วยงานของรัฐ (public authority) เจ้าหน้าที่ (agency) หรือองค์กรอื่น ๆ (other body) **ที่ทำการประมวลผลข้อมูลส่วนบุคคลในนามของผู้ควบคุมข้อมูลส่วนบุคคล** (on behalf of the controller) จากนิยามดังกล่าว เราอาจกล่าวได้ว่า ผู้ควบคุมข้อมูลส่วนบุคคลจะเป็นผู้ที่ตัดสินใจว่าเพราะเหตุใดจึงประมวลผลข้อมูลส่วนบุคคล และด้วยวิธีการอย่างไร[๑๔] ในขณะที่ผู้ประมวลผลข้อมูลส่วนบุคคลเป็นผู้ที่ประมวลผลตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล เช่น บริษัท ก. ทำสัญญาจ้างบริษัท ข. เพื่อดูแลเกี่ยวกับการจ่ายเงินเดือนให้แก่พนักงานในบริษัทของตน ซึ่งจะต้องมีการเก็บรวบรวมข้อมูลต่าง ๆ ไม่ว่าจะเป็นชื่อ ตำแหน่ง อัตราเงินเดือน โดยบริษัท ข. จะดำเนินการดังกล่าวตามข้อกำหนดในสัญญาที่ทำขึ้นกับ บริษัท ก. เช่นนี้ บริษัท ก. เป็นผู้ควบคุมข้อมูลส่วนบุคคล ในขณะที่บริษัท ข. เป็นผู้ประมวลผลข้อมูลส่วนบุคคล

**(๓.๒) หลักการในการประมวลผลตาม GDPR (Art. 5)**

ใน Article 5 ของ GDPR ได้กำหนดหลักการเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลไว้หลายประการ ซึ่งหลักการดังกล่าวได้แก่

๑) หลักความชอบด้วยกฎหมาย เป็นธรรม และโปร่งใส (lawfulness, fairness and transparency) กล่าวคือ การประมวลผลข้อมูลส่วนบุคคลจะต้องเป็นไปโดยชอบด้วยกฎหมาย อย่างเป็นธรรม และในประการที่โปร่งใส (Art 5 1. (a)) ซึ่งการประมวลผลอย่างไรที่จะถือได้ว่าชอบด้วยกฎหมาย เป็นธรรม และโปร่งใส ก็จะต้องพิจารณาจากบทบัญญัติอื่น ๆ ของ GDPR ต่อไป

๒) หลักข้อจำกัดตามวัตถุประสงค์ (purpose limitation) กล่าวคือ การเก็บรวบรวมข้อมูลส่วนบุคคลต้องเป็นไปเพื่อวัตถุประสงค์ที่เฉพาะเจาะจง แจ้งชัด และชอบด้วยกฎหมาย และข้อมูลดังกล่าวจะไม่ถูกนำไปประมวลผลในวัตถุประสงค์ที่แตกต่างจากวัตถุประสงค์ข้างต้น (Art. 5 1. (b))

๓) หลักการใช้ข้อมูลให้น้อยที่สุด (data minimalisation) กล่าวคือ ข้อมูลส่วนบุคคลนั้นจะมีได้เท่าที่เพียงพอ (adequate) เกี่ยวข้อง และจำกัดเฉพาะสิ่งที่จำเป็นตามวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลเท่านั้น (Art. 5 1. (c))

๔) หลักความถูกต้อง (accuracy) กล่าวคือ ข้อมูลส่วนบุคคลนั้นจะต้องถูกต้อง และในกรณีที่จำเป็นก็จะต้องทำให้เป็นปัจจุบัน ทั้งนี้ จะต้องมีการใช้วิธีการตามสมควรเพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลที่ไม่ถูกต้องตรงตามวัตถุประสงค์ของการประมวลผลจะถูกลบหรือได้รับการแก้ไขให้ถูกต้องโดยไม่ชักช้า (Art. 5 1. (d))

๕) หลักการเก็บข้อมูลอย่างจำกัด (storage limitation) กล่าวคือ การเก็บข้อมูลส่วนบุคคลในรูปแบบที่สามารถบ่งชี้ตัวเจ้าของข้อมูลได้นั้น จะเก็บได้ไม่นานเกินกว่าที่จำเป็นเพื่อวัตถุประสงค์ในการประมวลผล (เว้นแต่กรณีที่เป็นไปเพื่อประโยชน์สาธารณะ ทางวิทยาศาสตร์ การวิจัยทางประวัติศาสตร์ หรือในเชิงสถิติ ตาม Article 89 (1) ซึ่งมีรายละเอียดอีกสำหรับข้อยกเว้นเหล่านี้) (Art. 5 1. (e))

๖) หลักความเชื่อถือได้และการรักษาความลับ (integrity and confidentiality) กล่าวคือ ในการประมวลผลข้อมูลส่วนบุคคลจะต้องมีการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสม

---

[๑๔] European Union Agency for Fundamental Rights (FRA), Handbook on European data protection law, 2018 edition, p. 104.

จะต้องป้องกันข้อมูลดังกล่าวจากการประมวลผลโดยปราศจากอำนาจหรือโดยไม่ชอบด้วยกฎหมาย และป้องกันข้อมูลจากการสูญหาย ทำลาย หรือเกิดความเสียหายโดยอุบัติเหตุ โดยใช้เทคนิคหรือกระบวนการจัดข้อมูลที่เหมาะสม (Art. 5 1. (f))

๗) หลักความรับผิดชอบ (accountability) กล่าวคือ ผู้ควบคุมข้อมูลส่วนบุคคลมีภาระความรับผิดชอบที่จะต้องแสดงให้เห็นว่าตนสามารถปฏิบัติตามหลักการตามข้อ ๑) ถึง ๖) ที่ได้กล่าวมาข้างต้นได้ (Art. 5 2.)

ทั้งนี้ หลักการเหล่านี้ที่สะท้อนถึงเจตนารมณ์ของการคุ้มครองข้อมูลส่วนบุคคลมากกว่าที่จะเป็นการวางกฎเกณฑ์ที่ชัดเจนตายตัวเอาไว้ ซึ่งการปฏิบัติให้เป็นไปตามหลักการเหล่านี้จะเป็นพื้นฐานสำคัญสำหรับการสร้างแนวทางปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลที่ดีต่อไป[๑๕]

**(๓.๓) ฐานที่ทำให้การประมวลผลข้อมูลส่วนบุคคลชอบด้วยกฎหมาย**

ตามที่ได้กล่าวไว้แล้วข้างต้นว่า GDPR ได้วางหลักการที่สำคัญสำหรับการประมวลผลข้อมูลส่วนบุคคลเอาไว้ ซึ่งหลักการที่สำคัญประการหนึ่งก็คือ การประมวลผลข้อมูลส่วนบุคคลจะต้องเป็นไปโดยชอบด้วยกฎหมาย (Art. 5 1. (a)) ปัญหาที่เราต้องพิจารณาต่อมาก็คือ การประมวลผลข้อมูลส่วนบุคคลกรณีใดบ้างที่จะถือว่าสามารถทำได้โดยชอบด้วยกฎหมาย

คำตอบของคำถามนี้มีการกำหนดเอาไว้ใน Article 6 ซึ่งได้วางฐานที่ทำให้การประมวลผลข้อมูลส่วนบุคคลชอบด้วยกฎหมายเอาไว้ ดังนั้น ในกรณีที่จะทำการประมวลผลข้อมูลส่วนบุคคลก็จะต้องพิจารณาด้วยว่าการประมวลผลนั้นมีฐานรองรับตามบทบัญญัตินี้หรือไม่ ไม่เช่นนั้นแล้วการประมวลผลข้อมูลส่วนบุคคลดังกล่าวอาจมีผลเป็นการละเมิดต่อหลักการของ GDPR และนำไปสู่บทบังคับตาม GDPR ได้ ทั้งนี้ ฐานที่ทำให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปโดยชอบด้วยกฎหมายตาม Article 6 ได้แก่

๑) ฐานความยินยอม กล่าวคือ เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมสำหรับการประมวลผลข้อมูลส่วนบุคคลของตนเพื่อวัตถุประสงค์ใดวัตถุประสงค์หนึ่งหรือหลายวัตถุประสงค์[๑๖] ซึ่งความยินยอมตาม GDPR นั้น หมายความถึงการใด ๆ ที่แสดงถึงความประสงค์ของเจ้าของข้อมูลส่วนบุคคล ไม่ว่าจะในลักษณะของถ้อยคำแถลง (statement) หรือเป็นการกระทำที่แสดงการยืนยันอย่างแจ้งชัด (clear affirmative action) ว่าเห็นชอบกับการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับตน ซึ่งการให้ความยินยอมนั้นจะต้องเป็นการให้โดยเสรี (freely given) อย่างเฉพาะเจาะจง (specific) ต้องได้รับทราบข้อมูลที่ถูกต้องครบถ้วน (informed) และไม่คลุมเครือ (unambiguous) (Art. 4 (11)) สำหรับรูปแบบของการให้ความยินยอมนั้น อาจเป็นลายลักษณ์อักษร

---

[๑๕] ICO. Information Commissioner's Office, Guide to the General Data Protection Regulation (GDPR), p. 17.

[๑๖] นอกจากนี้ สำหรับกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ GDPR ได้กำหนดกรณีให้การเสนอบริการที่จัดให้มีขึ้นเพื่อประโยชน์ตอบแทนโดยอาศัยอุปกรณ์ทางอิเล็กทรอนิกส์ (information society services) โดยตรงต่อผู้เยาว์ การประมวลผลข้อมูลส่วนบุคคลกรณีนี้จะชอบด้วยกฎหมายก็ต่อเมื่อผู้เยาว์มีอายุอย่างน้อย ๑๖ ปี และหากผู้เยาว์มีอายุต่ำกว่านั้น ในการให้ความยินยอมของผู้เยาว์จะต้องได้รับการให้ความเห็นชอบโดยผู้มีอำนาจปกครองด้วย (Art. 8 1.) อนึ่ง กำหนดอายุ ๑๖ ปีดังกล่าว GDPR ได้เปิดช่องให้ประเทศสมาชิกสามารถกำหนดอายุขั้นต่ำของเด็กกรณีนี้ได้เอง แต่จะต้องไม่ต่ำกว่า ๑๓ ปี

ซึ่งรวมทั้งวิธีการทางอิเล็กทรอนิกส์ หรืออาจเป็นการให้ความยินยอมด้วยถ้อยคำวาจาก็ได้[๑๗] อย่างไรก็ดี GDPR ไม่ยอมรับวิธีการใช้ช่องกาเครื่องหมายที่กาเอาไว้ก่อน (pre-ticked opt-in boxes)[๑๘]

อนึ่ง ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ประมวลผลโดยอาศัยฐานแห่งความยินยอม ก็จะมีหน้าที่ต้องแสดงให้เห็นได้ด้วยว่าเจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมสำหรับการประมวลผลนั้น (Art. 7 1.)

๒) ฐานจากสัญญา กล่าวคือ หากการประมวลผลนั้นมีความเป็นจำเป็นแก่การปฏิบัติตามสัญญาที่เจ้าของข้อมูลส่วนบุคคลเข้าเป็นคู่สัญญาอยู่ด้วย หรือเพื่อที่จะดำเนินการให้เป็นไปตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนการเข้าทำสัญญา ก็จะทำให้การประมวลผลนั้นชอบด้วยกฎหมาย ตัวอย่างสำหรับกรณีหลังก็เช่น เจ้าของรถยนต์ผู้หนึ่งต้องการทำประกันภัยรถยนต์และได้ขอให้บริษัทประกันเสนอราคาเบี้ยประกันเพื่อพิจารณาทำประกันภัยรถยนต์ กรณีเช่นนี้บริษัทประกันภัยย่อมมีความจำเป็นที่จะต้องประมวลผลข้อมูลบางอย่างเกี่ยวกับผู้นั้นเพื่อที่จะสามารถเสนอราคาเบี้ยประกันได้ เป็นต้น[๑๙]

๓) ฐานจากหน้าที่ตามกฎหมาย กล่าวคือ การประมวลผลนั้นมีความจำเป็นในการปฏิบัติหน้าที่ตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งฐานแห่งการประมวลผลในข้อนี้ไม่ได้หมายความว่าจะต้องมีกฎหมายที่กำหนดโดยเฉพาะเจาะจงให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการประมวลผล เพียงแค่ผู้ควบคุมข้อมูลส่วนบุคคลมีวัตถุประสงค์ในภาพรวมที่จะต้องปฏิบัติให้เป็นไปตามหน้าที่ตามกฎหมายก็ถือได้ว่าสามารถอาศัยฐานในข้อนี้ได้แล้ว เช่น หากมีกฎหมายกำหนดหน้าที่ให้สถาบันการเงินต้องรายงานต่อพนักงานเจ้าหน้าที่เมื่อพบเหตุต้องสงสัยว่ามีบุคคลกระทำการอันเป็นการฟอกเงิน[๒๐] เช่นนี้ก็ถือได้ว่าเป็นการปฏิบัติหน้าที่ตามกฎหมายแล้ว

๔) ฐานจากการคุ้มครองชีวิต (vital interests) กล่าวคือ การประมวลผลนั้นจำเป็นสำหรับการปกป้องชีวิตของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น เช่น กรณีที่มีบุคคลผู้ประสบอุบัติเหตุทางรถยนต์ซึ่งอาจถึงขั้นเสียชีวิตได้ และโรงพยาบาลมีความจำเป็นที่จะต้องเปิดเผยประวัติทางการแพทย์ของบุคคลนั้นเพื่อรักษาชีวิตของบุคคลนั้น[๒๑] เป็นต้น

๕) ฐานจากหน้าที่ต่อสาธารณะ กล่าวคือ การประมวลผลนั้นจำเป็นสำหรับการปฏิบัติงานเพื่อประโยชน์สาธารณะ หรือเป็นการใช้อำนาจรัฐของผู้ควบคุมข้อมูลส่วนบุคคล

๖) ฐานจากประโยชน์โดยชอบด้วยกฎหมาย (legitimate interest) กล่าวคือ การประมวลผลนั้นเป็นการจำเป็นเพื่อให้ได้มาซึ่งประโยชน์โดยชอบด้วยกฎหมาย ซึ่งประโยชน์ดังกล่าวอาจเป็นของผู้ควบคุมข้อมูลส่วนบุคคลหรือบุคคลที่สามก็ได้ แต่ประโยชน์ดังกล่าวจะต้องไม่ถูกกลบกลืน (overridden) โดยประโยชน์หรือสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคลที่จำเป็นต้องได้รับการคุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ ตัวอย่างของประโยชน์โดยชอบด้วยกฎหมายนั้น

---

[๑๗] Recital 32

[๑๘] ICO. Information Commissioner's Office, Guide to the General Data Protection Regulation (GDPR), p. 62.

[๑๙] เพิ่งอ้าง, หน้า ๖๖.

[๒๐] เพิ่งอ้าง, หน้า ๗๐.

[๒๑] เพิ่งอ้าง, หน้า ๗๔.

รวมทั้งประโยชน์ในทางพาณิชย์ ประโยชน์ของปัจเจกบุคคล หรือประโยชน์ต่อสังคมที่กว้างกว่า เป็นต้น[๒๒] ซึ่งจะเห็นได้ว่าฐานของการประมวลผลในข้อนี้มีความยืดหยุ่นมากที่สุดเมื่อเทียบกับฐานอื่น ๆ

การพิจารณาว่าการประมวลผลจะชอบด้วยกฎหมายโดยอาศัยฐานข้อนี้ได้หรือไม่นั้น จะต้องพิจารณาจากบททดสอบสามประการ กล่าวคือ ๑. บททดสอบโดยหลักเกณฑ์ด้านวัตถุประสงค์ (purpose test) ซึ่งต้องพิจารณาว่าการประมวลผลนั้นเป็นไปเพื่อให้ได้มาซึ่งประโยชน์อันชอบด้วยกฎหมายหรือไม่ ๒. บททดสอบโดยหลักเกณฑ์ด้านความจำเป็น (necessity test) ซึ่งต้องพิจารณาว่าการประมวลผลข้อมูลนั้นจำเป็นสำหรับวัตถุประสงค์นั้นหรือไม่ และ ๓. บททดสอบโดยหลักเกณฑ์การชั่งน้ำหนัก (balancing test) ซึ่งต้องพิจารณาว่าสิทธิของเจ้าของข้อมูลนั้นเหนือกว่าประโยชน์อันชอบด้วยกฎหมายหรือไม่[๒๓]

ทั้งนี้ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลจะทำการประมวลผลข้อมูลส่วนบุคคล ก็จะต้องพิจารณาว่าตนควรจะประมวลผลโดยอาศัยฐานข้อใดเพื่อให้สอดคล้องกับการประมวลผลแต่ละกรณีที่ตนดำเนินการ ซึ่งอาจจะต้องพิจารณาปัจจัยหลายประการ เช่น วัตถุประสงค์ในการประมวลผล การทำให้บรรลุวัตถุประสงค์นั้นสามารถดำเนินการด้วยวิธีการอื่นนอกจากการประมวลผลข้อมูลส่วนบุคคลได้หรือไม่ ตนมีทางเลือกอื่นที่จะไม่ประมวลผลข้อมูลส่วนบุคคลนั้นหรือไม่ หรือตนเป็นเจ้าหน้าที่ของรัฐหรือไม่ เป็นต้น[๒๔] และในบางกรณีก็อาจจำเป็นต้องพิจารณาถึงฐานในการประมวลผลข้อมูลส่วนบุคคลไว้หลาย ๆ ฐานด้วย

จากแนวทางดังกล่าว หากทำการพิจารณากรณีดังต่อไปนี้

*ในกรณีที่มหาวิทยาลัยแห่งหนึ่งต้องการประมวลผลข้อมูลส่วนบุคคล มหาวิทยาลัยควรจะอาศัยฐานแห่งการประมวลผลในข้อใด*

หากเราสมมติว่ามหาวิทยาลัยนี้เป็นมหาวิทยาลัยของรัฐ ก็อาจนำฐานการประมวลผลจากการปฏิบัติหน้าที่ต่อสาธารณะมาปรับใช้กับการประมวลผลของมหาวิทยาลัยได้ แต่ก็จะต้องขึ้นอยู่กับการจัดตั้งและอำนาจตามกฎหมายของมหาวิทยาลัยด้วย แต่ถ้าการประมวลผลข้อมูลส่วนบุคคลของมหาวิทยาลัยได้กระทำลงโดยไม่เกี่ยวข้องกับหน้าที่ของมหาวิทยาลัยในฐานะที่เป็นหน่วยงานของรัฐ เช่นนี้ มหาวิทยาลัยก็ควรพิจารณาฐานในการประมวลผลข้อมูลส่วนบุคคลข้ออื่น เช่น อาจอาศัยจากฐานความยินยอม หรือประโยชน์อันชอบด้วยกฎหมายของตนเพื่อให้สอดคล้องกับการประมวลผลของตน ยกตัวอย่างเช่น หากมหาวิทยาลัยจะทำการประมวลผลข้อมูลเพื่อบริหารจัดการเกี่ยวกับสมาคมศิษย์เก่าหรือการระดมเงินทุน ก็อาจจะต้องพิจารณาจากฐานความยินยอมหรือประโยชน์อันชอบด้วยกฎหมายของมหาวิทยาลัย[๒๕]

**(๓.๔) สิทธิของเจ้าของข้อมูลส่วนบุคคล**

GDPR ได้กำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคลเอาไว้ในหมวดที่ ๓ ซึ่งประกอบไปด้วยสิทธิหลายประการ ซึ่งในที่นี้จะกล่าวถึงแต่ละสิทธิโดยสังเขป ได้แก่

---

[๒๒]เพิ่งอ้าง, หน้า ๘๑.

[๒๓]เพิ่งอ้าง, หน้า ๘๓.

[๒๔]เพิ่งอ้าง, หน้า ๕๔.

[๒๕]เพิ่งอ้าง, หน้า ๕๕.

๑) สิทธิที่จะได้รับการแจ้ง (the right to be informed) กล่าวคือ บุคคลมีสิทธิที่จะได้รับแจ้งเกี่ยวกับการเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลของตน ซึ่งสิทธินี้มีการกำหนดไว้ใน Article 13 และ Article 14 โดยกำหนดว่าบุคคลมีสิทธิที่จะได้รับแจ้งเกี่ยวกับ “ข้อมูลเกี่ยวกับความเป็นส่วนตัว” (privacy information) ซึ่งสำหรับกรณีตาม Article 13 จะเป็นข้อมูลที่ต้องแจ้งให้ทราบในกรณีที่เก็บรวบรวมข้อมูลส่วนบุคคลจากตัวเจ้าของข้อมูลเอง และสำหรับกรณีตาม Article 14 จะเป็นการแจ้งข้อมูลให้ทราบสำหรับกรณีที่ได้รับข้อมูลจากแหล่งอื่นนอกจากเจ้าของข้อมูลส่วนบุคคล ซึ่งตัวอย่างของข้อมูลต่าง ๆ ที่ต้องแจ้งให้ทราบ ก็เช่น ตัวตนของผู้ควบคุมข้อมูลส่วนบุคคลและรายละเอียดสำหรับการติดต่อ วัตถุประสงค์ของการประมวลผลข้อมูล ตลอดจนฐานทางกฎหมายในการประมวลผลข้อมูล หรือผู้รับหรือประเภทผู้ที่จะได้รับข้อมูลดังกล่าวในกรณีที่จะมีการเปิดเผยข้อมูลนั้นต่อไป เป็นต้น

๒) สิทธิที่จะเข้าถึงข้อมูลส่วนบุคคลของตน (the right of access) ซึ่งปรากฏอยู่ใน Article 15 โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะได้รับการยืนยันจากผู้ควบคุมข้อมูลส่วนบุคคลว่ามีการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับตนหรือไม่ และถ้าหากมีการประมวลผลดังกล่าว ผู้นั้นก็จะมีสิทธิในการเข้าถึงข้อมูลต่าง ๆ เช่น วัตถุประสงค์ของการประมวลผล ประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้อง ผู้รับหรือประเภทของผู้จะรับข้อมูลส่วนบุคคลนั้นในกรณีที่มีการเปิดเผย หรือได้รับแจ้งสิทธิในการร้องเรียนต่อหน่วยงานที่ทำหน้าที่กำกับดูแล (supervisory authority) เป็นต้น

๓) สิทธิที่จะแก้ไขข้อมูลให้ถูกต้อง (the right to rectification) โดย Article 16 ได้กำหนดว่าเจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะได้รับการแก้ไขข้อมูลส่วนบุคคลที่เกี่ยวกับตนที่ไม่ถูกต้องโดยไม่ชักช้า ตลอดจนมีสิทธิที่จะขอให้ทำข้อมูลที่ไม่สมบูรณ์ให้มีความสมบูรณ์ขึ้น ซึ่งอาจด้วยวิธีการให้คำอธิบายเพิ่มเติมเกี่ยวกับข้อมูลนั้นก็ได้ ทั้งนี้ โดยจะต้องพิจารณาถึงวัตถุประสงค์ของการประมวลผลด้วย

๔) สิทธิที่จะลบ (หรือสิทธิที่จะถูกลืม) (the right to erasure (the right to be forgotten)) ซึ่งปรากฏอยู่ใน Article 17 โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการลบข้อมูลส่วนบุคคลเกี่ยวกับตนโดยไม่ชักช้า และผู้ควบคุมข้อมูลส่วนบุคคลจะต้องลบข้อมูลดังกล่าวหากเป็นไปตามเงื่อนไขที่มาตรานี้กำหนด เช่น ข้อมูลส่วนบุคคลนั้นไม่มีความจำเป็นอันเกี่ยวเนื่องกับวัตถุประสงค์ที่ได้มีการเก็บรวบรวมหรือประมวลผลอีกต่อไป เจ้าของข้อมูลส่วนบุคคลได้เพิกถอนความยินยอม (ในกรณีที่การประมวลผลมีฐานจากความยินยอม) หรือข้อมูลส่วนบุคคลนั้นถูกประมวลผลโดยไม่ชอบด้วยกฎหมาย เป็นต้น ทั้งนี้ แม้จะเป็นกรณีตามเงื่อนไขที่อาจขอให้ลบข้อมูลได้แล้วก็ตาม สิทธิข้อนี้ก็ยังมีข้อยกเว้นอีกถ้าหากว่าการประมวลผลข้อมูลส่วนบุคคลนั้นมีความจำเป็นเพื่อกรณีต่าง ๆ ได้แก่ เพื่อการใช้สิทธิเสรีภาพในการแสดงออกและการเข้าถึงข้อมูลข่าวสาร เพื่อการปฏิบัติให้เป็นไปตามข้อผูกพันตามกฎหมายเพื่อการสาธารณสุข เพื่อบรรลุวัตถุประสงค์เพื่อประโยชน์สาธารณะ การศึกษาวิจัยทางวิทยาศาสตร์หรือประวัติศาสตร์ หรือทางสถิติ หรือเพื่อก่อตั้งหรือใช้สิทธิทางกฎหมาย หรือต่อสู้คดี

๕) สิทธิที่จะจำกัดการประมวลผล (the right to restrict processing) ซึ่งปรากฏตาม Article 18 โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะให้ผู้ควบคุมข้อมูลส่วนบุคคลจำกัดการประมวลผลในกรณีต่าง ๆ เช่น การประมวลผลนั้นไม่ชอบด้วยกฎหมาย หรือข้อมูลส่วนบุคคลนั้นไม่มีความจำเป็นสำหรับวัตถุประสงค์ของการประมวลผลอีกต่อไป แต่เจ้าของข้อมูลส่วนบุคคล

จำเป็นต้องอาศัยข้อมูลดังกล่าวเพื่อก่อตั้งหรือใช้สิทธิทางกฎหมาย หรือต่อสู้คดี เป็นต้น ทั้งนี้ ในกรณีที่การประมวลผลถูกจำกัดแล้ว ข้อมูลส่วนบุคคลดังกล่าวนอกจากการเก็บแล้วจะถูกนำมาประมวลผลได้ก็แต่โดยความยินยอมของเจ้าของข้อมูลส่วนบุคคล หรือเป็นไปเพื่อการก่อตั้งหรือใช้สิทธิทางกฎหมาย หรือต่อสู้คดี หรือเป็นไปเพื่อปกป้องคุ้มครองสิทธิของบุคคลธรรมดาหรือนิติบุคคลสำหรับเหตุผลเกี่ยวกับประโยชน์สาธารณะที่สำคัญของสหภาพหรือรัฐสมาชิก เท่านั้น

๖) สิทธิที่จะโอนย้ายข้อมูล (the right to data portability) ปรากฏตาม Article 20 โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะได้รับข้อมูลส่วนบุคคลที่เกี่ยวกับตนที่ให้ไว้แก่ผู้ควบคุมข้อมูลส่วนบุคคล โดยข้อมูลนั้นอยู่ในสภาพที่มีการจัดหมวดหมู่ และอยู่ในรูปแบบที่สามารถอ่านได้โดยเครื่องคอมพิวเตอร์ (machine-readable) นอกจากนี้ ยังมีสิทธิที่จะให้โอนข้อมูลดังกล่าวให้กับผู้ควบคุมข้อมูลส่วนบุคคลรายอื่นได้ด้วย ทั้งนี้ สิทธินี้จะใช้เฉพาะในกรณีที่การประมวลผลมีฐานมาจากความยินยอม และการประมวลผลนั้นได้ทำโดยวิธีการอัตโนมัติ (automated means) เท่านั้น

๗) สิทธิที่จะคัดค้าน (the right to object) ปรากฏตาม Article 21 โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะคัดค้านการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับตนได้ในกรณีต่าง ๆ เช่น กรณีที่การประมวลผลนั้นมีฐานมาจากการปฏิบัติงานเพื่อประโยชน์สาธารณะหรือเป็นการใช้อำนาจรัฐของผู้ควบคุมข้อมูลส่วนบุคคล หรือเป็นการจำเป็นเพื่อให้ได้มาซึ่งประโยชน์โดยชอบด้วยกฎหมาย รวมทั้งกรณีที่เป็นการนำข้อมูลส่วนบุคคลมาใช้ในการวิเคราะห์พฤติกรรมของบุคคลนั้น (profiling) เป็นต้น ซึ่งหากมีการคัดค้านแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องไม่ประมวลผลข้อมูลนั้นอีกต่อไปเว้นเสียแต่ว่าจะแสดงให้เห็นได้ว่าตนมีฐานที่ชอบด้วยกฎหมายสำหรับการประมวลผลที่เหนือกว่าประโยชน์ สิทธิ และเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือเป็นไปเพื่อการก่อตั้งหรือใช้สิทธิทางกฎหมาย หรือต่อสู้คดี เป็นต้น

๘) สิทธิเกี่ยวกับการตัดสินใจด้วยวิธีการอัตโนมัติและการใช้ข้อมูลเพื่อการวิเคราะห์พฤติกรรมบุคคล (profiling) ปรากฏอยู่ใน Article 22 โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะไม่ถูกตัดสินจากการประมวลผลข้อมูลส่วนบุคคลด้วยวิธีการอัตโนมัติเพียงอย่างเดียวเท่านั้น ซึ่งรวมไปถึงการนำข้อมูลมาใช้ในการวิเคราะห์พฤติกรรมบุคคลนั้น (profiling) ที่อาจก่อให้เกิดผลทางกฎหมายเกี่ยวกับตนหรือส่งผลที่มีความสำคัญในระดับเดียวกันด้วย อย่างไรก็ตาม สิทธิในข้อนี้มีข้อยกเว้นอยู่ กล่าวคือ หากเป็นไปเพื่อการเข้าสู่การทำสัญญา หรือเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคล หรือได้รับความยินยอมของเจ้าของข้อมูลส่วนบุคคลอย่างชัดแจ้งแล้ว เป็นต้น

ทั้งนี้ เจ้าของข้อมูลส่วนบุคคลจะสามารถใช้สิทธิใดของตนตามที่ได้กล่าวข้างต้นได้บ้างนั้น อาจขึ้นอยู่กับฐานในการประมวลผลข้อมูลส่วนบุคคลนั้นด้วย ยกตัวอย่างเช่น ในกรณีที่การประมวลผลข้อมูลส่วนบุคคลมีฐานมาจากการปฏิบัติหน้าที่ตามกฎหมาย เช่นนี้ เจ้าของข้อมูลส่วนบุคคลจะไม่สามารถใช้สิทธิในการลบข้อมูลส่วนบุคคลของตนได้หรือในกรณีที่การประมวลผลอาศัยฐานจากสัญญา เช่นนี้ก็จะไม่สามารถใช้สิทธิในการคัดค้านการประมวลผลได้ เป็นต้น[๒๖]

[๒๖]เพิ่งอ้าง, หน้า ๕๓.

**(๓.๕) การส่งข้อมูลไปยังประเทศที่สาม**

นอกจากหลักเกณฑ์ในการประมวลผลข้อมูลส่วนบุคคลและสิทธิของเจ้าของข้อมูลส่วนบุคคลแล้ว GDPR ยังได้กำหนดหลักเกณฑ์สำหรับการส่งข้อมูลส่วนบุคคลไปยังประเทศที่สามหรือองค์การระหว่างประเทศเอาไว้ด้วย โดยหากคณะกรรมาธิการ (commission) พิจารณาเห็นว่าประเทศที่จะมีการส่งข้อมูลส่วนบุคคลไป หรือดินแดนส่วนหนึ่งของประเทศดังกล่าว มีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (Art. 45) ก็จะทำให้สามารถส่งข้อมูลได้โดยไม่ต้องอาศัยการอนุญาตเป็นการเฉพาะ (specific authorisation) แต่สำหรับประเทศที่ไม่มีมาตรฐานการคุ้มครองที่เพียงพอ ในการส่งข้อมูลก็จะต้องพิจารณาเงื่อนไขอื่นที่ทำให้สามารถส่งข้อมูลระหว่างกันได้ เช่น ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้จัดหามาตรการป้องกันที่เหมาะสม (appropriate safeguards) และจะต้องสามารถบังคับตามสิทธิของเจ้าของข้อมูลส่วนบุคคลและบังคับตามมาตรการเยียวยาตามกฎหมายให้แก่เจ้าของข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพ (Art. 46 1.) ซึ่งกรณีที่จะถือได้ว่ามีมาตรการป้องกันที่เหมาะสมนั้น GDPR ตาม Article 46 ก็เช่น เป็นการปฏิบัติตามกฎเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร (binding corporate rules) เป็นต้น นอกจากนี้ ยังมีข้อยกเว้นอื่น ๆ สำหรับเฉพาะกรณีตาม Article 49 อีก เช่น เจ้าของข้อมูลได้ให้ความยินยอมโดยชัดแจ้งภายหลังจากที่ได้รับทราบข้อมูลความเสี่ยงของการส่งข้อมูลดังกล่าวแล้ว เป็นการส่งข้อมูลที่จำเป็นเพื่อปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคล หรือการส่งข้อมูลมีความจำเป็นสำหรับการก่อตั้งหรือใช้สิทธิทางกฎหมาย หรือต่อสู้คดี เป็นต้น

ที่กล่าวมาข้างต้นเป็นเพียงเนื้อหาบางส่วนของ GDPR เท่านั้น แต่นอกจากที่ได้กล่าวมาแล้ว GDPR ยังมีเนื้อหาอื่น ๆ ที่มีความสำคัญอีก เช่น การประมวลผลข้อมูลส่วนบุคคลที่มีลักษณะเฉพาะ ความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคลและของผู้ประมวลผลข้อมูลส่วนบุคคล การจัดตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data protection officer (DPO)) หลักการคุ้มครองข้อมูลส่วนบุคคลโดยสภาพตั้งแต่ขั้นการออกแบบ (by design and by default) การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล หน่วยงานอิสระที่ทำหน้าที่กำกับดูแล หรือเรื่องเกี่ยวกับการเยียวยา หรือค่าปรับทางปกครอง เป็นต้น และผู้ที่อยู่ในขอบข่ายจะต้องปฏิบัติตาม GDPR ก็ควรต้องศึกษารายละเอียดของเรื่องต่าง ๆ เหล่านี้เพื่อให้สามารถปฏิบัติได้โดยถูกต้องต่อไป

**๔. บทสรุป**

จากที่ได้กล่าวไปทั้งหมดข้างต้น จะเห็นได้ว่า GDPR ได้กำหนดมาตรการที่เป็นการปกป้องคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลเอาไว้หลายประการ ตั้งแต่การกำหนดหลักการเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลอย่างเช่น การประมวลผลจะต้องเป็นไปโดยชอบด้วยกฎหมาย เป็นธรรม และโปร่งใส หรือการให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลไว้ ตลอดไปจนถึงเรื่องอื่น ๆ ที่ไม่ได้กล่าวถึงในบทความนี้ด้วย ซึ่งหากผู้เขียนบทความมีเวลาและโอกาสเอื้ออำนวย จะได้เขียนบทความเกี่ยวกับ GDPR ในเรื่องอื่น ๆ หรือลงในรายละเอียดแต่ละประเด็นต่อไป

สำหรับสถานการณ์ของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยนั้น ปัจจุบันประเทศไทยเองยังไม่มีกฎหมายที่ให้ความคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป จะมีก็แต่กฎหมายรายฉบับที่กำหนดเกี่ยวกับข้อมูลส่วนบุคคลเฉพาะแต่ละเรื่องเอาไว้ เช่น ข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานของรัฐก็มีพระราชบัญญัติข้อมูลข่าวสารของทางราชการ

พ.ศ. ๒๕๔๐ กำหนดหลักเกณฑ์ต่าง ๆ เอาไว้ หรือข้อมูลด้านสุขภาพของบุคคลที่มาตรา ๗ แห่งพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. ๒๕๕๐ กำหนดให้เป็นความลับส่วนบุคคล และจะนำไปเปิดเผยในประการที่จะทำให้บุคคลนั้นเสียหายไม่ได้ เป็นต้น ซึ่งก็ได้มีความพยายามในการจัดทำร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... มาตั้งแต่ปี พ.ศ. ๒๕๔๙ โดยในขณะนั้นสำนักนายกรัฐมนตรีเป็นผู้เสนอร่างฯ และได้ผ่านการตรวจพิจารณาโดยสำนักงานคณะกรรมการกฤษฎีกาแล้วในปี พ.ศ. ๒๕๕๒ แต่ร่างฯ ดังกล่าวก็ไม่ได้ถูกตราขึ้นเป็นกฎหมายแต่อย่างใด ต่อมาในปี พ.ศ. ๒๕๕๘ ก็ได้มีความพยายามในการเสนอร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... อีกครั้ง โดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารในขณะนั้นเป็นผู้เสนอ และสำนักงานคณะกรรมการกฤษฎีกาก็ได้ดำเนินการตรวจพิจารณาร่างพระราชบัญญัติดังกล่าวแล้วเสร็จในปีเดียวกัน อย่างไรก็ดี คณะรัฐมนตรีได้มีมติเมื่อวันที่ ๘ กันยายน ๒๕๕๘ เห็นชอบให้ส่งร่างพระราชบัญญัติดังกล่าวไปให้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรับไปพิจารณาทบทวนร่วมกับสำนักงานคณะกรรมการกฤษฎีกาให้สอดคล้องกับนโยบายของรัฐบาลอีกครั้งหนึ่ง แล้วนำเสนอคณะรัฐมนตรีพิจารณา ก่อนเสนอสภานิติบัญญัติแห่งชาติต่อไป หลังจากนั้น กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารก็ได้ถูกเปลี่ยนเป็นกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยพระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม (ฉบับที่ ๑๗) พ.ศ. ๒๕๕๙ ซึ่งในช่วงไม่กี่เดือนที่ผ่านมากระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมก็ได้เสนอร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... อีกครั้ง และคณะรัฐมนตรีได้มีมติอนุมัติหลักการร่างพระราชบัญญัติดังกล่าวเมื่อวันที่ ๒๒ พฤษภาคม ๒๕๖๑[๒๗] ซึ่งร่างพระราชบัญญัติดังกล่าวจะเป็นกฎหมายกลางในการคุ้มครองข้อมูลส่วนบุคคล โดยมีเนื้อหาสาระโดยสรุป กล่าวคือ กำหนดให้มีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล กำหนดหลักเกณฑ์ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล กำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคล กำหนดให้มีสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเพื่อรับผิดชอบในงานวิชาการและงานธุรการให้แก่คณะกรรมการต่าง ๆ ตามร่างพระราชบัญญัตินี้ กำหนดกระบวนการในการร้องเรียนตลอดจนการไกล่เกลี่ยข้อพิพาทเกี่ยวกับข้อมูลส่วนบุคคล กำหนดความรับผิดจากการฝ่าฝืนบทบัญญัติของร่างกฎหมายนี้ โดยแบ่งออกเป็นความรับผิดทางแพ่ง ความรับผิดทางปกครอง และความรับผิดทางอาญา

เมื่อคณะรัฐมนตรีได้มีมติอนุมัติหลักการร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... แล้ว ก็มีการแสดงความคิดเห็นต่อร่างพระราชบัญญัติดังกล่าวอย่างมากหลาย แม้กระทั่งวารสาร Privacy Laws & Business[๒๘] ก็ได้ลงบทความแสดงความเห็นต่อร่างพระราชบัญญัตินี้เอาไว้เช่นเดียวกัน ซึ่งผู้เขียนบทความก็มีโอกาสได้รับฟังมุมมองที่แตกต่างต่อร่างพระราชบัญญัตินี้ทั้งจากในวงเสวนาและบทความต่าง ๆ ทั้งนี้ คำถามหนึ่งที่มักจะถูกหยิบยกขึ้นมาเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยก็คือ ทิศทางของกฎหมายดังกล่าวควรจะเป็นเช่นใด ควรจะมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เข้มงวดทัดเทียมกับ GDPR หรือไม่ โดยในมุมมองหนึ่งก็มีการเสนอความเห็นว่า หากกฎหมายของไทยมีมาตรฐานการคุ้มครอง

---

[๒๗]สำหรับเนื้อหาของร่างพระราชบัญญัติฯ ที่คณะรัฐมนตรีมีมติอนุมัติหลักการ สามารถอ่านได้ที่เว็บไซต์กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม http://www.mdes.go.th/view/1/home#

[๒๘]วารสาร Privacy Laws & Business เล่มที่ ๑๕๓ เดือนมิถุนายน ค.ศ. ๒๐๑๘ ในหัวข้อ Thailand’s draft data protection Bill: Strengths, many uncertainties โดย Graham Greenleaf และอาทิตย์ สุริยะวงศ์กุล

ข้อมูลส่วนบุคคลในระดับเดียวกับกฎหมายของสหภาพยุโรปแล้วก็จะส่งผลดีในการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล และอาจแก้ไขข้อกังวลเรื่องการส่งข้อมูลข้ามดินแดนกับประเทศในสหภาพยุโรปได้ ในขณะที่มุมมองอีกฝ่ายหนึ่งเห็นว่า หากกฎเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลมีความเข้มงวดมากเกินไปจะเป็นการสร้างภาระต้นทุนให้แก่ภาคธุรกิจโดยเฉพาะธุรกิจขนาดเล็ก และอาจส่งผลต่อการพัฒนานวัตกรรมได้ ซึ่งในเรื่องเกี่ยวกับการพิจารณาความสมดุลระหว่างการคุ้มครองข้อมูลส่วนบุคคลและภาระที่เกิดขึ้นแก่ภาคธุรกิจก็คงจะต้องติดตามต่อไปว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยจะมุ่งไปในทิศทางใด

สุดท้ายนี้ แม้ในปัจจุบันประเทศไทยจะยังไม่มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลก็ตาม แต่ก็ถือได้ว่าภาคสังคมมีความตื่นตัวในเรื่องการคุ้มครองข้อมูลส่วนบุคคลมากขึ้น และตัวเจ้าของข้อมูลส่วนบุคคลเองก็มีความตระหนักถึงสิทธิของตนในฐานะเจ้าของข้อมูลและผลกระทบที่อาจเกิดขึ้นต่อตนจากการถูกนำข้อมูลส่วนบุคคลไปหาประโยชน์โดยมิชอบ นอกจากนี้ภาคธุรกิจเองก็หันมาให้ความใส่ใจกับการคุ้มครองข้อมูลส่วนบุคคลมากขึ้น ไม่ว่าจะเป็นไปเพื่อสร้างแนวปฏิบัติที่ดีสำหรับนโยบายด้านความเป็นส่วนตัว หรือเพราะได้รับแรงกดดันจาก GDPR หรือเป็นการเตรียมการปฏิบัติตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ก็ตาม ซึ่งก็นับได้ว่าเป็นจุดเริ่มที่ดีสำหรับสถานการณ์การคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย