เอกสารวิชาการส่วนบุคคล
(Individual Study)

หลักนิติธรรมในการคุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงิน ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

จัดทำโดย นายพลากร หวั่งหลี
รหัส ๖๘๑๓๒๓

รายงานนี้เป็นส่วนหนึ่งของการอบรม
หลักสูตร “หลักนิติธรรมเพื่อประชาธิปไตย” (นธป.) รุ่นที่ ๑๓
วิทยาลัยศาลรัฐธรรมนูญ
สำนักงานศาลรัฐธรรมนูญ

หลักนิติธรรมในการคุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงิน ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

พลากร หวั่งหลี[๑]

บทคัดย่อ

หลักนิติธรรมเป็นหลักการพื้นฐานในรัฐธรรมนูญและการปกครองในระบอบประชาธิปไตย ที่ส่งผลโดยตรงต่อการออกกฎหมายและการบังคับใช้กฎหมาย รวมถึงในด้านการคุ้มครองข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งในบริบทของสถาบันการเงินที่มีการประมวลผลข้อมูลส่วนบุคคลในระดับสูง มีความเสี่ยงต่อสิทธิในความเป็นส่วนตัวของบุคคลอย่างมาก การบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ จึงต้องยึดโยงกับหลักนิติธรรมเพื่อให้การใช้ข้อมูลเป็นไปอย่างชอบด้วยกฎหมาย สำหรับแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคารที่จัดทำโดยสมาคมธนาคารไทยนับเป็นกรอบแนวนโยบายที่มีบทบาทสำคัญอย่างยิ่งในการกำกับดูแลและยกระดับมาตรฐาน การจัดการข้อมูลส่วนบุคคลของภาคการเงินไทย แนวปฏิบัติดังกล่าวไม่เพียงแต่ตอบสนองต่อข้อกำหนดทางกฎหมาย หากยังแสดงให้เห็นถึงความตระหนักของภาคธนาคารต่อความเสี่ยงด้านความเป็นส่วนตัวของลูกค้าในยุคดิจิทัล ที่ข้อมูลกลายเป็นทรัพย์สินอันมีคุณค่าและเป็นเป้าหมายของภัยคุกคามทางไซเบอร์ ด้วยลักษณะของธุรกิจธนาคารซึ่งมีการเก็บรวบรวม ใช้และเปิดเผยข้อมูลส่วนบุคคลในปริมาณมากและอย่างต่อเนื่อง ความรับผิดชอบในการดูแลข้อมูลเหล่านี้ย่อมต้องอาศัยกลไกการบริหารจัดการที่มีประสิทธิภาพ ซึ่งได้ให้ความสำคัญกับกระบวนการจัดการข้อมูลในทุกมิติ กล่าวได้ว่า แนวปฏิบัตินี้เป็นส่วนสำคัญในการขับเคลื่อนให้ภาคธนาคารสามารถดำเนินงานตามกรอบกฎหมายได้อย่างมีประสิทธิภาพและลดความเสี่ยงทางกฎหมาย อีกทั้งยังช่วยเสริมสร้างความเชื่อมั่นของประชาชนต่อระบบการเงินของประเทศในระยะยาว โดยเฉพาะในยุคที่ความน่าเชื่อถือและความโปร่งใสกลายเป็นหัวใจสำคัญของการทำธุรกิจทางการเงิน

คำสำคัญ หลักนิติธรรม, ข้อมูลส่วนบุคคล, ความเป็นส่วนตัว, สถาบันการเงิน, ยุคดิจิทัล

[๑] พลากร หวั่งหลี, อนุกรรมาธิการด้านตลาดทุนและประกันภัย ในคณะกรรมาธิการการเศรษฐกิจ การเงิน และการคลัง วุฒิสภา.

บทนำ

ในยุคเศรษฐกิจดิจิทัลซึ่งขับเคลื่อนด้วยข้อมูลเป็นหัวใจหลัก ข้อมูลส่วนบุคคลได้กลายเป็นทรัพยากรสำคัญของการดำเนินธุรกิจโดยเฉพาะในภาคธุรกิจธนาคาร ซึ่งต้องอาศัยการประมวลผลข้อมูลของลูกค้าอย่างต่อเนื่องและเป็นระบบ ความไว้วางใจของประชาชนที่มีต่อสถาบันการเงินจึงขึ้นอยู่กับระดับความรับผิดชอบในการจัดการและคุ้มครองข้อมูลส่วนบุคคลอย่างถูกต้องตามหลักกฎหมายและจริยธรรม ซึ่ง “หลักนิติธรรม” (Rule of Law) ทำหน้าที่เป็นกรอบคุณค่าสำคัญในการรับรอง สิทธิเสรีภาพและศักดิ์ศรีความเป็นมนุษย์ของเจ้าของข้อมูลพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ได้วางรากฐานของระบบการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย โดยบัญญัติให้ “ผู้ควบคุมข้อมูลส่วนบุคคล” และ “ผู้ประมวลผลข้อมูลส่วนบุคคล” ต้องดำเนินการอย่างมีความรับผิดชอบ โปร่งใส เป็นธรรม และภายใต้ขอบเขตตามวัตถุประสงค์ที่แจ้งไว้ล่วงหน้า แนวทางเหล่านี้สอดคล้องกับหลักนิติธรรมที่ให้ความสำคัญต่อการใช้กฎหมายโดยไม่เลือกปฏิบัติ การตรวจสอบได้ และการรับผิดของผู้ใช้อำนาจต่อประชาชน[๒]

ในบริบทของภาคธุรกิจธนาคาร สถาบันการเงินมีลักษณะเฉพาะในฐานะผู้ถือครองข้อมูลที่มีความอ่อนไหวสูง เช่น ข้อมูลทางการเงิน บัญชี รายได้ การกู้ยืม และพฤติกรรมการใช้บริการทางการเงิน ซึ่งอาจนำไปสู่ความเสียหายร้ายแรงหากเกิดการรั่วไหลหรือนำไปใช้โดยมิชอบ ด้วยเหตุนี้ สมาคมธนาคารไทยจึงได้จัดทำแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคาร เพื่อใช้เป็นกรอบเสริมในการปฏิบัติตามกฎหมาย โดยมีเป้าหมายเพื่อยกระดับมาตรฐานการคุ้มครองข้อมูลให้เทียบเท่าระดับสากล[๓] แนวปฏิบัติดังกล่าวได้แปลความหลักการตามพระราชบัญญัติฯ ให้เหมาะสมกับลักษณะการดำเนินงานของธนาคารพาณิชย์ไทย เช่น การบริหารจัดการคำยินยอม การจำกัดการเข้าถึงข้อมูลภายในองค์กร และการกำกับดูแลคู่สัญญาภายนอก

ดังนั้น การบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ควบคู่กับแนวปฏิบัติเฉพาะของภาคธนาคาร ต้องดำเนินการภายใต้หลักนิติธรรม โดยเน้นความชอบด้วยกฎหมาย ความโปร่งใส และความรับผิดชอบ ธนาคารต้องเคารพสิทธิของเจ้าของข้อมูล ดำเนินการตามหลักความจำเป็น พร้อมมีระบบกำกับตรวจสอบภายในที่ชัดเจน สร้างระบบการคุ้มครองข้อมูลส่วนบุคคลที่มีความสมดุลระหว่างประโยชน์เชิงธุรกิจกับสิทธิพื้นฐานของประชาชนในยุคข้อมูลเป็นศูนย์กลางเพื่อให้การประมวลผลข้อมูลเป็นธรรมและอยู่ภายใต้กรอบกฎหมายอย่างแท้จริง

---

[๒] ศาสตราจารย์ ดร.บวรศักดิ์ อุวรรณโณ, หลักนิติธรรมกับการบริหารราชการแผ่นดิน, (กรุงเทพฯ: วิญญูชน, ๒๕๕๑), หน้า ๑๘–๒๐.

[๓] สมาคมธนาคารไทย, แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคาร (Banking Sector Privacy Guidelines),ฉบับเดือนพฤษภาคม ๒๕๖๕, หน้า ๓–๕.

หลักนิติธรรม (Rule of Law)

หลักนิติธรรม (Rule of Law) คือ หลักการที่กำหนดให้การใช้อำนาจของรัฐต้องอยู่ภายใต้กฎหมายที่มีลักษณะเป็นกลาง เป็นธรรม และบัญญัติขึ้นเพื่อประโยชน์สาธารณะ ไม่ใช่เพื่อประโยชน์ของบุคคลหรือกลุ่มใดกลุ่มหนึ่งโดยเฉพาะ โดยเน้นการคุ้มครองสิทธิเสรีภาพของประชาชน การจำกัดอำนาจรัฐ และการให้ศาลทำหน้าที่ตรวจสอบความชอบด้วยกฎหมายของการใช้อำนาจรัฐ หลักนิติธรรมเป็นรากฐานสำคัญในการสร้างระบบกฎหมายที่ยึดหลักความยุติธรรม ความโปร่งใส และตรวจสอบได้ซึ่งหลักการนี้มีบทบาทสำคัญในการกำกับดูแลการประมวลผลข้อมูลส่วนบุคคลในยุคดิจิทัลที่ข้อมูลสามารถถูกเก็บ ใช้ หรือเปิดเผยได้อย่างง่ายดาย หากปราศจากการควบคุมตามหลักนิติธรรม อาจส่งผลให้เกิดการละเมิดสิทธิในความเป็นส่วนตัวอย่างร้ายแรง

องค์ประกอบของหลักนิติธรรม ตามแนวคิดของ A.V. Dicey[๔] นักนิติศาสตร์ชาวอังกฤษซึ่งเป็นผู้บุกเบิกแนวคิดเรื่องนี้ ได้เสนอหลักการของ Rule of Law ไว้ ๓ ประการหลัก ได้แก่

๑. ความมีอำนาจสูงสุดของกฎหมาย (Supremacy of Law) หมายถึง ไม่มีบุคคลใดไม่ว่าจะเป็นเจ้าหน้าที่รัฐหรือพลเมืองธรรมดาอยู่เหนือกฎหมายและไม่สามารถใช้อำนาจตามอำเภอใจได้

๒. ความเสมอภาคภายใต้กฎหมาย (Equality Before the Law) ทุกคนในประเทศไม่ว่าจะมีสถานะทางสังคมใด ต้องอยู่ภายใต้กฎหมายเดียวกัน และได้รับการพิจารณาคดีในศาลเดียวกัน

๓. สิทธิขั้นพื้นฐานของประชาชนได้รับการคุ้มครองผ่านกฎหมายทั่วไป (The Constitution is the Result of the Ordinary Law) สิทธิเสรีภาพของประชาชนไม่ได้เกิดจากรัฐธรรมนูญโดยตรง แต่เป็นผลมาจากคำพิพากษาและกฎหมายทั่วไปที่พัฒนาขึ้นตามแนวทางของศาล

แนวคิดร่วมสมัยของหลักนิติธรรม ในยุคปัจจุบันหลักนิติธรรมได้รับการขยายขอบเขตให้ครอบคลุมมากกว่าความหมายเชิงรูปแบบ โดยเพิ่มเนื้อหาเกี่ยวกับ “ความเป็นธรรม” เข้าไปในตัวกฎหมายด้วย ซึ่งนักนิติศาสตร์อย่าง Joseph Raz[๕] ได้เสนอว่าหลักนิติธรรมควรหมายถึงโครงสร้างของกฎหมายที่เอื้อให้สังคมสามารถดำเนินไปอย่างมีระบบและสามารถคาดการณ์ได้ เช่น กฎหมายต้องมีความชัดเจน ไม่ย้อนหลัง ถูกประกาศใช้และถูกบังคับใช้อย่างสม่ำเสมอ

หลักนิติธรรมในบริบทของไทย รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช ๒๕๖๐ ได้บัญญัติเรื่องหลักนิติธรรมไว้ในมาตรา ๓ วรรคสอง[๖] โดยระบุว่า“รัฐสภา คณะรัฐมนตรี ศาล องค์กรอิสระ และหน่วยงานของรัฐ ต้องปฏิบัติหน้าที่ตามรัฐธรรมนูญ กฎหมาย และหลักนิติธรรม” ซึ่งสะท้อนว่าการใช้อำนาจทั้งในทางนิติบัญญัติ บริหาร และตุลาการ ต้องอยู่ภายใต้กรอบของกฎหมาย และต้องมีธรรมาภิบาล นอกจากนี้ คณะกรรมการกฤษฎีกา[๗]ของไทยยังได้ให้คำจำกัดความว่า “หลักนิติธรรม” คือ หลักที่ให้อำนาจของรัฐถูกควบคุมโดยกฎหมาย โดยเน้นการมีส่วนร่วมของประชาชน การตรวจสอบถ่วงดุล และการคุ้มครองสิทธิเสรีภาพของบุคคล

---

[๔] A.V. Dicey,1885,“Introduction to the Study of the Law of the Constitution”, London: Macmillan, pp. 183–203.

[๕] Joseph Raz, 1979. “The Rule of Law and Its Virtue”, The Authority of Law: Essays on Law and Morality, Oxford: Clarendon Press, pp. 210–229.

[๖] รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช ๒๕๖๐, มาตรา ๓ วรรคสอง.

[๗] คณะกรรมการกฤษฎีกา, ๒๕๖๒. คู่มือหลักนิติธรรม, กรุงเทพฯ: สำนักงานคณะกรรมการกฤษฎีกา, หน้า ๘.

หลักนิติธรรมตามรัฐธรรมนูญแห่งราชอาณาจักรไทย หมายถึง แนวทางที่การใช้อำนาจรัฐต้องอยู่ภายใต้กรอบของกฎหมายที่เป็นธรรม ชอบธรรม และสามารถตรวจสอบได้ โดยมุ่งคุ้มครองสิทธิและเสรีภาพของประชาชน รวมทั้งส่งเสริมความยุติธรรมในสังคมไทยอย่างแท้จริง การใช้อำนาจของรัฐต้องไม่ขัดต่อเจตนารมณ์ของกฎหมาย และต้องมีความโปร่งใส มีเหตุผล และสอดคล้องกับหลักความได้สัดส่วนและความจำเป็นตามบริบทแห่งสิทธิขั้นพื้นฐานของประชาชน[๘] โดยหลักการแล้วหลักนิติธรรมมิได้หมายถึงเพียงการมี “กฎหมาย” แต่ต้องหมายถึง “กฎหมายที่เป็นธรรม” และมีการใช้อย่างเสมอภาคไม่เลือกปฏิบัติ การตีความและบังคับใช้กฎหมายจึงต้องคำนึงถึงคุณค่าแห่งสิทธิมนุษยชน ความเป็นกลางของฝ่ายตุลาการ และการมีส่วนร่วมของประชาชนในกระบวนการนิติบัญญัติและตรวจสอบอำนาจรัฐ ซึ่งทั้งหมดนี้เป็นเงื่อนไขเพื่อให้หลักนิติธรรมมีผลในทางปฏิบัติไม่ใช่เพียงถ้อยคำในกฎหมาย[๙]

หลักสิทธิเสรีภาพของคนไทย

สิทธิเสรีภาพของคนไทยเป็นหลักการสำคัญที่รับรองความเป็นมนุษย์และความเป็นประชาชนของประเทศ โดยสิทธิเสรีภาพเหล่านี้ได้รับการรับรองไว้ใน รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช ๒๕๖๐[๑๐] ซึ่งเป็นกฎหมายสูงสุดของประเทศ สิทธิเสรีภาพของประชาชนเป็นรากฐานสำคัญของระบอบประชาธิปไตยที่ยึดหลักนิติธรรม และเป็นกลไกสำคัญในการคุ้มครองประชาชนจากการใช้อำนาจรัฐอย่างไม่เป็นธรรม อย่างไรก็ตาม สิทธิเสรีภาพเหล่านี้อาจถูกจำกัดได้บ้างตามความจำเป็น เช่น เพื่อความมั่นคงของรัฐ หรือศีลธรรมอันดีของประชาชนแต่ต้องเป็นไปตามที่รัฐธรรมนูญและกฎหมายบัญญัติไว้เท่านั้นโดยหลักสิทธิเสรีภาพที่สำคัญมีดังนี้

๑. สิทธิในความเสมอภาค (Equality) รัฐธรรมนูญรับรองว่า “บุคคลย่อมเสมอกันในกฎหมาย ได้รับความคุ้มครองตามกฎหมาย และได้รับความเป็นธรรมทางกฎหมาย” สิทธิในความเสมอภาคนี้หมายถึงการที่ประชาชนทุกคนไม่ว่าจะเป็นเพศ เชื้อชาติ ศาสนา หรือฐานะทางเศรษฐกิจใด ๆ ต้องได้รับการปฏิบัติอย่างเท่าเทียมกัน ไม่มีการเลือกปฏิบัติอย่างไม่เป็นธรรมจากรัฐหรือบุคคลอื่น (มาตรา ๒๗)

๒. เสรีภาพในการแสดงความคิดเห็น (Freedom of Expression) รัฐธรรมนูญให้เสรีภาพแก่ประชาชนในการแสดงออกทางความคิด การพูด การเขียน และการสื่อสารโดยวิธีอื่น ๆ เสรีภาพข้อนี้มีความสำคัญอย่างยิ่งในระบอบประชาธิปไตย เพื่อให้ประชาชนสามารถเสนอความเห็นตรวจสอบการทำงานของรัฐ และร่วมกันแสดงความคิดเห็นในการพัฒนาสังคม (มาตรา ๓๔)

๓. เสรีภาพในการชุมนุมโดยสงบ (Freedom of Peaceful Assembly) ประชาชนมีสิทธิจัดการชุมนุมเพื่อเรียกร้องสิทธิหรือแสดงออกความคิดเห็นทางการเมืองและสังคม ตราบใดที่การชุมนุมนั้นเป็นไปอย่างสงบและปราศจากอาวุธ (มาตรา ๔๔)

---

[๘] ธานี ชัยวัฒน์, หลักนิติธรรมในระบอบประชาธิปไตย (กรุงเทพฯ: วิญญูชน, ๒๕๖๑), หน้า ๔๒-๔๕.

[๙] วิษณุ เครืองาม, รัฐธรรมนูญกับหลักนิติธรรม (กรุงเทพฯ: สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์, ๒๕๕๙), หน้า ๘๘-๙๐.

[๑๐] รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.๒๕๖๐”,ราชกิจจานุเบกษา. เล่ม ๑๓๔ ตอนที่ ๔๐ ก, วันที่ ๖ เมษายน ๒๕๖๐.

๔. สิทธิในกระบวนการยุติธรรม (Right to a Fair Trial) ผู้ที่ถูกจับหรือถูกกล่าวหาในคดีอาญามีสิทธิได้รับความเป็นธรรม เช่น การได้รับแจ้งข้อหา การมีทนายความ และการได้รับการพิจารณาคดีโดยเปิดเผยและเป็นธรรม (มาตรา ๒๙)

๕. สิทธิในความเป็นส่วนตัวและเกียรติยศ (Right to Privacy and Dignity) ประชาชนมีสิทธิในชีวิตและร่างกาย ความเป็นส่วนตัว รวมถึงเกียรติยศชื่อเสียง โดยรัฐจะละเมิดสิทธิเหล่านี้ไม่ได้เว้นแต่ตามที่กฎหมายกำหนดเพื่อประโยชน์สาธารณะ (มาตรา ๓๒)

สรุป

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช ๒๕๖๐ ได้บัญญัติหลักสิทธิเสรีภาพของบุคคลไว้อย่างชัดเจนในหมวด ๓ ซึ่งถือเป็นรากฐานสำคัญของระบอบประชาธิปไตยแบบมีพระมหากษัตริย์ทรงเป็นประมุข โดยรัฐธรรมนูญระบุให้สิทธิเสรีภาพของบุคคลมีผลใช้บังคับได้โดยตรง และให้รัฐมีหน้าที่ต้องเคารพ คุ้มครอง และไม่ละเมิดสิทธิเหล่านี้สิทธิเสรีภาพที่ได้รับการรับรองครอบคลุมในหลายด้าน ไม่ว่าจะเป็นเสรีภาพในชีวิตและร่างกายของบุคคล ซึ่งหมายรวมถึงการคุ้มครองจากการจับกุม ควบคุม หรือคุมขังโดยไม่ชอบ และห้ามมิให้มีการทรมานหรือกระทำอันโหดร้าย เสรีภาพในเคหสถาน การสื่อสารและข้อมูลส่วนบุคคลก็ได้รับการคุ้มครองจากการแทรกแซงโดยรัฐหรือบุคคลอื่น เว้นแต่จะมีกฎหมายที่บัญญัติไว้อย่างจำกัดและจำเป็นในด้านเสรีภาพในการแสดงออก บุคคลมีสิทธิที่จะแสดงความคิดเห็นพูด พิมพ์ และสื่อสารโดยเสรี ทั้งนี้ต้องไม่ขัดต่อกฎหมายและไม่กระทบต่อความมั่นคงของรัฐหรือศีลธรรมอันดีของประชาชนนอกจากนี้รัฐธรรมนูญยังรับรองเสรีภาพในการรวมกลุ่ม การจัดตั้งสมาคม และการชุมนุมโดยสงบ ซึ่งถือเป็นกลไกสำคัญในการมีส่วนร่วมของประชาชนในกระบวนการประชาธิปไตย เสรีภาพในการนับถือศาสนาและการปฏิบัติตามความเชื่อทางศาสนา ได้รับการรับรองอย่างกว้างขวาง โดยรัฐต้องอุปถัมภ์และคุ้มครองศาสนาทุกศาสนาอย่างเสมอภาคในด้านเสรีภาพในการประกอบอาชีพ การเลือกถิ่นที่อยู่ การเดินทางและการเลือกสังกัดทางการเมือง บุคคลย่อมสามารถใช้สิทธิเหล่านี้โดยไม่ถูกแทรกแซง เว้นแต่โดยอาศัยเหตุแห่งกฎหมายที่ชอบด้วยหลักนิติธรรมนอกจากนี้ รัฐธรรมนูญยังรับรองสิทธิและเสรีภาพในกระบวนการยุติธรรมเสรีภาพในด้านเศรษฐกิจและสังคมก็ได้รับการคุ้มครอง เช่น เสรีภาพในการเลือกศึกษาหรือประกอบอาชีพ และสิทธิในการเข้าถึงสวัสดิการของรัฐอย่างเป็นธรรมกล่าวโดยสรุปหลักสิทธิเสรีภาพตามรัฐธรรมนูญไทยฉบับปัจจุบันมีลักษณะเป็นกลไกที่ยึดโยงกับหลักสิทธิมนุษยชนสากล และมุ่งคุ้มครองบุคคลในฐานะพลเมืองของรัฐ โดยมีรัฐเป็นผู้รับผิดชอบในการส่งเสริมและปกป้องสิทธิเหล่านี้ เพื่อให้การใช้เสรีภาพเป็นไปโดยไม่ละเมิดผู้อื่นและไม่กระทบต่อความสงบเรียบร้อยของสังคมโดยรวม

หลักสิทธิมนุษยชน

สิทธิมนุษยชน หมายถึง สิทธิและเสรีภาพขั้นพื้นฐานที่บุคคลพึงมีโดยกำเนิดในฐานะที่เป็นมนุษย์ซึ่งได้รับการรับรองและคุ้มครองตามกฎหมาย โดยมุ่งหมายให้บุคคลทุกคนมีศักดิ์ศรีเท่าเทียมกันและสามารถดำรงชีวิตได้อย่างเสรีภายใต้กรอบของกฎหมาย[๑๑]ในประเทศไทย สิทธิมนุษยชนได้รับการรับรองโดยตรงจากรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช ๒๕๖๐ และกฎหมายลำดับรอง โดยระบุว่าทุกคนมีสิทธิในชีวิต เสรีภาพ ความปลอดภัย ความเสมอภาค และการไม่เลือกปฏิบัติ[๑๒] กฎหมายยังจัดตั้งกลไกเพื่อคุ้มครองสิทธิเหล่านี้ เช่น คณะกรรมการสิทธิมนุษยชนแห่งชาติ[๑๓] หลักสิทธิมนุษยชนตามกฎหมายไทยได้รับการรับรองไว้ทั้งในระดับรัฐธรรมนูญและกฎหมายลำดับรอง โดยมีเนื้อหาสำคัญดังนี้

๑. สิทธิและเสรีภาพตามรัฐธรรมนูญแห่งราชอาณาจักรไทย รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช ๒๕๖๐ รับรองสิทธิมนุษยชนไว้อย่างชัดเจน เช่นมาตรา ๒๕ บุคคลย่อมมีสิทธิและเสรีภาพในการดำเนินชีวิตและการกระทำต่าง ๆ โดยไม่ขัดต่อกฎหมายมาตรา ๒๗ บุคคลย่อมเสมอกันในกฎหมาย และต้องได้รับความคุ้มครองเท่าเทียมกันมาตรา ๒๘–๔๙ กล่าวถึงสิทธิเสรีภาพต่าง ๆ เช่น สิทธิในชีวิตและร่างกาย เสรีภาพในการแสดงความคิดเห็น เสรีภาพในการชุมนุม ฯลฯ

๒. การรับรองตามกฎหมายลำดับรอง

๒.๑ พระราชบัญญัติคุ้มครองสิทธิเสรีภาพของประชาชนในกระบวนการยุติธรรม พ.ศ. ๒๕๔๓ มุ่งเน้นการคุ้มครองสิทธิมนุษยชนในระบบยุติธรรมอาญา

๒.๒ พระราชบัญญัติคณะกรรมการสิทธิมนุษยชนแห่งชาติ พ.ศ. ๒๕๖๐ กำหนดให้มีองค์กรอิสระทำหน้าที่ตรวจสอบและส่งเสริมสิทธิมนุษยชนในประเทศไทย[๑๔]

๓. การผูกพันตามพันธกรณีระหว่างประเทศ ประเทศไทยเป็นภาคีในกติการะหว่างประเทศหลายฉบับ เช่น กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (ICCPR) กติการะหว่างประเทศว่าด้วยสิทธิทางเศรษฐกิจ สังคม และวัฒนธรรม (ICESCR) โดยกฎหมายระหว่างประเทศเหล่านี้มีผลผูกพันให้ประเทศไทยต้องปรับปรุงกฎหมายและนโยบายภายในให้สอดคล้องกับหลักสิทธิมนุษยชน[๑๕]

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช ๒๕๖๐ บัญญัติรับรองหลักสิทธิมนุษยชนไว้อย่างครอบคลุม โดยยึดหลักการพื้นฐานที่ว่า “บุคคลย่อมมีศักดิ์ศรีความเป็นมนุษย์ เท่าเทียมกันและได้รับความคุ้มครองตามกฎหมาย” ซึ่งเป็นหลักประกันสำคัญในการดำรงชีวิตในสังคมประชาธิปไตยที่เคารพสิทธิเสรีภาพของประชาชนอย่างแท้จริงรัฐธรรมนูญได้กำหนดไว้ชัดเจนว่าการเลือกปฏิบัติโดยไม่เป็นธรรมด้วยเหตุแห่งความแตกต่าง เช่น ถิ่นกำเนิด เชื้อชาติ เพศ อายุ

---

[๑๑] ศาสตราจารย์ ดร.เกษียร เตชะพีระ, ๒๕๖๑.สิทธิมนุษยชน: ความหมายและพัฒนาการ, พิมพ์ครั้งที่ ๒, กรุงเทพฯ: สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย, หน้า ๑๒.

[๑๒] รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช ๒๕๖๐, มาตรา ๒๕–๔๙.

[๑๓] พระราชบัญญัติคณะกรรมการสิทธิมนุษยชนแห่งชาติ พ.ศ. ๒๕๖๐, มาตรา ๒๖–๓๓.

[๑๔] พระราชบัญญัติคณะกรรมการสิทธิมนุษยชนแห่งชาติ พ.ศ. ๒๕๖๐.

[๑๕] กรมองค์การระหว่างประเทศ, ๒๕๖๓. กระทรวงการต่างประเทศ. รายงานการปฏิบัติตามพันธกรณีตามกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (ICCPR)

ความพิการ สถานะทางเศรษฐกิจ หรือความคิดเห็นทางการเมืองนั้นเป็นสิ่งที่ขัดต่อหลักสิทธิมนุษยชน ในด้านสิทธิในชีวิตและร่างกาย รัฐธรรมนูญรับรองว่าบุคคลจะถูกจับ ควบคุม หรือคุมขังได้เฉพาะตามเหตุและวิธีการที่กฎหมายกำหนด และต้องได้รับการปฏิบัติที่ไม่เป็นการทรมานหรือโหดร้าย อีกทั้งยังให้ความคุ้มครองในเรื่องความเป็นส่วนตัว รวมถึงสิทธิในเคหสถาน ความลับในการสื่อสาร และข้อมูลส่วนบุคคล ซึ่งไม่อาจถูกละเมิดได้ เว้นแต่โดยอาศัยอำนาจของกฎหมายอย่างจำกัดและจำเป็นเท่านั้นรัฐธรรมนูญยังรับรองเสรีภาพในการแสดงออก การพูด การพิมพ์ และการสื่อสารในรูปแบบต่าง ๆ โดยให้เสรีภาพเหล่านี้สามารถถูกจำกัดได้เฉพาะในกรณีที่มีเหตุจำเป็นเพื่อประโยชน์สาธารณะ ความมั่นคงของรัฐ หรือศีลธรรมอันดีนอกจากนี้ ยังรับรองสิทธิในการชุมนุมโดยสงบ เสรีภาพในการรวมกลุ่มทางการเมือง เศรษฐกิจ หรือแรงงาน ซึ่งเป็นสิ่งสำคัญในการสร้างความเข้มแข็งของภาคประชาชนในด้านกระบวนการยุติธรรม รัฐธรรมนูญกำหนดให้บุคคลมีสิทธิได้รับการพิจารณาคดีโดยเปิดเผยและเป็นธรรม รวมถึงสิทธิในการเข้าถึงทนายความและได้รับความช่วยเหลือทางกฎหมายจากรัฐในกรณีจำเป็นขณะเดียวกัน สิทธิด้านเศรษฐกิจ สังคม และวัฒนธรรมก็ได้รับการรับรองอย่างชัดเจน เช่น สิทธิในการประกอบอาชีพ การได้รับค่าตอบแทนและสวัสดิการอย่างเป็นธรรม การเข้าถึงการศึกษาและบริการสาธารณสุขขั้นพื้นฐาน ตลอดจนสิทธิในการอยู่อาศัยในสิ่งแวดล้อมที่ดีและปลอดภัยรัฐธรรมนูญยังให้ความสำคัญกับการคุ้มครองกลุ่มเปราะบาง ได้แก่ เด็ก เยาวชน ผู้สูงอายุ คนพิการ ผู้ด้อยโอกาส และกลุ่มชาติพันธุ์ โดยกำหนดให้รัฐต้องดำเนินมาตรการเพื่อส่งเสริมสิทธิเหล่านี้อย่างเหมาะสมและเท่าเทียม เพื่อสร้างความเป็นธรรมและลดความเหลื่อมล้ำในสังคม

หลักสิทธิมนุษยชนในการคุ้มครองข้อมูลส่วนบุคคล

หลักสิทธิมนุษยชนในการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยมีรากฐานจากสิทธิในความเป็นส่วนตัว ซึ่งได้รับการรับรองในรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช ๒๕๖๐ โดยระบุว่าบุคคลมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว[๑๖] นอกจากนี้ยังมีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งกำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคลและหน้าที่ของผู้ควบคุมข้อมูล รวมถึงการดำเนินการตามแนวทางของสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติที่ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลตามหลักสิทธิมนุษยชน[๑๗]

๑. สิทธิในความเป็นส่วนตัวและข้อมูลส่วนบุคคลตามรัฐธรรมนูญ รัฐธรรมนูญแห่งราชอาณาจักรไทยพุทธศักราช ๒๕๖๐ มาตรา ๓๒ รับรองสิทธิของบุคคลในการได้รับความคุ้มครองจากการแทรกแซงความเป็นส่วนตัว ชื่อเสียง เกียรติยศ และข้อมูลส่วนบุคคล โดยบัญญัติว่า “บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว การกระทำใด ๆ อันเป็นการละเมิดสิทธิดังกล่าวหรือการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย ย่อมไม่ได้”

๒. หลักสิทธิมนุษยชนในการคุ้มครองข้อมูลส่วนบุคคล หลักสิทธิมนุษยชนในการคุ้มครองข้อมูลส่วนบุคคลมีรากฐานอยู่ในหลักการของสิทธิในความเป็นส่วนตัว ซึ่งเป็นสิทธิขั้นพื้นฐาน

---

[๑๖] รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช ๒๕๖๐, มาตรา ๓๒.

[๑๗] สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ,๒๕๖๔.นโยบายการคุ้มครองข้อมูลส่วนบุคคล, สืบค้นจาก https://www.nhrc.or.th.

ของมนุษย์ตามหลักสากล เช่น ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (UDHR) ข้อ ๑๒ และกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (ICCPR) ข้อ ๑๗ ซึ่งประเทศไทยเป็นภาคี

๓. การนำไปสู่กฎหมายเฉพาะ – พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ที่มุ่งหมายเพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล โดยให้สิทธิในการเข้าถึงข้อมูล ขอแก้ไข ลบ ถอนความยินยอม หรือคัดค้านการประมวลผลข้อมูล ทั้งยังวางหลักการสำคัญ เช่น หลักความชอบด้วยกฎหมาย (Lawfulness) หลักความโปร่งใส (Transparency) และหลักความจำเป็น (Necessity)[๑๘]

๔. สิทธิของเจ้าของข้อมูลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เจ้าของข้อมูลส่วนบุคคลมีสิทธิต่าง ๆ ดังต่อไปนี้ สิทธิในการได้รับแจ้งเมื่อมีการเก็บรวบรวมข้อมูล (มาตรา ๒๓) สิทธิในการขอเข้าถึงหรือรับสำเนาข้อมูล (มาตรา ๓๐) สิทธิในการคัดค้านการประมวลผลข้อมูล (มาตรา ๓๒) สิทธิในการขอลบหรือทำลายข้อมูล (มาตรา ๓๓)[๑๙]

๕. ความสัมพันธ์กับหลักสิทธิมนุษยชน การคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายไทยมีลักษณะเป็นการส่งเสริมและคุ้มครองสิทธิมนุษยชน โดยเฉพาะสิทธิในความเป็นส่วนตัว และเป็นกลไกที่ช่วยลดความเสี่ยงจากการละเมิดสิทธิ เช่น การนำข้อมูลไปใช้ในทางที่ไม่เหมาะสมหรือโดยปราศจากความยินยอม

ตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช ๒๕๖๐ สิทธิในความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคลได้รับการรับรองไว้เป็นสิทธิมนุษยชนขั้นพื้นฐานของบุคคล โดยปรากฏชัดในมาตรา ๓๒ และมาตรา ๓๖ ที่มีเนื้อหาสำคัญเกี่ยวกับการคุ้มครองสิทธิในชีวิตส่วนตัวและการสื่อสารมาตรา ๓๒ รับรองว่า “บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว การกระทำหรือการใด ๆ ที่เป็นการละเมิดสิทธิดังกล่าว ไม่ว่าทางกายหรือทางใจ ย่อมกระทำมิได้ เว้นแต่มีบทบัญญัติแห่งกฎหมาย” ซึ่งตีความได้ว่าการเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอม หรือไม่เป็นไปตามกรอบกฎหมาย ถือเป็นการละเมิดสิทธิ ตามบทบัญญัตินี้มาตรา ๓๖ ระบุว่า “บุคคลย่อมมีเสรีภาพในการติดต่อสื่อสารถึงกันไม่ว่าในทางใด ๆ ความลับของการติดต่อสื่อสารนั้นย่อมได้รับความคุ้มครอง...” ซึ่งหมายถึงการคุ้มครองข้อมูลที่เกี่ยวข้องกับการติดต่อสื่อสาร เช่น ข้อมูลในโทรศัพท์ อีเมล ข้อความ หรือกิจกรรมออนไลน์ต่าง ๆ สิทธิเหล่านี้เป็นหลักประกันที่ให้แก่ประชาชนว่ารัฐต้องไม่ละเมิดข้อมูลส่วนบุคคลของตนโดยพลการ และต้องมีการออกกฎหมายลำดับรองเพื่อกำหนดกรอบการคุ้มครองเพิ่มเติม เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งเป็นการดำเนินการตามเจตนารมณ์ของรัฐธรรมนูญในการเสริมสร้างความมั่นคงในสิทธิด้านข้อมูลของประชาชน

---

[๑๘] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒, มาตรา ๓ วรรคสอง และ มาตรา ๒๔.

[๑๙] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒, หมวดที่ ๓ สิทธิของเจ้าของข้อมูลส่วนบุคคล.

สาระสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ลงประกาศในราชกิจจานุเบกษา เมื่อวันที่ ๒๗ พฤษภาคม ๒๕๖๒ ซึ่งในหมวด ๑ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และหมวด ๔ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล รวมถึงบทเฉพาะกาลที่บัญญัติเกี่ยวกับการจัดให้มีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ในวาระเริ่มมีผลใช้บังคับตั้งแต่วันที่ ๒๘ พฤษภาคม ๒๕๖๒ เพื่อให้มีระยะเวลาการเตรียมความพร้อมในด้านการคุ้มครองข้อมูลของประเทศในภาพรวมและบทบัญญัติในหมวดอื่นจะมีผลบังคับใช้ในวันที่ ๒๗ พฤษภาคม ๒๕๖๓ และบทเฉพาะกาลกำหนดให้สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทำหน้าที่สำนักงานตามพระราชบัญญัตินี้และรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมแต่งตั้งรองปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทำหน้าที่เลขาธิการคณะกรรมการฯ องค์ประกอบคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (วาระเริ่มแรก) บทเฉพาะกาลมาตรา ๙๑ กำหนดให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมีองค์ประกอบดังต่อไปนี้

๑.ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ (ชั่วคราว)

๒. ปลัดสำนักนายกรัฐมนตรีเป็นกรรมการ

๓. เลขาธิการคณะกรรมการกฤษฎีกาเป็นกรรมการ

๔. เลขาธิการคณะกรรมการคุ้มครองผู้บริโภคเป็นกรรมการ

๕. อธิบดีกรมคุ้มครองสิทธิและเสรีภาพเป็นกรรมการ

๖. อัยการสูงสุดเป็นกรรมการและ

๗. เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นกรรมการและเลขานุการ

บทความนี้มุ่งวิเคราะห์หลักนิติธรรมที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงินตามกฎหมายดังกล่าว โดยอ้างอิงหลักการและกรอบของกฎหมายไทย เพื่อสะท้อนความสำคัญของการบริหารจัดการข้อมูลส่วนบุคคลอย่างถูกต้อง โปร่งใส และเคารพสิทธิของประชาชน โดยสาระสำคัญของ PDPA (Personal Data Protection Act) หรือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒[๒๐] มีจุดมุ่งหมายเพื่อปกป้องสิทธิของเจ้าของข้อมูลส่วนบุคคลและกำหนดหน้าที่ความรับผิดชอบของผู้เก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยสาระสำคัญประกอบด้วย

๑. สิทธิของเจ้าของข้อมูลส่วนบุคคล

๑.๑ สิทธิในการขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล (Right of Access) เจ้าของข้อมูลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลของตนที่ผู้ควบคุมข้อมูลมีอยู่ รวมถึงขอให้เปิดเผยที่มาของข้อมูล (มาตรา ๓๐)

๑.๒ สิทธิในการขอให้โอนข้อมูลส่วนบุคคล (Right to Data Portability) สามารถขอให้ผู้ควบคุมข้อมูลโอนข้อมูลของตนให้แก่ตนเองหรือบุคคลอื่นโดยอัตโนมัติ หากเป็นข้อมูลที่ได้ให้ความยินยอมไว้หรือที่จำเป็นต่อการทำสัญญา (มาตรา ๓๑)

---

[๒๐] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒. ราชกิจจานุเบกษา. เล่ม ๑๓๖ ตอนที่ ๖๙ ก, ๒๗ พฤษภาคม ๒๕๖๒, หน้า ๕๒.

๑.๓ สิทธิในการคัดค้านการประมวลผลข้อมูล (Right to Object) มีสิทธิในการคัดค้านการเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล หากข้อมูลถูกประมวลผลโดยอาศัยฐานผลประโยชน์โดยชอบด้วยกฎหมาย (มาตรา ๓๒)

๑.๔ สิทธิในการขอให้ลบหรือทำลายข้อมูล (Right to Erasure / Right to be Forgotten) สามารถร้องขอให้ผู้ควบคุมข้อมูลลบ ทำลาย หรือทำให้ข้อมูลเป็นข้อมูลที่ไม่สามารถระบุตัวตนได้ (มาตรา ๓๓)

๑.๕ สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล (Right to Restriction of Processing) มีสิทธิขอให้ระงับการใช้ข้อมูลชั่วคราว หากข้อมูลยังอยู่ระหว่างการตรวจสอบความถูกต้องหรือกรณีพิพาทเกี่ยวกับการใช้ข้อมูล (มาตรา ๓๔)

๑.๖ สิทธิในการแก้ไขข้อมูลให้ถูกต้องและเป็นปัจจุบัน (Right to Rectification) เจ้าของข้อมูลสามารถร้องขอให้แก้ไขข้อมูลของตนให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด (มาตรา ๓๕)

๑.๗ สิทธิในการร้องเรียนต่อคณะกรรมการ (Right to Lodge a Complaint) สามารถร้องเรียนต่อสำนักงานหรือคณะกรรมการหากเห็นว่าการประมวลผลข้อมูลของตนละเมิดกฎหมาย (มาตรา ๗๓)

๒. หลักการขอความยินยอม (Consent) การขอความยินยอมในการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ต้องเป็นไปตามหลักการสำคัญดังนี้

๒.๑ ความยินยอมโดยชัดแจ้ง (Explicit Consent) ต้องได้รับการแสดงเจตนาโดยชัดแจ้งจากเจ้าของข้อมูล เช่น การลงลายมือชื่อหรือการกดยอมรับในระบบอิเล็กทรอนิกส์ (มาตรา ๑๙)

๒.๒ สมัครใจ (Voluntary) ความยินยอมต้องได้รับโดยปราศจากการบังคับ ข่มขู่หรือหลอกลวง และเจ้าของข้อมูลต้องมีเสรีภาพในการตัดสินใจ (มาตรา ๒๐ วรรคแรก)

๒.๓ การแยกข้อความความยินยอมการขอความยินยอมต้องแยกจากข้อความอื่น เช่น เงื่อนไขการให้บริการ เพื่อให้เจ้าของข้อมูลตัดสินใจได้อย่างอิสระ (มาตรา ๑๙(๒))

๒.๔ สิทธิในการเพิกถอนเจ้าของข้อมูลสามารถเพิกถอนความยินยอมได้ทุกเมื่อ โดยการเพิกถอนต้องง่ายและไม่ซับซ้อน (มาตรา ๑๙ วรรคสอง)

๒.๕ ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) เช่น ข้อมูลสุขภาพ ศาสนา หรือชีวภาพ ต้องมีการขอความยินยอมที่เข้มงวดและระมัดระวังยิ่งขึ้น (มาตรา ๒๖)

๓. หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดหน้าที่และความรับผิดชอบของ “ผู้ควบคุมข้อมูลส่วนบุคคล” (Data Controller) ซึ่งหมายถึงบุคคลหรือนิติบุคคลที่มีอำนาจในการตัดสินใจเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยมีหน้าที่สำคัญดังนี้

๓.๑ แจ้งวัตถุประสงค์ก่อนการเก็บข้อมูลต้องแจ้งให้เจ้าของข้อมูลทราบถึงวัตถุประสงค์ในการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลก่อนหรือขณะเก็บข้อมูล (มาตรา ๒๓)

๓.๒ ขอความยินยอมโดยชอบด้วยกฎหมายต้องขอความยินยอมจากเจ้าของข้อมูลก่อนดำเนินการ เว้นแต่เข้าข้อยกเว้นตามกฎหมาย (มาตรา ๑๙)

๓.๓ ดำเนินการให้เป็นไปตามวัตถุประสงค์การใช้หรือเปิดเผยข้อมูลต้องเป็นไปตามวัตถุประสงค์ที่แจ้งไว้ และไม่เกินความจำเป็น (มาตรา ๒๒)

๓.๔ จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการละเมิดข้อมูล เช่น การเข้ารหัสหรือการควบคุมการเข้าถึง (มาตรา ๓๗(๑))

๓.๕ แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ในบางกรณี เช่น หน่วยงานรัฐหรือกิจการที่มีการเก็บข้อมูลจำนวนมาก ต้องแต่งตั้ง DPO เพื่อดูแลการปฏิบัติตามกฎหมาย (มาตรา ๔๑)

๔. การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล (Data Breach Notification) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) กำหนดให้ “ผู้ควบคุมข้อมูลส่วนบุคคล” ต้องดำเนินการแจ้งเหตุเมื่อเกิดการละเมิดข้อมูลส่วนบุคคล (Data Breach) โดยเฉพาะในกรณีที่การละเมิดนั้นอาจก่อให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลตามมาตรา ๓๗ (๕) ของกฎหมายดังกล่าว หากเกิดเหตุละเมิดข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน๗๒ ชั่วโมง นับแต่รู้หรือควรรู้ว่ามีเหตุละเมิด เว้นแต่จะพิสูจน์ได้ว่าเหตุการณ์นั้นไม่มีความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล และหากมีความเสี่ยงสูง ผู้ควบคุมข้อมูลจะต้องแจ้งเจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า โดยเนื้อหาที่ควรระบุในการแจ้งเหตุละเมิดข้อมูล[๒๑] ได้แก่ ลักษณะของเหตุการณ์ที่เกิดขึ้นประเภทของข้อมูลส่วนบุคคลที่ได้รับผลกระทบผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูลมาตรการเยียวยาที่ดำเนินการช่องทางการติดต่อสอบถามเพิ่มเติมการไม่ปฏิบัติตามข้อกำหนดนี้อาจนำไปสู่การถูกลงโทษทั้งทางปกครองและทางอาญา ตามที่กฎหมายได้บัญญัติไว้

๕. บทกำหนดโทษของผู้ที่ฝ่าฝืน พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ได้กำหนดบทลงโทษไว้สำหรับผู้ที่ฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติของกฎหมาย ซึ่งแบ่งออกเป็น ๓ ประเภทหลัก ได้แก่ โทษทางปกครอง โทษทางแพ่ง และโทษทางอาญา ดังนี้

๕.๑ โทษทางปกครอง ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลที่ละเมิดกฎหมาย อาจถูกสั่งให้ชำระค่าปรับทางปกครองได้ไม่เกิน ๕ ล้านบาท ตามความร้ายแรงของการกระทำ เช่น การเก็บใช้หรือเปิดเผยข้อมูลโดยไม่ได้รับความยินยอม (มาตรา ๘๓)

๕.๒ โทษทางแพ่ง เจ้าของข้อมูลสามารถเรียกร้อง ค่าเสียหายตามจริง และในกรณีที่การกระทำของผู้ฝ่าฝืนเกิดจากเจตนาหรือประมาทเลินเล่ออย่างร้ายแรง ศาลอาจสั่งให้ชำระค่าเสียหายเชิงลงโทษเพิ่มเติม (Punitive Damages) ได้ แต่ไม่เกินสองเท่าของค่าเสียหายจริง (มาตรา ๗๗)

๕.๓ โทษทางอาญา หากมีการเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ อาจได้รับโทษ จำคุกไม่เกิน ๑ ปี หรือปรับไม่เกิน ๑ ล้านบาท หรือทั้งจำทั้งปรับ เช่น กรณีการเปิดเผยข้อมูลอ่อนไหวโดยเจตนาเพื่อให้ผู้อื่นได้รับความเสียหาย เสื่อมเสีย หรือเสียชื่อเสียง (มาตรา ๗๙ และ มาตรา ๘๐)

---

[๒๑] สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (๒๕๖๕). แนวทางการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล (Data Breach Notification). สืบค้นจากhttps://www.pdpc.go.th.

ในบริบทของการคุ้มครองข้อมูลส่วนบุคคล หลักนิติธรรมกำหนดให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลต้องเป็นไปอย่างชอบด้วยกฎหมาย มีวัตถุประสงค์ที่ชัดเจน โปร่งใส และไม่เกินความจำเป็น รวมถึงต้องคำนึงถึงสิทธิของเจ้าของข้อมูลด้วย เช่น สิทธิในการรับรู้ สิทธิในการขอเข้าถึงข้อมูล และสิทธิในการเพิกถอนความยินยอม[๒๒]นอกจากนี้ การใช้อำนาจของรัฐหรือเอกชนต่อข้อมูลส่วนบุคคลต้องอยู่ภายใต้ขอบเขตที่กฎหมายบัญญัติไว้อย่างชัดเจน และต้องสามารถตรวจสอบได้โดยกลไกทางกฎหมายที่เป็นอิสระ[๒๓]พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ของประเทศไทยก็รับรองหลักนิติธรรมไว้อย่างชัดเจน โดยมีวัตถุประสงค์เพื่อปกป้องสิทธิและเสรีภาพของบุคคลจากการถูกละเมิดข้อมูลส่วนบุคคล พร้อมทั้งกำหนดให้มีคณะกรรมการที่มีอำนาจในการกำกับดูแลและพิจารณาเรื่องร้องเรียนเพื่อให้เกิดการใช้อำนาจตามกฎหมายอย่างเป็นธรรมและตรวจสอบได้[๒๔]

แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคาร

ในโลกยุคดิจิทัลซึ่งเทคโนโลยีสารสนเทศเข้ามามีบทบาทอย่างลึกซึ้งต่อการดำเนินธุรกิจ การจัดเก็บและใช้ข้อมูลส่วนบุคคลกลายเป็นสิ่งสำคัญในการขับเคลื่อนการให้บริการอย่างมีประสิทธิภาพ โดยเฉพาะในภาคธุรกิจธนาคารที่จำเป็นต้องจัดการข้อมูลของลูกค้าอย่างรัดกุมและปลอดภัย ความก้าวหน้าทางเทคโนโลยีแม้จะเอื้อให้เกิดการให้บริการที่หลากหลายและตรงจุดมากขึ้น แต่ก็ส่งผลให้ความเสี่ยงด้านความเป็นส่วนตัวเพิ่มสูงขึ้นตามมา สมาคมธนาคารไทยจึงได้จัดทำแนวปฏิบัติฉบับนี้ขึ้นเพื่อให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งเป็นกฎหมายที่วางกรอบการจัดการข้อมูลส่วนบุคคลให้มีความปลอดภัยและโปร่งใส[๒๕]

๑. วัตถุประสงค์ของแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคาร

แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคารมีวัตถุประสงค์หลักเพื่อกำหนดกรอบการดำเนินงานสำหรับธนาคารพาณิชย์และสถาบันการเงินให้สามารถจัดการข้อมูลส่วนบุคคลของลูกค้าได้อย่างถูกต้องตามกฎหมาย และมีจริยธรรมในการบริหารข้อมูล แนวทางดังกล่าวช่วยให้องค์กรสามารถประเมินและจัดการความเสี่ยงด้านข้อมูล และสร้างระบบควบคุมภายในเพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล นอกจากนี้ยังช่วยยกระดับความเชื่อมั่นของลูกค้า และสร้างธรรมาภิบาลข้อมูลในระยะยาว การดำเนินธุรกิจของธนาคารจำเป็นต้องมีการจัดการข้อมูลส่วนบุคคลของลูกค้าอย่างหลีกเลี่ยงไม่ได้ ไม่ว่าจะเป็นข้อมูลประจำตัว ข้อมูลการเงิน หรือข้อมูลพฤติกรรมการใช้บริการ เพื่อให้สอดคล้องกับหลักการคุ้มครองสิทธิของเจ้าของข้อมูลและมาตรฐานทางกฎหมาย แนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลในภาคธุรกิจธนาคารจึงมีวัตถุประสงค์หลักดังนี้

---

[๒๒] กฤษฎา หารพานิช, ๒๕๖๕. หลักกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล. กรุงเทพมหานคร: สำนักพิมพ์วิญญูชน.

[๒๓] สมาคมนักกฎหมายสิทธิมนุษยชน, ๒๕๖๔. หลักนิติธรรมกับสิทธิความเป็นส่วนตัวในยุคดิจิทัล. กรุงเทพฯ: มูลนิธิไอแอลโอ.

[๒๔] สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, ๒๕๖๖. แนวปฏิบัติเกี่ยวกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒. สืบค้นจาก https://www.ppdc.go.th.

[๒๕] สมาคมธนาคารไทย, ๒๕๖๔. แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคาร. เข้าถึงจากhttps://www.tba.or.th/wp-content/uploads/pdf/Guideline-on-Personal-Data-Protection-for-Thai-Banks.pdf

๑.๑ เพื่อให้เป็นไปตามกรอบกฎหมายและกฎระเบียบที่เกี่ยวข้อง โดยเฉพาะพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งกำหนดหน้าที่ของผู้ควบคุมข้อมูลอย่างชัดเจนในการเก็บ ใช้ และเปิดเผยข้อมูลโดยได้รับความยินยอมอย่างเหมาะสม และมีมาตรการคุ้มครองที่เพียงพอ[๒๖]

๑.๒ เพื่อสร้างความเชื่อมั่นให้แก่ลูกค้าและสาธารณชน การกำหนดนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลที่เข้มงวดจะช่วยเสริมสร้างความเชื่อมั่นในระบบธนาคาร โดยเฉพาะในยุคที่ภัยคุกคามทางไซเบอร์และการละเมิดสิทธิความเป็นส่วนตัวเพิ่มมากขึ้น[๒๗]

๑.๓ เพื่อกำหนดมาตรฐานและแนวทางปฏิบัติภายในองค์กร ธนาคารควรมีแนวทางปฏิบัติที่ชัดเจนสำหรับพนักงานในทุกระดับ เช่น แนวทางการขอความยินยอมจากลูกค้า การจัดเก็บข้อมูลอย่างปลอดภัย และการตอบสนองต่อการใช้สิทธิของเจ้าของข้อมูล เพื่อให้เกิดการปฏิบัติที่สอดคล้องกันทั้งองค์กร[๒๘]

๑.๔ เพื่อส่งเสริมการบริหารจัดการความเสี่ยงด้านข้อมูล ข้อมูลส่วนบุคคลถือเป็นหนึ่งในสินทรัพย์ที่มีความเสี่ยงสูง แนวปฏิบัติที่ดีช่วยให้สามารถระบุ ประเมิน และควบคุมความเสี่ยงจากการรั่วไหลหรือการเข้าถึงโดยมิชอบได้อย่างมีประสิทธิภาพ[๒๙]

๑.๕ เพื่อส่งเสริมการใช้ข้อมูลอย่างมีจริยธรรมและรับผิดชอบต่อสังคม การนำข้อมูลไปใช้เพื่อวิเคราะห์หรือเสนอผลิตภัณฑ์ใหม่ ๆ ต้องไม่ละเมิดสิทธิหรือสร้างความเดือดร้อนแก่เจ้าของข้อมูล แนวปฏิบัติจะช่วยควบคุมไม่ให้เกิดการใช้ข้อมูลในลักษณะเอารัดเอาเปรียบหรือเกินขอบเขตวัตถุประสงค์[๓๐]

๒. หลักการพื้นฐานในการจัดการข้อมูลส่วนบุคคลตามแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคาร

ในภาคธุรกิจธนาคาร การจัดการข้อมูลส่วนบุคคลมีความสำคัญอย่างยิ่ง เนื่องจากการดำเนินธุรกรรมทางการเงินและการให้บริการต่าง ๆ จำเป็นต้องใช้ข้อมูลส่วนบุคคลของลูกค้าและผู้ใช้บริการ ดังนั้น ธนาคารและสถาบันการเงินจึงต้องมีแนวปฏิบัติที่ชัดเจนในการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้สอดคล้องกับมาตรฐานด้านความเป็นส่วนตัวและกฎหมายที่เกี่ยวข้อง โดยเฉพาะกฎหมายคุ้มครองข้อมูลส่วนบุคคล เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ของไทย หรือ GDPR ของสหภาพยุโรปการคุ้มครองข้อมูลส่วนบุคคลในภาคธุรกิจธนาคารยังคงมีการพัฒนาและปรับตัวตามกฎหมายและเทคโนโลยีที่เปลี่ยนแปลงไปอย่างต่อเนื่อง ซึ่งองค์กรธุรกิจจำเป็นต้องมีการกำหนดนโยบายและแนวทางในการจัดการข้อมูลเพื่อป้องกันการละเมิดข้อมูลส่วนบุคคลและสร้างความมั่นใจให้แก่ลูกค้า โดยหลักการพื้นฐานในการจัดการข้อมูลส่วนบุคคลในภาคธุรกิจธนาคาร ได้แก่

---

[๒๖] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒, ราชกิจจานุเบกษา, เล่ม ๑๓๖ ตอนที่ ๖๙ ก (๒๗ พฤษภาคม ๒๕๖๒).

[๒๗] ธนาคารแห่งประเทศไทย, ๒๕๖๓. แนวทางการกำกับดูแลด้านเทคโนโลยีสารสนเทศสำหรับสถาบันการเงิน, หน้า ๒๓.

[๒๘] สมาคมธนาคารไทย, แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของภาคธุรกิจธนาคาร (๒๕๖๕), หน้า ๖–๘.

[๒๙] คณะกรรมการกำกับดูแลด้านเทคโนโลยีสารสนเทศ ธปท., Cyber Resilience Assessment Framework (CRA) (๒๕๖๔), หน้า ๑๒.

[๓๐] Office of the Personal Data Protection Committee (PDPC), แนวปฏิบัติว่าด้วยจริยธรรมในการใช้ข้อมูลส่วนบุคคล (ร่างเพื่อรับฟังความคิดเห็น, ๒๕๖๕).

๒.๑ หลักความชอบด้วยกฎหมาย (Lawfulness) ธนาคารต้องได้รับความยินยอมจากเจ้าของข้อมูล หรือมีข้อบังคับทางกฎหมายที่อนุญาตให้ใช้ข้อมูลส่วนบุคคลได้ ซึ่งการเก็บรวบรวมข้อมูลจะต้องชัดเจนว่าเป็นไปเพื่อวัตถุประสงค์ใด เช่น การให้บริการทางการเงินหรือการตรวจสอบธุรกรรมทางการเงินตามกฎหมาย

๒.๒ หลักความโปร่งใสและการเปิดเผยข้อมูล (Transparency and Disclosure) ธนาคารต้องมีการเปิดเผยและแจ้งให้ลูกค้าทราบถึงวัตถุประสงค์ในการเก็บข้อมูล วิธีการเก็บข้อมูล และสิทธิของลูกค้าในการเข้าถึงและแก้ไขข้อมูลส่วนบุคคล โดยการให้ข้อมูลนี้ต้องเป็นไปในรูปแบบที่เข้าใจง่ายและชัดเจน

๒.๓ หลักการจำกัดการใช้ข้อมูล (Purpose Limitation) ข้อมูลส่วนบุคคลที่ธนาคารเก็บรวบรวมจะต้องใช้เฉพาะเพื่อวัตถุประสงค์ที่ได้รับการกำหนดไว้ เช่น การประมวลผลธุรกรรมทางการเงิน การตรวจสอบความถูกต้องของข้อมูลลูกค้า หรือการให้บริการตามข้อบังคับ

๒.๔ หลักการจำกัดการเก็บข้อมูล (Data Minimization) ธนาคารต้องเก็บข้อมูลส่วนบุคคลในปริมาณที่จำเป็นเท่านั้น เช่น หากข้อมูลบางประเภทไม่จำเป็นสำหรับการให้บริการ ก็ไม่ควรเก็บข้อมูลเหล่านั้น

๒.๕ หลักความถูกต้องและทันสมัยของข้อมูล (Accuracy and Up-to-date Information) ข้อมูลส่วนบุคคลที่ธนาคารเก็บรวบรวมต้องมีความถูกต้องและทันสมัย ซึ่งหมายถึงธนาคารต้องมีมาตรการเพื่อให้ข้อมูลถูกต้องและมีการอัพเดทตามความจำเป็น เช่น การยืนยันข้อมูลผู้ใช้บริการเมื่อมีการเปลี่ยนแปลงข้อมูลส่วนบุคคล

๒.๖ หลักการรักษาความปลอดภัย (Security) ธนาคารต้องใช้มาตรการทางเทคนิคและการจัดการที่เหมาะสมเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การสูญหาย หรือการทำลายข้อมูล เช่น การเข้ารหัสข้อมูล การจัดการสิทธิการเข้าถึง และการตรวจสอบความปลอดภัยของระบบสารสนเทศ

๒.๗ หลักการสิทธิของเจ้าของข้อมูล (Rights of Data Subjects) ลูกค้าหรือเจ้าของข้อมูลมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของตน แก้ไข หรือขอให้ข้อมูลถูกลบหากไม่มีเหตุผลทางกฎหมายที่สมเหตุสมผลในการเก็บข้อมูล

๒.๘ หลักการคำนึงถึงผลกระทบในการคุ้มครองข้อมูล (Data Protection Impact Assessment) ธนาคารต้องทำการประเมินผลกระทบที่อาจเกิดขึ้นจากการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคล เพื่อให้มั่นใจว่าจะไม่มีผลกระทบต่อความเป็นส่วนตัวและสิทธิของเจ้าของข้อมูล

๓. การขอความยินยอม (Consent) ตามแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคาร

ในการดำเนินธุรกิจของธนาคาร การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกค้า จำเป็นต้องอยู่ภายใต้กรอบกฎหมายตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) ซึ่งได้กำหนดให้ “การขอความยินยอม” (Consent) เป็นหนึ่งในฐานทางกฎหมายที่สำคัญ ธนาคารจึงต้องดำเนินการขอความยินยอมอย่างถูกต้อง ชัดเจน และโปร่งใส โดยมีแนวปฏิบัติสำคัญดังนี้

๓.๑ หลักความสมัครใจและการแยกการให้ความยินยอม ความยินยอมต้องเป็นไปโดย “สมัครใจ” (Freely Given) และต้องไม่มีการบีบบังคับหรือสร้างเงื่อนไข เช่น การบังคับให้ลูกค้าให้ความยินยอมในการใช้ข้อมูลเพื่อการตลาด จึงจะสามารถใช้บริการของธนาคารได้ ถือเป็นการขัดต่อกฎหมาย นอกจากนี้การขอความยินยอมต้องแยกออกจากเงื่อนไขอื่น ๆ อย่างชัดเจน (Granular Consent)[๓๑]

๓.๒ การให้ข้อมูลอย่างโปร่งใสลูกค้าต้องได้รับข้อมูลที่ “ชัดเจน ครบถ้วน และเข้าใจได้ง่าย” เกี่ยวกับวัตถุประสงค์ของการประมวลผลข้อมูล เช่น ธนาคารต้องชี้แจงว่า ข้อมูลจะถูกนำไปใช้เพื่อวิเคราะห์พฤติกรรมทางการเงิน หรือส่งเสริมการขายผ่านช่องทางใดบ้าง[๓๒]

๓.๓ รูปแบบการให้ความยินยอม การขอความยินยอมควรอยู่ในรูปแบบที่ตรวจสอบได้ เช่น ลายลักษณ์อักษร อิเล็กทรอนิกส์ หรือโดยการกระทำที่แสดงเจตนาอย่างชัดเจน (Explicit Consent) ตัวอย่างเช่น ลูกค้าทำเครื่องหมายในช่องยินยอมบนแบบฟอร์มอิเล็กทรอนิกส์[๓๓]

๓.๔ การถอนความยินยอมลูกค้ามีสิทธิที่จะ “ถอนความยินยอม” ได้ตลอดเวลา และธนาคารต้องจัดให้มีช่องทางที่สะดวก ไม่เป็นภาระเกินควร และต้องไม่ส่งผลกระทบต่อบริการอื่น ๆ เว้นแต่การให้ความยินยอมดังกล่าวมีความจำเป็นต่อการให้บริการนั้นโดยตรง[๓๔]

๓.๕ แนวปฏิบัติของธนาคารในประเทศไทย ธนาคารแห่งประเทศไทย (ธปท.) ได้ออกแนวทางกำกับการคุ้มครองข้อมูลส่วนบุคคลสำหรับสถาบันการเงิน โดยเน้นการบริหารจัดการความเสี่ยงจากการละเมิดข้อมูล รวมถึงการมีนโยบายความเป็นส่วนตัวที่ชัดเจนและการอบรมบุคลากรอย่างสม่ำเสมอ[๓๕]

๔. สิทธิของเจ้าของข้อมูลส่วนบุคคลตามแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคาร เจ้าของข้อมูลมีสิทธิตามกฎหมายในการควบคุมข้อมูลของตนเอง ซึ่งธนาคารต้องมีระบบและกระบวนการรองรับการใช้สิทธิเหล่านี้ ได้แก่

๔.๑ สิทธิในการเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล ธนาคารต้องจัดให้มีช่องทางสำหรับลูกค้าในการยื่นคำร้องขอข้อมูล เช่น ผ่านระบบธนาคารทางอินเทอร์เน็ต แอปพลิเคชัน หรือสาขาธนาคาร โดยต้องตอบกลับภายในระยะเวลาที่กฎหมายกำหนด (ภายใน ๓๐ วันนับแต่ได้รับคำขอ) เช่น ลูกค้าธนาคารสามารถขอรับรายการธุรกรรมย้อนหลังหรือข้อมูลเครดิตของตน ซึ่งบางธนาคารมีแบบฟอร์มขอข้อมูลผ่านเว็บไซต์ และส่งเอกสารยืนยันตัวตนแนบประกอบ

๔.๒ สิทธิในการโอนข้อมูลส่วนบุคคล (Data Portability) รองรับการโอนข้อมูลระหว่างธนาคารและผู้ให้บริการทางการเงินรายอื่น เช่น การให้ข้อมูลบัญชีเพื่อใช้กับบริการ Open Banking ซึ่งอยู่ในแผน Digital Finance ของประเทศไทย เช่น ลูกค้าสามารถขอให้ธนาคารโอนข้อมูล Statement ไปยังฟินเทคหรือแพลตฟอร์มเครดิต เพื่อประเมินสินเชื่อโดยไม่ต้องกรอกข้อมูลเองใหม่ทั้งหมด

---

[๓๑] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒, มาตรา ๑๙.

[๓๒] สำนักงานคณะกรรมการกำกับข้อมูลส่วนบุคคล (สคส.), แนวทางการขอความยินยอมที่ชัดเจนและเหมาะสม, ๒๕๖๕.

[๓๓] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1, 2020.

[๓๔] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒, มาตรา ๑๙ วรรคห้า.

[๓๕] ธนาคารแห่งประเทศไทย, แนวนโยบายกำกับการคุ้มครองข้อมูลลูกค้า, ๒๕๖๔.

๔.๓ สิทธิในการคัดค้านการใช้ข้อมูล หากธนาคารใช้ข้อมูลเพื่อการตลาดแบบตรง (Direct Marketing) ลูกค้าสามารถแจ้งไม่ประสงค์ให้ใช้ข้อมูลได้ทันที และธนาคารต้องมีช่องทาง “Opt-out” ที่ชัดเจนและไม่ซับซ้อน เช่น ธนาคารต้องอนุญาตให้ลูกค้า “ยกเลิก” การรับ SMS โปรโมชั่น หรือการโทรเสนอผลิตภัณฑ์ทางการเงินตามความประสงค์ของลูกค้า

๔.๔ สิทธิในการขอให้ลบหรือทำลายข้อมูล ธนาคารต้องลบหรือทำลายข้อมูลเมื่อลูกค้าถอนความยินยอม เว้นแต่มีเหตุจำเป็นต้องเก็บข้อมูลไว้ตามกฎหมาย เช่น พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน เช่น หากลูกค้าปิดบัญชีแล้วและไม่มีข้อพิพาท ธนาคารต้องจัดเก็บข้อมูลไว้ตามระยะเวลาที่กำหนด เช่น ๑๐ ปี แล้วจึงสามารถลบได้ตามคำร้องของลูกค้า

๔.๕ สิทธิในการระงับการใช้ข้อมูล ระหว่างการร้องเรียนหรือตรวจสอบความถูกต้อง ธนาคารต้องระงับการใช้ข้อมูลชั่วคราว และไม่ใช้ข้อมูลนั้นเพื่อการประเมินเครดิตหรือวิเคราะห์พฤติกรรมลูกค้า

๔.๖ สิทธิในการแก้ไขข้อมูลธนาคารต้องมีช่องทางให้ลูกค้าขอแก้ไขข้อมูล เช่น ชื่อ-นามสกุล ที่อยู่ หรือสถานภาพทางการเงิน และต้องตรวจสอบและดำเนินการภายในเวลาที่เหมาะสม เช่น ลูกค้าแจ้งเปลี่ยนนามสกุลหลังการสมรส ธนาคารต้องแก้ไขข้อมูลในระบบและแจ้งให้ลูกค้าได้รับทราบเมื่อแล้วเสร็จ

๔.๗ สิทธิในการถอนความยินยอม ลูกค้ามีสิทธิถอนความยินยอมที่เคยให้ธนาคารใช้ข้อมูลเพื่อวัตถุประสงค์ใด ๆ และธนาคารต้องแจ้งผลกระทบจากการถอนความยินยอมอย่างโปร่งใส

๕. มาตรการรักษาความมั่นคงปลอดภัยตามแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคาร

ข้อมูลส่วนบุคคลในระบบของธนาคารต้องได้รับการปกป้องทั้งทางกายภาพและทางเทคโนโลยี ธนาคารต้องกำหนดนโยบายด้านความมั่นคงปลอดภัย มีการเข้ารหัส การควบคุมการเข้าถึง และการตรวจสอบการใช้งานข้อมูล นอกจากนี้ยังต้องมีระบบแจ้งเหตุละเมิดข้อมูลให้แก่สำนักงานคุ้มครองข้อมูลส่วนบุคคล และเจ้าของข้อมูลโดยเร็วภายในระยะเวลาที่กฎหมายกำหนด หากข้อมูลนั้นมีความเสี่ยงสูงมาตรการรักษาความมั่นคงปลอดภัยตามแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคาร เป็นหัวใจสำคัญของการดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) โดยเฉพาะในภาคธุรกิจธนาคารที่มีการประมวลผลข้อมูลที่มีความอ่อนไหวในปริมาณมาก ซึ่งแนวปฏิบัตินี้อ้างอิงจากเอกสารสำคัญของสมาคมธนาคารไทย ได้แก่ แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลของภาคธุรกิจธนาคาร (Banking Sector Personal Data Protection Guidelines) ที่จัดทำขึ้นโดยคณะกรรมการ PDPA ของสมาคมเพื่อเป็นแนวทางในการยกระดับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลในระบบธนาคารไทยมาตรการรักษาความมั่นคงปลอดภัยประกอบด้วยหัวข้อหลัก ดังนี้

๕.๑ มาตรการด้านเทคนิค (Technical Measures) ธนาคารต้องใช้เทคโนโลยีเพื่อปกป้องข้อมูลส่วนบุคคล เช่น การเข้ารหัสข้อมูล (Encryption) ระบบการควบคุมการเข้าถึง (Access Control), และระบบตรวจจับและตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incident Detection and Response System)

๕.๒ มาตรการด้านการบริหารจัดการ (Organizational Measures) ต้องมีการกำหนดนโยบายภายในที่ชัดเจนเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล การแต่งตั้งเจ้าหน้าที่ DPO (Data Protection Officer) และมีการฝึกอบรมพนักงานเป็นระยะ รวมทั้งการควบคุมผู้ประมวลผลข้อมูลส่วนบุคคลภายนอก (Data Processors) ให้เป็นไปตามมาตรฐานที่กำหนด

๕.๓ มาตรการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต (Unauthorized Access Prevention) เช่น การจำกัดสิทธิ์ผู้ใช้งานตามความจำเป็น (Least Privilege Principle) การใช้ระบบยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication) และการจัดเก็บการใช้งานระบบอย่างเหมาะสมเพื่อตรวจสอบย้อนหลังได้

๕.๔ มาตรการประเมินความเสี่ยงและทบทวนระบบ (Risk Assessment and Review) ธนาคารต้องมีการประเมินความเสี่ยงเกี่ยวกับข้อมูลส่วนบุคคลเป็นประจำ รวมถึงการทำ Data Protection Impact Assessment (DPIA) สำหรับกิจกรรมการประมวลผลที่มีความเสี่ยงสูง

๕.๕ มาตรการกรณีเกิดเหตุละเมิดข้อมูล (Data Breach Response) มีแผนและกระบวนการในการตอบสนองต่อเหตุการณ์การละเมิดข้อมูล รวมถึงการแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และเจ้าของข้อมูลภายในเวลาที่กฎหมายกำหนด

๖. การประเมินผลกระทบด้านความเป็นส่วนตัวตามแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคาร

การประเมินผลกระทบด้านความเป็นส่วนตัว หมายถึง กระบวนการวิเคราะห์ความเสี่ยงที่อาจส่งผลกระทบต่อความเป็นส่วนตัวของเจ้าของข้อมูลจากกิจกรรมที่เกี่ยวข้องกับการเก็บ ใช้ เปิดเผย หรือโอนข้อมูลส่วนบุคคล โดยมุ่งเน้นให้เกิดความโปร่งใส มีความรับผิดชอบต่อการใช้ข้อมูล และสามารถป้องกันผลกระทบเชิงลบที่อาจเกิดขึ้นได้อย่างทันท่วงทีการประเมินนี้ไม่ใช่เพียงการตรวจสอบเชิงเทคนิค แต่ต้องครอบคลุมถึงประเด็นทางกฎหมาย จริยธรรม และสังคม โดยเฉพาะอย่างยิ่งเมื่อนำเทคโนโลยีใหม่มาใช้ เช่น ปัญญาประดิษฐ์ (AI) การวิเคราะห์พฤติกรรม (Behavioral Profiling) และการใช้ระบบอัตโนมัติในการตัดสินใจ (Automated Decision-Making) การดำเนินการดังกล่าวต้องเป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งบัญญัติให้ผู้ควบคุมข้อมูลต้องมีความรับผิดชอบในการออกแบบกระบวนการที่คำนึงถึงสิทธิของเจ้าของข้อมูลตั้งแต่ต้น โดยเฉพาะมาตรา ๓๗ วรรคสอง ซึ่งกำหนดให้ต้องมีมาตรการป้องกันความเสี่ยงในกรณีที่กิจกรรมใดมีแนวโน้มก่อให้เกิดผลกระทบสูงนอกจากนี้ ธนาคารแห่งประเทศไทยยังได้ออกแนวปฏิบัติเพิ่มเติมเกี่ยวกับการบริหารจัดการข้อมูลส่วนบุคคลของลูกค้า เพื่อให้การดำเนินงานเป็นไปอย่างโปร่งใส ปลอดภัย และอยู่ในขอบเขตที่เหมาะสมโดยขั้นตอนการประเมินผลกระทบด้านความเป็นส่วนตัวในภาคธนาคารดังนี้

๖.๑ การกลั่นกรองกิจกรรมที่ต้องประเมิน ธนาคารควรเริ่มจากการจำแนกกิจกรรมที่มีความเสี่ยงสูง เช่น การประมวลผลข้อมูลอ่อนไหว (เช่น ข้อมูลชีวมิติ ประวัติสุขภาพ) การใช้ข้อมูลเพื่อวิเคราะห์พฤติกรรมลูกค้า การโอนข้อมูลไปยังต่างประเทศ การใช้ระบบอัตโนมัติในการตัดสินใจเกี่ยวกับการให้บริการ

๖.๒ การกำหนดขอบเขตและวัตถุประสงค์ของกิจกรรมในขั้นตอนนี้ควรกำหนดอย่างชัดเจนว่าเก็บข้อมูลใด ใช้เพื่ออะไร เก็บไว้นานเพียงใด และมีใครบ้างที่สามารถเข้าถึงได้

๖.๓ การวิเคราะห์ผลกระทบที่อาจเกิดขึ้น ต้องวิเคราะห์ว่าเจ้าของข้อมูลจะได้รับผลกระทบอย่างไรบ้าง เช่นเสียสิทธิ์ในการควบคุมข้อมูลของตนเองถูกตัดสินใจโดยระบบอัตโนมัติโดยไม่มีโอกาสโต้แย้งความเสี่ยงต่อการละเมิดความลับหากข้อมูลรั่วไหล

๖.๔ การออกแบบมาตรการควบคุมเมื่อระบุความเสี่ยงแล้ว ธนาคารควรออกแบบมาตรการควบคุม เช่นการจำกัดการเข้าถึงข้อมูล (Access Control) การเข้ารหัส (Encryption) การกำหนดสิทธิของลูกค้าในการเข้าถึง ขอแก้ไข หรือคัดค้านการใช้ข้อมูล

๖.๕ การปรึกษาฝ่ายที่เกี่ยวข้องควรปรึกษาผู้เชี่ยวชาญด้านความมั่นคงไซเบอร์ กฎหมายและจริยธรรม รวมถึงเจ้าหน้าที่รับผิดชอบด้านข้อมูล เพื่อให้แน่ใจว่าการประเมินมีความครอบคลุมรอบด้าน

๖.๖ การติดตามและทบทวนผลการประเมินแม้จะดำเนินการไปแล้ว แต่ธนาคารควรมีการประเมินซ้ำอย่างสม่ำเสมอ โดยเฉพาะเมื่อมีการเปลี่ยนแปลงระบบ เทคโนโลยี หรือนโยบาย

การประเมินผลกระทบด้านความเป็นส่วนตัวควรถือเป็นกลไกเชิงป้องกัน ไม่ใช่เพียงเครื่องมือเชิงเอกสาร ธนาคารควรสร้างระบบที่เปิดรับความคิดเห็นของเจ้าของข้อมูล และออกแบบบริการทางการเงินให้คำนึงถึงสิทธิมนุษยชนเป็นสำคัญ

๗. การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล (DPO) ตามแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคาร

เพื่อให้การดำเนินงานเป็นไปอย่างต่อเนื่องและเป็นระบบ ธนาคารควรแต่งตั้ง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) ซึ่งมีหน้าที่หลักในการให้คำปรึกษา ตรวจสอบ และติดตามให้ธนาคารปฏิบัติตามกฎหมาย PDPA อย่างถูกต้อง DPO ยังเป็นผู้ประสานงานหลักกับสำนักงานคุ้มครองข้อมูลส่วนบุคคล และเจ้าของข้อมูลเมื่อมีปัญหาเกิดขึ้นการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล (Data Protection Officer : DPO) ตามแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคารการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล (DPO) เป็นกลไกสำคัญที่กำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เพื่อให้หน่วยงานควบคุมและบริหารความเสี่ยงจากการประมวลผลข้อมูลส่วนบุคคลอย่างเป็นระบบ โดยเฉพาะอย่างยิ่งในภาคธุรกิจธนาคารซึ่งมีการประมวลผลข้อมูลในปริมาณมาก และมีลักษณะอ่อนไหวหรือเสี่ยงต่อการละเมิดสิทธิของเจ้าของข้อมูล

๗.๑ กรอบกฎหมายและหลักเกณฑ์ในการแต่งตั้ง DPO ตามมาตรา ๔๑ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดให้องค์กรที่ดำเนินการประมวลผลข้อมูลส่วนบุคคลจำนวนมาก หรือประมวลผลข้อมูลส่วนบุคคลอ่อนไหว เป็นประจำ จำเป็นต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล โดยสำหรับภาคธนาคารนั้น การดำเนินธุรกิจล้วนเกี่ยวข้องกับข้อมูลการเงินข้อมูลส่วนบุคคลที่ละเอียดอ่อน และมีระบบเทคโนโลยีสารสนเทศที่ซับซ้อน จึงเข้าข่ายต้องมี DPO อย่างหลีกเลี่ยงไม่ได้

ธนาคารแห่งประเทศไทย (ธปท.) ได้เผยแพร่เอกสารแนวปฏิบัติเรื่อง “แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลสำหรับธุรกิจธนาคาร” ซึ่งเน้นย้ำว่า DPO ต้องมีความเป็นอิสระในบทบาทหน้าที่ และควรรายงานตรงต่อคณะกรรมการ หรือผู้บริหารระดับสูง โดยไม่ตกอยู่ภายใต้

ความขัดแย้งทางผลประโยชน์ (Conflict of Interest) และควรมีความรู้ ความเข้าใจด้านกฎหมายคุ้มครองข้อมูล เทคโนโลยี และการบริหารความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคล[๓๖]

๗.๒ บทบาทและหน้าที่ของ DPO ในภาคธุรกิจธนาคารมีบทบาทหลัก ๓ ด้าน คือ

๗.๒.๑ การกำกับดูแล การดำเนินงานขององค์กรให้เป็นไปตามกฎหมายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

๗.๒.๒ การให้คำแนะนำ ต่อผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล ในการประเมินความเสี่ยง และมาตรการควบคุม

๗.๒.๓ การเป็นจุดติดต่อ ระหว่างองค์กรกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล รวมถึงการรับเรื่องร้องเรียนจากเจ้าของข้อมูล

นอกจากนี้ DPO ยังควรมีบทบาทในการติดตามผลการประเมินผลกระทบด้านความเป็นส่วนตัวของโครงการใหม่ ๆ และให้ข้อเสนอแนะต่อการออกแบบระบบให้คำนึงถึงความเป็นส่วนตัวตั้งแต่ต้นทาง (Privacy by Design)[๓๗]

๗.๓ คุณสมบัติและการวางตำแหน่งในองค์กร DPO ต้องมีความรู้ด้านกฎหมายคุ้มครองข้อมูล รวมถึงเข้าใจบริบทของธุรกิจธนาคารและความเสี่ยงด้านข้อมูล นอกจากนี้ การวางตำแหน่ง DPO ในโครงสร้างองค์กรควรหลีกเลี่ยงการให้ DPO ทำหน้าที่ที่เกี่ยวข้องกับการตัดสินใจด้านวัตถุประสงค์หรือวิธีการประมวลผลข้อมูล เพื่อรักษาความเป็นอิสระในหลายธนาคาร DPO อาจเป็นตำแหน่งเฉพาะ หรืออาจมาจากฝ่ายบริหารความเสี่ยง กฎหมาย หรือกำกับดูแลกิจการ (Compliance) โดยต้องมีการแยกบทบาทให้ชัดเจนเพื่อหลีกเลี่ยงความขัดแย้ง[๓๘]

๘. การโอนข้อมูลไปต่างประเทศตามแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคารไทย

การโอนข้อมูลไปต่างประเทศตามแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคารไทย เป็นประเด็นที่มีความสำคัญอย่างยิ่ง โดยเฉพาะเมื่อพิจารณาถึงลักษณะการดำเนินธุรกิจของสถาบันการเงินที่มีความเกี่ยวข้องกับบริษัทแม่หรือสาขาในต่างประเทศ การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศต้องปฏิบัติตามข้อกำหนดของกฎหมายคุ้มครองข้อมูลส่วนบุคคลแห่งชาติ (PDPA) และแนวปฏิบัติของธนาคารแห่งประเทศไทย (ธปท.)

๘.๑ กรอบกฎหมายหลักของการโอนข้อมูลไปต่างประเทศ ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๒๘ ระบุว่า การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศสามารถกระทำได้ต่อเมื่อประเทศปลายทางมีมาตรฐานการคุ้มครองข้อมูลที่เทียบเท่าหรือสูงกว่าไทย และต้องผ่านการประเมินโดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หรือเป็นกรณีที่เข้าเงื่อนไขยกเว้นตามกฎหมาย เช่น การได้รับความยินยอมอย่างชัดเจนจากเจ้าของข้อมูล หรือจำเป็นเพื่อปฏิบัติตามสัญญา

---

[๓๖] ธนาคารแห่งประเทศไทย, แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลสำหรับธุรกิจธนาคาร, ๒๕๖๔, หน้า ๗-๙.

[๓๗] สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, คู่มือการแต่งตั้งและบทบาทหน้าที่ของ DPO, ๒๕๖๕.

[๓๘] European Data Protection Board (EDPB), Guidelines 1/2019 on Data Protection Officers (DPOs), version 2.0, 2020, หน้า ๑๑-๑๓.

๘.๒ แนวปฏิบัติของภาคธุรกิจธนาคาร ธนาคารแห่งประเทศไทยได้กำหนด “แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลสำหรับธุรกิจธนาคาร” ซึ่งระบุชัดเจนว่าการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศควรดำเนินการภายใต้หลักการของความโปร่งใส ความจำเป็น และมีมาตรการปกป้องข้อมูลอย่างเพียงพอ โดยควรมีสัญญาหรือข้อตกลงระหว่างธนาคารในประเทศและหน่วยงานรับข้อมูลในต่างประเทศ เพื่อกำหนดบทบาทความรับผิดชอบ และมาตรการควบคุมที่ชัดเจนในกรณีที่ธนาคารต้องใช้บริการจากผู้ให้บริการประมวลผลข้อมูลในต่างประเทศ เช่น บริการคลาวด์ แนวปฏิบัติยังแนะนำให้มีการประเมินความเสี่ยงและความเหมาะสมของผู้ให้บริการดังกล่าว รวมถึงการจัดทำบันทึกการโอนข้อมูล การเข้ารหัส และการควบคุมการเข้าถึงข้อมูล[๓๙]

๘.๓ กลไกการรับประกันความคุ้มครองข้อมูลกลไกที่นิยมใช้เพื่อรับประกันความปลอดภัยของการโอนข้อมูล[๔๐] ได้แก่

๘.๓.๑ สัญญามาตรฐาน (Standard Contractual Clauses) ที่กำหนดเงื่อนไขการปกป้องข้อมูลระหว่างผู้ส่งและผู้รับ

๘.๓.๒ Binding Corporate Rules (BCRs) สำหรับกลุ่มบริษัทที่มีการโอนข้อมูลภายในเครือ

๘.๓.๓ มาตรการทางเทคนิค เช่น การเข้ารหัส การควบคุมการเข้าถึง และการติดตามตรวจสอบ

๘.๔ ข้อควรระวังและแนวโน้มในอนาคตด้วยการเพิ่มขึ้นของความร่วมมือทางการเงินระหว่างประเทศ การโอนข้อมูลจึงมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง ธนาคารจำเป็นต้องติดตามพัฒนาการทางกฎหมายทั้งในและต่างประเทศ

แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคารที่จัดทำโดยสมาคมธนาคารไทยเป็นกรอบที่สำคัญในการกำกับดูแลข้อมูลในองค์กรทางการเงิน เพื่อรองรับกฎหมาย PDPA ที่มุ่งเน้นการปกป้องสิทธิของเจ้าของข้อมูล แนวทางดังกล่าวไม่เพียงแต่ลดความเสี่ยงทางกฎหมาย แต่ยังสร้างความไว้วางใจจากผู้บริโภคในระยะยาว องค์กรที่ดำเนินธุรกิจอย่างมีจริยธรรมและโปร่งใสจะสามารถยืนหยัดในยุคดิจิทัลได้อย่างยั่งยืน

ความรับผิดของสถาบันการเงินไทยต่อการรั่วไหลของข้อมูลส่วนบุคคล

สถาบันการเงินเป็นองค์กรที่ต้องดำเนินกิจกรรมโดยอาศัยข้อมูลส่วนบุคคลของลูกค้าในปริมาณสูงและมีความอ่อนไหว เช่น ข้อมูลบัตรประจำตัวประชาชน หมายเลขบัญชีเงินฝาก ข้อมูลบัตรเครดิตรวมถึงข้อมูลการทำธุรกรรมทางการเงินข้อมูลดังกล่าวหากรั่วไหลย่อมส่งผลเสียหายอย่างกว้างขวางทั้งในระดับบุคคลและระบบการเงินโดยรวม ด้วยเหตุนี้กฎหมายจึงกำหนดให้สถาบันการเงินมีหน้าที่และความรับผิดชอบโดยตรงในการคุ้มครองข้อมูลดังกล่าวอย่างเคร่งครัด พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) กำหนดให้สถาบันการเงินในฐานะ

---

[๓๙] ธนาคารแห่งประเทศไทย, “แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลสำหรับธุรกิจธนาคาร,” มีนาคม ๒๕๖๖.

[๔๐] คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, “แนวทางการโอนข้อมูลส่วนบุคคลไปต่างประเทศ,” (๒๕๖๕).

“ผู้ควบคุมข้อมูลส่วนบุคคล” ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมตามมาตรฐานสากลและเมื่อเกิดเหตุข้อมูลรั่วไหลผู้ควบคุมข้อมูลต้องแจ้งเหตุแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน ๗๒ ชั่วโมงนับแต่ทราบเหตุ และในกรณีที่มีความเสี่ยงกระทบสิทธิและเสรีภาพของเจ้าของข้อมูลต้องแจ้งให้เจ้าของข้อมูลทราบโดยไม่ชักช้า[๔๑] การละเลยหน้าที่ดังกล่าวถือเป็นการฝ่าฝืนกฎหมายและต้องรับผิดตามบทบัญญัติที่กำหนด โดยความรับผิดของสถาบันการเงินในกรณีการรั่วไหลของข้อมูลส่วนบุคคลแบ่งออกเป็น ๓ มิติหลัก ได้แก่

๑. โทษทางแพ่ง ผู้เสียหายมีสิทธิเรียกร้องค่าเสียหายจากสถาบันการเงิน และศาลสามารถสั่งให้ชดใช้ค่าเสียหายเชิงลงโทษ (Punitive Damages) ได้ไม่เกินสองเท่าของค่าเสียหายที่แท้จริง[๔๒]

๒. โทษทางอาญา หากมีการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยโดยมิชอบ เช่น เพื่อแสวงหาประโยชน์ที่ไม่ชอบด้วยกฎหมาย ผู้กระทำอาจถูกลงโทษจำคุกไม่เกิน ๑ ปีหรือปรับไม่เกิน ๑ ล้านบาท หรือทั้งจำทั้งปรับ[๔๓]

๓. โทษทางปกครอง การฝ่าฝืนกฎหมาย เช่น การใช้หรือเปิดเผยข้อมูลโดยไม่ชอบหรือการละเลยไม่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เพียงพออาจถูกสั่งปรับทางปกครองได้สูงสุด ๕ ล้านบาทต่อครั้ง[๔๔]

นอกจากนี้ สถาบันการเงินยังต้องปฏิบัติตามหลักเกณฑ์ของ ธนาคารแห่งประเทศไทย (ธปท.) ซึ่งมีอำนาจกำหนดแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศหากฝ่าฝืน ธปท. สามารถใช้มาตรการกำกับ เช่น การสั่งแก้ไข การจำกัดธุรกรรมหรือบทลงโทษทางการเงินเพิ่มเติมเพื่อรักษาเสถียรภาพของระบบการเงินและความมั่นใจของประชาชน กล่าวโดยสรุปความรับผิดของสถาบันการเงินไทยต่อการรั่วไหลของข้อมูลส่วนบุคคลมีความชัดเจนในหลายมิติทั้งการชดใช้ค่าเสียหายทางแพ่ง การรับโทษทางอาญา และการถูกปรับทางปกครอง ซึ่งสะท้อนให้เห็นว่ากฎหมายมุ่งคุ้มครองสิทธิของเจ้าของข้อมูลอย่างเข้มงวด ดังนั้นการป้องกันไม่ให้เกิดการรั่วไหลตั้งแต่ต้นด้วยมาตรการทางเทคนิคและการบริหารจัดการที่มีประสิทธิภาพจึงเป็นแนวทางที่สำคัญที่สุดในการสร้างความเชื่อมั่นและรักษามาตรฐานของระบบการเงินไทย

สรุป

แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคารที่จัดทำโดยสมาคมธนาคารไทยถือเป็นแนวทางเชิงนโยบายที่มีความสำคัญอย่างยิ่งต่อระบบการเงินของประเทศในบริบทของการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งได้กำหนดหลักเกณฑ์และแนวทางในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของประชาชน โดยมีเป้าหมายหลักเพื่อให้เกิดการคุ้มครองสิทธิในความเป็นส่วนตัวของเจ้าของข้อมูล และยกระดับมาตรฐานการบริหารจัดการข้อมูลขององค์กรให้เป็นไปตามหลักธรรมาภิบาลและความรับผิดชอบในระดับสากลภาคธุรกิจ

---

[๔๑] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒, มาตรา ๓๗.

[๔๒] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒, มาตรา ๗๗.

[๔๓] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒, มาตรา ๗๙.

[๔๔] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒, มาตรา ๘๓.

ธนาคารซึ่งมีลักษณะการดำเนินงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของลูกค้าจำนวนมาก ทั้งในด้านธุรกรรมทางการเงินการเปิดบัญชี การให้สินเชื่อ และการตรวจสอบประวัติเครดิต ล้วนแต่ต้องอาศัยความน่าเชื่อถือและความไว้วางใจของลูกค้าเป็นพื้นฐาน จึงจำเป็นอย่างยิ่งที่จะต้องมีแนวทางปฏิบัติที่ชัดเจน และเป็นระบบเพื่อรองรับกฎหมายดังกล่าว

สาระสำคัญของแนวปฏิบัตินี้อยู่ที่การกำหนดกรอบแนวคิดและหลักการพื้นฐานในการคุ้มครองข้อมูลส่วนบุคคล อาทิ หลักความชอบด้วยกฎหมาย ความเป็นธรรม และความโปร่งใสในการดำเนินการกับข้อมูล หลักการเก็บรวบรวมข้อมูลเท่าที่จำเป็นต่อการให้บริการตามวัตถุประสงค์ที่ชัดเจน หลักความถูกต้องและการปรับปรุงข้อมูลให้ทันสมัยอยู่เสมอ รวมถึงการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลทั้งในระดับทางกายภาพและทางดิจิทัลนอกจากนี้ ธนาคารยังต้องคำนึงถึงสิทธิของเจ้าของข้อมูลซึ่งครอบคลุมถึงสิทธิในการรับรู้ เข้าถึง แก้ไข หรือขอลบข้อมูล สิทธิในการถอนความยินยอม และสิทธิในการคัดค้านหรือขอให้จำกัดการประมวลผลข้อมูล โดยต้องมีการจัดช่องทางที่ชัดเจนและสะดวกต่อการใช้งานของลูกค้าอีกประเด็นที่แนวปฏิบัตินี้ให้ความสำคัญคือการออกแบบระบบงานและบริการดิจิทัลในลักษณะที่สอดคล้องกับแนวคิด “Data Privacy by Design and by Default” กล่าวคือ การคำนึงถึงความเป็นส่วนตัวของข้อมูลตั้งแต่ขั้นตอนการวางแผน ออกแบบ และพัฒนาระบบใหม่ๆ ทั้งแอปพลิเคชัน ช่องทางบริการออนไลน์ และการติดต่อสื่อสารกับลูกค้า โดยธนาคารต้องแสดงข้อมูลนโยบายความเป็นส่วนตัวอย่างชัดเจน และให้ลูกค้าสามารถจัดการความยินยอมได้ตามสิทธิของตนในกรณีที่มีการเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลภายนอกหรือคู่สัญญาทางธุรกิจ เช่น ผู้ให้บริการคลาวด์ ระบบชำระเงิน หรือบริษัทประกันภัย แนวปฏิบัติกำหนดให้ต้องมีการจัดทำข้อตกลงควบคุมการใช้ข้อมูลอย่างชัดเจน โดยผู้ประมวลผลข้อมูล (Data Processor) ต้องดำเนินการภายใต้ขอบเขตและเงื่อนไขที่ได้รับอนุญาตจากธนาคารเท่านั้นในด้านการบริหารจัดการองค์กร แนวปฏิบัติยังเน้นการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) ซึ่งมีบทบาทในการกำกับดูแลและให้คำปรึกษาด้านการปฏิบัติตามกฎหมาย ตลอดจนตรวจสอบกระบวนการภายในเพื่อให้มั่นใจว่าการประมวลผลข้อมูลเป็นไปอย่างเหมาะสมนอกจากนี้ ธนาคารต้องมีแผนจัดการเหตุการณ์ข้อมูลรั่วไหล (Data Breach Incident) และมาตรการตอบสนองอย่างทันท่วงทีตามข้อกำหนดของกฎหมาย เช่น การแจ้งเหตุภายใน ๗๒ ชั่วโมงนับแต่ทราบเหตุการณ์

ในระดับนโยบาย สมาคมธนาคารไทยยังให้ความสำคัญกับการส่งเสริมการปลูกฝังวัฒนธรรมองค์กรที่เคารพสิทธิในข้อมูลส่วนบุคคล โดยสนับสนุนให้มีการอบรมให้ความรู้แก่พนักงานในทุกระดับเกี่ยวกับหน้าที่ความรับผิดชอบ และผลกระทบทางกฎหมายหากละเมิดกฎหมายคุ้มครองข้อมูลส่วนบุคคล อีกทั้งยังมีบทบาทในการเป็นตัวกลางเชื่อมโยงระหว่างธนาคารสมาชิกกับหน่วยงานกำกับดูแล อาทิ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เพื่อร่วมกันจัดทำแนวทางการตีความที่ชัดเจน และแก้ไขปัญหาการดำเนินงานที่อาจเกิดขึ้นจากความไม่ชัดเจนของกฎหมายหรือข้อปฏิบัติในบางประเด็นแนวปฏิบัตินี้จึงมิได้เป็นเพียงการปฏิบัติตามข้อกำหนดทางกฎหมายเท่านั้น หากแต่เป็นการกำหนดยุทธศาสตร์ในระดับองค์กรเพื่อสร้างความเชื่อมั่นให้แก่ลูกค้าและผู้เกี่ยวข้องทุกฝ่ายในการจัดการข้อมูลส่วนบุคคลอย่างมีคุณธรรม โปร่งใส และรับผิดชอบ อันเป็นรากฐานของความยั่งยืนในระบบสถาบันการเงินยุคดิจิทัล

บรรณานุกรม

หนังสือ

เกษียร เตชะพีระ. สิทธิมนุษยชน : ความหมายและพัฒนาการ.พิมพ์ครั้งที่ ๒, กรุงเทพฯ : สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย, หน้า ๑๒.๒๕๖๑.

กฤษฎา หารพานิช. หลักกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล. กรุงเทพฯ : สำนักพิมพ์วิญญูชน, ๒๕๖๕.

คณะกรรมการกฤษฎีกา.คู่มือหลักนิติธรรม.กรุงเทพฯ : สำนักงานคณะกรรมการกฤษฎีกา, หน้า ๘, ๒๕๖๒.

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, สำนักงาน. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒. กรุงเทพฯ: สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, ๒๕๖๒.

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, สำนักงาน. แนวทางการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล. กรุงเทพฯ: สคส, ๒๕๖๖.

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, สำนักงาน. แนวทางการประมวลผลข้อมูลส่วนบุคคลสำหรับหน่วยงานภาคธุรกิจ. กรุงเทพฯ : สคส., ๒๕๖๕.

ธนาคารแห่งประเทศไทย.แนวทางการกำกับดูแลด้านเทคโนโลยีสารสนเทศสำหรับสถาบันการเงิน. กรุงเทพฯ : ธนาคารแห่งประเทศไทย,หน้า ๒๓, ๒๕๖๓.

ธนาคารแห่งประเทศไทย. แนวทางการกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคลสำหรับสถาบันการเงิน. กรุงเทพฯ : ธนาคารแห่งประเทศไทย, ๒๕๖๕.

ธนาคารแห่งประเทศไทย.แนวนโยบายกำกับการคุ้มครองข้อมูลลูกค้า. กรุงเทพฯ : ธนาคารแห่งประเทศไทย, ๒๕๖๔.

ธนาคารแห่งประเทศไทย, แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลสำหรับธุรกิจธนาคาร. กรุงเทพฯ : ธนาคารแห่งประเทศไทย, หน้า ๗-๙, ๒๕๖๔.

ธานี ชัยวัฒน์, หลักนิติธรรมในระบอบประชาธิปไตย. กรุงเทพฯ : วิญญูชน, หน้า ๔๒-๔๕, ๒๕๖๑.

นักกฎหมายสิทธิมนุษยชน, สมาคม, หลักนิติธรรมกับสิทธิความเป็นส่วนตัวในยุคดิจิทัล. กรุงเทพฯ : มูลนิธิไอแอลโอ, ๒๕๖๔.

บวรศักดิ์ อุวรรณโณ, หลักนิติธรรมกับการบริหารราชการแผ่นดิน. กรุงเทพฯ : วิญญูชน, หน้า ๑๘–๒๐, ๒๕๕๑.

วิษณุ เครืองาม, รัฐธรรมนูญกับหลักนิติธรรม. กรุงเทพฯ : สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์, หน้า ๘๘-๙๐, ๒๕๕๙.

วรเจตน์ ภาคีรัตน์. หลักนิติธรรม: ความหมายและการประยุกต์ใช้. กรุงเทพฯ : สำนักพิมพ์วิญญูชน, ๒๕๕๙.

สมาคมธนาคารไทย. แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคาร. กรุงเทพฯ : สมาคมธนาคารไทย, ๒๕๖๕.

วารสาร

ปรัชญา เวสารัชช์. “การคุ้มครองข้อมูลส่วนบุคคลกับหลักนิติธรรมในภาคธุรกิจธนาคาร.” วารสารกฎหมายและนโยบายสาธารณะ, ปีที่ ๑๐, ฉบับที่ ๒, หน้า ๔๕–๖๒, ๒๕๖๕.

กฎหมาย

“พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒”.ราชกิจจานุเบกษา. เล่ม ๑๓๖ ตอนที่ ๖๙ ก, ๒๗ พฤษภาคม ๒๕๖๒, หน้า ๕๒.

“รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.๒๕๖๐”, ราชกิจจานุเบกษา. เล่ม ๑๓๔ ตอนที่ ๔๐ ก, วันที่ ๖ เมษายน ๒๕๖๐, หน้า ๑.

ฐานข้อมูลอิเล็กทรอนิกส์

สมาคมธนาคารไทย. “แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคาร”. (ออนไลน์). เข้าถึงได้จาก: https://www.tba.or.th/wp-content/uploads/pdf/Guideline-on-Personal-Data-Protection-for-Thai-Banks.pdf, ๒๕๖๔.

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, สำนักงาน. “แนวทางการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล (Data Breach Notification)”. (ออนไลน์). เข้าถึงได้จาก :https://www.pdpc.go.th., ๒๕๖๕.

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, สำนักงาน. “แนวปฏิบัติเกี่ยวกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒”. (ออนไลน์). เข้าถึงได้จาก : https://www.ppdc.go.th, ๒๕๖๖.

คณะกรรมการสิทธิมนุษยชนแห่งชาติ, สำนักงาน.“นโยบายการคุ้มครองข้อมูลส่วนบุคคล”, (ออนไลน์). เข้าถึงได้จาก :https://www.nhrc.or.th, ๒๕๖๔.

ภาษาต่างประเทศ

A.V. Dicey,1885,“ Introduction to the Study of the Law of the Constitution”, London: Macmillan, pp. 183–203.

European Data Protection Board. Guidelines on Data Protection Impact Assessment (DPIA), 2020.

Information Commissioner’s Office. Conducting privacy impact assessments code of practice, 2014.

Joseph Raz. “The Rule of Law and Its Virtue”, The Authority of Law: Essays on Law and Morality, Oxford: Clarendon Press, pp. 210–229, 1979.

Mantelero, A. The future of data protection: effective protection or risk management? Computer Law & Security Review, 2014.