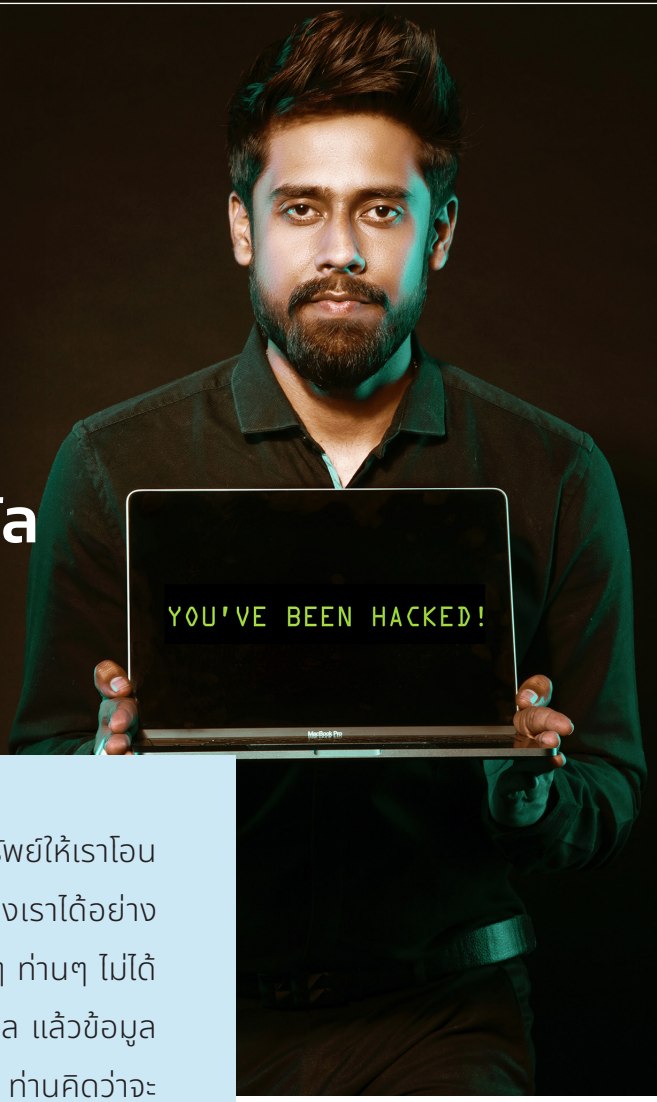
ดร.ภัทราวุฒิ แสงศิริ
สถาบันวิจัยวิทยาศาสตร์และเทคโนโลยีแห่งประเทศไทย (วว.)
35 หมู่ที่ 3 เทคโนธานี ตำบลคลองห้า อำเภอคลองหลวง จังหวัดปทุมธานี 12120

PDPA
กับบทบาทของเทคโนโลยีดิจิทัล



แก็งค์คอลเซ็นเตอร์หลอกลวง ที่พยายามโทรมาตกทรัพย์ให้เราโอนเงินให้ด้วยสารพัดรูปแบบ โดยอาศัยการอ้างข้อมูลส่วนตัวของเราได้อย่างถูกต้อง แก็งค์พวกนี้เอาข้อมูลมาได้อย่างไร หรือกรณีหากเราๆ ท่านๆ ไม่ได้รับความเป็นธรรมจากการถูกกลั่นแกล้งคุกคามของผู้มีอิทธิพล แล้วข้อมูลการร้องเรียนและข้อมูลส่วนตัวของท่านรั่วไหลออกสู่สาธารณะ ท่านคิดว่าจะเกิดความเสี่ยงหรืออันตรายใดตามมาหรือไม่

ปัจจุบันการละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคล สร้างความเดือดร้อนรำคาญ ก่อความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคลเป็นจำนวนมาก ประกอบกับความก้าวหน้าของเทคโนโลยีดิจิทัลทำให้การเก็บรวบรวม ใช้ หรือเปิดเผย แชร์ส่งต่อข้อมูลส่วนบุคคล ทำได้โดยง่าย กระจายได้ไวและไกล จึงเป็นช่องทางของการกระทำความผิดได้หลายประเภททั้งทางแพ่งและอาญา ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวมของประเทศ

จึงเป็นสาเหตุสำคัญของการออกพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยมีวัตถุประสงค์ก็เพื่อคุ้มครองสิทธิเจ้าของข้อมูลส่วนบุคคล กำหนดหลักเกณฑ์มาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล ขึ้นมาหรือที่เรียกกันย่อๆ ว่า PDPA หรือ Personal Data Protection Act

หลักสำคัญของกฎหมาย PDPA ก็คือ

1) การประมวลผลโดยชอบธรรมและโปร่งใส (Lawful processing and transparency)

2) ใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์และเท่าที่จำเป็น (Necessity and purpose limitation)

3) ปรับปรุงแก้ไขให้ข้อมูลส่วนบุคคลให้ถูกต้องและเป็นปัจจุบัน (Data accuracy)

4) กำหนดระยะเวลาในการจัดเก็บข้อมูลที่แน่นอน (Limitation of stroage)

5) มีมาตรการรักษาความปลอดภัยที่เหมาะสม (Security)

6) เคารพสิทธิ์ของเจ้าของข้อมูลส่วนบุคคล (Data subject rights)

ทั้งนี้กฎหมาย PDPA ยังมีความเชื่อมโยงกับกฎหมายอื่นๆ อีก ได้แก่ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พระราชบัญญัติข้อมูลข่าวสารราชการ พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ และพระราชบัญญัติบัตรประจำตัวประชาชน แต่ละกฎหมายล้วนมีส่วนเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ด้วยทั้งสิ้น ซึ่งในมาตรา 3 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้บังคับใช้พระราชบัญญัตินี้ เป็นการเพิ่มเติมในการคุ้มครองข้อมูลส่วนบุคคล ถึงแม้จะซ้ำกับกฎหมายอื่น

ผลลัพธ์จากกฎหมาย PDPA มี 3 มิติ ได้แก่

1. สร้างความเชื่อมั่น (Trust) คือ สร้างความเชื่อมั่นให้กับเจ้าของข้อมูลส่วนบุคคลในการเข้ารับบริการ หรือดำเนินกิจกรรมร่วมกับหน่วยงานที่ทำการใช้ข้อมูลส่วนบุคคล โดยเชื่อมั่นได้ว่าหน่วยงานจะมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่มีมาตรฐาน

2. ยกระดับธรรมาภิบาลข้อมูล (Data Governance) คือ สร้างหน้าที่ให้กับหน่วยงานทั้งภาครัฐและเอกชนในการสร้างมาตรการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นปัจจัยสำคัญในการยกระดับธรรมาภิบาลข้อมูล

3. ยกระดับสู่มาตรฐานการคุ้มครองข้อมูลส่วนบุคคล ให้สอดคล้องกับกฎเกณฑ์และมาตรฐานสากล เพื่อสร้างความเชื่อมั่นให้กับหน่วยงานในต่างประเทศในการดำเนินการค้าและการลงทุนกับประเทศไทย

บทบาทในกิจกรรมการประมวล (Data Protection Roles)

1.เจ้าของข้อมูลส่วนบุคคล (Datasubject) หมายถึง บุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคล

2. ผู้ควบคุมข้อมูลส่วนบุคคล (Data controller) หมายถึง บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

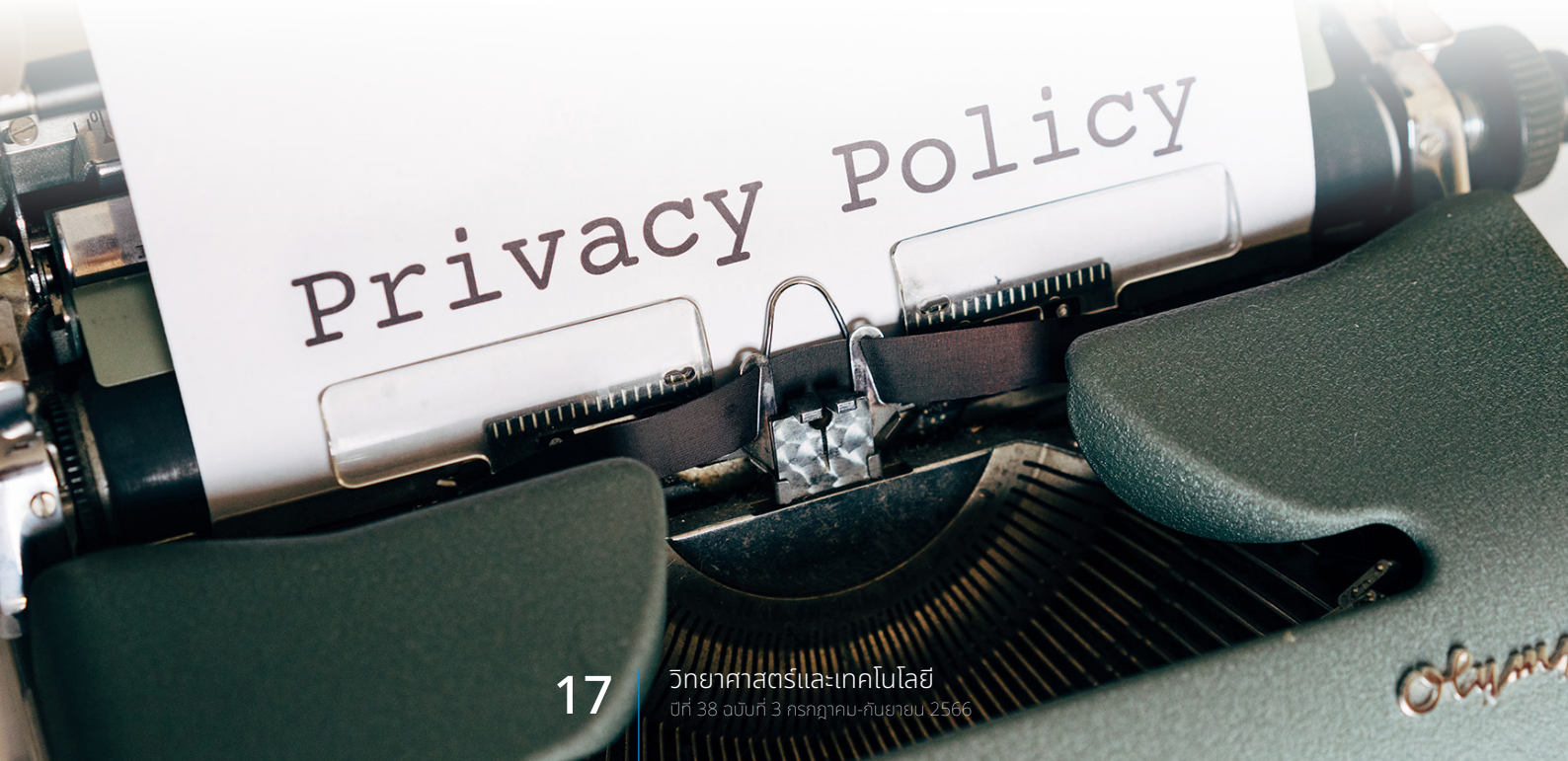
3. ผู้ประมวลผลข้อมูลส่วนบุคคล (Data processor) หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล (ทั้งนี้บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล)

4. หน่วยงานกำกับดูแล หมายถึง สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

บทบาทของเทคโนโลยีดิจิทัลและความเกี่ยวข้องของกฎหมาย PDPA

จากหลักการของหลักสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล สามารถนำไปสู่บทบาทของเทคโนโลยีดิจิทัลได้ดังนี้

1. การจัดทำธรรมาภิบาลข้อมูล (Data Governance) บทบาทสำคัญของเทคโนโลยีดิจิทัลที่เข้าไปมีส่วนร่วมในการดำเนินการร่วมกับหน่วยงานอื่นๆ ขององค์กร



ได้แก่ การจัดเตรียมอุปกรณ์ทั้งฮาร์ดแวร์และซอฟต์แวร์สำหรับจัดเก็บและบันทึกระบบบัญชีข้อมูล (Data Catalog System) ทั้งนี้การดำเนินการดังกล่าว จำเป็นต้องมีแนวปฏิบัติที่ชัดเจนในการบริหารจัดการข้อมูลตลอดวงจรชีวิตของข้อมูล ได้แก่ การเก็บรวบรวม (ทั้งจากเจ้าของข้อมูลส่วนบุคคลและแหล่งอื่น), การใช้ การเผยแพร่ข้อมูล, ระยะเวลาในการเก็บรวบรวมและวิธีการทำลายข้อมูล (กรณีที่ข้อมูลอยู่ในสื่อบันทึกต่างๆ อาทิ ฮาร์ดไดรฟ์ หรือซีดีรอม) นอกจากนี้การดำเนินการตามธรรมาภิบาลข้อมูลยังรวมถึงความโปร่งใส ให้เจ้าของข้อมูลสามารถตรวจสอบข้อมูลของตนเอง และมีการจัดเก็บข้อมูลเท่าที่จำเป็น ซึ่งปัจจุบันสำนักงานสถิติแห่งชาติได้มีการพัฒนาและให้บริการระบบบัญชีข้อมูลภาครัฐ (Government Data Catalog) (https://gdhelppage.nso.go.th/) และสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ โดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ได้ดำเนินการพัฒนาระบบ C-KAN Open-D เพื่อให้แต่ละหน่วยงานสามารถนำไปใช้งานในองค์กร (https://gitlab.nectec.or.th/opend/installing-ckan)

2. การรักษาความมั่นคงปลอดภัยของสารสนเทศ (Information Security) เป็นมาตรการการคุ้มครองข้อมูลส่วนบุคคลที่ครอบคลุมใน 3 เรื่องที่สำคัญ ได้แก่

2.1 การรักษาความลับ (Confidentiality) หมายถึง ผู้ที่สามารถเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคลต้องเป็นบุคคลที่ได้รับอนุญาตหรือมีอำนาจในการเข้าถึงข้อมูลนั้น โดยหน่วยงานอาจใช้วิธีการป้องกันการเข้าถึงทั้งในด้านนโยบายและการปฏิบัติ โดยใช้ซอฟต์แวร์ในการพิสูจน์และยืนยันตัวตน (identify proofing and authentication) เช่น OTP, Finger print ฯลฯ

2.2 ความถูกต้อง (Integrity) คือ ข้อมูลส่วนบุคคลต้องมีความถูกต้อง สมบูรณ์ และครบถ้วน ตั้งแต่การเก็บรวบรวม การใช้งาน โดยอาศัยการใช้เทคโนโลยีดิจิทัล เช่น การตรวจสอบความถูกต้องของการบันทึกข้อมูล (Validate input data) และการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงและใช้งานที่เหมาะสม (Authorization) เช่น ระบบ Active directory

2.3 ความพร้อมใช้งาน (Availability) ข้อมูลส่วนบุคคลสามารถเข้าถึงและอยู่ในสภาพพร้อมใช้งาน ทั้งในด้านกายภาพและระบบ เช่น มีการสำรองและกู้คืนข้อมูลเมื่อมีเหตุฉุกเฉิน (Data backup and restore) การจัดให้มีเครื่องสำรองไฟกรณีฉุกเฉินเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

นอกจากนี้ส่วนที่ฝ่ายดิจิทัลต้องดำเนินการควบคู่กันไป ได้แก่ มาตรการรักษาความปลอดภัยใน 3 มาตรการ

- **มาตรการเชิงองค์กร** (Organizational measures) หมายถึง การจัดทำแผนเผชิญเหตุและแผนรับมือเมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคล รวมถึงมีการกำกับดูแลอย่างเหมาะสม พร้อมอบรมและสร้างความตระหนักรู้
- **มาตรการเชิงเทคนิค** (Technical measures) หมายถึง การนำระบบเทคโนโลยีดิจิทัลมาใช้เพื่อควบคุมและกับ เช่น การกำหนดสิทธิการเข้าถึง การเข้ารหัส การป้องกันด้วย Antivirus software Firewalls หรือ Data leak prevention
- **มาตรการกายภาพ** (Physical measures) หมายถึง การป้องกันทางกายภาพไม่ให้บุคคลที่ไม่มีสิทธิหรือไม่เกี่ยวข้องเข้าถึงด้านกายภาพ (เช่น สร้างแนวกั้นทางกายภาพหรือมีหน่วยรักษาความปลอดภัย) หรือการจัดให้มีระบบรักษาความปลอดภัยที่เหมาะสม เช่น ระบบควบคุมการเปิด-ปิดประตู (Access control) ระบบป้องกันอัคคีภัยและระงับอัคคีภัย

3. การบันทึกกิจกรรมประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities : RoPA) เนื่องจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ได้กำหนดให้หน่วยงานต้องบันทึกกิจกรรมประมวลผลข้อมูลส่วนบุคคล ซึ่งในความเป็นจริงกิจกรรมดังกล่าวหน่วยงานสามารถใช้การบันทึกลงในรูปแบบกระดาษได้เช่นกัน อย่างไรก็ตามเมื่อกิจกรรมประมวลผลมีจำนวนมากขึ้น การแก้ไขเปลี่ยนแปลงอาจไม่สะดวกในการดำเนินการ ดังนั้นจึงมีการประยุกต์ซอฟต์แวร์สเปรดชีตในการบันทึกกิจกรรมประมวลผลข้อมูลส่วนบุคคล จนถึงการใช้แพลตฟอร์มต่างๆ เข้ามาร่วมในการจัดทำบันทึกกิจกรรมประมวลผลข้อมูลส่วนบุคคล ปัจจุบันประเทศไทยมีแพลตฟอร์มภาครัฐเพื่อรองรับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Government Platform for PDPA Compliance: GPPC) ของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) เพื่อสนับสนุนการปฏิบัติงานในด้านดังกล่าว (https://gppc.onde.go.th) ร่วมกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

4. สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data subject rights) หมายถึง เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอรับข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนเอง จากผู้ควบคุมข้อมูลส่วนบุคคลที่เก็บรวบรวม ใช้ หรือเปิดเผย และในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ทำให้ข้อมูลส่วนบุคคลนั้นอยู่ในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติ (machine readable) และสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ ก็จะสามารถใช้สิทธิในการโอนย้ายข้อมูลส่วนบุคคล ทั้งนี้ต้องขึ้นอยู่กับกฎหมายในการให้สิทธิ Portability data (มาตรา 32) ซึ่งแยกออกเป็น 2 เรื่อง คือ

- เจ้าของข้อมูลส่วนบุคคลสามารถขอให้ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นเมื่อสามารถทำได้ด้วยวิธีการอัตโนมัติ
- เจ้าของข้อมูลส่วนบุคคลสามารถขอรับข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยตรง เว้นแต่โดยสภาพทางเทคนิคไม่สามารถทำได้

5. การทำ Data marking หมายถึง การทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนได้ โดยอาจใช้วิธีปิดทับข้อมูล หรือเปลี่ยนส่วนใดส่วนหนึ่งของข้อมูลโดยการใช้กลุ่มของตัวอักษรที่ได้จากการสุ่ม เช่น ถ้าต้องการลบข้อมูลที่เป็นชื่อ อาจมีการนำชื่อบุคคลไปจับคู่กับข้อมูลตัวอักษรที่สร้างขึ้นจากวิธีการสุ่ม หลังจากนั้นจึงเอาข้อมูลตัวอักษร ดังกล่าวมาแทนที่ชื่อบุคคล สำหรับอีกวิธีที่ได้รับความนิยมคือการใช้ในการเปลี่ยนข้อมูลอาศัยฟังก์ชันแฮช (Hash function) ซึ่งฟังก์ชันแฮชเป็นการใช้ฟังก์ชันทางคณิตศาสตร์สำหรับใช้ในการเปลี่ยนค่าต่างๆ ไปเป็นค่าอื่นที่ต่างจากค่าเดิม วิธีการของฟังก์ชันแฮชนับได้ว่าเป็นวิธีการที่ไม่สามารถทำย้อนกลับได้ จึงทำให้ข้อมูลส่วนบุคคลมีความปลอดภัยสูงมากยิ่งขึ้น วิธีการทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวตนดีมีหลายวิธี แต่ในที่นี้ขอยกมาเพียง 2 แบบ

5.1 Anonymization data หมายถึง การทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลนิรนาม วิธีการนี้จะทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวตนได้อีก ทั้งนี้เทคนิคของ Anonymization สามารถใช้วิธีการเปลี่ยนข้อมูลแบบสุ่ม (Randomization) หรือการทำข้อมูลให้เป็นข้อมูลแบบทั่วไป (Generlization)

5.2 Pesudonimization data เป็นวิธีการทำให้ข้อมูลไม่สามารถระบุตัวตนได้โดยตรง โดยวิธีการนี้จะนำเอาข้อมูลไปแทนที่ด้วยตัวอักษรหรือรหัสที่กำหนด แต่เมื่อใช้ข้อมูลประกอบอื่นก็อาจจะสามารถระบุตัวตนได้

6. การทำสัญญาประมวลผลข้อมูล (Data Processing Agreement : DPA) ซึ่งสัญญาดังกล่าวสามารถทำในรูปแบบดิจิทัลได้เช่นกัน ทั้งนี้เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลมีการกำกับดูแลจึงต้องดำเนิน การจัดทำสัญญาประมวลผลข้อมูลขึ้นมาเป็นข้อตกลงระหว่างกัน เช่น เมื่อองค์กรมีการพิจารณาในการใช้ระบบคลาวด์ในการประมวลผลข้อมูลส่วนบุคคล หน่วยงานที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลจึงจำเป็นต้องมีการจัดทำข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล และควรประกอบด้วยเงื่อนไขอย่างน้อยดังต่อไปนี้

6.1 ข้อกำหนดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

6.2 ข้อกำหนดเกี่ยวกับหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมีชอบ

6.3 ข้อกำหนดเกี่ยวกับหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลในการจัดทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

6.4 ข้อกำหนดเกี่ยวกับหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลในการแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

7. การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล (Breach notification) หน้าที่หนึ่งของผู้ควบคุมข้อมูลส่วนบุคคล คือการรับแจ้งเหตุละเมิดข้อมูลส่วนบุคคลสามารถ ทั้งนี้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถใช้ช่องทางการจดหมายอิเล็กทรอนิกส์ในการแจ้งเหตุละเมิด หรืออาจใช้แบบฟอร์มในรูปแบบดิจิทัลเพื่อแจ้งเหตุละเมิดได้เช่นกัน แต่ทั้งนี้เมื่อเลือกช่องทางใดผู้ควบคุมข้อมูลส่วนบุคคลควรพิจารณาความมีประสิทธิภาพของช่องทางที่ดำเนินการ

8. การเก็บข้อมูลการจราจรทางคอมพิวเตอร์ (Log server) เนื่องจากความเกี่ยวข้องของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ 2550 ตามมาตรา 26 ที่กำหนดให้ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินสองปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้ ดังนั้นการจัดเก็บข้อมูลดังกล่าวนอกจากเป็นการปฏิบัติตามกฎหมายแล้วยังเป็นส่วนหนึ่งของการดูแลรักษาความปลอดภัยของข้อมูลส่วนบุคคลเมื่อเกิดเหตุการละเมิด

ดังนั้นพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงมีบทบาทเกี่ยวข้องสัมพันธ์กับเทคโนโลยีดิจิทัลช่วยในการสนับสนุนการปฏิบัติงานทั้งในด้านการรักษาความปลอดภัยและการปฏิบัติตามกฎหมาย จะเห็นได้ว่าการดำเนินการคุ้มครองข้อมูลส่วนบุคคลจะต้องมีบุคลากรทางด้านดิจิทัลเข้ามามีส่วนในการส่งเสริมการปฏิบัติงานคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับพระราชบัญญัติดังกล่าว อย่างไรก็ตามข้อเท็จจริงอาจจะมีการเปลี่ยนแปลงไปตามเทคโนโลยีและสภาพแวดล้อม ดังนั้นจึงควรมั่นตรวจสอบข้อมูลต่างๆ ให้มั่นใจอยู่เสมอว่ายังมีความถูกต้องและสามารถใช้งานได้ในสถานการณ์ปัจจุบัน

เอกสารอ้างอิง

ปิยะบุตร บุญอร่ามเรือง, พัฒนาพร โกวพัฒกิจ, พีรพัฒ โชคสุวัฒนสกุล, เสกสิริ นิวัติศัยวงศ์, ปิติ เอี่ยมจำรูญลาภ, ชวิน อุ่นภัทร, ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล, ภูมิศิริ ดำรงวุฒิ และ โมกข์พิศุทธิ์ รตารุณ. 2563. แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล 3.0. กรุงเทพฯ: ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.

พีรดล สามะศิริ. 2566. การจัดทำข้อมูลนิรนาม (Data Anonymization). เข้าถึงได้จาก: https://bigdata.go.th/big-data101-/data-anonymization/, [เข้าถึงเมื่อ 16 สิงหาคม 2566].

สำนักงานพัฒนารัฐบาลดิจิทัล. 2566. เอกสารประกอบการสอนหลักสูตรเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลภาครัฐ. กรุงเทพฯ: สำนักงานพัฒนารัฐบาลดิจิทัล.