A case study of assessing PDPA compliance of the elderly care robot

Songsakdi Rongviriyapanish, Patcharat Meemano
Department of Computer Science, Faculty of Science and Technology, Thammasat

Abstract

Thailand's Personal Data Protection Act B.E. 2562 imposes the directives to organizations that collect, publish, proceed or make use of personal data to protect the rights of the personal data subject. However, an assessment of whether an organization is able to handle personal data in accordance with the Act, a PDPA noncompliance identifying is required. This research presents a 6-step sample guideline for health IT service providers to assess PDPA compliance. This guideline based on a case study of the assessment of an elderly care robot can be used by health IT service providers to self-assess and improve their personal information management processes.

Keywords: PDPA; Self-Assessment Guideline; PDPA Compliance

Received 23 March 2021; Accepted 25 May 2021

Correspondence: Songsakdi Rongviriyapanish, songsak_r@sci.tu.ac.th, Department of Computer Science, Faculty of Science and Technology, Thammasat University Rangsit Campus

กรณีศึกษาการประเมินการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของระบบหุ่นยนต์ดูแลผู้สูงอายุ

ทรงศักดิ์ รองวิริยะพานิช, พัชรัตน์ มีมะโน
สาขาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยธรรมศาสตร์

บทคัดย่อ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ กำหนดหลักเกณฑ์ให้องค์กรที่มีการจัดเก็บ เปิดเผย ประมวลผลใช้ประโยชน์จากข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อปกป้องสิทธิของเจ้าของข้อมูลส่วนบุคคล อย่างไรก็ดี การประเมินว่าองค์กรสามารถจัดการข้อมูลส่วนบุคคลได้สอดคล้องกับพ.ร.บ. หรือไม่ จำเป็นต้องมีการประเมินการหาจุดบกพร่องที่ไม่เป็นไปตามข้อกำหนดในพ.ร.บ. งานวิจัยฉบับนี้นำเสนอตัวอย่างแนวทางการประเมินการปฏิบัติตามพ.ร.บ.ที่ประกอบด้วยขั้นตอน 6 ขั้นตอน โดยยกตัวอย่างจากกรณีศึกษาการประเมินระบบหุ่นยนต์ดูแลผู้สูงอายุ เพื่อให้องค์กรผู้ให้บริการไอทีด้านสาธารณสุขใช้ในการประเมินตนเองและปรับปรุงกระบวนการจัดการข้อมูลส่วนบุคคล

คำสำคัญ: *พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล แนวทางการประเมินตนเอง การปฏิบัติตามพระราชบัญญัติ*

วันที่รับต้นฉบับ 23 มีนาคม 2564; วันที่ตอบรับ 25 พฤษภาคม 2564

บทนำ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ (Personal Data Protection Act : PDPA) เป็นกฎหมายที่มีวัตถุประสงค์เพื่อ คุ้มครองข้อมูลส่วนบุคคลให้การประมวลผลข้อมูลส่วนบุคคลขององค์กรใดใดที่มีการดำเนินการกับข้อมูลส่วนบุคคลของผู้บริโภค ต้องชอบด้วยกฎหมาย เพื่อปกป้อง "บุคคล" จากผลร้ายที่อาจเกิดขึ้นจากการจัดการและการประมวลผลข้อมูลส่วนบุคคล [1] โดยจะมีผลบังคับใช้เดือนพฤษภาคม พ.ศ. 2564

ผู้ให้บริการไอทีด้านสาธารณสุขถูกจัดอยู่ในกลุ่มที่ต้องปฏิบัติตามพ.ร.บ.ฉบับนี้ เนื่องจากข้อมูลสุขภาพส่วนบุคคล เช่น ข้อมูลการแพทย์ (กรุ๊ปเลือด) ข้อมูลประวัติการวัดค่าสุขภาพ (ชีพจร ความดันโลหิต) ข้อมูลโรคประจำตัว ข้อมูลการทานยา และข้อมูลบางส่วนถือเป็นข้อมูลที่มีความละเอียดอ่อน (Sensitive Personal Data) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลดังกล่าวจะมีหลักการที่เข้มงวดกว่าข้อมูลส่วนบุคคลทั่วไป [1]

ในปัจจุบัน พบว่ามีบริษัทภาคธุรกิจเสนอวิธีการลัดในการจัดทำให้องค์กรที่ไม่พร้อมเรื่องการจัดการข้อมูลส่วนบุคคลเพื่อให้สามารถผ่านข้อกำหนดตามพ.ร.บ.ได้ [2] โดยสร้างหน้าเว็บอัตโนมัติเพื่อแสดงรายละเอียดการคุ้มครองข้อมูลส่วนบุคคลขององค์กร (Privacy Policy) ตามที่พ.ร.บ.กำหนดและให้เจ้าของข้อมูลรับทราบ ยอมรับให้ความยินยอมหรือปฏิเสธผ่านหน้าเว็บ ซึ่งการดำเนินการในลักษณะดังกล่าวเป็นเพียงการทำให้มีเอกสารตามพ.ร.บ.กำหนดเท่านั้น ผู้รับบริการจะไม่ได้รับประโยชน์ตามเจตจำนงค์ของพ.ร.บ.ที่ต้องการให้เกิดคุณสมบัติ 3 ประการคือ 1) สิทธิของเจ้าของข้อมูลในการยอมรับหรือปฏิเสธเงื่อนไขการจัดการข้อมูลส่วนบุคคลโดยยังสามารถได้รับบริการ (Consumer Empowerment) [3] 2) ความรับผิดชอบขององค์กรที่เก็บข้อมูลให้มีการเก็บที่ปลอดภัย ชดเชยความเสียหายกรณีมีการรั่วไหลของข้อมูล (Company Accountability) [3] 3) การจัดการข้อมูลส่วนบุคคลต้องอยู่บนหลักการความจำเป็น คือประมวลผลข้อมูลเท่าที่จำเป็น และเป็นไปตามวัตถุประสงค์ที่ตกลงกับเจ้าของข้อมูล หลักความโปร่งใสและความเป็นธรรม คือ ต้องแจ้งให้เจ้าของข้อมูลทราบว่ามีการประมวลผลข้อมูลและบันทึกไว้ พร้อมแจ้งวัตถุประสงค์และระยะเวลาในการใช้ประโยชน์ข้อมูล และหลักความปลอดภัย คือ ต้องใช้มาตรการรักษาความปลอดภัยที่เหมาะสมกับการคุ้มครองข้อมูล [4]

งานวิจัยฉบับนี้จึงขอนำเสนอตัวอย่างแนวทาง 6 ขั้นตอนในการประเมินการปฏิบัติตามพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA Compliance Checking) ที่เป็นผลจากการศึกษาและวิเคราะห์คำอธิบายพ.ร.บ.ที่เผยแพร่ไว้หลายแหล่งข้อมูลและจาก

ผู้นิพนธ์ประสานงาน: ทรงศักดิ์ รองวิริยะพานิช, songsak_r@sci.tu.ac.th, สาขาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยธรรมศาสตร์

การถอดความรู้จากการตรวจกระบวนการคุ้มครองข้อมูลส่วนบุคคลของบริษัทผู้ผลิตหุ่นยนต์ดูแลผู้สูงอายุ แนวทางตัวอย่างที่นำเสนออาจนำไปใช้ประเมินการจัดการข้อมูลส่วนบุคคลขององค์กรที่ให้บริการไอทีด้านสาธารณสุข เพื่อนำไปสู่การปรับปรุงการจัดการข้อมูลส่วนบุคคลขององค์กรให้เป็นไปตามพ.ร.บ.และเพื่อให้ผู้รับบริการได้รับประโยชน์ตามเจตจำนงค์ของพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลทั้ง 3 ประการ

วรรณกรรมที่เกี่ยวข้อง

A. ข้อกำหนดตามพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ [1] ยึดเนื้อหามาจาก General Data Protection Regulation หรือ GDPR ของสหภาพยุโรปซึ่งเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคล แยกหัวข้อที่สำคัญของพ.ร.บ.ออกเป็น 4 หัวข้อ [1] ดังนี้ 1) ความหมายของข้อมูลส่วนบุคคล และ ข้อมูลส่วนบุคคลประเภทละเอียดอ่อน โดย ข้อมูลส่วนบุคคลหมายถึง ข้อมูลใดๆ ที่ระบุไปถึง “เจ้าของข้อมูล” (Data Subject) ได้ไม่ว่าทางตรงหรือทางอ้อม โดยไม่รวมถึงข้อมูลของผู้ที่ถึงแก่กรรม ส่วนข้อมูลประเภทละเอียดอ่อนเป็นข้อมูลส่วนบุคคลที่สุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม จำเป็นต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ ได้แก่ เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ 2) สิทธิของเจ้าของข้อมูลส่วนบุคคล ได้แก่ สิทธิในการได้รับแจ้ง ในการเข้าถึงข้อมูลส่วนบุคคล ในการขอลบหรือทำลาย เป็นต้น 3) หน้าที่และความรับผิดชอบของผู้ควบคุมและผู้ประมวลผลข้อมูล ในทางกฎหมายการกำหนดผู้ควบคุมและผู้ประมวลผลข้อมูลส่วนบุคคล ถือเป็นการกำหนดผู้รับผิดชอบทางแพ่งและทางอาญาเมื่อเกิดความเสียหายขึ้นกับเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) [3] คือ บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เช่น หน่วยงานของรัฐ หรือเอกชนโดยทั่วไป ที่เก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลของประชาชนหรือลูกค้าที่มาใช้บริการ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่สำคัญ เช่น จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล ดำเนินการเพื่อป้องกันมิให้ผู้อื่นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลให้สำนักงานคุ้มครองข้อมูลส่วนบุคคลทราบภายใน 72 ชั่วโมงนับแต่ทราบเหตุ แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) เพื่อตรวจสอบการดำเนินการคุ้มครองข้อมูลส่วนบุคคลขององค์กรว่าเป็นไปตามกระบวนการและนโยบายที่องค์กรได้วางไว้ เป็นต้น ส่วนผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) [3] คือ บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่หลัก คือ ดำเนินการตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล 4) ฐานในการประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นเหตุผลของการประมวลผลข้อมูลส่วนบุคคลโดยฐานความยินยอม เป็นเหตุผลที่เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมอนุญาตให้ประมวลผลข้อมูลได้ แต่หากไม่ใช้ฐานความยินยอม ยังสามารถประมวลผลข้อมูลได้หากเหตุผลอยู่ในฐานอื่นที่กฎหมายอนุญาตไว้ [4] จากความเข้าใจเรื่องฐานในการประมวลผลข้อมูลส่วนบุคคล สรุปได้ว่าข้อมูลส่วนบุคคลที่ถูกนำมาใช้ประโยชน์ไม่จำเป็นต้องมาจากการได้รับความยินยอมพียงอย่างเดียว

แนวทางการประเมินการปฏิบัติตามพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA Compliance Checking)

ที่มาของแนวทางตัวอย่างการประเมิน 6 ขั้นตอน ที่นำเสนอในงานวิจัยนี้มาจากการวิเคราะห์หัวข้อหลักที่องค์กรที่มีการจัดการข้อมูลส่วนบุคคลจำเป็นต้องจัดการเพื่อให้เป็นไปตามพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล [8] และ จากการรวบรวมผลการวิเคราะห์พ.ร.บ.จากหลายแหล่งข้อมูล [1,3,4] สรุปได้ว่าหัวข้อหลักที่พ.ร.บ.กำหนดจะเกี่ยวข้องกับกระบวนการจัดการข้อมูล (Procedure) นโยบายที่เกี่ยวข้องกับข้อมูลอย่างมีระบบ (Policy) การกำกับดูแลข้อมูลตั้งแต่การเกิดของข้อมูล การจัดเก็บ การวิเคราะห์ การทำลาย การเข้าถึง การรักษาความปลอดภัย และการนำไปใช้ โดยให้ความสำคัญทั้งในมุมกระบวนการ บุคลากร และเทคโนโลยี ซึ่งสอดคล้องกับ การจัดทำธรรมาภิบาลข้อมูล (Data Governance) [9] นอกจากนั้นพ.ร.บ.ยังกำหนดการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล

ในงานวิจัยนี้เสนอตัวอย่างแนวทางการประเมินการจัดการข้อมูลส่วนบุคคลขององค์กรว่าเป็นไปตามพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลพ.ศ.๒๕๖๒ หรือไม่นั้น ประกอบด้วย 6 ขั้นตอน ซึ่งจะครอบคลุมเรื่องการจัดทำธรรมาภิบาลข้อมูลและการปกป้องสิทธิของเจ้าของข้อมูลส่วนบุคคล มีรายละเอียดดังนี้

1. การประเมินมาตรการทางเทคโนโลยีที่ใช้เพื่อคุ้มครองข้อมูลส่วนบุคคล โดยวิเคราะห์จากสถาปัตยกรรมระบบ (System) เครือข่าย (Network) สถาปัตยกรรมซอฟต์แวร์ (Software Architecture)

a. ให้องค์กรผู้ให้บริการด้านสาธารณสุขระบุข้อมูลส่วนบุคคลที่องค์กรจัดการ(Data Identification and Classification) พร้อมระบุมาตรการรักษาความปลอดภัยที่ใช้คุ้มครองข้อมูลส่วนบุคคลแต่ละรายการ (มาตรการทางกายภาพ มาตรการทางเทคโนโลยีโดยใช้ซอฟต์แวร์หรือฮาร์ดแวร์หรือการออกแบบระบบเครือข่าย) และประเมินว่ามาตรการที่ใช้เหมาะสมหรือไม่

b. ให้องค์กรระบุมาตรการรักษาความปลอดภัยของข้อมูลบันทึกการทำงานของระบบ (Application Log)

c. ให้องค์กรระบุนโยบายการจัดเก็บข้อมูลโดยใช้คุกกี้หรือเซสชันหรือวิธีการอื่นที่แอพพลิเคชันใช้ในการบันทึกข้อมูลระหว่างประมวลผลพร้อมวิธีป้องกัน

d. กรณีมีการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ เช่น การสำรองข้อมูลไปเก็บที่คลาวด์ให้ประเมินมาตรฐานการคุ้มครองข้อมูลของผู้ให้บริการคลาวด์หรือองค์กรในต่างประเทศ

2. การประเมินการธรรมาภิบาลข้อมูล (Data Governance) หมายถึงการประเมินกระบวนการจัดการข้อมูล การกำหนดความรับผิดชอบในการจัดการข้อมูลในองค์กร สิทธิการเข้าถึงข้อมูลแต่ละประเภท

a. ให้ประเมินว่าองค์กรมีการระบุข้อมูลส่วนบุคคลที่มีการรวบรวม จัดเก็บ ประมวลผล ใช้ประโยชน์ แจ้งวัตถุประสงค์การใช้ ระยะเวลา กำหนดตำแหน่งบุคลากรที่สามารถเข้าถึงข้อมูลอย่างชัดเจนหรือไม่ และองค์กรใช้ฐานใด (ฐานสัญญา จดหมายเหตุ/วิจัย ฐานความยินยอม ฐานระงับอันตรายต่อชีวิต/ร่างกาย/สุขภาพ ฐานอำนาจรัฐหรือภารกิจเพื่อประโยชน์สาธารณะ ฐานประโยชน์โดยชอบด้วยกฎหมาย ฐานปฏิบัติตามกฎหมาย) ในการอนุญาตให้รวบรวม จัดเก็บ ประมวลผล ใช้ประโยชน์ พิจารณาแต่ละขั้นตอนในวงจรชีวิต (Software Development Life Cycle) โดยเฉพาะขั้นตอนการทดสอบ การบำรุงรักษา การให้บริการ ว่ามีโอกาสที่ข้อมูลจะรั่วไหลหรือไม่

b. ตรวจสอบว่าข้อมูลส่วนบุคคลของผู้เยาว์หรือของผู้พิการที่ไม่สามารถให้ความยินยอมได้ด้วยตนเอง มีการให้ความยินยอมโดยผู้ปกครองของผู้เยาว์หรือผู้แทนโดยชอบธรรมของผู้พิการหรือไม่

c. ประเมินว่ามีการแต่งตั้งและระบุหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลหรือไม่ และผู้ปฏิบัติงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคลถูกแต่งตั้งเป็นผู้ประมวลข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลทำหน้าที่รับผิดชอบเฉพาะที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคลหรือไม่

d. ประเมินสิทธิที่ผู้ประมวลผลข้อมูลส่วนบุคคลได้รับว่าเป็นสิทธิเท่าที่จำเป็นสำหรับทำหน้าที่ผู้ประมวลผลข้อมูลส่วนบุคคลเหรือไม่

e. ประเมินว่ามีกระบวนการติดตามตรวจสอบ (Monitor) ให้มีการจัดการข้อมูลส่วนบุคคลอย่างที่ควรจะเป็น เช่น ลบข้อมูลเมื่อหมดระยะเวลาที่เจ้าของข้อมูลให้ความยินยอม การเฝ้าระวังเหตุการณ์ผิดปกติที่เกี่ยวข้องกับข้อมูลส่วนบุคคล มีการทบทวนมาตรการรักษาความมั่นคงปลอดภัยให้มีความเหมาะสมเสมอ

3. การประเมินกระบวนการจัดการสิทธิของเจ้าของข้อมูล (Data Subject Right)

a. ให้ความยินยอมหรือปฏิเสธการรวบรวม จัดเก็บ เปิดเผย ประมวลผลข้อมูล การใช้ประโยชน์ข้อมูลส่วนบุคคล โดยผู้รับบริการยังสามารถได้รับบริการแม้จะมีการปฏิเสธไม่ให้ความยินยอม

b. สิทธิในการคัดค้าน ห้ามมิให้มีการประมวลผลข้อมูลส่วนบุคคล (Right to Restriction of Processing)

c. แจ้งให้ทราบรายการข้อมูลส่วนบุคคลที่ถูกรวบรวม จัดเก็บ ประมวลผล ใช้ประโยชน์ และ วัตถุประสงค์ ระยะเวลาที่จัดเก็บ (Right to be Informed)

d. มีช่องทางในการแก้ไขข้อมูลส่วนบุคคลที่จัดเก็บให้มีความถูกต้อง (Right to Rectification) ขอยุติการให้ความยินยอม (Right to Withdraw Consent) ขอลบข้อมูล (Right to Erasure) มีช่องทางยื่นคำร้องต่อผู้ควบคุมข้อมูลส่วนบุคคล

e. สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (Right of Access) โดยเจ้าของข้อมูลและสามารถขอสำเนาข้อมูลส่วนบุคคลของตนที่จัดเก็บในระบบ

f. สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล (Right to Data Portability) ไปยังผู้ให้บริการรายอื่น

g. สิทธิที่จะไม่ใช้การตัดสินใจโดยอัตโนมัติในการประมวลผลข้อมูล (Right Not to be Subject to Automated Individual Decision-Making, including Profiling) [5]

4. การประเมินข้อกำหนดการปฏิบัติงานของบุคลากรให้มีมาตรฐานสอดคล้องกับพ.รบ.การคุ้มครองข้อมูลส่วนบุคคล

a. ประเมินข้อกำหนดที่แจ้งให้ผู้ปฏิบัติงานรับทราบและปฏิบัติตามเรื่องการไม่จัดเก็บ รวบรวม เปิดเผย ประมวลผลใช้ประโยชน์ข้อมูลส่วนบุคคลของผู้รับบริการนอกเหนือขอบเขตที่ได้รับมอบหมายจากผู้ควบคุมข้อมูล

b. ประเมินกระบวนการตรวจสอบการปฏิบัติงานของบุคลากรที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามที่กำหนด

5. การประเมินนโยบายและมาตรการรับมือกรณีเกิดเหตุการณ์การรั่วไหล (Data Breach Response Procedure)

a. ให้องค์กรแสดงขั้นตอนการดำเนินการเมื่อเกิดเหตุการณ์ผิดปกติที่เกี่ยวกับข้อมูลส่วนบุคคล โดยมีการระบุผู้รับผิดชอบหลักในการจัดการเหตุการณ์ ต้องมีขั้นตอนการวิเคราะห์ผลกระทบ การแจ้งผลกระทบให้แก่เจ้าของข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง

b. ประเมินการรับรู้กระบวนการจัดการเหตุการณ์ผิดปกติของผู้ปฏิบัติงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

c. ประเมินการมีมาตรการที่ใช้เฝ้าระวังเหตุการณ์ผิดปกติ (Incident Monitoring)

6. การประเมินความเสี่ยง (Risk Assessment)

a. ระบุความเสี่ยงที่ยังไม่บรรลุเป้าหมาย เช่น มาตรการป้องกันความปลอดภัยยังไม่เพียงพอสำหรับข้อมูลส่วนบุคคลบางประเภท หรือ มาตรการปกป้องไม่ให้เกิดการรั่วไหลข้อมูลยังไม่ครอบคลุมกรณีการรั่วไหลจากระบบเครือข่ายภายในองค์กร

b. ระบุแผนการจัดการความเสี่ยงที่ยังหลงเหลือประเมินแผนการจัดความเสี่ยงว่าอยู่ในระดับที่รับได้หรือไม่

กรณีศึกษาการประเมินการปฏิบัติตามพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลของระบบหุ่นยนต์ดูแลผู้สูงอายุ

ในงานวิจัยนี้ ขอยกตัวอย่างระบบหุ่นยนต์ดูแลผู้สูงอายุเป็นกรณีศึกษาเพื่อแสดงการประเมินการปฏิบัติตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลตามแนวทาง 6 ขั้นตอน โดยผู้วิจัยดำเนินการประเมินป็น 3 รอบคือ 1) ให้บริษัทผู้ผลิตหุ่นยนต์จัดเตรียมข้อมูลก่อนรับการประเมินโดยพิจารณาตามแนวทางการประเมิน 2) ผู้วิจัยประเมินระบบหุ่นยนต์ดูแลผู้สูงอายุตามแนวทาง 6 ขั้นตอนโดยตรวจจากเอกสารการนำเสนอ จากระบบหุ่นยนต์จริง และจากเข้าตรวจสอบกระบวนการทำงานจริง 3) ผู้วิจัยสรุปสิ่งที่บริษัทไม่ได้ดำเนินการให้เป็นไปตามพ.ร.บ. นำไปปรับปรุง ผลจากการประเมินการปฏิบัติตามพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลระบบหุ่นยนต์ดูแลผู้สูงอายุ และการนำผลการประเมินไปปรับปรุงกระบวนการจัดการข้อมูลส่วนบุคคลเป็นปัจจัยส่วนหนึ่งที่ทำให้บริษัทสามารถนำหุ่นยนต์ขึ้นทะเบียนนวัตกรรมได้สำเร็จ

ระบบหุ่นยนต์ที่ถูกประเมิน เป็นหุ่นยนต์ที่ถูกใช้งานร่วมกับโปรแกรมมือถือเพื่อให้ผู้ดูแลผู้สูงอายุสามารถสั่งการหุ่นยนต์ได้จากทางไกล สามารถติดต่อผู้สูงอายุได้ผ่านVDO Call จากอุปกรณ์มือถือ สามารถเรียกผู้ดูแล แจ้งเตือนเมื่อผู้สูงอายุหายไปจากกล้อง สามารถตั้งเตือนการทานยา เป็นต้น นอกจากนั้นบริษัทผู้ผลิตหุ่นยนต์มีแผนกบริการลูกค้าหลังการขายที่รับซ่อมหุ่นยนต์และบริการลูกค้าทั้งส่วนการใช้โปรแกรมและการจัดการคำร้องของลูกค้า จากการประเมิน 6 ขั้นตอน ผลที่ได้เป็นดังนี้

1) ผลการประเมินมาตรการทางเทคโนโลยีที่ใช้เพื่อคุ้มครองข้อมูลส่วนบุคคล a) ข้อมูลในระบบหุ่นยนต์ที่จัดเป็นประเภทข้อมูลส่วนบุคคล ได้แก่ ข้อมูล Profile ของผู้สูงอายุ เช่น หมายเลข Serial No. ของหุ่นยนต์ ชื่อนามสกุล รูป เบอร์โทรศัพท์ ส่วนข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) ได้แก่ ข้อมูลโรคประจำตัว ข้อมูลยาที่ทานประจำ [6] มีการใช้มาตรการในการปกป้องข้อมูลส่วนบุคคลทั้งการทำ Pseudonymization คือ จำเป็นต้องรู้ทั้ง Serial No. ของหุ่นยนต์และรหัสผู้สูงอายุในการระบุตัวตนผู้สูงอายุได้ และ ใช้มาตรการทางเทคโนโลยีเพื่อจำกัดสิทธิการเข้าถึงฐานข้อมูลจริงโดยต้องต่อ VPN และผ่านการเรียกใช้ API หรือ เฉพาะผู้มีสิทธิบทบาท root เท่านั้น b) ไม่มีการจัดเก็บข้อมูลในรูปแบบคุกกี้หรือ เซสชัน c) มีเฉพาะการจัดเก็บ Log การทำงานของระบบเป็นไฟล์ซึ่งมีข้อมูล Serial No. หุ่นยนต์ที่สามารถใช้ในการระบุตัวตนของผู้สูงอายุ d) มีการย้ายข้อมูลไปต่างประเทศ โดยทำการสำรองข้อมูล Log การทำงานและไฟล์รูปภาพไปที่เครื่องแม่ข่ายของผู้ให้บริการ Microsoft Azure ซึ่งผ่านมาตรฐาน GDPR

2) ผลการประเมินการธรรมาภิบาลข้อมูล (Data Governance) a) ข้อมูลส่วนบุคคลของผู้สูงอายุและผู้ดูแล มีการจัดเก็บ รวบรวม เปิดเผยเฉพาะผู้สูงอายุและผู้ดูแลที่ได้รับคำยินยอมจากผู้สูงอายุ หรือผู้แทน มีการกำหนดระยะเวลาการจัดเก็บจนกว่าผู้สูงอายุจะยกเลิกการใช้ระบบหรือร้องขอให้มีการลบหรือกด Reset ระบบหุ่นยนต์ใหม่ มีการกำหนดสิทธิให้บุคลากรเข้าถึงฐานข้อมูลจริงของผู้สูงอายุ ตำแหน่งที่ทำหน้าที่บำรุงรักษาฐานข้อมูลจะทำได้แค่การสำรองฐานข้อมูลและกู้คืนข้อมูลเท่านั้น องค์กรใช้ฐานความยินยอมและฐานสัญญาเท่านั้นในการเข้าถึงข้อมูล การประมวลผล การจัดเก็บ ข้อมูลส่วนบุคคล พนักงานทดสอบระบบหรือพนักงานพัฒนาระบบจะต้องสร้างข้อมูลสำหรับการทดสอบชุดใหม่ ขั้นตอนการ Support พนักงานจะเชื่อมต่อ VPN เข้าหุ่นยนต์ได้แต่ VPN Account ที่ใช้จะไม่สามารถเข้าถึงข้อมูล Log บนหุ่นยนต์ b) มีการตรวจสอบผู้แทนโดยชอบธรรมในการดำเนินการแทนผู้สูงอายุในช่วงเปิดใช้บริการหุ่นยนต์และให้ความยินยอมได้ผ่านแบบฟอร์มเอกสาร c) ในองค์กรไม่มีการแต่งตั้งผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อให้ผ่านพ.ร.บ. องค์กรได้แต่งตั้งให้ผู้จัดการผลิตภัณฑ์ เป็นผู้ควบคุมข้อมูลส่วนบุคคลและบุคลากรทุกคนที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเป็นผู้ประมวลข้อมูลส่วนบุคคล d) สิทธิในระบบหุ่นยนต์มีเพียง ตำแหน่งที่จำกัดที่สามารถเข้าถึงข้อมูลจริงของผู้สูงอายุบนเครื่องแม่ข่ายและบนหุ่นยนต์ e) องค์กรมีการกระบวนการในการรับแจ้งขอแก้ไข ลบ ข้อมูลส่วนบุคคลตามคำร้องขอทางโทรศัพท์หรือผ่านแบบคำร้อง แต่องค์กรส่วนมากมักขาดกระบวนการติดตามจัดการข้อมูล เช่น การลบข้อมูลเมื่อหมดระยะเวลาที่ได้รับความยินยอม ขาดเครื่องมือช่วยเฝ้าระวังเหตุการณ์ผิดปกติที่เกี่ยวข้องกับข้อมูลส่วนบุคคล มีการมอบหมายให้บุคลากรตำแหน่ง System Engineer เสนอมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม แต่ขาดกระบวนการทบทวนมาตรการรักษาความมั่นคงปลอดภัยให้มีความเหมาะสม

3) ผลการประเมินกระบวนการจัดการสิทธิของเจ้าของข้อมูล (Data Subject Right) a) มีหน้าจอบนหุ่นยนต์และบนโปรแกรมมือถือเป็นช่องทางให้เจ้าของข้อมูลให้ความยินยอมหรือปฏิเสธการจัดเก็บ เปิดเผย ประมวลผลข้อมูลส่วนบุคคลในเอกสารการเปิดใช้งานระบบและบนหน้าจอโปรแกรมมีการแจ้งที่ติดต่อบริษัทสำหรับขอให้ดำเนินการสำเนาโอนย้าย คัดค้านการประมวลผลข้อมูล แจ้งมิให้มีการประมวลผลข้อมูลส่วนบุคคล b) โปรแกรมมือถือเปิดให้ใช้แก้ไข ลบข้อมูลส่วนบุคคลได้ c) การยุติการเปิดเผยข้อมูลเพียงบางส่วนไม่สามารถทำได้เมื่อยุติการใช้บริการจึงจะยุติการเปิดเผยข้อมูลทั้งหมด d) โปรแกรมและหุ่นยนต์ไม่สามารถให้ผู้รับบริการเลือกที่จะไม่ใช้การตัดสินใจโดยอัตโนมัติในการประมวลผลข้อมูล

4) ผลการประเมินข้อกำหนดการปฏิบัติงานของบุคลากร a) องค์กรมีการกำหนดข้อตกลงการไม่เปิดเผยข้อมูลส่วนบุคคล (Non Disclosure Agreement) และ การไม่นำข้อมูลส่วนบุคคลของผู้รับบริการไปใช้นอกเหนือหน้าที่ความรับผิดชอบในสัญญาจ้าง b) องค์กรขาดการตรวจสอบภายใน (Internal Audit) จึงขาดการตรวจสอบการปฏิบัติงานของบุคลากรที่เกี่ยวข้องกับข้อมูลส่วนบุคคลว่าเป็นไปตามที่กำหนดหรือไม่

5) ผลการประเมินนโยบายและมาตรการรับมือกรณีเกิดเหตุการณ์การรั่วไหล (Data Breach Response Procedure) a) องค์กรขาดการกำหนดขั้นตอนการดำเนินการที่ชัดเจนเมื่อเกิดเหตุการณ์ผิดปกติที่เกี่ยวกับข้อมูลส่วนบุคคล b) บุคลากรในองค์กรไม่ทราบกระบวนการในการจัดการเหตุการณ์ผิดปกติ ยังขาดการจัดการผลกระทบ และขาดนโยบายที่ชัดเจนให้แจ้งเจ้าของข้อมูลส่วนบุคคล c) องค์กรขาดเครื่องมือที่ใช้ช่วยในการเฝ้าระวังเหตุการณ์ผิดปกติ

6) การประเมินความเสี่ยง (Risk Assessment) a) ความเสี่ยงที่ยังหลงเหลือที่ควรจัดการ ได้แก่ มาตรการป้องกันข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน เช่น ชื่อยา โรคประจำตัว มาตรการปกป้องไม่ให้เกิดการรั่วไหลข้อมูลยังไม่ครอบคลุมกรณีการรั่วไหลจากระบบเครือข่ายภายในองค์กร การขาดการทบทวนมาตรการความปลอดภัยให้มีความเหมาะสม b) แผนการจัดการความเสี่ยง คือเพิ่มการเข้ารหัสข้อมูล (Encryption) สำหรับข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน ใช้โพรโตคอล HTTPS ในการสื่อสารภายใน และเพิ่มนโยบายการทบทวนมาตรการความปลอดภัยเป็นประจำทุกปี

บทสรุป

งานวิจัยนี้ได้เสนอตัวอย่างแนวทางการประเมินการปฏิบัติตามพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลที่ประกอบด้วย 6 ขั้นตอน โดยแนวทางที่นำเสนอได้จากการประเมินหุ่นยนต์ดูแลผู้สูงอายุให้สามารถผ่านการขึ้นทะเบียนนวัตกรรมได้ องค์กรผู้ให้บริการไอทีด้านสาธารณสุข อาจนำแนวทางไปใช้เพื่อประเมินวิเคราะห์หาจุดอ่อนอย่างเป็นระบบและนำผลการประเมินที่ได้ไปปรับปรุงกระบวนการจัดการข้อมูลส่วนบุคคลให้มีประสิทธิภาพยิ่งขึ้น เพื่อให้ผู้รับบริการได้ประโยชน์ตามเจตจำนงค์ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

เอกสารอ้างอิง

[1] ปิยะบุตร. บุญอร่ามเรือง, พีรพัฒ. โชคสุวัฒนสกุล, ปิติ. เอี่ยมจารุญลาภ, ชวิน. อุ่นภัทร และ ฐิติรัตน์. ทิพย์สัมฤทธิ์กุล, “Thailand Data Protection Guidelines 2.0 : แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล” ISBN 978-616-407-458-3, พิมพ์ครั้งที่ 1 ตุลาคม 2562.

[2] Ingfah. Insawang, “เริ่มตอนนี้ทันไหม? คู่มือการทำ PDPA สำหรับ SMEs และ Startup ใน 10 นาที”, https://techsauce.co/news/easy-pdpa

[3] Chaiwat. Jirakitpaibool. (2019),“ผู้ช่วยวิจัยได้อะไรบ้างจากการเข้าร่วมงาน PDPA — Privacy for All”,[ออนไลน์]. ได้จาก: https://medium.com/@mybooboy/ผู้ช่วยวิจัยได้อะไรบ้างจากการเข้าร่วม-pdpa-privacy-for-all-7fbef5a83d82 [สืบค้นเมื่อ 31 สิงหาคม 2563]

[4] ฐิติรัตน์. ทิพย์สัมฤทธิ์กุล.(2563), “กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) สิทธิหน้าที่ และความเป็นส่วนตัวในยุคดิจิทัล”, [ออนไลน์].ได้จาก: https://jla.coj.go.th/th/file/getfile/20200525b2cd14942c955d825d9f1b0c53875159094947.pdf [สืบค้นเมื่อ 31 สิงหาคม 2563]

[5] Can I be subject to automated individual decision-making, including profiling?.[Online].Available from: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-be-subject-automated-individual-decision-making-including-profiling_en [accessed 31 August 2020]

[6] What personal data is considered sensitive?. [Online].Available from: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en [accessed 31 August 2020]

[7] PDPC | Data Protection Officers. [Online].Available from: https://www.pdpc.gov.sg/overview-of-pdpa/data-protection/business-owner/data-protection-officers

[8] ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับสำนักงานคณะกรรมการกฤษฎีกาตรวจเสร็จ 1395/2561 กันยายน 2561 สำหรับสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (กลต.) [Online].Available from: https://www.sec.or.th/TH/Documents/Seminars/DataProtectionRegime.pdf

[9] Data Governance คืออะไร [Online].Available from: https://www.coraline.co.th/single-post/data-governance