

## Data Privacy: บรรทัดฐานกฎหมายระดับโลกสู่บริบทประเทศไทย

โดย เอกสยาม ชัยศรี ที่ปรึกษากฎหมาย  
บริษัท เอกสยาม แอนด์ पार्टเนอร์ส จำกัด

เนื้อหานี้เป็นข้อมูลกฎหมายทั่วไป ไม่ใช่ความเห็นทางกฎหมายเฉพาะ กรณี การพิจารณาแต่ละเรื่อง ต้องอาศัย  
ข้อเท็จจริง และ พยานหลักฐาน ของ เรื่อง นั้น ฉบับ ออนไลน์ ที่ ปรับปรุง ล่าสุด อยู่ ที่ <https://eksiamlegal.com/articles/data-privacy-evolution.html>

### สาระสำคัญโดยสรุป

- สรุปสาระสำคัญ
- I. บทนำ: นัยสำคัญของข้อมูลส่วนบุคคลในบริบทโลก
- II. ปฐมบท: ภูมิหลังทางประวัติศาสตร์และสิทธิความเป็นส่วนตัวส่วนตัวหลังสงครามโลก
- III. พัฒนาการยุคแรก: แนวทางของ OECD และการวางรากฐานของสหภาพยุโรป
- IV. จุดเปลี่ยนสำคัญ: บรรทัดฐานใหม่ภายใต้ระเบียบ GDPR ของสหภาพยุโรป
- V. บริบทของประเทศไทย: การบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)
- VI. บทวิเคราะห์เปรียบเทียบแบบการคุ้มครองข้อมูลส่วนบุคคล (Privacy Models)
- VII. ความท้าทายในอนาคต: ปัญญาประดิษฐ์ (AI) กับข้อจำกัดของกฎหมาย
- VIII. แนวโน้มและประเด็นทางกฎหมายที่ต้องจับตา



- IX. บทสรุป
- รากของกฎหมายคุ้มครองข้อมูลคือบทเรียนสงคราม ไม่ใช่การค้า ปณิญาสากล่าวด้วยสิทธิมนุษยชน ค.ศ. 1948 ข้อ 12 รับรองสิทธิที่จะไม่ถูกแทรกแซงโดยพลการต่อความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย และการติดต่อสื่อสาร เป็นครั้งแรกในระดับสากล
- OECD Guidelines ค.ศ. 1980 วาง โครง ที่ กฎหมาย ทุก ฉบับ ยัง ใช้ อยู่ ทั้ง การ จำกัด การ เก็บ การ ระบุ วัตถุประสงค์ และ ความรับผิดชอบ ของ ผู้ควบคุม ข้อมูล ซึ่ง ปรากฏ ต่อมา ในมาตรา 21 ถึงมาตรา 23 ของ PDPA
- GDPR เปลี่ยนเกมด้วยผลบังคับนอกอาณาเขต ข้อ 3 ขยายไปถึงองค์กรทั่วโลกที่เสนอสินค้าหรือบริการแก่คนในสหภาพยุโรป และข้อ 83 วางโทษปรับสูงถึง 20 ล้านยูโรหรือร้อยละ 4 ของรายได้ทั่วโลก
- ไทยรับโครงของ GDPR มาโดยลดเพดานโทษลงมาก PDPA พ.ศ. 2562 ถือความยินยอมตามมาตรา 19 เป็นหลัก มีข้อยกเว้นหกประการในมาตรา 24 ส่วนโทษปรับทางปกครองตามมาตรา 82 ถึงมาตรา 84 อยู่ที่หนึ่ง สาม และห้าล้านบาท
- ฐานทางรัฐธรรมนูญอยู่ที่มาตรา 32 รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 รับรองสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และ ครอบครัว อันเป็นฐานให้แก่การตรากฎหมายคุ้มครองข้อมูลส่วนบุคคล
- ปัญหาประดิษฐ์ท้าทายหลักความจำกัดของวัตถุประสงค์ การฝึกโมเดลใช้ข้อมูลในลักษณะที่ระบุวัตถุประสงค์ล่วงหน้าได้ยาก ซึ่งปะทะกับมาตรา 21 ของ PDPA ขณะที่สหภาพยุโรปตอบด้วย Regulation (EU) 2024/1689 หรือ AI Act

บทความนี้ติดตามเส้นทางของกฎหมาย คุ้มครองข้อมูลส่วนบุคคลจากปณิญาสากล่าวด้วยสิทธิมนุษยชน ค.ศ. 1948 ผ่าน OECD Guidelines และ GDPR มาจนถึงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของไทย แล้ววิเคราะห์ว่า สาม โมเดล ของ โลก ต่างกัน อย่างไร และ กฎหมาย จะ รับมือ ปัญหา ประดิษฐ์ได้เพียงใด



## I. บทนำ: นัยสำคัญของข้อมูลส่วนบุคคลในบริบทโลก

ข้อมูลส่วนบุคคลกลายเป็นสินทรัพย์ทางเศรษฐกิจที่ฝ่ายผู้ประมวลผลควบคุมประโยชน์ไว้ฝ่ายเดียว รัฐจึงเข้าแทรกแซงเพื่อ จัดสรร สิทธิ เสียใหม่ พระราชบัญญัติคุ้มครอง ข้อมูล ส่วนบุคคล พ.ศ. 2562 มาตรา 19 และมาตรา 24 คือกลไกที่ทำหน้าที่นั้นในระบบกฎหมายไทย

ในทศวรรษที่ผ่านมา การขยายตัวของแพลตฟอร์มดิจิทัลได้พลิกโฉมพฤติกรรมของมนุษย์ชาติอย่างมีนัยสำคัญ ข้อมูลส่วนบุคคล (Personal Data) ไม่ว่าจะเป็นข้อมูลระบุตัวตน ประวัติการค้นหา หรือพฤติกรรม การบริโภค ถูกรวบรวมและนำไปประมวลผลโดยบรรดาบริษัทเทคโนโลยีขนาดใหญ่ ข้อมูลเหล่านี้ได้แปรสภาพกลายเป็นสินทรัพย์ทางเศรษฐกิจที่มีมูลค่ามหาศาล กระบวนการนี้เองที่นักวิชาการหลายท่านเปรียบเทียบข้อมูลส่วนบุคคลว่าเป็น "น้ำมันของยุคดิจิทัล" ที่หล่อเลี้ยงเศรษฐกิจแพลตฟอร์มและเป็นแรงขับเคลื่อนหลักของการเติบโตทางเศรษฐกิจในศตวรรษที่ 21

จากมุมมองเชิงนิติเศรษฐศาสตร์ การที่ฝ่ายหนึ่งสามารถควบคุมผลประโยชน์จากข้อมูลได้แต่เพียงฝ่ายเดียวย่อมก่อให้เกิดความไม่สมดุลและสร้างความเสียเปรียบต่อเจ้าของข้อมูล ด้วยเหตุนี้ รัฐจึงมีความจำเป็นต้องใช้กลไกทางกฎหมายเข้ามาแทรกแซง เพื่อจัดสรรสิทธิในข้อมูลเสียใหม่ และรักษาสมดุลระหว่างการขับเคลื่อนเศรษฐกิจดิจิทัลกับการคุ้มครองสิทธิความเป็นส่วนตัวของปัจเจกชน

บทความนี้มุ่งทบทวนพัฒนาการทางกฎหมายความเป็นส่วนตัว นับตั้งแต่บทเรียนจากสงครามโลกครั้งที่สอง จนถึงการใช้กฎหมายยุคใหม่อย่าง GDPR และ PDPA โดยวิเคราะห์ผ่านกรอบเปรียบเทียบสามโมเดลโลก และ ประเมินแนวโน้มที่กฎหมายต้องรับมือต่อไปในยุคที่ปัญญาประดิษฐ์ (AI) กำลังเปลี่ยนแปลงวิถีที่โลกประมวลผลข้อมูลอย่างพื้นฐาน

## II. ปฐมบท: ภูมิหลังทางประวัติศาสตร์และสิทธิความเป็นส่วนตัวหลังสงครามโลก

รากของกฎหมายคุ้มครองข้อมูลไม่ได้ มาจากการค้า แต่ มาจาก บทเรียน ที่รัฐเผด็จการใช้ทะเบียนข้อมูล ประชากรเป็นเครื่องมือเลือกปฏิบัติและประหัตประหาร ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1948 ข้อ 12 จึงรับรองว่าบุคคลย่อมไม่ถูกแทรกแซงโดยพลการต่อความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย และการติดต่อสื่อสาร



แนวคิดเรื่องการคุ้มครองข้อมูลส่วนบุคคลไม่ได้เกิดขึ้นจากเจตจำนงในการส่งเสริมการค้า หากแต่มีรากฐานมาจากบทเรียนทางประวัติศาสตร์ที่เจ็บปวด ภายหลังสิ้นสุดสงครามโลกครั้งที่สอง ประชาคมโลกได้ประจักษ์อย่างชัดเจนว่า การที่รัฐบาลเผด็จการสามารถรวบรวมข้อมูลส่วนบุคคลของประชาชนอย่างเป็นระบบ ไม่ว่าจะเป็นข้อมูลเชื้อชาติ ศาสนา หรือที่อยู่อาศัย และนำไปใช้เป็นเครื่องมือในการเลือกปฏิบัติและประหัตประหาร ได้ก่อให้เกิดความหายนะต่อมนุษยชาติ

ด้วยเหตุนี้ ในปี ค.ศ. 1948 สมัชชาใหญ่แห่งสหประชาชาติจึงได้ให้การรับรอง **ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights: UDHR)**<sup>1</sup> ซึ่งข้อ 12 ได้บัญญัติรับรองสิทธิความเป็นส่วนตัวไว้เป็นครั้งแรกในระดับสากล

**UDHR ข้อ 12: ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1948**

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

(ไม่มีบุคคลใดจะถูกแทรกแซงโดยพลการต่อความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย หรือการติดต่อสื่อสาร หรือถูกโจมตีต่อเกียรติยศและชื่อเสียง ทุกคนมีสิทธิที่จะได้รับความคุ้มครองจากกฎหมายต่อการแทรกแซงหรือการโจมตีดังกล่าว)

ต่อมาในปี ค.ศ. 1950 สภายุโรปได้ตรา **อนุสัญญาเพื่อการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน (European Convention on Human Rights: ECHR)**<sup>2</sup> ซึ่งมาตรา 8 ได้รับรองสิทธิในการดำรงชีวิตส่วนตัวและครอบครัวในลักษณะที่มีผลผูกพันทางกฎหมายต่อรัฐภาคี

**ECHR มาตรา 8: อนุสัญญายุโรปว่าด้วยสิทธิมนุษยชน ค.ศ. 1950**

"Everyone has the right to respect for his private and family life, his home and his correspondence."

(ทุกคนมีสิทธิที่จะได้รับความเคารพต่อชีวิตส่วนตัวและครอบครัว บ้านพัก และการติดต่อสื่อสารของตน)

เอกสารทั้งสองฉบับนี้สะท้อนให้เห็นถึงการยกระดับความเป็นส่วนตัวให้เป็นสิทธิมนุษยชนขั้นพื้นฐาน มิใช่เพียงความสะดวกสบายหรือเรื่องส่วนตัว แต่เป็นเงื่อนไขที่จำเป็นต่อการดำรงอยู่ของความเป็นมนุษย์ในสังคมที่เสรีและเป็นธรรม หลักการเหล่านี้ต่อมากลายเป็นรากฐานของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศต่างๆ ทั่วโลก



### III. พัฒนาการยุคแรก: แนวทางของ OECD และการวางรากฐานของสหภาพยุโรป

เมื่อการประมวลผลด้วยคอมพิวเตอร์แพร่หลายในทศวรรษ 1970 ถึง 1980 OECD Guidelines ค.ศ. 1980 ได้วางหลักพื้นฐานที่ยังเป็นโครงของกฎหมายทุกฉบับจนวันนี้ ทั้งการจำกัดการเก็บ การระบุวัตถุประสงค์ และความรับผิดชอบ ของ ผู้ควบคุม ข้อมูล อันเป็นหลักเดียวกับ ที่ปรากฏในมาตรา 21 ถึงมาตรา 23 ของ PDPA

ในช่วงทศวรรษ 1970-1980 เมื่อระบบคอมพิวเตอร์เริ่มแพร่หลายและการประมวลผลข้อมูลส่วนบุคคลในเชิงพาณิชย์เริ่มมีบทบาทสำคัญ องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD) ได้เผยแพร่แนวปฏิบัติว่าด้วยการคุ้มครองความเป็นส่วนตัวและการส่งผ่านข้อมูลส่วนบุคคลระหว่างประเทศ (OECD Privacy Guidelines 1980)<sup>3</sup> แม้จะไม่มีสภาพบังคับโดยกฎหมาย อย่างเด็ดขาด (Soft Law) แต่ได้วางบรรทัดฐาน 8 ประการที่กลายเป็นรากฐานของกฎหมายคุ้มครองข้อมูลส่วนบุคคลทั่วโลก ได้แก่

#### OECD Privacy Guidelines 1980: หลักการ 8 ประการ

1. Collection Limitation: หลักข้อจำกัดการเก็บรวบรวม | 2. Data Quality: หลักคุณภาพของข้อมูล | 3. Purpose Specification: หลักวัตถุประสงค์ | 4. Use Limitation: หลักข้อจำกัดการใช้ | 5. Security Safeguards: หลักความมั่นคงปลอดภัย | 6. Openness: หลักความโปร่งใส | 7. Individual Participation: หลักการมีส่วนร่วมของเจ้าของข้อมูล | 8. Accountability: หลักความรับผิดชอบ

ต่อมาในปี ค.ศ. 1995 สหภาพ ยุโรปได้ยกระดับ การ คุ้มครอง เป็น กฎหมาย ที่มีผลผูกพัน ด้วยการ ตรา Directive 95/46/EC of the European Parliament and of the Council<sup>4</sup> ซึ่งเป็นกฎหมายแม่แบบที่บังคับให้รัฐสมาชิกทั้ง 15 ประเทศในขณะนั้นต้องออกกฎหมายคุ้มครองข้อมูลส่วนบุคคลภายในประเทศให้สอดคล้องกับ มาตรฐานของสหภาพยุโรป นับเป็นการเปลี่ยนผ่านจาก "หลักการ อ่อน" สู่ "พันธกรณีทางกฎหมาย" อย่างเป็นทางการครั้งแรก

### IV. จุดเปลี่ยนสำคัญ: บรรทัดฐานใหม่ภายใต้ระเบียบ GDPR ของสหภาพยุโรป

Regulation (EU) 2016/679 หรือ GDPR มีผลบังคับเต็มรูปแบบเมื่อ 25 พฤษภาคม ค.ศ. 2018 จุดเด่นคือผลบังคับนอกอาณาเขตตามข้อ 3 ที่ครอบคลุมองค์กรทั่วโลกซึ่งเสนอสินค้าหรือบริการแก่คนในสหภาพยุโรป และโทษปรับตามข้อ 83 ที่สูงถึง 20 ล้านยูโรหรือร้อยละ 4 ของรายได้ทั่วโลก



ในปี ค.ศ. 2016 สหภาพยุโรปได้สร้างบรรทัดฐานใหม่ด้วยการตรา **กฎหมายคุ้มครองข้อมูลส่วนบุคคลแห่งสหภาพยุโรป (General Data Protection Regulation: GDPR)**<sup>5</sup> ซึ่งมีผลบังคับใช้อย่างเต็มรูปแบบในวันที่ 25 พฤษภาคม ค.ศ. 2018 ความโดดเด่นที่สุดของ GDPR คือการมีผลบังคับใช้นอกอาณาเขต (Extraterritorial Effect) กล่าวคือ ตามข้อ 3(2) องค์กรที่ไม่มีสถานประกอบการในสหภาพยุโรปย่อมตกอยู่ภายใต้บังคับของกฎหมายฉบับนี้ เมื่อเสนอสินค้าหรือบริการแก่บุคคลซึ่งอยู่ในสหภาพยุโรป หรือติดตามพฤติกรรมของบุคคลดังกล่าวที่เกิดขึ้นในสหภาพยุโรป โดยไม่คำนึงว่าองค์กรนั้นจะตั้งอยู่ที่ใดในโลก

GDPR ได้วางมาตรการที่เข้มงวดหลายประการ ได้แก่ การขอความยินยอม (Consent) ที่ต้องชัดแจ้งและเพิกถอนได้โดยง่าย การรับรองสิทธิของเจ้าของข้อมูล (Data Subject Rights) อาทิ สิทธิขอให้ลบข้อมูล (Right to Erasure) และสิทธิในการโอนย้ายข้อมูล (Right to Data Portability) ตลอดจนมาตรการรักษาความมั่นคงปลอดภัยและการแจ้งเหตุละเมิดข้อมูล (Data Breach Notification) ภายใน 72 ชั่วโมง

#### GDPR มาตรา 83: โทษปรับทางปกครอง

**ระดับที่ 1:** โทษปรับสูงสุด 10 ล้านยูโร หรือร้อยละ 2 ของรายได้รวมทั่วโลกของปีบัญชีก่อนหน้า แล้วแต่จำนวนใดจะสูงกว่า สำหรับการละเมิดข้อกำหนดทั่วไป เช่น การไม่มี DPO เมื่อกฎหมายกำหนด

**ระดับที่ 2:** โทษปรับสูงสุด 20 ล้านยูโร หรือร้อยละ 4 ของรายได้รวมทั่วโลกของปีบัญชีก่อนหน้า แล้วแต่จำนวนใดจะสูงกว่า สำหรับการละเมิดหลักการพื้นฐาน เงื่อนไขความยินยอม และสิทธิของเจ้าของข้อมูล

ผลกระทบของ GDPR ต่อธุรกิจทั่วโลกนั้นมีนัยสำคัญอย่างยิ่ง บริษัทเทคโนโลยีชั้นนำหลายแห่งถูกลงโทษปรับใน ระดับ หลัก ร้อย ล้าน ถึง พัน ล้าน ยูโร โดย ในปี ค.ศ. 2023 Meta Platforms ถูกปรับ สูงสุด เป็น ประวัติการณ์ถึง 1.2 พันล้านยูโร จากการโอนย้ายข้อมูลผู้ใช้ชาวยุโรปไปยังสหรัฐอเมริกาโดยไม่ชอบ GDPR จึงไม่ใช่เพียงกฎหมายของยุโรป แต่เป็นมาตรฐานโลกที่ภาคธุรกิจต้องปฏิบัติตามโดยปริยาย

## V. บริบทของประเทศไทย: การบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 มาตรา 32 รับรองสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว อันเป็นฐานทางรัฐธรรมนูญของ PDPA พ.ศ. 2562 ซึ่งวางหลักว่าการเก็บ ใช้ หรือเปิดเผยข้อมูลต้องมีความยินยอมตามมาตรา 19 เว้นแต่เข้าข้อยกเว้นหกประการในมาตรา 24



รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560<sup>6</sup> ได้รับรองสิทธิความเป็นส่วนตัวของบุคคลไว้ในมาตรา 32 และ วรรคสอง ห้าม นำ ข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ เว้นแต่โดยอาศัยอำนาจตามกฎหมาย ซึ่งวางรากฐานทางรัฐธรรมนูญให้แก่การคุ้มครองข้อมูลส่วนบุคคล

#### รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560: มาตรา 32

"บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว

การกระทำความผิดเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ"

ต่อมาประเทศไทยได้มีการตรา พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)<sup>7</sup> ซึ่งมีผลบังคับใช้อย่างเต็มรูปแบบ เมื่อวันที่ 1 มิถุนายน 2565 กฎหมายกำหนด นิยาม ของ "ข้อมูลส่วนบุคคล" ไว้ในมาตรา 6 ดังนี้

#### พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562: มาตรา 6

"ข้อมูลส่วนบุคคล" หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ"

หลักการสำคัญที่สุดของ PDPA คือผู้ควบคุมข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนหรือในขณะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล (มาตรา 19) เว้นแต่เข้าข้อยกเว้นที่กฎหมายกำหนด สำหรับข้อมูลส่วนบุคคลทั่วไป มาตรา 24 กำหนด ข้อยกเว้น ที่ให้เก็บ รวบรวม ได้โดยไม่ต้อง ขอ ความยินยอม 6 ประการ ได้แก่ (1) เอกสาร ประวัติศาสตร์ จดหมายเหตุ การศึกษาวิจัยหรือสถิติ ที่มีมาตรการปกป้องที่เหมาะสม (2) การป้องกัน หรือ ระวังอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ (Vital Interest) (3) สัญญา (Contract) (4) ภารกิจเพื่อประโยชน์สาธารณะหรือการใช้อำนาจรัฐ (Public Task) (5) ประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest) และ (6) การปฏิบัติตามกฎหมาย (Legal Obligation) ความยินยอมจึงเป็นหลัก ส่วนทกรณีนี้เป็นข้อยกเว้น (คำอธิบายเต็มพร้อมตัวบทอยู่ในหน้า รฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล)

สำหรับข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Personal Data) ซึ่งได้แก่ ข้อมูลเชื้อชาติ ศาสนา ข้อมูลสุขภาพ ข้อมูลชีวภาพ (ลายนิ้วมือ ใบหน้า) ประวัติอาชญากรรม เป็นต้น มาตรา 26 กำหนดข้อห้ามที่เข้มงวดกว่า โดยต้องได้รับ ความยินยอมโดยชัดแจ้ง (Explicit Consent) เว้นแต่จะเข้าข้อยกเว้นที่กฎหมายกำหนดไว้โดยเฉพาะ



พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562: บทกำหนดโทษ (มาตรา 79-90)

**โทษทางปกครอง:** สูงสุด 1 ล้านบาท สำหรับการไม่แจ้งรายละเอียดการเก็บรวบรวมแก่เจ้าของข้อมูล  
ตามมาตรา 23 หรือไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 (มาตรา 82) / สูงสุด 3 ล้านบาท  
สำหรับการเก็บหรือใช้ข้อมูลโดยไม่มีฐานทางกฎหมาย หรือการส่งหรือโอนข้อมูลไปต่างประเทศโดยไม่เป็นไป  
ตามมาตรา 28 หรือมาตรา 29 (มาตรา 83) / สูงสุด 5 ล้านบาท สำหรับการเก็บ ใช้เปิดเผย หรือส่งข้อมูล  
อ่อนไหวตามมาตรา 26 โดยมีขอบ (มาตรา 84)

**โทษอาญา:** จำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ สำหรับการใช้หรือเปิดเผย  
ข้อมูลอ่อนไหวโดยมิชอบในประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือ  
ได้รับความอับอาย / จำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งล้านบาท หรือทั้งจำทั้งปรับ หากกระทำเพื่อแสวงหา  
ประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมาย (มาตรา 79 ซึ่งเป็นความผิดอันยอมความได้)

หัวใจสำคัญของการบังคับใช้ PDPA คือการส่งสัญญาณว่า มาตรฐานสากลด้านการคุ้มครองข้อมูลส่วนบุคคล  
ได้ถูกผนวกเข้าเป็นส่วนหนึ่งของระบบกฎหมายไทยแล้ว และองค์กรธุรกิจจำเป็นต้องปรับปรุงกระบวนการ  
ทำงานและสร้างธรรมาภิบาลข้อมูล (Data Governance) ให้เกิดขึ้นอย่างเป็นรูปธรรม

### แนวปฏิบัติอย่างเป็นทางการและกรณีศึกษาจากการบังคับใช้

นับตั้งแต่ PDPA มีผลบังคับใช้เต็ม รูปแบบ ใน วันที่ 1 มิถุนายน 2565 คณะกรรมการ คุ้มครอง ข้อมูล ส่วน  
บุคคลได้เผยแพร่ แนวปฏิบัติสำหรับผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล: กรณี  
ศึกษา จาก ข้อหารือเกี่ยวกับการบังคับใช้ พระราชบัญญัติ คุ้มครอง ข้อมูล ส่วนบุคคล พ.ศ. 2562<sup>8</sup> ฉบับ  
เผยแพร่ 10 กุมภาพันธ์ 2566 ซึ่งรวบรวม สรุป ความเห็น ของ คณะ อนุกรรมการ เฉพาะกิจ ในการ ตอบ ข้อ  
หารือ ครอบคลุมหน่วยงานรัฐ ภาคเอกชน นิติบุคคล และบุคคลธรรมดา เอกสารดังกล่าวสะท้อนให้เห็นว่า  
แม้ตัวบทกฎหมายจะกำหนดหลักการไว้อย่างชัดเจน แต่การประยุกต์ใช้ในบริบทต่างๆ ยังต้องอาศัยการ  
ตีความที่ละเอียดรอบคอบในแต่ละกรณี

หนึ่งในประเด็นที่ได้รับการวินิจฉัยบ่อยครั้ง คือขอบเขตของการยกเว้นการบังคับใช้ตามมาตรา 4 โดยเฉพาะ  
การยกเว้นสำหรับกระบวนการยุติธรรมทางอาญาตามมาตรา 4 (5) ซึ่งมีนัยสำคัญต่อหน่วยงานรัฐและ  
องค์กรกำกับดูแลที่มีหน้าที่ด้านการบังคับใช้กฎหมาย ข้อยกเว้นนี้ไม่ได้ลดสิทธิของบุคคลที่ถูกดำเนินคดี  
สิทธิได้รับแจ้งข้อกล่าวหา สิทธิที่จะไม่ให้การ และสิทธิมีทนายความยังอยู่ในประมวลกฎหมายวิธีพิจารณา  
ความอาญา ดู สิทธิของผู้ถูกจับและผู้ต้องหา



คำวินิจฉัยคณะกรรมการ PDPA: ขอบเขตการยกเว้น มาตรา 4 (5) กระบวนการยุติธรรมทางอาญา

**กรณีที่ได้รับยกเว้น:** การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อนำไปใช้ในกระบวนการที่นำไปสู่การลงโทษผู้กระทำความผิดทางอาญา รวมถึงภารกิจของ ป.ป.ช. ในฐานะที่ใช้อำนาจสอบสวนเทียบเท่าพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา

**กรณีที่ไม่ได้รับยกเว้น:** การดำเนินงานธุรการทั่วไปของหน่วยงานเดียวกันที่ไม่เกี่ยวกับกระบวนการอาญา และการลงโทษทางวินัยที่ไม่เกี่ยวเนื่องกับความผิดอาญา ซึ่งต้องปฏิบัติตาม PDPA ตามปกติ

**หมายเหตุสำคัญ:** แม้ได้รับ ยกเว้น หน่วยงาน ยังคง ต้อง รักษา ความมั่นคง ปลอดภัย ของ ข้อมูล ส่วนบุคคล ตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด ตามมาตรา 4 วรรคสาม

ประเด็นที่สร้างความสับสนอย่างมากในทางปฏิบัติคือการนำ **ข้อมูลชีวภาพ (Biometric Data)** มาใช้ในชีวิตประจำวัน งานวิจัยทางวิชาการ<sup>9</sup> ได้วิเคราะห์กรณีที่มีผู้ประกอบการหอพักเอกชนต้องการใช้ระบบสแกนใบหน้าของผู้พักเพื่อควบคุมการเข้าออก ซึ่งแสดงให้เห็นความแตกต่างระหว่างข้อมูลส่วนบุคคลทั่วไปและข้อมูลอ่อนไหวในเชิงปฏิบัติอย่างชัดเจน

**กรณีศึกษา: ข้อมูลชีวภาพ (Biometric Data) กับการควบคุมการเข้าออกหอพัก: มาตรา 24 และมาตรา 26 PDPA**

**ข้อมูลทั่วไป (มาตรา 24):** การเก็บข้อมูลทั่วไปเพื่อควบคุมการเข้าออก เช่น ข้อมูลบัตรอิเล็กทรอนิกส์ อาจอ้างฐานทางกฎหมาย "ประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest)" ตามมาตรา 24 (5) ได้ หากประโยชน์ดังกล่าวไม่มีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูล

**ข้อมูลชีวภาพ (มาตรา 26):** ภาพจำลองใบหน้าที่ได้จากการสแกนจัดเป็น "ข้อมูลชีวภาพ" ซึ่งเป็นข้อมูลส่วนบุคคลอ่อนไหวตามมาตรา 26 ต้องมีฐานทางกฎหมายพิเศษ ได้แก่ ความยินยอมโดยชัดแจ้ง (Explicit Consent) หรือข้อยกเว้นตามมาตรา 26 (1) ถึง (5) เช่น มาตรา 26 (5) ซึ่งต้องเป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ที่กำหนด อาทิ ประโยชน์สาธารณะที่สำคัญ อย่างไรก็ตาม ไม่มีกฎหมายใดกำหนดให้ผู้ประกอบการหอพักต้องเก็บข้อมูลชีวภาพเพื่อควบคุมการเข้าออก จึงไม่เข้าข้อยกเว้น

**ข้อสรุปทางกฎหมาย:** ต้องขอ Explicit Consent ตามเงื่อนไขกฎหมาย หรือปรับเปลี่ยนมาตรการโดยใช้วิธีที่ไม่เก็บข้อมูลชีวภาพ เช่น Key Card แทน ซึ่งเป็นทางเลือกที่ได้สัดส่วนกว่าและสอดคล้องกับหลัก Data Minimisation

ภาคสุขภาพเป็นหนึ่งในภาคส่วนที่ต้องเผชิญกับความท้าทายสูงสุดในการปฏิบัติตาม PDPA เนื่องจากข้อมูลสุขภาพเป็นข้อมูลอ่อนไหวตามมาตรา 26 และโรงพยาบาลต้องทำงานอยู่ในกรอบกฎหมายหลายฉบับซ้อนทับกัน ได้แก่ พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 มาตรา 7 และพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 24 ก่อนที่ PDPA จะมีผลบังคับใช้ งานวิจัยที่ตีพิมพ์ในวารสาร Rangsit Journal of Law and Society ปี 2025<sup>10</sup> ได้ระบุปัญหาหลักสี่ประการในการบังคับใช้ PDPA กับโรงพยาบาลของรัฐ ดังนี้



ปัญหาในการบังคับใช้ PDPA กับโรงพยาบาลของรัฐ: วารสารกฎหมายและสังคมรังสิต ปีที่ 7 ฉบับที่ 1 (2568)

- (1) ความคลุมเครือใน นิยาม: พ.ร.บ. ไม่ได้บัญญัติ นิยาม "ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data)" และ "ข้อมูลสุขภาพ" อย่างเป็นทางการและชัดเจน ก่อให้เกิดปัญหาการตีความว่าข้อมูลใดคือ "ข้อมูลสุขภาพ" และอยู่ภายใต้มาตรา 26 หรือเพียงแค่อข้อมูลที่เกี่ยวข้องกับสุขภาพ
- (2) การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO): ยังไม่มีหลักเกณฑ์ที่ชัดเจนสำหรับ คุณสมบัติของ DPO ในสถานพยาบาล ซึ่งต้องการความรู้ทั้งด้านกฎหมายคุ้มครองข้อมูล ด้านเทคโนโลยีสารสนเทศ และด้านการแพทย์ควบคู่กัน
- (3) การประเมินผลกระทบด้านการคุ้มครองข้อมูล (DPIA): การกำหนดอำนาจหน้าที่ของ DPO ในการประเมินความเสี่ยงของผลกระทบจากการประมวลผลข้อมูลขนาดใหญ่ในบริบทโรงพยาบาลยังขาดความชัดเจน
- (4) การแจ้งเหตุละเมิดข้อมูล (Data Breach Notification): ไม่มีข้อกำหนดการบันทึกรายละเอียดเหตุละเมิดข้อมูลไว้เป็นหลักฐาน ส่งผลให้ยากต่อการตรวจสอบย้อนหลังและการวิเคราะห์แนวโน้ม อันอาจนำไปสู่ความบกพร่องในการป้องกันเหตุการณ์ซ้ำในอนาคต

นอกจากนี้ กฎหมายยังกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) ในกรณีที่กิจกรรมหลักเกี่ยวข้องกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอ่อนไหวตามมาตรา 26 อย่างเป็นระบบ โดยมาตรา 41 วรรคเจ็ดเปิดช่องให้ DPO เป็นได้ทั้งพนักงานภายในองค์กรหรือผู้รับจ้างจากภายนอก ซึ่งมีข้อดีข้อเสียที่แตกต่างกันไปตามลักษณะและขนาดขององค์กร

## VI. บทวิเคราะห์เปรียบเทียบแบบการคุ้มครองข้อมูลส่วนบุคคล (Privacy Models)

กฎหมายคุ้มครองข้อมูลทั่วโลกแยกได้สามโมเดล คือโมเดลสิทธิมนุษยชนแบบยุโรปที่ถือความเป็นส่วนตัวเป็นสิทธิขั้นพื้นฐาน โมเดลขับเคลื่อนด้วยตลาดแบบสหรัฐอเมริกาที่ใช้กฎหมายรายสาขา และโมเดลสมดุลแบบเอเชีย ไทยรับโครงของ GDPR มาไว้ในมาตรา 19 ถึงมาตรา 28 ของ PDPA แต่กำหนดเพดานโทษให้เข้ากับบริบทของตน จึงจัดอยู่ในกลุ่มที่แสวงหาจุดสมดุล

เมื่อ พิจารณา กฎหมาย คุ้มครอง ข้อมูล ส่วนบุคคล ใน ระดับโลก สามารถ จำแนก ได้เป็น สาม โมเดล หลัก ซึ่ง แต่ละโมเดล สะท้อนปรัชญาทางกฎหมายและการเมืองที่แตกต่างกันอย่างมีนัยสำคัญ



### โมเดลที่ 1: โมเดลยุโรป (The Human Rights Model)

สหภาพยุโรปมองว่าความเป็นส่วนตัวคือสิทธิมนุษยชนขั้นพื้นฐาน กฎหมายจึงมีความเข้มงวดและมุ่งเน้นการควบคุมอำนาจของภาคธุรกิจในการประมวลผลข้อมูล หลักการ "ความเป็นส่วนตัวโดยการออกแบบ" (Privacy by Design) และ "ความเป็นส่วนตัวโดยค่าเริ่มต้น" (Privacy by Default) ถูกบังคับใช้อย่างจริงจัง GDPR เป็นตัวแทนที่ชัดเจนที่สุดของโมเดลนี้

### โมเดลที่ 2: โมเดลสหรัฐอเมริกา (The Market-Driven Model)

สหรัฐอเมริกายังไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลในระดับประเทศ แต่ใช้กลไกตลาดและกฎหมายเฉพาะสาขา (Sectoral Laws) เป็นหลัก โดยถือว่าความเป็นส่วนตัวเป็นเรื่องของการเลือกของผู้บริโภคในตลาด รัฐแคลิฟอร์เนียเป็นผู้นำด้วยการออก California Consumer Privacy Act (CCPA)<sup>11</sup> ซึ่งมีผลบังคับใช้ตั้งแต่ปี ค.ศ. 2020 และถือเป็นต้นแบบของกฎหมายระดับมลรัฐหลายฉบับที่ตามมา

### โมเดลที่ 3: โมเดลเอเชีย (The Balanced Model)

หลายประเทศในเอเชียกำลังมุ่งแสวงหาจุดสมดุลระหว่างการเติบโตทางเศรษฐกิจดิจิทัลและการคุ้มครองสิทธิ ตัวอย่างที่โดดเด่นที่สุดคือ Personal Information Protection Law of the People's Republic of China (PIPL)<sup>12</sup> ของสาธารณรัฐประชาชนจีน ซึ่งมีมาตรฐานความเข้มงวดสูงในระดับเดียวกับ GDPR แต่มีปรัชญาที่แตกต่างกันอย่างสิ้นเชิง ขณะที่ GDPR มุ่งคุ้มครองบุคคลจากอำนาจขององค์กรธุรกิจ PIPL กลับมุ่งควบคุมการไหลเวียนของข้อมูลออกนอกประเทศ และรักษาอำนาจของรัฐในการเข้าถึงข้อมูล PDPA ของไทยอยู่ในกลุ่มโมเดลเอเชียที่พยายามสร้างสมดุลดังกล่าว

## VII. ความท้าทายในอนาคต: ปัญญาประดิษฐ์ (AI) กับข้อจำกัดของกฎหมาย

การเรียนรู้ของโมเดลปัญญาประดิษฐ์ใช้ข้อมูลในลักษณะที่ระบุวัตถุประสงค์ล่วงหน้าได้ยาก จึงปะทะกับหลักความจำกัดของวัตถุประสงค์ที่ PDPA วางไว้ในมาตรา 21 สหภาพยุโรปตอบด้วย Regulation (EU) 2024/1689 ซึ่งกำกับดูแลตามระดับความเสี่ยง ส่วนไทยยังไม่มีกฎหมายเฉพาะรองรับ



วิวัฒนาการของปัญญาประดิษฐ์ (AI) ที่ต้องอาศัยชุดข้อมูลขนาดใหญ่ในการประมวลผล กำลังสร้างความท้าทายต่อหลักการของ PDPA โดยเฉพาะ "หลักความจำกัดของวัตถุประสงค์ (Purpose Limitation)" ที่ห้ามมิให้นำข้อมูลไปใช้เกินกว่าวัตถุประสงค์ที่ได้แจ้งและขอความยินยอมไว้แต่แรก กระบวนการเรียนรู้ของโมเดล AI มักใช้ข้อมูลในลักษณะที่กว้างและยากต่อการกำหนดวัตถุประสงค์ล่วงหน้าได้อย่างชัดเจน ซึ่งอาจขัดกับหลักความโปร่งใสที่ PDPA กำหนด

ในปี ค.ศ. 2024 สหภาพยุโรปได้ตรา **Artificial Intelligence Act (AI Act)**<sup>13</sup> ซึ่งเป็นกฎหมายกำกับดูแล AI แบบครอบคลุมฉบับแรกของโลก มีผลใช้บังคับวันที่ 1 สิงหาคม ค.ศ. 2024 และทยอยใช้บังคับกับปัญญาประดิษฐ์แต่ละส่วนเป็นระยะตั้งแต่ปี ค.ศ. 2025 โดยจำแนก AI ตามระดับความเสี่ยง (Risk-based Approach)

Regulation (EU) 2024/1689: EU AI Act หรือ กฎระเบียบว่าด้วยปัญญาประดิษฐ์แห่งสหภาพยุโรป: การจำแนกระดับความเสี่ยง

- (1) ความเสี่ยงที่ยอมรับไม่ได้ (Unacceptable Risk): ห้ามโดยเด็ดขาด เช่น ระบบคะแนนทางสังคม (Social Scoring) และการใช้ระบบระบุตัวบุคคลด้วยข้อมูลชีวภาพจากระยะไกลแบบเวลาจริง (Real-time) ในพื้นที่สาธารณะเพื่อการบังคับใช้กฎหมาย เว้นแต่กรณีจำเป็นที่ข้อ 5 กำหนดไว้อย่างจำกัด
- (2) ความเสี่ยงสูง (High Risk): ต้องมีการตรวจสอบ ประเมินความเสี่ยง และลงทะเบียนก่อนใช้งาน เช่น AI ในระบบสินเชื่อ การจ้างงาน และการบังคับใช้กฎหมาย
- (3) ความเสี่ยงจำกัด (Limited Risk): ต้องแจ้งผู้ใช้งานที่กำลังติดต่อกับ AI เช่น Chatbot
- (4) ความเสี่ยงต่ำ (Minimal Risk): ไม่มีข้อกำหนดเฉพาะ

สำหรับประเทศไทย แม้ปัจจุบันจะยังไม่มีกฎหมายกำกับดูแล AI โดยเฉพาะ แต่องค์กรกำกับดูแลจำเป็นต้องตีความ และ ปรับใช้ หลักเกณฑ์ ของ PDPA ให้เท่าทัน ต่อ พลวัต ของ เทคโนโลยี เพื่อ รักษา สมดุล ระหว่าง นวัตกรรมและสิทธิความเป็นส่วนตัว

## VIII. แนวโน้มและประเด็นทางกฎหมายที่ต้องจับตา

แนวโน้มสามประการที่ต้องจับตาคือ ประสิทธิภาพของการบังคับใช้เมื่อองค์กรมองค่าปรับตามมาตรา 82 ถึงมาตรา 84 เป็นเพียงต้นทุนในการดำเนินธุรกิจ การเกิดตลาดซื้อขายข้อมูลที่กฎหมายยังไม่มีกรอบรองรับ และการที่เทคโนโลยีเดินเร็วกว่ากฎหมายจนต้องอาศัยประกาศของคณะกรรมการเป็นเครื่องมือตามให้ทัน

จากการวิเคราะห์พัฒนาการของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในภาพรวม สามารถระบุแนวโน้มสำคัญสามประการที่จะมีผลต่อทิศทางกฎหมายในระยะข้างหน้า



1. ความท้าทายในการบังคับใช้กฎหมาย (Enforcement Challenges): องค์กรบางแห่งยังคงมองค่าปรับเป็นเพียง "ต้นทุนในการดำเนินธุรกิจ" ซึ่งเป็นประเด็นที่หน่วยงานกำกับดูแลต้องพัฒนากลไกบังคับใช้ให้มีประสิทธิภาพและสร้างความเกรงกลัวต่อการละเมิดอย่างแท้จริง รวมถึงการพัฒนาแนวทางปฏิบัติที่ชัดเจนสำหรับภาคธุรกิจในสาขาต่างๆ
2. นวัตกรรมตลาดข้อมูล (Data Monetization): เมื่อข้อมูลมีมูลค่าเชิงพาณิชย์สูงขึ้น รูปแบบการทำธุรกิจซื้อขายและแลกเปลี่ยนข้อมูลจะทวีความซับซ้อน กฎหมายต้องสร้างความชัดเจนในประเด็นความโปร่งใสและอำนาจควบคุมของเจ้าของข้อมูล รวมถึงกรอบกฎหมายสำหรับ "ตลาดข้อมูล" (Data Marketplace) ที่กำลังเติบโตอย่างรวดเร็ว
3. ข้อจำกัดของหลักความยินยอม (Consent Fatigue): แนวคิดที่พึ่งพา "ความยินยอม" เพียงฐานเดียวเริ่มแสดงข้อจำกัดในทางปฏิบัติ เนื่องจากผู้บริโภคมักกดยินยอมโดยไม่ได้อ่านเงื่อนไข แนวโน้มทางปฏิบัติในหลายเขตอำนาจจึงมุ่งไปสู่การพิจารณาใช้ "ฐานประโยชน์อันชอบธรรม (Legitimate Interests)" มากยิ่งขึ้น ซึ่งต้องอาศัยการตีความของผู้ควบคุมข้อมูลที่ระมัดระวังและโปร่งใส

## IX. บทสรุป

PDPA พ.ศ. 2562 ประกาศว่ามาตรฐานสากลด้านการคุ้มครองข้อมูลได้กลายเป็นส่วนหนึ่งของระบบกฎหมายไทยแล้ว สำหรับภาคธุรกิจ การปฏิบัติตามมาตรา 19 มาตรา 23 และมาตรา 37 จึงไม่ใช่ภาระตามกฎหมายเพียงอย่างเดียว แต่เป็นเงื่อนไขของความน่าเชื่อถือในตลาดที่คู่ค้าตรวจสอบเรื่องนี้จริง

สิทธิความเป็นส่วนตัวไม่ใช่เพียงข้อเรียกร้องเพื่อความสะดวกสบายในโลกยุคดิจิทัล หากแต่เป็นสิทธิขั้นพื้นฐานที่ผลักดันมาจากบทเรียนทางประวัติศาสตร์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของไทย แม้จะเป็นเพียงจุดเริ่มต้นและอาจต้องเผชิญกับการปรับปรุงแก้ไขเพื่อให้สอดคล้องกับพลวัตของเทคโนโลยี แต่กฎหมายฉบับนี้ได้วางรากฐานอันสำคัญให้แก่ประเทศ ด้วยการประกาศว่ามาตรฐานสากลด้านการคุ้มครองข้อมูลส่วนบุคคลได้กลายเป็นส่วนหนึ่งของระบบกฎหมายไทยแล้ว

สำหรับภาคธุรกิจ การปฏิบัติตาม PDPA ไม่ควรถูกมองเป็นเพียงภาระในการปฏิบัติตามกฎหมาย (Legal Compliance) แต่ควรตระหนักว่าเป็นกลยุทธ์สำคัญในการสร้างความเชื่อมั่น (Trust) และยกระดับมาตรฐานทางธุรกิจให้สามารถแข่งขันได้ในระดับสากลอย่างยั่งยืน ในยุคที่ผู้บริโภคทั่วโลกตื่นตัวและให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลมากขึ้นทุกวัน การมีระบบ Data Governance ที่ดีจึงมิใช่ทางเลือก แต่เป็นมาตรฐานพื้นฐานที่ธุรกิจยุคใหม่ต้องมี



## เชิงอรรถ

1. Universal Declaration of Human Rights (UDHR), Article 12, adopted by UN General Assembly Resolution 217A (III), 10 December 1948. [ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน]
2. European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), Article 8, signed Rome 4 November 1950. [มาตรา 8 ECHR รับประกันสิทธิในความเป็นส่วนตัว]
3. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), Organisation for Economic Co-operation and Development, Paris. [แนวปฏิบัติ OECD 8 หลักการ]
4. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data [1995] OJ L 281/31. [กฎหมายคุ้มครองข้อมูลฉบับแรกของ EU]
5. Regulation (EU) 2016/679 (GDPR) [2016] OJ L 119/1, entered into force 24 May 2016 and applicable from 25 May 2018 (Article 99). [GDPR มีผลบังคับนอกอาณาเขต EU]
6. รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560, มาตรา 32. [รัฐธรรมนูญไทยรับรองสิทธิในความเป็นส่วนตัว]
7. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, ประกาศในราชกิจจานุเบกษา เล่ม 136 ตอนที่ 69 ก วันที่ 27 พฤษภาคม 2562 มีผลบังคับใช้เต็มรูปแบบวันที่ 1 มิถุนายน 2565. [PDPA ไทย]
8. สำนักงาน คณะกรรมการ คุ้มครอง ข้อมูลส่วนบุคคล, แนวปฏิบัติ สำหรับ ผู้ควบคุม ข้อมูล ส่วนบุคคล และ ผู้ประมวลผลข้อมูล ส่วนบุคคล: กรณีศึกษาจากข้อหาหรือเกี่ยวกับการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, เผยแพร่ 10 กุมภาพันธ์ 2566, คณะอนุกรรมการเฉพาะกิจตอบข้อหารือและให้คำแนะนำหน่วยงานของรัฐ. [แนวปฏิบัติ PDPA อย่างเป็นทางการจากคณะกรรมการ PDPA]
9. ขาญชัย แสงศักดิ์ และ คณาธิป ทองรวีวงศ์, "การคุ้มครองสิทธิผู้พักของหอพักเอกชนในกรณีการเก็บรวบรวมข้อมูลสแกนใบหน้าเพื่อควบคุมการผ่านเข้าออก: ศึกษาข้อยกเว้นของความยินยอมตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562", วารสารบริหารธุรกิจและสังคมศาสตร์ มหาวิทยาลัยรามคำแหง, ปีที่ 9 ฉบับพิเศษการประชุมวิชาการระดับชาติ HTLC ครั้งที่ 14, คณะนิติศาสตร์ มหาวิทยาลัยเกษมบัณฑิต. [การวิเคราะห์ Biometric Data กับมาตรา 24 และ 26 PDPA]
10. ศิริกร สีสดี, "ปัญหา การบังคับใช้ กฎหมาย คุ้มครอง ข้อมูล ส่วนบุคคล ใน โรงพยาบาล ของ รัฐ", *Rangsit Journal of Law and Society*, ปีที่ 7 ฉบับที่ 1 (มกราคม ถึง เมษายน 2568), หน้า 16-30, สำนักงานสาธารณสุขจังหวัดฉะเชิงเทรา โรงพยาบาลพุทธโสธร, กระทรวงสาธารณสุข; Received 11 December 2024, Accepted 20 March 2025. [ปัญหาการบังคับใช้ PDPA ในภาคสาธารณสุข]
11. California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code § 1798.100 et seq., in effect 1 January 2020. [CCPA เป็นตัวอย่างโมเดลอเมริกา]
12. Personal Information Protection Law of the People's Republic of China (PIPL), promulgated 20 August 2021, effective 1 November 2021. [กฎหมาย PIPL ของจีน]
13. Regulation (EU) 2024/1689 of the European Parliament and of the Council on Artificial Intelligence (AI Act) [2024] OJ L 2024/1689, in force August 2024. [EU AI Act จัดประเภท AI ตามระดับความเสี่ยง]

