สคส.
สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

หลักสูตรการปฏิบัติหน้าที่ของ

ผู้ควบคุมข้อมูลส่วนบุคคล
ผู้ประมวลผลข้อมูลส่วนบุคคล
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
ลูกจ้าง ผู้รับจ้าง (e-learning)

ความรู้เบื้องต้นกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

บทที่ 1

- บทนำ
- หลักการพื้นฐานที่สำคัญเกี่ยวกับการคุ้มครองสิทธิมนุษยชน
- หลักสิทธิมนุษยชนสากล
- สิทธิในความเป็นส่วนตัวที่ได้รับการรับรองจากรัฐธรรมนูญ
- ความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล
- กรณีตัวอย่างการละเมิดข้อมูลส่วนบุคคล
- พื้นฐานและแนวคิดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล
- กฎหมายอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

• บทนำ

บทนี้จะได้อธิบายถึง

- ❑ หลักการพื้นฐานที่สำคัญเกี่ยวกับการคุ้มครองสิทธิมนุษยชน
- ❑ สิทธิในความเป็นส่วนตัวทั้งที่ได้รับการรับรองโดยกฎหมายระหว่างประเทศและรัฐธรรมนูญ
- ❑ ความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล
- ❑ กฎหมายอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

• หลักการพื้นฐานที่สำคัญเกี่ยวกับการคุ้มครองสิทธิมนุษยชน

หลักสิทธิมนุษยชนสากล

ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal declaration on Human Rights) ได้รับรองสิทธิในความเป็นส่วนตัว (Right to Privacy) ในข้อ 12 ซึ่งบัญญัติว่า

> “บุคคลใดจะถูกแทรกแซงตามอำเภอใจใน**ความเป็นส่วนตัว** ครอบครัว ที่อยู่อาศัย หรือการสื่อสาร หรือจะถูกลบหลู่เกียรติยศและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองของกฎหมายต่อการแทรกแซงสิทธิหรือการลบหลู่ดังกล่าวนั้น”

สิทธิในความเป็นส่วนตัว (Right to Privacy) หมายถึง

> “สิทธิที่จะอยู่ตามลำพังโดยปราศจากการแทรกแซงในความเป็นส่วนตัวที่ทำให้ได้รับความอับอาย เดือดร้อนรำคาญใจ หรือนำภาพหรือชื่อไปใช้ประโยชน์ในทางแสวงหาประโยชน์โดยมิชอบ”

• หลักการพื้นฐานที่สำคัญเกี่ยวกับการคุ้มครองสิทธิมนุษยชน

สิทธิในความเป็นส่วนตัว ประกอบด้วย 4 ด้าน คือ

- **ความเป็นส่วนตัวในชีวิตร่างกาย** (Bodily Privacy) เป็นการให้ความคุ้มครองในชีวิตร่างกายของบุคคลในทางกายภาพที่จะไม่ถูกดำเนินการใด ๆ อันละเมิดความเป็นอยู่ส่วนตัว
- **ความเป็นส่วนตัวในที่อยู่อาศัย บ้านเรือน เคหสถาน** (Territorial privacy) เป็นการกำหนดขอบเขตหรือข้อจำกัดที่บุคคลอื่นจะบุกรุกเข้าไปในสถานที่ส่วนตัวมิได้
- **ความเป็นส่วนตัวในการติดต่อสื่อสาร** (Communications Privacy) เป็นการให้ความคุ้มครองในความปลอดภัย และความเป็นอยู่ส่วนตัวในการติดต่อสื่อสารทางจดหมาย โทรศัพท์ ไปรษณีย์อิเล็กทรอนิกส์ หรือวิธีการติดต่อสื่อสารอื่นใดที่ผู้อื่นจะล่วงรู้มิได้
- **ความเป็นส่วนตัวในข้อมูลและสารสนเทศ** (Information privacy) เป็นการให้ความคุ้มครองข้อมูลส่วนบุคคลโดยการวางหลักเกณฑ์เกี่ยวกับการเก็บรวบรวมและการบริหารจัดการข้อมูลส่วนบคคล

"ความเป็นส่วนตัว" หรือ "Privacy" เป็นสิทธิมนุษยชนขั้นพื้นฐานที่มีความสำคัญเป็นอย่างยิ่งในสังคมยุคใหม่ โดยเฉพาะความเป็นอยู่ส่วนตัวในข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยในรูปแบบต่าง ๆ ที่หลากหลายอันเนื่องมาจากการพัฒนาของเทคโนโลยีสารสนเทศและการสื่อสารในปัจจุบัน

• หลักการพื้นฐานที่สำคัญเกี่ยวกับการคุ้มครองสิทธิมนุษยชน

สิทธิในความเป็นส่วนตัวที่ได้รับการรับรองในรัฐธรรมนูญ

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 ได้ให้การรับรองสิทธิในความเป็นส่วนตัวไว้ในมาตรา 32 ซึ่งบัญญัติไว้ ดังนี้

> “บุคคลย่อมมี**สิทธิในความเป็นอยู่ส่วนตัว** เกียรติยศ ชื่อเสียง และครอบครัว การกระทำอันเป็นการละเมิดหรือ กระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ”

• หลักการพื้นฐานที่สำคัญเกี่ยวกับการคุ้มครองสิทธิมนุษยชน

ความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลมีความสำคัญมากยิ่งขึ้นในปัจจุบัน ด้วยเหตุผลดังนี้

- การพัฒนาขึ้นอย่างมากของเทคโนโลยีสารสนเทศ ส่งผลให้มีฐานของข้อมูลส่วนบุคคลจำนวนมาก
- การขยายตัวของการค้าระหว่างประเทศ ประกอบกับการพัฒนาของเทคโนโลยีสารสนเทศทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลระหว่างประเทศเป็นไปได้ง่ายมากขึ้น
- รัฐบาลมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพิ่มมากขึ้น เพราะข้อมูลส่วนบุคคลของประชาชนจำเป็นสำหรับการบริหารงานภาครัฐ
- การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้บริโภค เนื่องจากข้อมูลของลูกค้ามีความสำคัญอย่างมากในการดำเนินธุรกิจ

• หลักการพื้นฐานที่สำคัญเกี่ยวกับการคุ้มครองสิทธิมนุษยชน

พื้นฐานและแนวคิดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

หลักการสากลที่เป็นพื้นฐานและแนวคิดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการยอมรับคือแนวปฏิบัติเกี่ยวกับการคุ้มครองความเป็นส่วนตัวและการส่งข้อมูลข้ามพรมแดนของข้อมูลส่วนบุคคล (Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data) ขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD) ซึ่งได้วางหลักการสำคัญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลไว้ 8 ประการ ดังนี้

(1) หลักข้อจำกัดในการเก็บรวบรวมข้อมูลส่วนบุคคล (Collection Limitation Principle)
(2) หลักคุณภาพของข้อมูลส่วนบุคคล (Data Quality Principle)
(3) หลักการกำหนดวัตถุประสงค์ในการจัดเก็บ (Purpose Specification Principle)
(4) หลักข้อจำกัดในการนำไปใช้ (Use Limitation Principle)
(5) หลักการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล (Security Safeguards Principle)
(6) หลักโปร่งใส (Openness Principle)
(7) หลักการมีส่วนร่วมของบุคคล (Individual Participation Principle)
(8) หลักความรับผิดชอบ (Accountability Principle)

• กฎหมายอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

ในการคุ้มครองข้อมูลส่วนบุคคลนั้น ไม่ได้มีเพียงแต่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เท่านั้น แต่ยังมีกฎหมายอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล มาตรา 3 วรรคแรก ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงบัญญัติว่า “ในกรณีที่มีกฎหมายว่าด้วยการใดบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ในลักษณะใด กิจการใด หรือหน่วยงานใดไว้โดยเฉพาะแล้ว ให้บังคับตามบทบัญญัติแห่งกฎหมายว่าด้วยการนั้น”

อย่างไรก็ตาม กฎหมายได้กำหนดข้อยกเว้นไว้ 2 ประการ คือ

(1) ในกรณีที่เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และสิทธิของเจ้าของข้อมูลส่วนบุคคล รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นการเพิ่มเติม ไม่ว่าจะซ้ำกับบทบัญญัติแห่งกฎหมายว่าด้วยการนั้นหรือไม่ก็ตาม ดังนั้น ไม่ว่ากฎหมายอื่นจะมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลอย่างไรก็ตาม ในส่วนที่เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และสิทธิของเจ้าของข้อมูลส่วนบุคคล รวมทั้งบทกำหนดโทษต้องเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ด้วย

เช่น มาตรา 23 (1) และ (5) ของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 กำหนดให้หน่วยงานของรัฐต้องจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลเพียงเท่าที่เกี่ยวข้อง และจำเป็นเพื่อการดำเนินงานของหน่วยงานของรัฐให้สำเร็จตามวัตถุประสงค์เท่านั้น และจัดระบบรักษาความปลอดภัยให้แก่ระบบข้อมูลข่าวสารส่วนบุคคลตามความเหมาะสม แต่ไม่ได้กำหนดรายละเอียดว่าต้องดำเนินการอย่างไร กรณีนี้หน่วยงานของรัฐก็ต้องดำเนินการตามที่กำหนดในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นการเพิ่มเติม

• กฎหมายอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

(2) ในกรณีที่เกี่ยวกับการร้องเรียน บทบัญญัติที่ให้อำนาจแก่คณะกรรมการผู้เชี่ยวชาญออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในกรณีดังต่อไปนี้

- ในกรณีที่กฎหมายว่าด้วยการนั้นไม่มีบทบัญญัติเกี่ยวกับการร้องเรียน
- ในกรณีที่กฎหมายว่าด้วยการนั้นมีบทบัญญัติที่ให้อำนาจแก่เจ้าหน้าที่ผู้มีอำนาจพิจารณาเรื่องร้องเรียนออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล แต่ไม่เพียงพอเท่ากับอำนาจของคณะกรรมการผู้เชี่ยวชาญ และเจ้าหน้าที่ผู้มีอำนาจตามกฎหมายดังกล่าวร้องขอต่อคณะกรรมการผู้เชี่ยวชาญหรือเจ้าของข้อมูลส่วนบุคคลผู้เสียหายยื่นคำร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ด้วยเหตุนี้ ในการทำความเข้าใจกฎหมายคุ้มครองข้อมูลส่วนบุคคล จึงมีความจำเป็นต้องเรียนรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายอื่นด้วย เพื่อที่จะได้เข้าใจการคุ้มครองข้อมูลส่วนบุคคลทั้งระบบ

• กฎหมายอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม
- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540
- พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562
- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม
- พระราชบัญญัติบัตรประจำตัวประชาชน พ.ศ. 2526 และที่แก้ไขเพิ่มเติม

• พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม

มีหลักการสำคัญ ดังนี้

• ป้องกันการใช้คอมพิวเตอร์ในทางที่ผิดที่ก่อให้เกิดความเดือดร้อนและเป็นอันตรายต่อบุคคลอื่น เช่น กำหนดให้ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตนให้เป็นความผิด (มาตรา 5) หรือกำหนดให้ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นเป็นความผิด (มาตรา 6)

• ป้องกันเผยแพร่ข้อมูลอันเป็นเท็จในระบบคอมพิวเตอร์ เช่น กำหนดให้ผู้ใดโดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน เป็นความผิด (มาตรา 14)

• คุ้มครองข้อมูลส่วนบุคคล โดยการห้ามทำให้เสียหาย ทำลาย แก้ไขเปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ (มาตรา 9) หรือห้ามการส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของผู้อื่นโดยปกติสุข (มาตรา 11 วรรคแรก) หรือห้ามส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นอันมีลักษณะเป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับข้อมูลโดยไม่เปิดโอกาสให้ผู้รับสามารถปฏิเสธได้ (มาตรา 11 วรรคสอง)

กฎหมายฉบับนี้มีเจตนารมณ์ คือ การกำหนดฐานความผิดและบทลงโทษรวมทั้งการกำหนดเกี่ยวกับอำนาจพนักงานเจ้าหน้าที่ ผู้ให้บริการ และผู้ใช้บริการ โดยครอบคลุมถึงการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ในลักษณะต่าง ๆ โดยเน้นการเจาะระบบคอมพิวเตอร์หรือเจาะข้อมูลคอมพิวเตอร์ ที่มีผลกระทบต่อความลับ (Confidentiality) ความครบถ้วน (Integrity) สภาพพร้อมใช้งาน (Availability) ของข้อมูล

• พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

มีหลักการสำคัญ ดังนี้

• ป้องกัน หรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที เนื่องจากในปัจจุบันการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียม มีความเสี่ยงจากภัยคุกคามทางไซเบอร์อันอาจกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ ที่จะทำให้ระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII) ไม่สามารถทำงานได้ปกติ หรือกระทบต่อการให้บริการประชาชน

• มาตรการคุ้มครองความปลอดภัยไซเบอร์ เช่น การจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อกำหนดมาตรการจัดการด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ และกำหนดกลไกการประสานงานระหว่างรัฐและเอกชน และสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ หรือกำหนดมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ใน 3 ระดับ ภัยระดับไม่ร้ายแรง ภัยระดับร้ายแรง และภัยระดับวิกฤติ (มาตรา 63 ถึง 69) หรือกำหนดให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องรายงานเหตุภัยคุกคามทางไซเบอร์ หากไม่ดำเนินการโดยไม่มีเหตุอันสมควรจะมีความผิด (มาตรา 73 ประกอบมาตรา 57)

• มาตรการคุ้มครองข้อมูลส่วนบุคคล เช่น ห้ามมิให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามพระราชบัญญัตินี้ให้แก่บุคคลใด (มาตรา 70) หรือห้ามพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้กระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลของผู้ใช้บริการหรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ที่ได้มาตามพระราชบัญญัตินี้ (มาตรา 71) หรือห้ามผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลของผู้ใช้บริการ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใดโดยมิชอบ (มาตรา 72)

• พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

มีหลักการสำคัญ ดังนี้

• ความโปร่งใสของการให้ข้อมูลจากหน่วยงานของรัฐ เนื่องจากการให้ประชาชนมีโอกาสกว้างขวางในการได้รับข้อมูลข่าวสารเกี่ยวกับการดำเนินการต่าง ๆ ของรัฐเป็นสิ่งจำเป็นเพื่อที่ประชาชนจะสามารถแสดงความคิดเห็นและใช้สิทธิทางการเมืองได้โดยถูกต้องกับความจริง อันเป็นการส่งเสริมให้มีความเป็นรัฐบาล โดยประชาชนมากยิ่งขึ้น จึงสมควรกำหนดให้ประชาชนมีสิทธิได้รู้ข้อมูลข่าวสารของราชการ และกำหนดให้หน่วยงานของรัฐ “เปิดเผยเป็นหลัก ปกปิดเป็นข้อยกเว้น” (มาตรา 6 – 9) โดยรัฐไม่ต้องเปิดเผยข้อมูลเฉพาะที่มีกฎหมายกำหนดเท่านั้น

• คุ้มครองความมั่นคงของรัฐ และประโยชน์สาธารณะ ข้อมูลข่าวสารบางประการ หน่วยงานของรัฐอาจมีคำสั่งไม่เปิดเผยได้ เช่น การเปิดเผยจะก่อให้เกิดความเสียหายต่อความมั่นคงของประเทศ ความสัมพันธ์ระหว่างประเทศ และความมั่นคงในทางเศรษฐกิจหรือการคลังของประเทศ (มาตรา 14 และ 15)

• คุ้มครองข้อมูลส่วนบุคคล เช่น หน่วยงานของรัฐต้องจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลเพียงเท่าที่เกี่ยวข้อง และจำเป็นเพื่อการดำเนินงานของหน่วยงานของรัฐให้สำเร็จตามวัตถุประสงค์เท่านั้น (มาตรา 23 (1)) และจัดระบบรักษาความปลอดภัยให้แก่ระบบข้อมูลข่าวสารส่วนบุคคลตามความเหมาะสม (มาตรา 23 (5)) หรือหน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่นหรือผู้อื่น จะต้องขอความยินยอมจากเจ้าของข้อมูลเสียก่อน เว้นแต่เป็นการใช้เพื่อให้บรรลุวัตถุประสงค์ของการจัดให้มีข้อมูลนั้น หรือเป็นการป้องกันการฝ่าฝืนกฎหมาย (มาตรา 24)

• พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

มีหลักการสำคัญ ดังนี้

• การเชื่อมโยงข้อมูลของหน่วยงานภาครัฐ ให้มีการนำเทคโนโลยีที่เหมาะสมมาประยุกต์ใช้ในการบริหารราชการแผ่นดินและการจัดทำบริการสาธารณะ และให้มีการบูรณาการฐานข้อมูลของหน่วยงานของรัฐทุกหน่วยงานเข้าด้วยกันเพื่อให้เป็นระบบข้อมูล เพื่อประโยชน์ในการบริหารราชการแผ่นดินและเพื่ออำนวยความสะดวกให้แก่ประชาชน อันจะนำไปสู่การเป็นรัฐบาลดิจิทัลที่มีระบบการทำงานและข้อมูลเชื่อมโยงกันระหว่างหน่วยงานของรัฐอย่างมั่นคงปลอดภัย มีประสิทธิภาพ รวดเร็ว เปิดเผยและโปร่งใส โดยกำหนดให้มีแผนพัฒนารัฐบาลดิจิทัลเพื่อกำหนดกรอบและทิศทางการบริหารงานภาครัฐ และการจัดทำบริการสาธารณะในรูปแบบของเทคโนโลยีดิจิทัลเพื่อการพัฒนาประเทศ (มาตรา 5)

• Open Government Data กำหนดให้การเปิดเผยข้อมูลหรือข่าวสารสาธารณะที่หน่วยงานของรัฐจัดทำและครอบครองในรูปแบบและช่องทางดิจิทัล เพื่อให้ประชาชนเข้าถึงได้โดยสะดวก (มาตรา 4)

• ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance) ซึ่งมีการกำหนดหลักการในมาตรา 8 โดยจะต้องการกำหนดสิทธิ หน้าที่และความรับผิดชอบในการบริหารจัดการข้อมูลของหน่วยงานของรัฐ มีระบบบริหารและกระบวนการจัดการและคุ้มครองข้อมูลที่ครบถ้วน การมีมาตรการในการควบคุมและพัฒนาคุณภาพข้อมูล การกำหนดนโยบายหรือกฎเกณฑ์การเข้าถึงและใช้ประโยชน์จากข้อมูลที่ชัดเจนและมีระบบบริหารจัดการ การจัดทำคำอธิบายชุดข้อมูลดิจิทัลของภาครัฐ

• มาตรการหรือระบบรักษาความมั่นคงปลอดภัยในการเข้าสู่บริการดิจิทัล โดยกำหนดให้จัดให้มีมาตรการหรือระบบรักษาความมั่นคงปลอดภัยในการเข้าสู่บริการดิจิทัลของหน่วยงานของรัฐ เพื่อให้มีความพร้อมใช้ น่าเชื่อถือ และสามารถตรวจสอบได้ (มาตรา 12)

• คุ้มครองข้อมูลส่วนบุคคล โดยในกรณีที่หน่วยงานของรัฐได้มาซึ่งข้อมูลส่วนบุคคลหรือมีข้อมูลส่วนบุคคลอยู่ในความครอบครอง หากหน่วยงานของรัฐประสงค์จะใช้ข้อมูลส่วนบุคคลดังกล่าวในรูปแบบข้อมูลดิจิทัลเพื่อประโยชน์ในการบริหารราชการแผ่นดินหน่วยงานของรัฐนั้นสามารถขอเชื่อมโยงและแลกเปลี่ยนข้อมูลส่วนบุคคลนั้นจากหน่วยงานของรัฐที่ครอบครอง เพื่อนำมาวิเคราะห์หรือประมวลผลได้ แต่ทั้งนี้ต้องเป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลด้วย (มาตรา 16)

• พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม

มีหลักการสำคัญ ดังนี้

• รองรับสถานะทางกฎหมายของข้อมูลทางอิเล็กทรอนิกส์ เนื่องจากการทำธุรกรรมในปัจจุบันมีแนวโน้มที่จะปรับเปลี่ยนวิธีการในการติดต่อสื่อสารที่อาศัยการพัฒนาการเทคโนโลยีทางอิเล็กทรอนิกส์ซึ่งมีความสะดวก รวดเร็วและมีประสิทธิภาพ แต่เนื่องจาก การทำธุรกรรมทางอิเล็กทรอนิกส์ดังกล่าวมีความแตกต่างจากวิธีการทำธุรกรรมซึ่งมีกฎหมายรองรับอยู่ในปัจจุบันเป็นอย่างมาก อันส่งผลให้ต้องมีการรองรับสถานะทางกฎหมายของข้อมูลทางอิเล็กทรอนิกส์ให้เสมอกับการทำเป็นหนังสือ หรือหลักฐานเป็นหนังสือ การรับรองวิธีการส่งและรับข้อมูลอิเล็กทรอนิกส์ การใช้ลายมือชื่ออิเล็กทรอนิกส์ ตลอดจนการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ เพื่อเป็นการส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ให้น่าเชื่อถือ และมีผลในทางกฎหมายเช่นเดียวกับการทำธุรกรรมโดยวิธีการทั่วไปที่เคยปฏิบัติอยู่เดิม

• คุ้มครองข้อมูลส่วนบุคคล กำหนดให้ผู้ให้บริการออกใบรับรองเพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์ให้มีผลทางกฎหมายเสมือนหนึ่งลงลายมือชื่อ ต้องดำเนินการให้ข้อมูลที่เกี่ยวกับการยืนยันตัวตนทางดิจิทัลเป็นข้อมูลที่ถูกต้องและสมบูรณ์ และจัดให้มีวิธีการเข้าถึงให้คู่กรณีที่เกี่ยวข้องตรวจสอบข้อเท็จจริงได้ นอกจากนี้ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ยังกำหนดให้ในกรณีที่หน่วยงานของรัฐมีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูล หรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคลไม่ว่าโดยตรงหรือโดยอ้อม ให้หน่วยงานของรัฐจัดทำแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

• พระราชบัญญัติบัตรประจำตัวประชาชน พ.ศ. 2526 และที่แก้ไขเพิ่มเติม

มีหลักการสำคัญ ดังนี้

• คุ้มครองข้อมูลส่วนบุคคล โดยกำหนดให้ข้อมูลที่อยู่ในบัตร จะต้องประกอบไปด้วย ชื่อ นามสกุล วัน เดือน ปีเกิด ที่อยู่ตามทะเบียนบ้าน รูปถ่าย และเลขประจำตัวประชาชน ส่วนข้อมูลศาสนาจะมีหรือไม่ก็ได้ (มาตรา 7) และกำหนดให้ข้อมูลอื่นของผู้ถือบัตรประจำตัวประชาชนในหน่วยความจำนอกเหนือจากที่ปรากฏในบัตรไม่สามารถเปิดเผยต่อบุคคลหรือหน่วยงานซึ่งมิใช่เป็นผู้จัดทำหรือรวบรวมข้อมูลนั้นได้ เว้นแต่เป็นข้อมูลทั่วไปที่ปรากฏอยู่บนบัตร หรือเป็นการเปิดเผยต่อหน่วยงานที่มีความจำเป็นต้องทราบข้อมูลนั้นเท่าที่จำเป็นเพื่อประโยชน์ของผู้ถือบัตรโดยได้รับความยินยอมจากผู้ถือบัตรหรือเพื่อประโยชน์ของรัฐ หรือเพื่อความสงบเรียบร้อยของบ้านเมือง (มาตรา 7/1)

• ความรู้เบื้องต้นกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

สรุปความสำคัญและความเกี่ยวข้องของกฎหมายอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

จากที่กล่าวมาข้างต้นเกี่ยวกับกฎหมายอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล จะเห็นได้ว่ากฎหมายเหล่านี้มีความเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลไม่มากก็น้อย เช่น พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 อาจจะให้ความสำคัญในเรื่องความมั่นคงปลอดภัยไซเบอร์ แต่อาจจะไม่ได้พูดถึงเรื่องความชอบธรรมหรือความโปร่งใส ในขณะที่พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 อาจจะให้ความคุ้มครองข้อมูลส่วนบุคคลในมิติการใช้ข้อมูลส่วนบุคคลเพียงเท่าที่จำเป็น แต่ไม่ได้กำหนดรายละเอียดในเรื่องความมั่นคงปลอดภัยของข้อมูล เป็นต้น กฎหมายอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล เมื่อพิจารณาโดยภาพรวมแล้วสามารถคุ้มครองข้อมูลส่วนบุคคลได้ แต่อาจจะไม่ครบถ้วนในทุกมิติ โดยเฉพาะในเรื่องของสิทธิของเจ้าของข้อมูลส่วนบุคคล การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และรายละเอียดเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ด้วยเหตุนี้ ในการบังคับใช้กฎหมายอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลจึงจำเป็นต้องใช้บังคับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพิ่มเติมด้วย ไม่ว่าจะซ้ำกับกฎหมายอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลหรือไม่ก็ตาม

แบบทดสอบ บทที่ 1

ข้อที่ 1

Q : สิทธิในความเป็นอยู่ส่วนตัวจะประกอบด้วยสาระสำคัญ 4 ด้าน อะไรบ้าง

แบบทดสอบ บทที่ 1

ข้อที่ 2

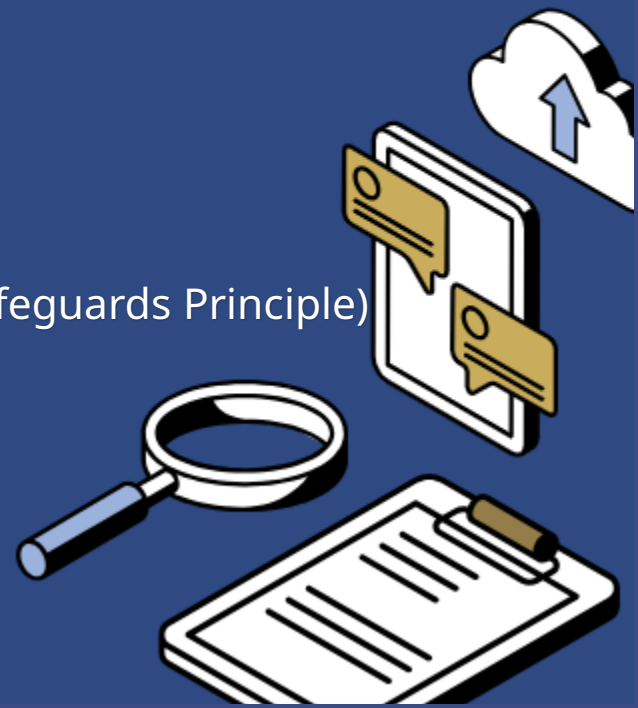
Q : ข้อใดไม่ใช่หลักการพื้นฐานของแนวปฏิบัติเกี่ยวกับการคุ้มครองความเป็นส่วนตัวและการส่งข้อมูลข้ามพรมแดนของข้อมูลส่วนบุคคล (Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data) ตอบได้มากกว่า 1 ข้อ

ก. หลักคุณภาพของข้อมูลส่วนบุคคล (Data Quality Principle)

ข. หลักความเสมอภาค (Equality Principle)

ค. หลักความรับผิดชอบ (Accountability Principle)

ง. หลักการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล (Security Safeguards Principle)



แบบทดสอบ บทที่ 1

ข้อที่ 3

Q : <u>จริงหรือเท็จ</u>

กฎหมายที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลนั้น
มีเฉพาะพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เท่านั้น

• เฉลยแบบทดสอบบทที่ 1

ข้อที่	เฉลย
1.	ความเป็นอยู่ส่วนตัวในชีวิตร่างกาย (Bodily Privacy) / ความเป็นอยู่ส่วนตัวในที่อยู่อาศัย บ้านเรือน เคหสถาน (Territorial privacy) / ความเป็นอยู่ส่วนตัวในการติดต่อสื่อสาร (Communications Privacy) / ความเป็นอยู่ส่วนตัวในข้อมูลและสารสนเทศ (Information privacy)
2.	ข.
3.	เท็จ

ข้อมูลส่วนบุคคล

บทที่ 2

- บทนำ
- ความหมายของข้อมูลส่วนบุคคล
- หลักเกณฑ์ในการพิจารณาว่าข้อมูลใดเป็นข้อมูลส่วนบุคคล
- ข้อมูลนิรนาม (Anonymous data)
- ข้อมูลแฝง (Pseudonymous data)
- ประเภทของข้อมูลส่วนบุคคล

• บทนำ

บทนี้จะได้อธิบายความแตกต่างระหว่าง

- ❑ ข้อมูลส่วนบุคคล (Personal Data)
- ❑ ข้อมูลนิรนาม (Anonymous Data)
- ❑ ข้อมูลแฝง (Pseudonymous Data)
- ❑ การแบ่งแยกประเภทของข้อมูลส่วนบุคคล

• ความหมายของข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล

มาตรา 6 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติว่า “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

จากบทบัญญัติข้างต้น สิ่งที่ถือว่าเป็น “ข้อมูลส่วนบุคคล” จะต้องมีองค์ประกอบทั้ง 4 ประการครบถ้วน ดังนี้

- ต้องเป็นข้อมูล
- ข้อมูลดังกล่าวต้องเกี่ยวข้องสัมพันธ์กับบุคคล
- ข้อมูลดังกล่าวทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม
- บุคคลนั้นหมายถึงเฉพาะบุคคลธรรมดา ไม่รวมถึงนิติบุคคลและผู้ถึงแก่กรรม

ทั้ง 4 องค์ประกอบจะต้องมีครบถ้วนจึงจะถือได้ว่าเป็น “ข้อมูลส่วนบุคคล”

ตัวอย่างของข้อมูลส่วนบุคคล เช่น เลขบัตรประจำตัวประชาชน ชื่อ - นามสกุล ที่อยู่ เบอร์โทรศัพท์ อีเมล ข้อมูลทางการเงิน เชื้อชาติ ศาสนา ข้อมูลสุขภาพ ประวัติอาชญากรรม ข้อมูลสภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลเกี่ยวกับเพศสภาพ และพฤติกรรมทางเพศ เป็นต้น

• ข้อมูลนิรนาม

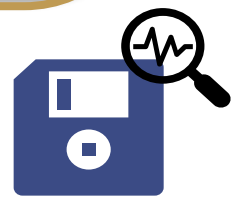
ข้อมูลนิรนาม (Anonymous data)

- ข้อมูลที่ไม่สัมพันธ์กับบุคคลที่ถูกระบุตัวตนหรือสามารถระบุตัวตนใด ๆ ได้
- ข้อมูลส่วนบุคคลที่ถูกทำให้ระบุตัวตนไม่ได้ด้วยวิธีการที่ทำให้ไม่สามารถระบุตัวตนเจ้าของข้อมูลได้หรือไม่สามารถระบุตัวตนได้อีกต่อไป
- โดยทั่วไปข้อมูลนิรนามไม่ตกอยู่ภายใต้บังคับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล อย่างไรก็ตาม ในกรณีที่มีข้อมูลแวดล้อมเพิ่มเติมที่อาจทำให้ข้อมูลนิรนามระบุตัวตนเจ้าของข้อมูลส่วนบุคคล ข้อมูลนิรนามก็อาจเข้าข่ายกลายเป็นข้อมูลส่วนบุคคลที่อยู่ภายใต้บังคับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลได้

• ข้อมูลแฝง

ข้อมูลแฝง (Pseudonymous data)

- ข้อมูลที่ยังไม่ถูกทำให้นิรนามโดยสมบูรณ์
- เป็นข้อมูลที่ถูกผ่านกระบวนการแฝงหรือพรางข้อมูลบ่งชี้ตัวบุคคลเอาไว้ โดยกระบวนการดังกล่าวจะทำให้การใช้ข้อมูลมีความเสี่ยงน้อยลง
- กระบวนการแฝงหรือพรางข้อมูลบ่งชี้ตัวบุคคลอาจใช้วิธีเปลี่ยนข้อมูลที่ระบุตัวบุคคล (Identifier) ด้วยข้อมูล เลข หรือรหัสอื่น
- ข้อมูลแฝงยังตกอยู่ภายใต้บังคับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เนื่องจากข้อมูลดังกล่าวยังสามารถระบุตัวเจ้าของข้อมูลส่วนบุคคลได้



• ทดสอบความรู้

จงทำให้ข้อมูลต่อไปนี้เป็นข้อมูลนิรนาม

“นาย ก. ประธานบริหารบริษัท กรุงเทพมหานคร จำกัด มีรายได้ 15 ล้านบาท”

• ข้อมูลส่วนบุคคล (Personal Data)

ข้อมูลส่วนบุคคล แบ่งออกเป็น 2 ประเภท คือ

- ข้อมูลส่วนบุคคล ตามที่ได้ให้ความหมายไว้ข้างต้น ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลต้องเป็นไปตามมาตรา 24 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน จะกระทบต่อสิทธิของเจ้าของข้อมูลมากกว่าข้อมูลส่วนบุคคลโดยทั่วไป ดังนั้น กฎหมายจึงมีความจำเป็นต้องคุ้มครองข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนมากกว่าข้อมูลส่วนบุคคลธรรมดา โดยในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน จะต้องเป็นไปตามมาตรา 26 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน ตามมาตรา 26 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้แก่ ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ เป็นต้น

นอกจากนี้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจออกประกาศกำหนดข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน เพิ่มเติมก็ได้ หากเห็นว่ามีข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกัน

• ทดสอบความรู้

จงยกตัวอย่างข้อมูลส่วนบุคคลที่ถือว่าเป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน
ที่ตกอยู่ภายใต้บังคับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

แบบทดสอบ บทที่ 2

ข้อที่ 1

Q : อะไรคือหน้าที่ของหลักเกณฑ์การพิจารณาว่าข้อมูลใดเป็นข้อมูลส่วนบุคคล

ก. เพื่อกำหนดว่าข้อมูลส่วนบุคคลใดเป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน

ข. เพื่อกำหนดว่าข้อมูลส่วนบุคคลใดเป็นข้อมูลนิรนาม

ค. เพื่อกำหนดว่าข้อมูลใดเป็นข้อมูลส่วนบุคคล

ง. เพื่อกำหนดว่าข้อมูลส่วนบุคคลใดเป็นข้อมูลแฝง

แบบทดสอบ บทที่ 2

ข้อที่ 2

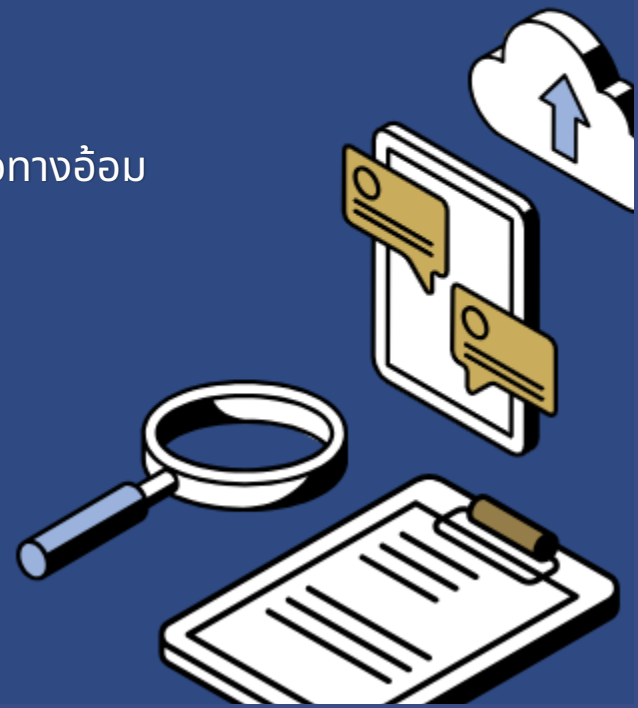
Q : หลักเกณฑ์ใดบ้างต่อไปนี้ที่ใช้สำหรับกำหนดว่าข้อมูลใดเป็นข้อมูลส่วนบุคคล สามารถตอบได้มากกว่า 1 ข้อ

ก. ต้องเป็นข้อมูล

ข. ข้อมูลดังกล่าวต้องเกี่ยวข้องสัมพันธ์กับบุคคล

ค. ข้อมูลดังกล่าวทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม

ง. เป็นข้อมูลนิรนาม



แบบทดสอบ บทที่ 2

ข้อที่ 3

Q : ข้อมูลใดต่อไปนี้เป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน สามารถตอบได้มากกว่า 1 ข้อ

ก. ข้อมูลส่วนบุคคลที่เกี่ยวกับความคิดเห็นทางการเมือง

ข. ข้อมูลส่วนบุคคลที่เกี่ยวกับความเชื่อในลัทธิ ศาสนา หรือปรัชญา

ค. ข้อมูลส่วนบุคคลที่เกี่ยวกับรายละเอียดทางการเงิน

ง. ข้อมูลพันธุกรรมที่ใช้สำหรับบ่งชี้บุคคลธรรมดาโดยเฉพาะ

แบบทดสอบ บทที่ 2

ข้อที่ 4

Q : <u>จริงหรือเท็จ</u>

ข้อมูลส่วนบุคคลสามารถถูกทำให้เป็นข้อมูลนิรนามได้เสมอ

แบบทดสอบ บทที่ 2

ข้อที่ 5

Q : <u>จริงหรือเท็จ</u>

ข้อมูลแฝงตกอยู่ภายใต้บังคับของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

แบบทดสอบ บทที่ 2

ข้อที่ 6

Q : ข้อมูลของอุปกรณ์หรือเครื่องมือต่าง ๆ
เช่น IP Address เป็นข้อมูลส่วนบุคคลหรือไม่ เพราะเหตุใด

• เฉลยแบบทดสอบบทที่ 2

ข้อที่	เฉลย
1.	ค.
2.	ก. ข. และ ค.
3.	ก. ข. และ ง.
4.	เท็จ
5.	จริง
6.	ข้อมูลของอุปกรณ์หรือเครื่องมือต่างๆ เช่น IP Address อาจเป็นข้อมูลส่วนบุคคลได้ เพราะข้อมูลดังกล่าวอาจระบุตัวบุคคลได้หากมีข้อมูลแวดล้อมประกอบ

ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล

บทที่ 3

- บทนำ
- บทบาทในการคุ้มครองข้อมูลส่วนบุคคล
  - เจ้าของข้อมูลส่วนบุคคล
  - ผู้ควบคุมข้อมูลส่วนบุคคล
  - ผู้ประมวลผลข้อมูลส่วนบุคคล
  - หน่วยงานกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคล
- องค์ประกอบพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคล
- แบบทดสอบ

บทนำ

มาตรา 6 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดนิยามของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล มีรายละเอียดดังนี้

ผู้ควบคุมข้อมูลส่วนบุคคล คือ บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

จากนิยามดังกล่าวเห็นได้ว่าผู้ควบคุมข้อมูลส่วนบุคคลเป็นได้ทั้งบุคคลธรรมดาและนิติบุคคล เช่น ผู้ประกอบธุรกิจในรูปแบบเจ้าของคนเดียว ผู้ประกอบธุรกิจ SME บริษัทจำกัด บริษัทมหาชนจำกัด มหาวิทยาลัย โดยผู้ควบคุมข้อมูลส่วนบุคคลมีอำนาจในการตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เช่น กำหนดวัตถุประสงค์และวิธีการในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล คือ บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

จากนิยามข้างต้นพบว่าผู้ประมวลผลข้อมูลส่วนบุคคลเป็นได้ทั้งบุคคลธรรมดาและนิติบุคคล และทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในนามหรือตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล กล่าวคือ ผู้ประมวลผลข้อมูลส่วนบุคคลไม่มีอำนาจในการตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลแต่อย่างใด

นอกจากนี้ ผู้ประมวลผลข้อมูลส่วนบุคคลต้องไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล กล่าวคือ ผู้ประมวลผลข้อมูลส่วนบุคคลต้องเป็นหน่วยงานแยกต่างหากจากผู้ควบคุมข้อมูลส่วนบุคคล โดยอาจให้บริการในลักษณะเป็น Outsource หรือเป็นผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคล

บทบาทในการคุ้มครองข้อมูลส่วนบุคคล

บทบาทในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

1. กรณีตัวอย่างเพื่อใช้ในการเรียนรู้เกี่ยวกับบทบาทในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

นาย ก. ทำงานกับบริษัทค้าปลีกในกรุงเทพมหานคร แผนกทรัพยากรบุคคลของบริษัททำการเก็บรวบรวมข้อมูลส่วนบุคคลของนาย ก. ในรูปแบบไฟล์เอกสาร และบริษัทแห่งนี้ได้ทำสัญญากับบริษัทบริหารจัดการเงินเดือนเพื่อโอนเงินเดือนของนาย ก. เข้าบัญชีธนาคารโดยตรง โดยมีสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ให้การกำกับดูแลเพื่อให้มั่นใจว่าบริษัทดังกล่าวได้ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

กรณีตัวอย่างข้างต้นประกอบด้วยบุคคลและนิติบุคคลที่มีบทบาทในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ดังนี้

เจ้าของข้อมูลส่วนบุคคล: บุคคลที่ข้อมูลส่วนบุคคลของตนถูกเก็บรวบรวม ใช้ หรือเปิดเผย

ผู้ควบคุมข้อมูลส่วนบุคคล: บุคคลหรือนิติบุคคลที่มีอำนาจตัดสินใจว่าจะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอย่างไรและเพื่อวัตถุประสงค์ใด

ผู้ประมวลผลข้อมูลส่วนบุคคล: บุคคลหรือนิติบุคคลที่ทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในนามหรือตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล

หน่วยงานกำกับดูแล: หน่วยงานที่ตั้งขึ้นเพื่อบังคับใช้กฎหมายและกฎระเบียบด้านความเป็นส่วนตัวหรือการคุ้มครองข้อมูลส่วนบุคคลในเขตอำนาจศาลหนึ่ง ๆ

บทบาทในการคุ้มครองข้อมูลส่วนบุคคล

2. บทบาทในการคุ้มครองข้อมูลส่วนบุคคล

ในบริบทของการคุ้มครองข้อมูลส่วนบุคคล มีการแบ่งบุคคลหรือกลุ่มบุคคลออกเป็น 4 บทบาทหลัก ๆ ซึ่งทุกคนและทุกองค์กรจะต้องมีบทบาทใดบทบาทหนึ่งดังต่อไปนี้

1) เจ้าของข้อมูลส่วนบุคคล คือ บุคคลที่ข้อมูลส่วนบุคคลของตนถูกเก็บรวบรวม ใช้ หรือเปิดเผย

2) ผู้ควบคุมข้อมูลส่วนบุคคล คือ บุคคลหรือนิติบุคคลที่มีอำนาจในการตัดสินใจว่าจะเก็บข้อมูลอะไร นำไปใช้อย่างไร และเพื่อวัตถุประสงค์ใด โดยผู้ควบคุมข้อมูลส่วนบุคคลไม่จำเป็นต้องเป็นองค์กรทางธุรกิจเสมอไป อาจเป็นหน่วยงานของรัฐหรือองค์กรไม่แสวงหากำไรก็ได้

3) ผู้ประมวลผลข้อมูลส่วนบุคคล คือ บุคคลหรือนิติบุคคลผู้ให้บริการที่ดำเนินการในนามหรือตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เช่น การเก็บข้อมูลในคลาวด์ โดยผู้ประมวลผลข้อมูลส่วนบุคคลจะทำสิ่งใดไม่ได้เลยนอกจากสิ่งที่ผู้ควบคุมข้อมูลส่วนบุคคลกำหนดให้กระทำ

4) หน่วยงานกำกับดูแล คือ หน่วยงานที่มีหน้าที่ตรวจสอบและควบคุมการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อให้แน่ใจว่ามีการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

บทบาทในการคุ้มครองข้อมูลส่วนบุคคล

ในบางประเทศ เช่น สหรัฐอเมริกา ยังไม่มีการกำหนดนิยามของ "ผู้ควบคุมข้อมูลส่วนบุคคล" หรือ "ผู้ประมวลผลข้อมูลส่วนบุคคล" อย่างชัดเจนในกฎหมาย โดยผู้ควบคุมข้อมูลส่วนบุคคลในสหรัฐอเมริกา มีบทบาทในการกำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ในการคุ้มครองข้อมูลส่วนบุคคลจากการเข้าถึงที่ไม่ได้รับอนุญาต การทำลาย การเปลี่ยนแปลง หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต นอกจากนี้ ผู้ควบคุมข้อมูลส่วนบุคคลยังมีหน้าที่แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงรายละเอียดการใช้ข้อมูลส่วนบุคคลผ่านนโยบายความเป็นส่วนตัว

ส่วน GDPR ได้ให้นิยามทางกฎหมายอย่างชัดเจนว่า ผู้ควบคุมข้อมูลส่วนบุคคล คือ บุคคลหรือองค์กรที่ตัดสินใจว่าจะเก็บรวบรวมข้อมูลอะไร เก็บรวบรวมเพื่อวัตถุประสงค์ใด และจะใช้งานอย่างไร กล่าวคือผู้ควบคุมข้อมูลส่วนบุคคล เป็นผู้ตัดสินใจหลักเกี่ยวกับการใช้ข้อมูลนั้น ในขณะที่ผู้ประมวลผลข้อมูลส่วนบุคคล คือ บุคคลหรือองค์กรที่ดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล โดยผู้ประมวลผลข้อมูลส่วนบุคคลจะไม่มีอำนาจในการตัดสินใจใด ๆ เกี่ยวกับข้อมูลนั้น

สำหรับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีการกำหนดนิยามของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลอย่างชัดเจน และสอดคล้องกับ GDPR โดยได้ให้นิยามของผู้ควบคุมข้อมูลส่วนบุคคลว่าคือ บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

บทบาทในการคุ้มครองข้อมูลส่วนบุคคล

ส่วนผู้ประมวลผลข้อมูลส่วนบุคคล คือ บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

แม้ว่าทั้งผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลจะมีความรับผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในกรณีที่มีการละเมิดกฎหมาย แต่ผู้ควบคุมข้อมูลส่วนบุคคลจะมีภาระหน้าที่มากกว่า เช่น การตัดสินใจเกี่ยวกับข้อมูลว่าจะเก็บเป็นระยะเวลาเท่าใด หรือจะอนุญาตให้บุคคลใดสามารถเข้าถึงข้อมูลได้บ้าง ในขณะที่ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่หลักในการบันทึกรายการกิจกรรมและแจ้งเตือนเมื่อมีการละเมิดข้อมูล

ด้วยเหตุนี้ ในทางปฏิบัติจึงมักมีการเจรจาต่อรองโดยกำหนดบทบาทของตนให้เป็นผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งในความเป็นจริงแล้วการกำหนดบทบาทไม่ได้ขึ้นอยู่กับการตัดสินใจว่าจะเป็นผู้ประมวลผลข้อมูลส่วนบุคคลหรือผู้ควบคุมข้อมูลส่วนบุคคลแต่อย่างใด แต่ขึ้นอยู่กับว่าบุคคลหรือนิติบุคคลนั้นทำอะไรกับข้อมูลส่วนบุคคล อีกทั้งต้องพิจารณาว่าบุคคลหรือนิติบุคคลดังกล่าวมีอำนาจในการตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลหรือไม่

บทบาทในการคุ้มครองข้อมูลส่วนบุคคล

3.การจำแนกบทบาทในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามกรณีตัวอย่างข้อ 1

จากกรณีตัวอย่างในข้อ 1 สามารถระบุบทบาทของแต่ละฝ่ายที่เกี่ยวข้องในกระบวนการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้ดังนี้

1) นาย ก. เป็น**เจ้าของข้อมูลส่วนบุคคล** ซึ่งเป็นบุคคลที่ข้อมูลส่วนบุคคลของตนถูกเก็บรวบรวม ใช้ หรือเปิดเผย

2) บริษัทค้าปลีก เป็น**ผู้ควบคุมข้อมูลส่วนบุคคล** ซึ่งบริษัทนี้มีอำนาจในการตัดสินใจว่าจะเก็บรวบรวมข้อมูลส่วนบุคคลของนาย ก. และนำข้อมูลนั้นไปใช้ในวัตถุประสงค์ใด

3) บริษัทบริหารจัดการเงินเดือน เป็น**ผู้ประมวลผลข้อมูลส่วนบุคคล** ซึ่งทำหน้าที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งของบริษัทค้าปลีก เช่น การจัดการโอนเงินเดือนให้กับนาย ก.

4) สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) เป็น **หน่วยงานกำกับดูแล** ซึ่งมีหน้าที่ตรวจสอบให้มั่นใจว่าบริษัทค้าปลีกปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

บทบาทในการคุ้มครองข้อมูลส่วนบุคคล

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

1.หน้าที่ในการแจ้งรายละเอียดเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคล

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในการแจ้งรายละเอียดเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคล แบ่งแยกเป็น 3 กรณีย่อย ได้แก่ กรณีเก็บรวบรวมข้อมูลจากเจ้าของข้อมูลส่วนบุคคล กรณีเก็บรวบรวมข้อมูลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคล และกรณีมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างจากวัตถุประสงค์ที่แจ้งไว้

1.1 กรณีเก็บรวบรวมข้อมูลจากเจ้าของข้อมูลส่วนบุคคล

มาตรา 23 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่แจ้งรายละเอียดเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคล เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

รายละเอียดเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบมีดังต่อไปนี้

1) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคล
2) กรณีที่เจ้าข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญา
3) ประเภทของข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวม
4) บุคคลที่สามที่เป็นผู้รับข้อมูลส่วนบุคคล
5) รายละเอียดเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล ตัวแทน และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
6) สิทธิของเจ้าของข้อมูลส่วนบุคคล

บทบาทในการคุ้มครองข้อมูลส่วนบุคคล

1.2 กรณีเก็บรวบรวมข้อมูลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคล

มาตรา 25 วรรคหนึ่ง บัญญัติห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่กรณีต่อไปนี้

1) ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
2) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26

อย่างไรก็ตาม มาตรา 25 วรรคสอง กำหนดให้การเก็บรวบรวมข้อมูลส่วนบุคคลที่ต้องได้รับความยินยอม ต้องนำบทบัญญัติเกี่ยวกับการแจ้งวัตถุประสงค์ใหม่ตามมาตรา 21 และการแจ้งรายละเอียด ตามมาตรา 23 มาใช้บังคับ เว้นแต่กรณีต่อไปนี้

1) เจ้าของข้อมูลส่วนบุคคลทราบวัตถุประสงค์ใหม่หรือรายละเอียดนั้นอยู่แล้ว
2) ผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่าการแจ้งวัตถุประสงค์ใหม่หรือรายละเอียดดังกล่าวไม่สามารถทำได้หรือจะเป็นอุปสรรคต่อการใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ในกรณีนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิ เสรีภาพ และประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
3) การใช้หรือการเปิดเผยข้อมูลส่วนบุคคลต้องกระทำโดยเร่งด่วนตามที่กฎหมายกำหนด ซึ่งได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
4) เมื่อผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้ซึ่งล่วงรู้หรือได้มาซึ่งข้อมูลส่วนบุคคลจากหน้าที่ หรือจากการประกอบอาชีพหรือวิชาชีพ และต้องรักษาวัตถุประสงค์ใหม่หรือรายละเอียดบางประการ ตามมาตรา 23 ไว้เป็นความลับตามที่กฎหมายกำหนด

บทบาทในการคุ้มครองข้อมูลส่วนบุคคล

ส่วนมาตรา 25 วรรคสาม บัญญัติเกี่ยวกับการแจ้งรายละเอียดตามมาตรา 25 วรรคสอง โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบภายในสามสิบวันนับแต่วันที่เก็บรวบรวมตามมาตรานี้ เว้นแต่กรณีที่นำข้อมูลส่วนบุคคลไปใช้เพื่อการติดต่อกับเจ้าของข้อมูลส่วนบุคคลต้องแจ้งในการติดต่อครั้งแรก และกรณีที่จะนำข้อมูลส่วนบุคคลไปเปิดเผย ต้องแจ้งก่อนที่จะนำข้อมูลส่วนบุคคลไปเปิดเผยเป็นครั้งแรก

1.3 กรณีมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างจากวัตถุประสงค์ที่แจ้งไว้

มาตรา 21 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวม การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างไปจากวัตถุประสงค์ที่ได้แจ้งไว้จะกระทำมิได้ เว้นแต่กรณีต่อไปนี้

1) ได้แจ้งวัตถุประสงค์ใหม่นั้นให้เจ้าของข้อมูลส่วนบุคคลทราบและได้รับความยินยอมก่อนเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลแล้ว
2) บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

บทบาทในการคุ้มครองข้อมูลส่วนบุคคล

2. หน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

มาตรา 37 (1) กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการเชิงองค์กรและมาตรการเชิงเทคนิค เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องมีการพิจารณาทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป

ตัวอย่างมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล เช่น

1) มีการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล
2) มีการเข้ารหัสข้อมูลส่วนบุคคล และการแยกข้อมูลออกไปเพื่อไม่ให้สามารถระบุตัวบุคคลได้
3) มีความสามารถในการทำให้พร้อมใช้งานและเข้าถึงข้อมูลส่วนบุคคลได้ในเวลาที่เหมาะสม
4) มีมาตรการในการรักษาความลับและความถูกต้องครบถ้วนของข้อมูล
5) มีกระบวนการในการทดสอบ ประเมิน และวัดประสิทธิภาพของมาตรการการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

บทบาทในการคุ้มครองข้อมูลส่วนบุคคล

3. หน้าที่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

มาตรา 37 (4) กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมงนับแต่ทราบเหตุ เว้นแต่เหตุที่เกิดนั้นไม่มีความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล โดยข้อมูลที่ต้องแจ้ง ได้แก่

1) ข้อมูลเกี่ยวกับลักษณะและประเภทของการละเมิดข้อมูลส่วนบุคคล
2) ข้อมูลในการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและผู้ประสานงานของผู้ควบคุมข้อมูลส่วนบุคคล
3) ผลกระทบที่อาจเกิดขึ้นจากเหตุการละเมิดข้อมูลส่วนบุคคล
4) มาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลจะใช้ในการป้องกัน ระงับ แก้ไขเหตุการละเมิดข้อมูลส่วนบุคคล

นอกจากนี้ ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลดังกล่าวให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า โดยข้อมูลที่ต้องแจ้ง ได้แก่

1) ข้อมูลเกี่ยวกับลักษณะของการละเมิดข้อมูลส่วนบุคคล
2) ข้อมูลในการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและผู้ประสานงานของผู้ควบคุมข้อมูลส่วนบุคคล
3) ผลกระทบที่อาจเกิดขึ้นจากเหตุการละเมิดข้อมูลส่วนบุคคล
4) แนวทางการเยียวยาความเสียหายของเจ้าของข้อมูลส่วนบุคคล และมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลจะใช้ในการป้องกัน ระงับ แก้ไขเหตุการละเมิดข้อมูลส่วนบุคคล

บทบาทในการคุ้มครองข้อมูลส่วนบุคคล

4. หน้าที่บันทึกรายการกิจกรรมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

มาตรา 39 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่บันทึกรายการกิจกรรมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้

รายละเอียดที่ต้องระบุในบันทึกรายการกิจกรรมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลมีดังต่อไปนี้

1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น
6) การใช้หรือเปิดเผยตามมาตรา 27 วรรคสาม
7) การปฏิเสธคำขอหรือการคัดค้านตามมาตรา 30 วรรคสาม มาตรา 31 วรรคสาม มาตรา 32 วรรคสาม และมาตรา 36 วรรคหนึ่ง
8) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 37 (1)

บทบาทในการคุ้มครองข้อมูลส่วนบุคคล

อย่างไรก็ตาม ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก ได้รับยกเว้นไม่ต้องดำเนินการตามมาตรา 39 วรรคหนึ่ง (1) (2) (3) (4) (5) (6) และ (8) แต่หากผู้ควบคุมข้อมูลส่วนบุคคลเป็นกิจการขนาดเล็กที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงจะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26 ผู้ควบคุมข้อมูลส่วนบุคคลดังกล่าวมีหน้าที่ต้องบันทึกรายการกิจกรรมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กที่ได้รับยกเว้นไม่ต้องดำเนินการตามมาตรา 39 วรรคหนึ่ง (1) (2) (3) (4) (5) (6) และ (8) จะต้องมีลักษณะอย่างใดอย่างหนึ่งต่อไปนี้

1) เป็นวิสาหกิจขนาดย่อมหรือวิสาหกิจขนาดกลางตามกฎหมายว่าด้วยการส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม
2) เป็นวิสาหกิจชุมชนหรือเครือข่ายวิสาหกิจชุมชนตามกฎหมายว่าด้วยการส่งเสริมวิสาหกิจชุมชน
3) เป็นวิสาหกิจเพื่อสังคมหรือกลุ่มกิจการเพื่อสังคมตามกฎหมายว่าด้วยการส่งเสริมวิสาหกิจเพื่อสังคม
4) เป็นสหกรณ์ ชุมนุมสหกรณ์ หรือกลุ่มเกษตรกรตามกฎหมายว่าด้วยสหกรณ์
5) เป็นมูลนิธิ สมาคม องค์กรศาสนา หรือองค์กรที่ไม่แสวงหากำไร
6) เป็นกิจการในครัวเรือนหรือกิจการอื่นในลักษณะเดียวกัน

ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กที่ได้รับยกเว้นไม่ต้องดำเนินการข้างต้น จะต้องไม่เป็นผู้ให้บริการที่ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เว้นแต่จะเป็นผู้ให้บริการประเภทผู้ให้บริการร้านอินเทอร์เน็ต

บทบาทในการคุ้มครองข้อมูลส่วนบุคคล

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
เรื่อง การยกเว้นการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก
พ.ศ. ๒๕๖๗

โดยที่เป็นการสมควรปรับปรุงหลักเกณฑ์การยกเว้นการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก

อาศัยอำนาจตามความในมาตรา ๑๖ (๔) และมาตรา ๓๙ วรรคสาม แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การยกเว้นการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก พ.ศ. ๒๕๖๗”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดเก้าสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ให้ยกเลิกประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การยกเว้นการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก พ.ศ. ๒๕๖๕

ข้อ ๔ ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก ที่ได้รับยกเว้นไม่ต้องบันทึกรายการตามมาตรา ๓๙ วรรคหนึ่ง (๑) (๒) (๓) (๔) (๕) (๖) และ (๘) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ จะต้องมีลักษณะอย่างใดอย่างหนึ่ง ดังต่อไปนี้

(๑) เป็นวิสาหกิจขนาดย่อมหรือวิสาหกิจขนาดกลางตามกฎหมายว่าด้วยการส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม

(๒) เป็นวิสาหกิจชุมชนหรือเครือข่ายวิสาหกิจชุมชนตามกฎหมายว่าด้วยการส่งเสริมวิสาหกิจชุมชน

(๓) เป็นวิสาหกิจเพื่อสังคมหรือกลุ่มกิจการเพื่อสังคมตามกฎหมายว่าด้วยการส่งเสริมวิสาหกิจเพื่อสังคม

(๔) เป็นสหกรณ์ ชุมนุมสหกรณ์ หรือกลุ่มเกษตรกรตามกฎหมายว่าด้วยสหกรณ์

(๕) เป็นมูลนิธิ สมาคม องค์กรศาสนา หรือองค์กรเอกชนที่ไม่แสวงหากำไร

(๖) เป็นนิติบุคคลอาคารชุดตามกฎหมายว่าด้วยอาคารชุด หรือนิติบุคคลหมู่บ้านจัดสรรตามกฎหมายว่าด้วยการจัดสรรที่ดิน

(๗) เป็นกิจการในครัวเรือนหรือกิจการอื่นในลักษณะเดียวกัน

(๘) เป็นกิจการที่ดำเนินการโดยผู้ควบคุมข้อมูลส่วนบุคคลที่เป็นบุคคลธรรมดา

ข้อ ๕ ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กที่ได้รับยกเว้นตามข้อ ๔ จะต้องไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคลที่มีหน้าที่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของตน ตามมาตรา ๔๑ (๑) (๒) หรือ (๓) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กที่ได้รับยกเว้นตามข้อ ๔ จะต้องบันทึกรายการตามมาตรา ๓๙ วรรคหนึ่ง (๑) ถึง (๘) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เฉพาะกรณีที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีลักษณะใดลักษณะหนึ่งดังต่อไปนี้

(๑) มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

(๒) มิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว (occasional collection, use, or disclosure of personal data)

(๓) เป็นข้อมูลส่วนบุคคลตามมาตรา ๒๖ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ข้อ ๖ ให้ประธานกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้รักษาการตามประกาศนี้

บทบาทในการคุ้มครองข้อมูลส่วนบุคคล

5. หน้าที่ในการจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

มาตรา 41 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของตน (Data Protection Officer) เพื่อทำหน้าที่ตรวจสอบการดำเนินงานขององค์กรให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

กรณีที่ต้องมีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ได้แก่

1) ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด เช่น

- กรมบัญชีกลาง กระทรวงการคลัง
- กรมการกงสุล กระทรวงการต่างประเทศ
- กรมการขนส่งทางบก กระทรวงคมนาคม
- กรมทรัพย์สินทางปัญญา กระทรวงพาณิชย์
- การรถไฟแห่งประเทศไทย
- ธนาคารแห่งประเทศไทย
- มหาวิทยาลัยและสถาบันอุดมศึกษาของรัฐที่มีสถานพยาบาลในสังกัด

บทบาทในการคุ้มครองข้อมูลส่วนบุคคล

2) การดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผยจำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด

ข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนดพิจารณาจากปัจจัยดังนี้ เช่น

- จำนวนเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง
- ปริมาณ ประเภท หรือลักษณะของข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม ใช้ หรือเปิดเผย
- ระยะเวลาหรือความคงอยู่ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อประโยชน์ในการดำเนินกิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

3) กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26

บทบาทในการคุ้มครองข้อมูลส่วนบุคคล

หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ดังต่อไปนี้

1. **<u>หน้าที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคล</u>**

มาตรา 40 (1) กำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2. **<u>หน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม</u>**

มาตรา 40 (2) กำหนดให้ผู้ประมวลข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

บทบาทในการคุ้มครองข้อมูลส่วนบุคคล

3. <u>หน้าที่จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล</u>

มาตรา 40 (3) กำหนดให้ผู้ประมวลข้อมูลส่วนบุคคลมีหน้าที่จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด โดยจะต้องมีรายละเอียดอย่างน้อยต่อไปนี้

1) ชื่อและข้อมูลเกี่ยวกับผู้ประมวลผลข้อมูลส่วนบุคคล และตัวแทนของผู้ประมวลผลข้อมูลส่วนบุคคลในกรณีที่มีการแต่งตั้งตัวแทน
2) ชื่อและข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลที่ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลนั้น และตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคล ในกรณีที่มีการแต่งตั้งตัวแทน
3) ชื่อและข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล รวมถึงสถานที่ติดต่อและวิธีการติดต่อ ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
4) ประเภทหรือลักษณะของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งรวมถึงข้อมูลส่วนบุคคลและวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล
5) ประเภทของบุคคลหรือหน่วยงานที่ได้รับข้อมูลส่วนบุคคล ในกรณีที่มีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ
6) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 40 วรรคหนึ่ง (2)

บทบาทในการคุ้มครองข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลข้างต้นเป็นลายลักษณ์อักษร โดยจะจัดทำเป็นหนังสือหรือในรูปแบบอิเล็กทรอนิกส์ก็ได้ ทั้งนี้ บันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลดังกล่าวจะต้องเข้าถึงได้ง่าย และสามารถแสดงให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล หรือบุคคลที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายตรวจสอบได้อย่างรวดเร็วเมื่อมีการร้องขอ

บทบาทในการคุ้มครองข้อมูลส่วนบุคคล

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
เรื่อง การยกเว้นการจัดทำและเก็บรักษาบันทึกรายการ
ของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก
พ.ศ. ๒๕๖๗

โดยที่เป็นการสมควรกำหนดหลักเกณฑ์การยกเว้นการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก

อาศัยอำนาจตามความในมาตรา ๑๖ (๔) และมาตรา ๔๐ วรรคสี่ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การยกเว้นการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก พ.ศ. ๒๕๖๗”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก ที่ได้รับยกเว้นไม่ต้องจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลตามมาตรา ๔๐ วรรคหนึ่ง (๓) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ จะต้องมีลักษณะอย่างใดอย่างหนึ่งดังต่อไปนี้

(๑) เป็นวิสาหกิจขนาดย่อมหรือวิสาหกิจขนาดกลางตามกฎหมายว่าด้วยการส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม

(๒) เป็นวิสาหกิจชุมชนหรือเครือข่ายวิสาหกิจชุมชนตามกฎหมายว่าด้วยการส่งเสริมวิสาหกิจชุมชน

(๓) เป็นวิสาหกิจเพื่อสังคมหรือกลุ่มกิจการเพื่อสังคมตามกฎหมายว่าด้วยการส่งเสริมวิสาหกิจเพื่อสังคม

(๔) เป็นสหกรณ์ ชุมนุมสหกรณ์ หรือกลุ่มเกษตรกรตามกฎหมายว่าด้วยสหกรณ์

(๕) เป็นมูลนิธิ สมาคม องค์กรศาสนา หรือองค์กรเอกชนที่ไม่แสวงหากำไร

(๖) เป็นนิติบุคคลอาคารชุดตามกฎหมายว่าด้วยอาคารชุด หรือนิติบุคคลหมู่บ้านจัดสรรตามกฎหมายว่าด้วยการจัดสรรที่ดิน

(๗) เป็นกิจการในครัวเรือนหรือกิจการอื่นในลักษณะเดียวกัน

(๘) เป็นกิจการที่ดำเนินการโดยผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นบุคคลธรรมดา

ข้อ ๔ ผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กที่ได้รับยกเว้นตามข้อ ๓ จะต้องไม่เป็นผู้ประมวลผลข้อมูลส่วนบุคคลที่มีหน้าที่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของตนตามมาตรา ๔๑ (๑) (๒) หรือ (๓) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กที่ได้รับยกเว้นตามข้อ ๓ จะต้องจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลตามมาตรา ๔๐ วรรคหนึ่ง (๓) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เฉพาะกรณีที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีลักษณะใดลักษณะหนึ่ง ดังต่อไปนี้

(๑) มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

(๒) มิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว (occasional collection, use, or disclosure of personal data)

(๓) เป็นข้อมูลส่วนบุคคลตามมาตรา ๒๖ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ข้อ ๕ ให้ประธานกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้รักษาการตามประกาศนี้

บทบาทในการคุ้มครองข้อมูลส่วนบุคคล

4. หน้าที่ในการจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

มาตรา 41 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของตน (Data Protection Officer) เพื่อทำหน้าที่ตรวจสอบการดำเนินงานขององค์กรให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

กรณีที่ต้องมีการจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ได้แก่

1) ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด เช่น

- กรมบัญชีกลาง กระทรวงการคลัง
- กรมการกงสุล กระทรวงการต่างประเทศ
- กรมการขนส่งทางบก กระทรวงคมนาคม
- กรมทรัพย์สินทางปัญญา กระทรวงพาณิชย์
- การรถไฟแห่งประเทศไทย
- ธนาคารแห่งประเทศไทย
- มหาวิทยาลัยและสถาบันอุดมศึกษาของรัฐที่มีสถานพยาบาลในสังกัด

บทบาทในการคุ้มครองข้อมูลส่วนบุคคล

2) การดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด

ข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนดพิจารณาจากปัจจัยดังนี้ เช่น

- จำนวนเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง
- ปริมาณ ประเภท หรือลักษณะของข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม ใช้ หรือเปิดเผย
- ระยะเวลาหรือความคงอยู่ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อประโยชน์ในการดำเนินกิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

3) กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26

บทบาทในการคุ้มครองข้อมูลส่วนบุคคล

หน้าที่ของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) มีหน้าที่หลักในการกำกับ ดูแล และบังคับใช้กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย ซึ่งมีรายละเอียดดังนี้

1. คุ้มครองข้อมูลส่วนบุคคล รวมทั้งส่งเสริมและสนับสนุนให้เกิดการพัฒนาด้านการคุ้มครองข้อมูลส่วนบุคคลของประเทศ
2. ปฏิบัติงานวิชาการและงานธุรการให้แก่คณะกรรมการ คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการผู้เชี่ยวชาญ และคณะอนุกรรมการ
3. จัดทำร่างแผนแม่บทการดำเนินงานด้านการส่งเสริมและการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับนโยบาย ยุทธศาสตร์ชาติ และแผนระดับชาติที่เกี่ยวข้อง รวมทั้งร่างแผนแม่บทและมาตรการแก้ไขปัญหาอุปสรรคการปฏิบัติการตามนโยบาย ยุทธศาสตร์ชาติ และแผนระดับชาติดังกล่าว เพื่อเสนอต่อคณะกรรมการ
4. ส่งเสริมและสนับสนุนการวิจัย เพื่อพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล
5. วิเคราะห์และรับรองความสอดคล้องและความถูกต้องตามมาตรฐานหรือตามมาตรการ หรือกลไกการกำกับดูแลที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งตรวจสอบและรับรองนโยบายในการคุ้มครองข้อมูลส่วนบุคคลตามมาตรา 29
6. สำรวจ เก็บรวบรวมข้อมูล ติดตามความเคลื่อนไหวของสถานการณ์ด้านการคุ้มครองข้อมูลส่วนบุคคล และแนวโน้มการเปลี่ยนแปลงด้านการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งวิเคราะห์และวิจัยประเด็นทางด้านการคุ้มครองข้อมูลส่วนบุคคลที่มีผลต่อการพัฒนาประเทศเพื่อเสนอต่อคณะกรรมการ

บทบาทในการคุ้มครองข้อมูลส่วนบุคคล

7. ประสานงานกับส่วนราชการ รัฐวิสาหกิจ ราชการส่วนท้องถิ่น องค์การมหาชน หรือ หน่วยงานอื่นของรัฐเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

8. ให้คำปรึกษาแก่หน่วยงานของรัฐและหน่วยงานของเอกชนเกี่ยวกับการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

9. เป็นศูนย์กลางในการให้บริการทางวิชาการหรือให้บริการที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแก่หน่วยงานของรัฐ หน่วยงานของเอกชน และประชาชน รวมทั้งเผยแพร่และให้ความรู้ ความเข้าใจในเรื่องการคุ้มครองข้อมูลส่วนบุคคล

10. กำหนดหลักสูตรและฝึกอบรมการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง หรือประชาชนทั่วไป

11. ทำความตกลงและร่วมมือกับองค์การหรือหน่วยงานทั้งในประเทศและต่างประเทศในกิจการที่เกี่ยวกับการดำเนินการตามหน้าที่และอำนาจของสำนักงาน เมื่อได้รับความเห็นชอบจากคณะกรรมการ

12. ติดตามและประเมินผลการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

13. ปฏิบัติหน้าที่อื่นตามที่คณะกรรมการ คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการผู้เชี่ยวชาญ หรือคณะอนุกรรมการมอบหมาย หรือตามที่กฎหมายกำหนด

องค์ประกอบพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคล

ฐานทางกฎหมายในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ก่อนทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องพิจารณาว่ามีฐานทางกฎหมายรองรับหรือไม่ ซึ่งฐานทางกฎหมายถูกบัญญัติในมาตรา 24 มาตรา 26 และมาตรา 27 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยมาตรา 24 บัญญัติเกี่ยวกับฐานในการเก็บรวบรวมข้อมูลส่วนบุคคลทั่วไป และมาตรา 26 บัญญัติเกี่ยวกับฐานในการเก็บรวบรวมข้อมูลส่วนบุคคลตามมาตรา 26 ส่วนมาตรา 27 บัญญัติเกี่ยวกับฐานในการใช้และเปิดเผยข้อมูลส่วนบุคคล

องค์ประกอบพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคล

1. ฐานในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลข้อมูลส่วนบุคคลทั่วไป

1.1 ฐานหน้าที่ตามกฎหมาย (Legal Obligation)

เป็นกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลจำเป็นต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมาย โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องแสดงให้เห็นว่าถ้าไม่ดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าวจะทำให้ไม่สามารถบรรลุวัตถุประสงค์ตามกฎหมายได้

1.2 ฐานภารกิจของรัฐ (Public Task)

เป็นกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลจำเป็นต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งผู้ควบคุมข้อมูลส่วนบุคคลมักเป็นหน่วยงานของรัฐ

นอกจากนี้ฐานภารกิจของรัฐยังรวมถึงกรณีผู้ควบคุมข้อมูลส่วนบุคคลที่เป็นหน่วยงานเอกชน จำเป็นต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

1.3 ฐานประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest)

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยอาศัยฐานประโยชน์โดยชอบด้วยกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลต้องแสดงให้เห็นว่าการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อประโยชน์โดยชอบด้วยกฎหมายของตนหรือบุคคลที่สาม และประโยชน์ดังกล่าวมีความสำคัญไม่น้อยกว่าสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล

องค์ประกอบพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคล

1.4 ฐานสัญญา (Contract)

เป็นกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลจำเป็นต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อให้สามารถปฏิบัติการชำระหนี้แก่เจ้าของข้อมูลส่วนบุคคลตามสัญญาได้ รวมถึงกรณีจำเป็นต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อปฏิบัติตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนที่จะเข้าทำสัญญา ซึ่งการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยใช้ฐานสัญญา ต้องเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของคู่สัญญาเท่านั้น ไม่รวมถึงบุคคลที่สาม

1.5 ฐานประโยชน์สำคัญต่อชีวิต (Vital Interest)

เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้โดยไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ฐานประโยชน์สำคัญต่อชีวิตจะใช้ในกรณีที่เป็นเหตุฉุกเฉิน ซึ่งไม่อาจขอความยินยอมได้ หากเป็นการรักษาพยาบาลที่มีการวางแผนไว้ล่วงหน้า จะไม่สามารถทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยอาศัยฐานประโยชน์สำคัญต่อชีวิตได้

1.6 ฐานความยินยอม (Consent)

เป็นกรณีที่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่มีฐานทางกฎหมายอื่นรองรับ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องนำฐานความยินยอมตามมาตรา 24 และหลักการขอความยินยอมตามมารตรา 19 มาใช้ กล่าวคือ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนหรือขณะประมวลผลข้อมูล การขอความยินยอมต้องแจ้งถึงวัตถุประสงค์การประมวลผลข้อมูล การขอความยินยอมต้องมีความชัดเจน ใช้ภาษาที่ง่ายเข้าใจได้ เอกสารที่ขอความยินยอมต้องแยกส่วนจากเอกสารอื่น และเจ้าของข้อมูลส่วนบุคคลต้องมีอิสระในการให้ความยินยอมและสามารถที่จะถอนความยินยอมเมื่อใดก็ได้

องค์ประกอบพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคล

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ซึ่งยังไม่บรรลุนิติภาวะโดยการสมรส หรือไม่มีฐานะเสมือนดังบุคคลซึ่งบรรลุนิติภาวะแล้วตามมาตรา 27 ตามประมวลกฎหมายแพ่งและพาณิชย์ การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลดังกล่าว ต้องดำเนินการตามมาตรา 20ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ดังนี้

1) ในกรณีที่การให้ความยินยอมของผู้เยาว์ไม่ใช่การใด ๆ ซึ่งผู้เยาว์อาจให้ความยินยอม โดยลำพังได้ตามที่บัญญัติไว้ในมาตรา 22 มาตรา 23 หรือมาตรา 24 ตามประมวลกฎหมายแพ่งและพาณิชย์ ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ด้วย
2) ในกรณีที่ผู้เยาว์มีอายุไม่เกินสิบปี ให้ขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจ กระทำการแทนผู้เยาว์

ส่วนกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นคนไร้ความสามารถ การขอความยินยอมจากเจ้าของ ข้อมูลส่วนบุคคลดังกล่าวให้ขอความยินยอมจากผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ และในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นคนเสมือนไร้ความสามารถ การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลดังกล่าว ให้ขอความยินยอมจากผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ

1.7 ฐานจดหมายเหตุ วิจัย สถิติ (Research)

เป็นกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีความจำเป็นต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการการรักษาความมั่นคงปลอดภัยของข้อมูล มีการทำข้อมูลให้เป็นนิรนาม และเป็นไปตามมาตรฐานจริยธรรมของระเบียบวิธีวิจัย ทั้งนี้เพื่อเป็นการคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

องค์ประกอบพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคล

2. ฐานในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลข้อมูลส่วนบุคคลตามมาตรา 26

2.1 ฐานความยินยอมโดยชัดแจ้ง (Explicit Consent)

เป็นกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26 โดยใช้หลักการขอความยินยอมทั่วไปตามที่บัญญัติในมาตรา 19 ซึ่งได้แก่ การขอความยินยอมต้องทำก่อนหรือขณะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล แจ้งถึงวัตถุประสงค์การประมวลผลข้อมูล การขอความยินยอมต้องแยกส่วนจากเอกสารอื่น เป็นต้น ประกอบกับผู้ควบคุมข้อมูลส่วนบุคคลจะต้องขอความยินยอมโดยทำเป็นลายลักษณ์อักษรที่ชัดเจนด้วย ผู้ควบคุมข้อมูลส่วนบุคคลอาจจัดให้เจ้าของข้อมูลส่วนบุคคลทำการลงนามในเอกสารหรืออาจให้ความยินยอมในเอกสารอิเล็กทรอนิกส์ เช่น การใช้ลายมือชื่ออิเล็กทรอนิกส์

2.2 ฐานความจำเป็นในการปฏิบัติตามกฎหมายเกี่ยวกับการคุ้มครองแรงงาน การประกันสังคม และความคุ้มครองทางสังคม

เป็นกรณีผู้ควบคุมข้อมูลส่วนบุคคลมีความจำเป็นต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26 เพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล กรณีนี้แม้ผู้ควบคุมข้อมูลส่วนบุคคลไม่ต้องขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล แต่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลด้วย

องค์ประกอบพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคล

2.3 ฐานประโยชน์สำคัญต่อชีวิต (Vital Interest)

เป็นกรณีที่จำเป็นต้องมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26 เพื่อป้องกันหรือระงับอันตรายต่อร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล ซึ่งเจ้าของข้อมูลส่วนบุคคลดังกล่าวไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม

การไม่สามารถให้ความยินยอมได้อาจเกิดจากกรณีเจ้าของข้อมูลส่วนบุคคลไม่สามารถ ให้ความยินยอมได้เพราะเหตุทางกายภาพ เช่น เจ้าของข้อมูลส่วนบุคคลอยู่ในภาวะหมดสติ หรืออาจเกิดจาก เหตุทางกฎหมาย เช่น เจ้าของข้อมูลส่วนบุคคลอยู่ในภาวะหมดสติ

2.4 ฐานการดำเนินกิจกรรมของมูลนิธิ สมาคม หรือองค์กรไม่แสวงกำไร

เป็นกรณีการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรไม่แสวงหากำไร โดยหน่วยงานดังกล่าวต้องมีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานเท่านั้น และจะต้องเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26 ของสมาชิก ผู้เคยเป็นสมาชิก หรือผู้มีการติดต่ออย่างสม่ำเสมอกับหน่วยงาน ดังนั้น ฐานนี้จึงไม่รวมถึงการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของพนักงานหรือคู่ค้าของหน่วยงานแต่อย่างใด

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26 โดยใช้ฐานการดำเนินกิจกรรมของมูลนิธิ สมาคม หรือองค์กรไม่แสวงกำไรข้างต้น ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการภายใต้มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม และต้องไม่เปิดเผยข้อมูลส่วนบุคคลออกไปภายนอกมูลนิธิ สมาคม หรือองค์กรไม่แสวงกำไร

องค์ประกอบพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคล

2.5 ฐานข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล

เป็นกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26 ด้วยความยินยอมโดยชัดแจ้ง และการเปิดเผยข้อมูลนั้นกระทำต่อสาธารณะ กล่าวคือ เป็นข้อมูลที่ไม่ว่าประชาชนทั่วไปหรือเจ้าหน้าที่รัฐ ก็สามารถเข้าถึงข้อมูลได้

2.6 ฐานความจำเป็นเพื่อดำเนินการเกี่ยวกับการใช้สิทธิเรียกร้องตามกฎหมาย

เป็นกรณีที่มีความจำเป็นต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26 เพื่อดำเนินการใช้สิทธิเรียกร้องตามกฎหมายหรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย ซึ่งการใช้สิทธิเรียกร้องตามกฎหมายได้แก่กรณีต่อไปนี้ คือ การดำเนินการตามกระบวนการทางกฎหมายที่เกิดขึ้นแล้ว การดำเนินการกับข้อมูลที่จำเป็นเพื่อเตรียมการก่อนเข้าสู่กระบวนการทางกฎหมาย การขอรับคำปรึกษาทางกฎหมาย และการก่อตั้งใช้สิทธิเรียกร้องโดยวิธีการอื่น

องค์ประกอบพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคล

2.7 ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะที่สำคัญ

เป็นกรณีที่จำเป็นต้องมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26 เพื่อปฏิบัติตามกฎหมาย กล่าวคือ มีกฎหมายบัญญัติให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิบัติหน้าที่ดังกล่าว และเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับประโยชน์สาธารณะที่สำคัญ โดยผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

2.8 ฐานความจำเป็นในการปฏิบัติตามกฎหมายเกี่ยวกับการให้บริการด้านสุขภาพหรือสังคม

เป็นกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีความจำเป็นต้องปฏิบัติตามกฎหมายในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26 โดยมีวัตถุประสงค์ต่อไปนี้คือ เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

องค์ประกอบพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคล

2.9 ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะด้านสาธารณสุข

เป็นกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีความจำเป็นต้องปฏิบัติตามกฎหมายในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตามมาตรา 26 โดยมีวัตถุประสงค์เกี่ยวกับประโยชน์สาธารณะด้านสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตราย หรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ โดยผู้ควบคุมข้อมูลต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล โดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคล ตามหน้าที่หรือจริยธรรมแห่งวิชาชีพ

2.10 ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ หรือประโยชน์สาธารณะอื่น

เป็นกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีความจำเป็นต้องปฏิบัติตามกฎหมายในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตามมาตรา 26 โดยมีวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ หรือประโยชน์สาธารณะอื่น ผู้ควบคุมข้อมูลส่วนบุคคลต้องกระทำเพื่อให้บรรลุวัตถุประสงค์เพียงเท่าที่จำเป็นเท่านั้น และต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

องค์ประกอบพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคล

การแบ่งแยกบทบาทและหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลอาจเป็นบุคคลธรรมดาหรือนิติบุคคลก็ได้ ทั้งผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต่างก็มีหน้าที่ความรับผิดชอบตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เช่นเดียวกัน เช่น หน้าที่ในการบันทึกรายการกิจกรรมที่สามารถนำเสนอต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้เมื่อมีการร้องขอ

นอกจากนี้ ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลมีความรับผิดชอบร่วมกันในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล และต้องมั่นใจว่ามีการปฏิบัติตามกฎระเบียบเกี่ยวกับการโอนข้อมูลระหว่างประเทศ

หากไม่ปฏิบัติตามหน้าที่ของตน ทั้งผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลอาจถูกปรับในอัตราสูง และยังต้องชดเชยความเสียหายให้กับบุคคลที่ได้รับผลกระทบ

องค์ประกอบพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคล

การแบ่งแยกระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลอาจไม่ชัดเจนเสมอไป อย่างไรก็ตาม มาตรา 6 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดนิยามของผู้ควบคุมข้อมูลส่วนบุคคลว่าเป็น “บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล” ซึ่งการแยกแยะนี้ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลมีความรับผิดชอบตามกฎหมายมากกว่า

ส่วนผู้ประมวลผลข้อมูลตามที่กำหนดในมาตราเดียวกัน คือ “บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล” ซึ่งการดำเนินการของผู้ประมวลผลข้อมูลส่วนบุคคลต้องมีความโปร่งใสต่อผู้ควบคุมข้อมูลส่วนบุคคล และการตัดสินใจใด ๆ ที่เกี่ยวข้องกับสถานที่หรือบุคคลที่จะทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น จะต้องได้รับการอนุมัติจากผู้ควบคุมข้อมูลส่วนบุคคลก่อนเสมอ

บทบาทเหล่านี้ขึ้นอยู่กับการดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เฉพาะเจาะจง กล่าวอีกนัยหนึ่งคือ บุคคลธรรมดาหรือนิติบุคคลหนึ่งอาจเป็นผู้ควบคุมข้อมูลส่วนบุคคลในการประมวลผลหนึ่ง ๆ และอาจเป็นผู้ประมวลผลข้อมูลส่วนบุคคลในการประมวลผลอื่น ๆ ได้

แบบทดสอบ บทที่ 3

ข้อที่ 1

Q : <u>จริงหรือเท็จ</u>

ผู้ควบคุมข้อมูลส่วนบุคคลอาจเป็นบุคคลธรรมดาหรือนิติบุคคลก็ได้ ในขณะที่ผู้ประมวลผลข้อมูลส่วนบุคคลต้องเป็นนิติบุคคลเท่านั้น

แบบทดสอบ บทที่ 3

ข้อที่ 2

Q : <u>จริงหรือเท็จ</u>

ผู้ประมวลผลข้อมูลส่วนบุคคลอาจตัดสินใจว่าจะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ไหนและอย่างไร

แบบทดสอบ บทที่ 3

ข้อที่ 3

Q : <u>จริงหรือเท็จ</u>

เมื่อมีการประมวลผลข้อมูลส่วนบุคคล
จะต้องมีผู้ควบคุมข้อมูลข้อมูลส่วนบุคคลเสมอ

• เฉลยแบบทดสอบบทที่ 3

ข้อที่	เฉลย
1.	เท็จ
2.	เท็จ
3.	จริง

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

บทที่ 4

• บทนำ

บทนี้จะได้อธิบายถึงประเด็นสำคัญ ดังนี้

- ❑ การดำเนินการในวงจรชีวิตของข้อมูลที่ถือว่าเป็นเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- ❑ อธิบายหลักการ 7 ประการในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะที่เกี่ยวข้องกับการกำหนดวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- ❑ อธิบายขอบเขตการใช้บังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคลทั้งในเชิงพื้นที่และเชิงเนื้อหา
- ❑ อธิบายหลักเกณฑ์ที่ชอบธรรมในการดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล

• การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ความหมายของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลจะได้รับความคุ้มครองตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลตามหลักการจัดการวงจรชีวิตของข้อมูล (Data life cycle) การดำเนินการที่เกี่ยวข้องกับข้อมูลส่วนบุคคล (Any operation performed upon data) ย่อมได้รับความคุ้มครองตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ดังนี้

- การเก็บรวบรวมข้อมูล (Collection) เช่น การรับข้อมูลเข้ามา การกรอกแบบฟอร์ม
- การใช้ข้อมูล (Usage) เช่น การวิเคราะห์ข้อมูล การตรวจข้อมูล การแปรผลข้อมูล
- การเปิดเผยข้อมูล (Disclosure) เช่น การแบ่งปันข้อมูล การโอนข้อมูลให้ผู้อื่น
- การเก็บรักษา (Storage) หรือทำลาย (Disposal) เช่น การเก็บข้อมูลไว้ในที่จัดเก็บ ไม่ว่าจะใช้งานหรือไม่ใช้งาน การลบหรือทำลายข้อมูลไม่ว่าจะเป็นข้อมูลอิเล็กทรอนิกส์หรือข้อมูลในรูปแบบอื่น

• การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ขอบเขตการบังคับใช้กฎหมายในเชิงเนื้อหาและในเชิงพื้นที่ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ขอบเขตการใช้บังคับในเชิงเนื้อหา (การยกเว้นการบังคับใช้)

1) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตน หรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น
2) การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์
3) บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น
4) สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี
5) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินการตามกระบวนการยุติธรรมทางอาญา
6) การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

• การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

อย่างไรก็ตาม...

แม้ว่าการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลข้างต้นจะได้รับยกเว้นไม่ถูกบังคับตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แต่ผู้ควบคุมข้อมูลส่วนบุคคลที่ได้รับยกเว้นต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานด้วย

• การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ขอบเขตการใช้บังคับในเชิงพื้นที่ (การบังคับใช้)

มาตรา 5 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ดังต่อไปนี้อยู่ภายใต้บังคับของกฎหมายดังกล่าว

มาตรา 5 พระราชบัญญัตินี้ให้ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่า การเก็บรวบรวม ใช้ หรือเปิดเผยนั้น ได้กระทำในหรือนอกราชอาณาจักรก็ตาม

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่นอกราชอาณาจักร พระราชบัญญัตินี้ให้ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักรโดยการดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว เมื่อเป็นกิจกรรม ดังต่อไปนี้

(1) การเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่า จะมีการชำระเงินของเจ้าของข้อมูลส่วนบุคคลหรือไม่กี่ตาม

(2) การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร

• การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

กรณีศึกษา

นาย ก. ได้โพสต์ภาพใบสำคัญการหย่าใน TikTok ที่มีชื่อและนามสกุลของนาง ข.
อยู่ภายใต้บังคับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือไม่

• หลักการ 7 ประการในการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล

1) **ยุติธรรมและชอบด้วยกฎหมาย (Lawfulness, fairness and transparency)** การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลต้องเป็นไปโดยชอบด้วยกฎหมาย เป็นธรรม และโปร่งใส มีการสื่อสารอย่างชัดเจนเปิดเผยกับเจ้าของข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
2) **กำหนดวัตถุประสงค์ที่เฉพาะเจาะจง (Purpose limitation)** การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลต้องเป็นไปตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวม และใช้ข้อมูลส่วนบุคคลเพียงเท่าที่จำเป็นตามวัตถุประสงค์เท่านั้น โดยพิจารณาถึงความสัมพันธ์กันระหว่างวัตถุประสงค์ธรรมชาติของข้อมูล วิธีการเก็บรวบรวม ผลของการใช้ต่อไป (secondary uses) และมาตรการรักษาความมั่นคงปลอดภัย
3) **เก็บข้อมูลให้น้อยที่สุดเท่าที่จำเป็น (Data minimization)** การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลต้องกระทำเพียงเท่าที่จำเป็นและเกี่ยวข้องกับวัตถุประสงค์เท่านั้น ไม่ควรเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเกินความจำเป็น
4) **ข้อมูลต้องมีความถูกต้องและเป็นปัจจุบัน (Data quality and accuracy)** ต้องทำให้ข้อมูลถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด
5) **การเก็บรักษาข้อมูลอย่างจำกัดเวลา (Storage limitation)** ต้องตรวจสอบระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล โดยการเก็บข้อมูลส่วนบุคคลต้องอยู่ภายในระยะเวลาที่กำหนดแน่นอนเท่านั้น ทั้งนี้ ขึ้นอยู่กับความจำเป็นและความเกี่ยวข้องกับวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และจะต้องทำลายหรือลบข้อมูลส่วนบุคคลอย่างเหมาะสมเมื่อพ้นระยะเวลาที่กำหนด ยกเว้นกรณีที่กฎหมายกำหนดไว้เป็นอย่างอื่น
6) **การรักษาความถูกต้องครบถ้วนและความลับของข้อมูลส่วนบุคคล (Integrity and confidentiality)** ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม
7) **ความรับผิดชอบ (Accountability)** ต้องรับผิดชอบในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

• หลักการ 7 ประการในการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล

กรณีศึกษา

บริษัทรถแท็กซี่เก็บข้อมูลชื่อผู้โดยสารและหมายเลขโทรศัพท์ โดยจะทำการลบข้อมูลชื่อผู้โดยสารทั้งหมดหลังจากผ่านไปแล้ว 2 ปี อย่างไรก็ตาม บริษัทยังคงเก็บหมายเลขโทรศัพท์ของผู้โดยสารไว้แม้ว่าจะลบชื่อผู้โดยสารไปแล้ว บริษัทรถแท็กซี่กระทำการฝ่าฝืนหลักการพื้นฐานสำคัญ ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลข้อใด

• หลักการ 7 ประการในการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล

ทดสอบความรู้

ระบบควบคุมการเข้าออกซึ่งถูกใช้เพื่อเป็นมาตรการเฝ้าระวังติดตามเพื่อการรักษาความปลอดภัยของอาคาร ต่อมานายจ้างได้เข้าถึงข้อมูลดังกล่าวเพื่อตรวจสอบความตรงต่อเวลาของลูกจ้าง โดยที่ลูกจ้างไม่ได้รับการแจ้งข้อมูลใด ๆ เกี่ยวกับการดำเนินการตรวจสอบดังกล่าว และผู้ควบคุมข้อมูลส่วนบุคคลก็ไม่ได้ดำเนินการบันทึกการดำเนินการดังกล่าวอย่างสม่ำเสมอ การกระทำดังกล่าวฝ่าฝืนต่อหลักการพื้นฐานพื้นฐานสำคัญในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลข้อใด

• ฐานทางกฎหมายในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลใดที่ตกอยู่ภายใต้บังคับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ทั้งในเชิงเนื้อหาและในเชิงพื้นที่ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องอ้างฐานความชอบธรรมทางกฎหมาย (Lawful basis) ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นให้ได้ว่าในแต่ละกิจกรรมที่ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการนั้นมีฐานทางกฎหมายในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือไม่

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดฐานทางกฎหมายในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเอาไว้ 2 กรณี คือ

1. ฐานทางกฎหมายในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตาม**มาตรา 24**
2. ฐานทางกฎหมายในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตาม**มาตรา 26**

• ฐานทางกฎหมายในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ตามมาตรา 24 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดฐานทางกฎหมายในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไว้ 7 ฐาน คือ

(1) ฐานการจัดทำเอกสารประวัติศาสตร์เพื่อประโยชน์สาธารณะหรือการวิจัย

(2) ฐานป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล (Vital interest)

(3) ฐานจำเป็นเพื่อปฏิบัติตามสัญญา (Contract)

(4) ฐานจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะหรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐ (Public interest/ Public task)

(5) ฐานจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย (Legitimate interest)

(6) ฐานการปฏิบัติตามกฎหมาย (Legal obligation)

(7) ฐานความยินยอม (Consent)

• การใช้ฐานความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

การพิจารณาเลือกใช้ฐานความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

การใช้ฐานความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นจะต้องเป็นกรณีที่มีวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เฉพาะเจาะจง หากไม่ได้รับความยินยอมโดยชอบด้วยกฎหมายก่อนหรือในขณะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จะไม่สามารถดำเนินการดังกล่าวได้ ซึ่งการให้ความยินยอมโดยชอบด้วยกฎหมายในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะมีเงื่อนไขเป็นการเฉพาะ หากไม่เป็นไปตามเงื่อนไขที่กฎหมายกำหนดความยินยอมที่ให้ย่อมไม่มีผลผูกพันเจ้าของข้อมูลส่วนบุคคล นอกจากนี้เจ้าของข้อมูลส่วนบุคคลสามารถถอนความยินยอมได้เสมอ ฐานความยินยอมจึงเป็นฐานทางกฎหมายที่ไม่มั่นคงที่สุดจากบรรดาฐานการการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลทั้งหมด ด้วยเหตุที่กล่าวมาฐานความยินยอมจึงควรเป็นทางเลือกสุดท้าย (Last resort) ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

• การใช้ฐานความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

หลักเกณฑ์ในการให้ความยินยอมโดยชอบด้วยกฎหมาย

การให้ความยินยอมโดยชอบด้วยกฎหมายต้องเป็นไปตามเงื่อนไขตามที่กำหนดในมาตรา 19 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งมีรายละเอียด ดังนี้

- การขอความยินยอมต้องดำเนินการก่อนหรือในขณะที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- การขอความยินยอมต้องทำโดยชัดแจ้ง
- การให้ความยินยอมต้องทำเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้
- การขอความยินยอมต้องขอจากเจ้าของข้อมูลส่วนบุคคลเท่านั้น
- ความยินยอมต้องให้โดยอิสระ (freely given) ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
- การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย
- เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้โดยจะต้องถอนความยินยอมได้ง่ายเช่นเดียวกับการให้ความยินยอม

การขอความยินยอมจะต้องเป็นไปตามเงื่อนไขที่กฎหมายกำหนดอย่างเคร่งครัด การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลที่ไม่เป็นไปตามที่กำหนดไว้ในกฎหมาย ไม่มีผลผูกพันเจ้าของข้อมูลส่วนบุคคล และไม่ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้

• การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26 จะไม่สามารถดำเนินการได้หากไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล

สำหรับข้อมูลส่วนบุคคลตามมาตรา 26 นั้น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดฐานทางกฎหมายในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไว้เป็นการเฉพาะ ซึ่งมีรายละเอียดดังนี้

(1) ฐานป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล (Vital interest) ซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม

(2) ฐานการดำเนินกิจกรรมโดยชอบด้วยกฎหมายของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงาน ทั้งนี้ต้องมีการคุ้มครองที่เหมาะสม และไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรนั้น

(3) ฐานข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

(4) ฐานจำเป็นเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

• การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26

(5) ฐานจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

- ประโยชน์ด้านการแพทย์ การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ
- ประโยชน์สาธารณะด้านการสาธารณสุข เช่น ป้องกันโรคติดต่อหรือโรคระบาด
- การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม
- การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ซึ่งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ออกประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการที่เหมาะสมสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติตามมาตรา 24 (1) และการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่นตามมาตรา 26 (5) (ง) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566 กำหนดรายละเอียดเกี่ยวกับมาตรการที่เหมาะสมแล้ว
- ประโยชน์สาธารณะที่สำคัญ ทั้งนี้ต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

• การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26

นอกจากนี้ ในการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดเงื่อนไขเพิ่มเติม โดยกรณีดังกล่าวต้องกระทำภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย หรือในกรณีที่มิได้ดำเนินการภายใต้การควบคุมของหน่วยงานข้างต้น ต้องได้จัดให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลตามหลักเกณฑ์ที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด ซึ่งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ออกประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์เกี่ยวกับมาตรการคุ้มครองสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมที่มิได้กระทำภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย พ.ศ. 2566 กำหนดรายละเอียดในกรณีนี้แล้ว

• กรณีศึกษา

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลสุขภาพของเจ้าหน้าที่ของหน่วยงานรัฐ โดยเก็บข้อมูลชื่อและนามสกุล โรคที่เข้ารับการรักษา ชื่อสถานพยาบาล และจำนวนเงินค่ารักษา เพื่อประกอบการพิจารณาอนุมัติการใช้สิทธิเบิกสวัสดิการเกี่ยวกับการรักษาพยาบาลสำหรับเจ้าหน้าที่นั้น หน่วยงานของรัฐในฐานะผู้ควบคุมข้อมูลส่วนบุคคลจำเป็นต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าหน้าที่และครอบครัว หรือไม่ อย่างไร

ข้อมูลส่วนบุคคลเกี่ยวกับโรคที่เข้ารับการรักษาและรายละเอียดเกี่ยวกับการรักษาพยาบาล ในใบเบิกเงินสวัสดิการเกี่ยวกับการรักษาพยาบาลและเอกสารที่ใช้ประกอบการเบิกเงินสวัสดิการ เช่น ใบรับรองแพทย์และใบเสร็จรับเงิน เป็นข้อมูลส่วนบุคคลเกี่ยวกับข้อมูลสุขภาพตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าวเพื่อใช้ประกอบการเบิกจ่ายค่าใช้จ่ายที่เป็นสวัสดิการเกี่ยวกับการรักษาพยาบาลให้กับบุคลากรของหน่วยงานของตน ซึ่งเป็นผู้มีสิทธิตามระเบียบของหน่วยงานรัฐตามกฎหมาย ถือว่าเป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับสวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย ตามนัยมาตรา 26 (5) (ค) ประกอบมาตรา 27 วรรคหนึ่ง แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงได้รับยกเว้นไม่ต้องขอความยินยอมโดยชัดแจ้งจากเจ้าหน้าที่ ผู้ขอเบิกเงินสวัสดิการหรือบุคคลในครอบครัวก่อนแต่อย่างใด

แบบทดสอบ บทที่ 4

ข้อที่ 1

Q : การดำเนินการใดที่เกี่ยวข้องกับข้อมูลส่วนบุคคลได้รับความคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ก. การเก็บรวบรวมข้อมูลส่วนบุคคล (Collection)

ข. การใช้ข้อมูลส่วนบุคคล (Usage)

ค. การเปิดเผยข้อมูลส่วนบุคคล (Disclosure)

ง. ถูกทุกข้อ

แบบทดสอบ บทที่ 4

ข้อที่ 2

Q : ข้อใดต่อไปนี้อยู่ภายใต้การบังคับใช้ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ตอบได้มากกว่า 1 ข้อ

ก. บริษัท ก. ตั้งอยู่ในประเทศไทย ดำเนินการเก็บข้อมูลชื่อ นามสกุล และที่อยู่ของนาย A. ลูกค้าซึ่งอยู่ต่างประเทศ เพื่อดำเนินการส่งสินค้าที่นาย A สั่งซื้อ

ข. บริษัท A ซึ่งจดทะเบียนจัดตั้งและมีสำนักงานอยู่ในประเทศญี่ปุ่น เสนอขายสินค้าทางระบบออนไลน์ให้แก่นาย ก.ซึ่งอยู่ในประเทศไทย โดยมีเก็บชื่อ นามสกุล ที่อยู่ ของนาย ก.

ค. นาย ข. ไปสังสรรค์กับครอบครัว ได้ทำการโพสต์ภาพหมู่ที่ได้ถ่ายในงานสังสรรค์ลงในเฟสบุ๊ก

ง. สถาบันนิติวิทยาศาสตร์ดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อใช้ในการตรวจพิสูจน์หลักฐานด้านวิทยาศาสตร์และการแพทย์ประการดำเนินคดี

แบบทดสอบ บทที่ 4

ข้อที่ 3

Q : ฐานทางกฎหมายใดที่สามารถใช้อ้างในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26 ตอบได้มากกว่า 1 ข้อ

ก. ฐานความยินยอม

ข. ฐานจำเป็นเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย

ค. ฐานป้องกันหรือระงับอันตรายต่อชีวิต

ง. ฐานจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะด้านสาธารณสุข

• เฉลยแบบทดสอบบทที่ 4

ข้อที่	เฉลย
1.	ง.
2.	ก. และ ข.
3.	ก. ข. ค. และ ง.

สิทธิของเจ้าของข้อมูลส่วนบุคคล

บทที่ 5

- บทนำ
- สิทธิของเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ที่เกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล
- แบบทดสอบ

บทนำ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีเจตนารมณ์ในการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล โดยมีการบัญญัติถึงสิทธิของเจ้าของข้อมูลส่วนบุคคลไว้ ซึ่งได้แก่ สิทธิในการขอเข้าถึงข้อมูลส่วนบุคคลและขอสำเนาข้อมูลส่วนบุคคล สิทธิในการขอแก้ไขข้อมูลส่วนบุคคล สิทธิในการขอให้ลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ สิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคล และสิทธิในการขอโอนย้ายข้อมูลส่วนบุคคล

ในบทนี้จะอธิบายเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล การนำไปใช้ และหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล

สิทธิในการขอเข้าถึงและขอสำเนาข้อมูลส่วนบุคคล

1. สถานการณ์เพื่อใช้ในการเรียนรู้เกี่ยวกับสิทธิในการเข้าถึงและขอสำเนาข้อมูลส่วนบุคคล

จิตตรีพบว่าชื่อของตนเองในระบบของผู้ให้บริการโทรศัพท์มือถือถูกบันทึกผิดจาก "จิตตรี" เป็น "จิตตรีย์" จิตตรีจึงโทรศัพท์ติดต่อผู้ให้บริการเพื่อขอเข้าถึงข้อมูลส่วนบุคคล และยืนยันข้อผิดพลาด

มาตรา 30 วรรคหนึ่ง ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติเกี่ยวกับสิทธิในการเข้าถึงข้อมูลส่วนบุคคล โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนเอง ซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล รวมถึงมีสิทธิขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลไม่ได้เป็นผู้ให้ความยินยอม

สิทธิในการขอเข้าถึงและขอสำเนาข้อมูลส่วนบุคคล

เมื่อยืนยันตัวตนแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการตามคำขอนั้น อย่างไรก็ตาม ผู้ควบคุมข้อมูลสามารถปฏิเสธคำขอได้เฉพาะในกรณีที่เป็นการปฏิเสธตามกฎหมายหรือคำสั่งศาล และการเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลนั้นจะส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น ตามที่บัญญัติในมาตรา 30 วรรคสอง

ส่วนมาตรา 30 วรรคสาม บัญญัติว่าในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธคำขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกการปฏิเสธคำขอดังกล่าวพร้อมด้วยเหตุผลไว้ในรายการบันทึกกิจกรรมการเก็บรวมรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 39

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลมีคำขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลตามมาตรา 30 วรรคหนึ่ง และเป็นกรณีที่ไม่อาจปฏิเสธคำขอได้ตามมาตรา 30 วรรคสอง ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามคำขอโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่ได้รับคำขอ ตามที่บัญญัติในมาตรา 30 วรรคสี่

สิทธิในการขอเข้าถึงและขอสำเนาส่วนบุคคล

การมีขั้นตอนที่ชัดเจนสำหรับพนักงานในการจัดการคำขอเข้าถึงข้อมูลส่วนบุคคลจะสามารถช่วยให้มั่นใจได้ว่ามีการปฏิบัติตามกฎหมายอย่างถูกต้อง

ขั้นตอนที่ควรมีในการจัดการคำขอเข้าถึงข้อมูลส่วนบุคคล เช่น การกำหนดหน้าที่ความรับผิดชอบ หลักเกณฑ์ในการยืนยันตัวตนของผู้ที่ยื่นคำขอ วิธีการยื่นคำขอ ประเภทของข้อมูลที่อาจไม่สามารถเปิดเผยได้ ระยะเวลาที่กำหนดในการตอบคำขอ และวิธีจัดการกับสถานการณ์พิเศษ นอกจากนี้ บริษัทควรจัดการฝึกอบรมและจัดเตรียมทรัพยากรที่เพียงพอ รวมถึงแผนการติดตามเพื่อให้แน่ใจว่ามีการปฏิบัติตามกฎหมายอย่างถูกต้อง

เมื่อพนักงานฝ่ายบริการลูกค้าตรวจสอบยืนยันตัวตนของจิตตรีและยืนยันว่าชื่อในระบบนั้นสะกดผิดจริง บริษัทต้องให้สิทธิจิตตรีในการเข้าถึงข้อมูลส่วนบุคคล โดยข้อมูลและรายละเอียดควรได้รับการจัดหาให้แก่เจ้าของข้อมูลส่วนบุคคลในรูปแบบเดียวกับที่มีการยื่นคำขอ ในกรณีนี้ การแจ้งข้อมูลเกี่ยวกับการสะกดชื่อผิดทางโทรศัพท์ถือเป็นการดำเนินการที่เหมาะสม

สิทธิในการขอเข้าถึงและขอสำเนาข้อมูลส่วนบุคคล

2. สถานการณ์เพื่อใช้ในการเรียนรู้เกี่ยวกับสิทธิในการเข้าถึงและขอสำเนาข้อมูลส่วนบุคคล

ในกรณีที่จิตตรีมีข้อสงสัยเกี่ยวกับใบแจ้งหนี้ค่าโทรศัพท์ของตนเองและต้องการข้อมูลเพิ่มเติม เช่น จำนวนข้อความที่ส่งและรับในช่วงรอบการเรียกเก็บเงินที่ผ่านมา ในการให้ข้อมูลนี้กับจิตตรี พนักงานฝ่ายบริการลูกค้าอาจขอให้จิตตรีกรอกแบบฟอร์มออนไลน์ผ่านเว็บไซต์ของบริษัท เพื่อให้จิตตรีได้รับข้อมูลในรูปแบบดิจิทัล

สิทธิในการขอเข้าถึงและขอสำเนาข้อมูลส่วนบุคคล

นอกจากการได้รับสำเนาข้อมูลส่วนบุคคลแล้ว พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังให้สิทธิจิตตรีในการเข้าถึงรายละเอียดเพิ่มเติมที่ได้แจ้งไว้ล่วงหน้าในประกาศความเป็นส่วนตัว ซึ่งได้แก่

1) รายละเอียดเกี่ยวกับข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวม ใช้ หรือเปิดเผย
2) แหล่งที่มาของข้อมูลส่วนบุคคล (หากไม่ได้รวบรวมจากเจ้าของข้อมูลส่วนบุคคลโดยตรง)

สิทธิในการขอแก้ไขข้อมูลส่วนบุคคล

เมื่อจิตตรีต้องการแก้ไขการสะกดชื่อที่ผิดในระบบของบริษัท มาตรา 35 ให้สิทธิในการแก้ไขข้อมูลส่วนบุคคลโดยไม่ล่าช้า

หากผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธไม่ดำเนินการตามคำร้องดังกล่าว มาตรา 36 วรรคหนึ่ง กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องบันทึกคำร้องของเจ้าของข้อมูลส่วนบุคคลและเหตุผลของการปฏิเสธสิทธินั้นไว้ในรายการตามมาตรา 39 และเจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการแก้ไขข้อมูลให้ถูกต้องได้ ตามมาตรา 36 วรรคสอง ประกอบมาตรา 34 วรรคสอง

ชื่อของจิตตรีที่สะกดผิดสามารถแก้ไขได้ง่ายในระบบ อย่างไรก็ตาม การจัดการข้อมูลในระบบดิจิทัลบางครั้งก็ทำให้การแก้ไขข้อมูลมีความซับซ้อนมากขึ้น พนักงานฝ่ายบริการลูกค้าที่ช่วยเหลือจิตตรีจะต้องตรวจสอบให้แน่ใจว่าชื่อที่สะกดผิดในทุกส่วนของระบบของบริษัทได้รับการแก้ไขเรียบร้อยแล้ว หากบริษัทใช้ระบบจัดการข้อมูลหลายระบบ เช่น ระบบสำหรับการเรียกเก็บเงินและระบบสำหรับการตลาด บริษัทต้องมั่นใจว่าทั้งสองระบบได้รับการแก้ไขให้ถูกต้อง

สิทธิในการขอโอนย้ายข้อมูลส่วนบุคคล

1. สิทธิในการขอโอนย้ายข้อมูลส่วนบุคคล

สิทธิในการขอโอนย้ายข้อมูลส่วนบุคคลเป็นสิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 31 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และเป็นการขยายสิทธิในการเข้าถึงข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมไว้เกี่ยวกับเจ้าของข้อมูลส่วนบุคคล โดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ตระหนักว่าข้อมูลส่วนบุคคลส่วนใหญ่ถูกเก็บในรูปแบบอิเล็กทรอนิกส์ เช่น บริการคลาวด์หรือโซเชียลมีเดีย และข้อมูลส่วนบุคคลอาจจำเป็นต้องย้ายจากบริการหนึ่งไปยังอีกบริการหนึ่ง

อย่างไรก็ตาม ด้วยเหตุที่มีข้อกังวลว่าข้อมูลส่วนบุคคลอาจถูกล็อกให้อยู่ในบริการหนึ่งเนื่องจากถูกเก็บในรูปแบบที่เป็นกรรมสิทธิ์เฉพาะ ไม่สามารถโอนย้ายได้โดยง่าย กฎหมายจึงได้นำแนวคิดเรื่องการโอนย้ายข้อมูลส่วนบุคคลมาใช้ ซึ่งอนุญาตให้เจ้าของข้อมูลส่วนบุคคลได้รับข้อมูลส่วนบุคคลในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติ และสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ โดยสามารถถ่ายโอนข้อมูลส่วนบุคคลไปยังแพลตฟอร์มอื่นได้ด้วยความช่วยเหลือของผู้ควบคุมข้อมูลส่วนบุคคล

สิทธิในการโอนย้ายข้อมูลส่วนบุคคลมีข้อจำกัดมากกว่าสิทธิในการเข้าถึงข้อมูลส่วนบุคคล เพราะสิทธิในการโอนย้ายข้อมูลส่วนบุคคลนี้จะมีผลบังคับใช้ในสถานการณ์ที่เฉพาะเจาะจงเท่านั้น การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีฐานทางกฎหมายที่แตกต่างกัน และฐานทางกฎหมายดังกล่าวจะเป็นตัวกำหนดสิทธิเฉพาะ เช่น ในกรณีเป็นการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะหรือการปฏิบัติหน้าที่ตามกฎหมาย หรือการใช้สิทธินั้นละเมิดสิทธิหรือเสรีภาพของบุคคลอื่น การโอนย้ายข้อมูลส่วนบุคคลจะไม่สามารถกระทำได้ ตามมาตรา 31 วรรคสาม

สิทธิในการขอโอนย้ายข้อมูลส่วนบุคคล

ด้วยเหตุนี้ ผู้ควบคุมข้อมูลส่วนบุคคลจึงจำเป็นต้องมีการเปิดเผยฐานทางกฎหมายสำหรับกิจกรรมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในประกาศความเป็นส่วนตัว ซึ่งแต่ละฐานทางกฎหมายจะมาพร้อมกับภาระหน้าที่และข้อยกเว้นที่แตกต่างกัน โดยสิทธิบางประการจะใช้ได้เมื่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นไปตามฐานทางกฎหมายที่เฉพาะเจาะจงเท่านั้น

หากเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยอาศัยฐานสัญญาหรือฐานความยินยอม เจ้าของข้อมูลส่วนบุคคลจะสามารถใช้สิทธิในการโอนย้ายข้อมูลส่วนบุคคลได้ ตามมาตรา 31 วรรคสอง ซึ่งหมายความว่าหากบุคคลใดใช้สิทธินี้ บุคคลนั้นมีสิทธิที่จะได้รับข้อมูลส่วนบุคคลในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติ และสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ หรือให้ข้อมูลส่วนบุคคลนั้นถูกโอนย้ายโดยตรงไปยังผู้ควบคุมข้อมูลส่วนบุคคลรายอื่น ตามมาตรา 31 วรรคหนึ่ง

หากข้อมูลส่วนบุคคลถูกโอนย้ายให้กับบุคคล ก็อาจสามารถดาวน์โหลดได้โดยตรง หรือหากเป็นการโอนย้ายข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลรายอื่น ก็อาจส่งข้อมูลผ่านทาง Application Programming Interface (API)

วัตถุประสงค์ของสิทธินี้ คือ เพื่อให้บุคคลสามารถย้ายข้อมูลส่วนบุคคลของตนจากบริการหนึ่งไปยังอีกบริการหนึ่งได้ เช่น การย้ายจาก Spotify ไปยัง Apple Music โดยใช้การส่งออกข้อมูลในรูปแบบที่ทั้งสองบริการสามารถอ่านและเข้าใจได้

สิทธิในการขอโอนย้ายข้อมูลส่วนบุคคล

2. การอภิปรายเกี่ยวกับการโอนย้ายข้อมูลส่วนบุคคล

หากเจ้าของข้อมูลส่วนบุคคลต้องการโอนย้ายข้อมูลส่วนบุคคลของตนจาก Google Photos ไปยัง Amazon Photo สิทธินี้จะทำให้เจ้าของข้อมูลส่วนบุคคลสามารถขอให้ Google โอนข้อมูลส่วนบุคคลของตนไปยัง Amazon โดยตรงได้ ประเด็นคำถามที่ตามมา คือ สิทธินี้จะเป็นประโยชน์ต่อองค์กรอย่างไร

สิทธิในการขอโอนย้ายข้อมูลส่วนบุคคล

3. คำตอบที่เป็นไปได้

1 ประการแรก ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดเตรียมข้อมูลในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ ซึ่งหมายความว่าหากผู้ควบคุมข้อมูลส่วนบุคคลตั้งใจจะใช้ระบบ backend ที่เป็นกรรมสิทธิ์เฉพาะและจัดเก็บข้อมูลในรูปแบบเฉพาะเพื่อความสะดวกในการทำงาน ระบบนั้นอาจมีผลกระทบต่อการพัฒนาเทคโนโลยีเบื้องหลัง (backend engineering)

2 ประการที่สอง สิทธินี้อาจช่วยเหลือคู่แข่งของผู้ควบคุมข้อมูลส่วนบุคคล เนื่องจากจะทำให้ผู้ใช้บริการสามารถย้ายข้อมูลส่วนบุคคลออกจากบริการของผู้ควบคุมข้อมูลส่วนบุคคลได้ง่ายขึ้น

ถึงแม้ว่าหลักเกณฑ์ข้างต้นจะมีความสำคัญ แต่ก็มีขอบเขตการใช้ที่ค่อนข้างจำกัด เนื่องจากเกี่ยวข้องเฉพาะกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่อยู่ในรูปแบบอิเล็กทรอนิกส์ และเป็นข้อมูลส่วนบุคคลที่รวบรวมจากเจ้าของข้อมูลส่วนบุคคลเท่านั้น

หากผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยอาศัยฐานความยินยอมหรือฐานสัญญา ผู้ควบคุมข้อมูลส่วนบุคคลต้องให้สิทธิในการโอนย้ายข้อมูลส่วนบุคคลนี้ อย่างไรก็ตาม หากผู้ควบคุมข้อมูลส่วนบุคคลอาศัยฐานผลประโยชน์โดยชอบด้วยกฎหมาย สิทธิในการโอนย้ายข้อมูลจะไม่สามารถนำมาใช้ได้

ดังนี้ รายละเอียดที่องค์กรระบุในเว็บไซต์และฐานทางกฎหมายที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะมีผลกระทบสำคัญต่อการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ และควรได้รับการพิจารณาอย่างรอบคอบ

สิทธิในการขอโอนย้ายข้อมูลส่วนบุคคล

4. แนวทางในการโอนย้ายข้อมูลส่วนบุคคล

1) วัตถุประสงค์ของสิทธิในการโอนย้ายข้อมูลส่วนบุคคลคืออะไร ?

สิทธินี้อนุญาตให้เจ้าของข้อมูลส่วนบุคคลได้รับและนำข้อมูลของตนไปใช้ใหม่ตามวัตถุประสงค์ของตนเองและในบริการที่ต่างกัน ซึ่งประโยชน์ที่อาจได้รับ ได้แก่ “เพิ่มอำนาจให้กับผู้บริโภค" "สร้างโอกาสในการพัฒนานวัตกรรม" และ "สร้างโอกาสในการแบ่งปันข้อมูลส่วนบุคคลระหว่างผู้ควบคุมข้อมูลส่วนบุคคลในลักษณะที่ปลอดภัยและอยู่ภายใต้การควบคุมของเจ้าของข้อมูลส่วนบุคคล"

2) สิทธิในการโอนย้ายข้อมูลส่วนบุคคลอนุญาตให้ทำอะไรได้บ้าง ?

สิทธินี้อนุญาตให้เจ้าของข้อมูลส่วนบุคคลได้รับข้อมูลส่วนบุคคลที่เกี่ยวกับตนเอง ซึ่งได้ให้ไว้กับผู้ควบคุมข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลนั้นสามารถโอนย้ายโดยตรงไปยังเจ้าของข้อมูลส่วนบุคคลเพื่อเก็บไว้ในอุปกรณ์ส่วนตัว หรือโอนย้ายไปยังผู้ควบคุมข้อมูลส่วนบุคคลรายอื่น ข้อมูลต้องอยู่ในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติ และสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ โดยมีเป้าหมายในการทำให้ข้อมูลส่วนบุคคลสามารถใช้งานร่วมกันได้

สิทธิในการขอโอนย้ายข้อมูลส่วนบุคคล

3) สิทธิในการโอนย้ายข้อมูลส่วนบุคคลมีผลเมื่อใด ?

กรณีนี้มีเงื่อนไขสามข้อที่ต้องปฏิบัติตาม ดังนี้

1. ข้อมูลส่วนบุคคลที่ถูกขอให้โอนย้าย จะต้องสามารถใช้หรือเปิดเผยได้ด้วยวิธีการอัตโนมัติ บนพื้นฐานของความยินยอมของเจ้าของข้อมูลส่วนบุคคลหรือการปฏิบัติตามสัญญาที่เจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาฝ่ายหนึ่ง
2. ข้อมูลส่วนบุคคลที่ถูกขอให้โอนย้าย จะต้องเกี่ยวข้องกับเจ้าของข้อมูลส่วนบุคคล และเป็นข้อมูลที่ได้ให้ไว้กับผู้ควบคุมข้อมูลส่วนบุคคล (ไม่ใช่ข้อมูลที่ถูกอนุมานหรือสร้างขึ้นจากข้อมูลที่ให้มา)
3. การโอนย้ายข้อมูลส่วนบุคคลจะต้องไม่ส่งผลกระทบต่อสิทธิและเสรีภาพของผู้อื่น (เช่น ชุดข้อมูลที่มีข้อมูลส่วนบุคคลของบุคคลอื่น) ด้วย

สิทธิในการขอให้ลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้

1. สิทธิในการลบข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องส่งเสริมสิทธิของเจ้าของข้อมูลส่วนบุคคล รวมถึงสิทธิในการลบข้อมูลส่วนบุคคล หรือที่รู้จักกันว่าสิทธิที่จะถูกลืม (Right to be forgotten) ตามที่ระบุในมาตรา 33

สิทธิในการลบข้อมูลส่วนบุคคล หมายความว่า เจ้าของข้อมูลส่วนบุคคลสามารถร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ซึ่งเจ้าของข้อมูลส่วนบุคคลสามารถร้องขอให้ลบข้อมูลส่วนบุคคลของตนได้ในกรณีต่อไปนี้ ตามที่บัญญัติในมาตรา 33 วรรคหนึ่ง

1) เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
2) เมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลไม่มีอำนาจตามกฎหมายที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นได้ต่อไป
3) เมื่อเจ้าของข้อมูลส่วนบุคคลคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามมาตรา 32 (1) และผู้ควบคุมข้อมูลส่วนบุคคลไม่อาจปฏิเสธคำขอตามมาตรา 32 (1) (ก) หรือ (ข) ได้ หรือเป็นการคัดค้านตามมาตรา 32 (2)
4) เมื่อข้อมูลส่วนบุคคลได้ถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมาย

สิทธิในการขอให้ลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้

2. สิทธิในการลบข้อมูลส่วนบุคคล

การลบข้อมูลส่วนบุคคลอาจขยายขอบเขตไปมากกว่าการลบข้อมูลจากบันทึกของผู้ควบคุมข้อมูลส่วนบุคคล กล่าวคือ เมื่อข้อมูลส่วนบุคคลถูกเปิดเผยต่อสาธารณะโดยผู้ควบคุมข้อมูลส่วนบุคคล เช่น การโพสต์ข้อมูลส่วนบุคคลบนเว็บไซต์ที่สามารถเข้าถึงได้โดยสาธารณะ หากเจ้าของข้อมูลส่วนบุคคลร้องขอให้ลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ในกรณีนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องเป็นผู้รับผิดชอบดำเนินการทั้งในทางเทคโนโลยีและค่าใช้จ่ายเพื่อให้เป็นไปตามคำขอนั้น โดยแจ้งผู้ควบคุมข้อมูลส่วนบุคคลอื่น ๆ เพื่อให้ได้รับคำตอบในการดำเนินการให้เป็นไปตามคำขอ ซึ่งเป็นไปตามมาตรา 33 วรรคสาม

การขยายสิทธิของเจ้าของข้อมูลส่วนบุคคลในลักษณะข้างต้น ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องติดตามจากบุคคลที่สาม ซึ่งอาจสร้างภาระให้กับผู้ควบคุมข้อมูลส่วนบุคคล โดยปัญหาที่อาจเกิดขึ้น ได้แก่

1) การระบุผู้รับข้อมูลส่วนบุคคลทั้งหมด
2) การแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลรายอื่นทราบ (ซึ่งอาจเพิ่มความเสี่ยงในการเปิดเผยข้อมูล)
3) การคัดค้านจากผู้ควบคุมข้อมูลส่วนบุคคลโดยอ้างสิทธิพื้นฐานในการแสดงความเห็นและการรับข้อมูลข่าวสาร

สิทธิในการขอให้ลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้

3. ข้อยกเว้น

ข้อยกเว้นของการใช้สิทธิในการลบข้อมูลส่วนบุคคลของเจ้าของข้อมูล ถูกบัญญัติในมาตรา 33 วรรคสอง ซึ่งได้แก่กรณีต่อไปนี้

1) การเก็บรักษาข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น
2) การเก็บรักษาข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ เพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ
3) การเก็บรักษาข้อมูลส่วนบุคคลเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล
4) การเก็บรักษาข้อมูลส่วนบุคคลเพื่อการปฏิบัติตามกฎหมายเพื่อการให้บริการด้านสุขภาพหรือสังคม
5) การเก็บรักษาข้อมูลส่วนบุคคลเพื่อการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะด้านการสาธารณสุข
6) การใช้ข้อมูลส่วนบุคคลเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย

สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล

สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล ตามที่ระบุในมาตรา 34 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แตกต่างจากสิทธิในการลบข้อมูลส่วนบุคคล เนื่องจากการระงับการใช้ข้อมูลส่วนบุคคลนั้นยังคงอนุญาตให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรักษาข้อมูลส่วนบุคคลไว้ได้ โดยไม่มีการใช้ข้อมูลเพิ่มเติม

การระงับการใช้ข้อมูลส่วนบุคคลเป็นทางเลือกหนึ่งที่ใช้แทนการลบข้อมูลส่วนบุคคล ในกรณีที่กฎหมายกำหนดให้ต้องเก็บรักษาข้อมูลส่วนบุคคลไว้เพื่อปกป้องสิทธิของผู้อื่นหรือเพื่อประโยชน์สาธารณะ

วิธีในการระงับการใช้ข้อมูลส่วนบุคคล ได้แก่

1) ทำให้ข้อมูลส่วนบุคคลไม่สามารถเข้าถึงได้ชั่วคราว
2) ทำเครื่องหมายหรือบันทึกในระบบว่าข้อมูลส่วนบุคคลนั้นถูกจำกัดการประมวลผล
3) ย้ายข้อมูลส่วนบุคคลไปยังระบบที่แยกออกมา

สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคลสามารถร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคลของตนได้ด้วยเหตุผลต่อไปนี้ ตามที่บัญญัติในมาตรา 34 วรรคหนึ่ง

1) เมื่อผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในระหว่างการตรวจสอบตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้ดำเนินการแก้ไขข้อมูลส่วนบุคคล ตามมาตรา 36
2) เมื่อข้อมูลส่วนบุคคลได้ถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมาย ซึ่งเป็นข้อมูลส่วนบุคคลที่ต้องลบหรือทำลาย ตามมาตรา 33 (4) แต่เจ้าของข้อมูลส่วนบุคคลขอให้ให้ระงับการใช้แทน
3) เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล แต่เจ้าของข้อมูลส่วนบุคคลมีความจำเป็นต้องขอให้เก็บรักษาไว้เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
4) เมื่อผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในระหว่างการพิสูจน์ตามมาตรา 32 (1) หรือตรวจสอบตามมาตรา 32 (3) เพื่อปฏิเสธการคัดค้านของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 32 วรรคสาม

สิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคลสามารถคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนเมื่อใดก็ได้ ตามที่ระบุในมาตรา 32 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

อย่างไรก็ตาม สิทธินี้มีข้อจำกัด กล่าวคือสิทธินี้จะมีผลเฉพาะเมื่อเหตุในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นไปตามกรณีดังต่อไปนี้ ตามที่บัญญัติในมาตรา 32 วรรคหนึ่ง

1) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยใช้ฐานภารกิจรัฐหรือผลประโยชน์โดยชอบด้วยกฎหมาย : เจ้าของข้อมูลส่วนบุคคลสามารถคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่อ้างอิงถึงฐานภารกิจรัฐหรือผลประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลได้ โดยอ้างอิงจากสถานการณ์เฉพาะของตน ส่วนผู้ควบคุมข้อมูลส่วนบุคคลสามารถปฏิเสธการใช้สิทธิดังกล่าวได้ โดยจะต้องแสดงให้เห็นว่ามีเหตุผลที่ชอบด้วยกฎหมายที่มีน้ำหนักมากกว่าผลประโยชน์ สิทธิ และเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือพิสูจน์ได้ว่าการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย ในการตัดสินใจว่าจะให้ความสำคัญกับการคัดค้านหรือผลประโยชน์โดยชอบด้วยกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลอาจจัดการประชุมภายในระหว่างผู้ที่เป็นตัวแทนขององค์กรและบุคคลที่เป็นกลาง

สิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

2) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง : เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของตนสำหรับวัตถุประสงค์เกี่ยวกับการตลาดแบบตรงได้ สิทธินี้เป็นสิทธิที่สมบูรณ์และจะทำให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องหยุดทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

3) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ :

เจ้าของข้อมูลส่วนบุคคลสามารถคัดค้านการประมวลผลข้อมูลส่วนบุคคลได้ โดยอ้างอิงจากสถานการณ์เฉพาะของตน อย่างไรก็ตาม สิทธินี้จะถูกระงับ หากการประมวลผลนั้นจำเป็นสำหรับการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล

หน้าที่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ที่เกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล

1. หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่เฉพาะที่เกี่ยวข้องกับสิทธิของเจ้าของข้อมูลส่วนบุคคล ดังนี้

1) แจ้งรายละเอียดเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่แจ้งรายละเอียดเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคล เช่น แจ้งวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล แจ้งสิทธิของเจ้าของข้อมูลส่วนบุคคล

2) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการเชิงองค์กรและมาตรการเชิงเทคนิค เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องมีการพิจารณาทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป

3) ตอบสนองต่อคำร้องขอของเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องตอบสนองต่อคำร้องขอของเจ้าของข้อมูลส่วนบุคคล เช่น คำร้องขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล คำร้องขอแก้ไขข้อมูลส่วนบุคคล คำร้องขอลบข้อมูลส่วนบุคคล โดยจะต้องดำเนินการตามกรอบเวลาที่กฎหมายกำหนด

หน้าที่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ที่เกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล

2. หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ในการดำเนินการกับข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น โดยต้องปฏิบัติหน้าที่ที่เกี่ยวข้องกับสิทธิของเจ้าของข้อมูลส่วนบุคคลดังต่อไปนี้

1) ดำเนินการตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการตามคำสั่งที่ชัดเจนและเฉพาะเจาะจงจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น และต้องไม่กระทำการใด ๆ ที่นอกเหนือจากคำสั่งนั้น

2) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม ผู้ประมวลข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

แบบทดสอบ บทที่ 5

ข้อที่ 1

Q : ข้อใดต่อไปนี้เป็นสิทธิของเจ้าของข้อมูลส่วนบุคคลในการขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล

ก. สิทธิในการโอนย้ายข้อมูลส่วนบุคคล

ข. สิทธิในการเข้าถึงข้อมูลส่วนบุคคล

ค. สิทธิในการลบข้อมูลส่วนบุคคล

ง. สิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

แบบทดสอบ บทที่ 5

ข้อที่ 2

Q : สิทธิในการเข้าถึงข้อมูลส่วนบุคคล ให้สิทธิเจ้าของข้อมูลส่วนบุคคลในการเข้าถึงข้อมูลใดต่อไปนี้ (เลือกทั้งหมดที่ถูกต้อง)

ก. วัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ข. ระยะเวลาในการเก็บข้อมูลส่วนบุคคล

ค. วิธีการจัดเก็บข้อมูลส่วนบุคคล

ง. ผู้รับข้อมูลส่วนบุคคล

แบบทดสอบ บทที่ 5

ข้อที่ 3

Q : เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการอย่างไร

ก. ดำเนินการแก้ไขข้อมูลส่วนบุคคล
ข. ดำเนินการโอนย้ายข้อมูลส่วนบุคคล
ค. ดำเนินการลบข้อมูลส่วนบุคคล
ง. ไม่มีข้อใดถูก

แบบทดสอบ บทที่ 5

ข้อที่ 4

Q : กรณีใดต่อไปนี้ที่เจ้าของข้อมูลส่วนบุคคลสามารถคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของตนได้ (เลือกทั้งหมดที่ถูกต้อง)

ก. การก่อตั้ง การใช้สิทธิ หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

ข. การตลาดแบบตรง

ค. การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยอาศัยฐานภารกิจรัฐ หรือฐานผลประโยชน์โดยชอบด้วยกฎหมาย

ง. การวิจัยหรือวัตถุประสงค์ทางสถิติ

• เฉลยแบบทดสอบบทที่ 5

ข้อที่	เฉลย
1.	ข.
2.	ก. ข. และ ง.
3.	ค.
4.	ข. ค. และ ง.

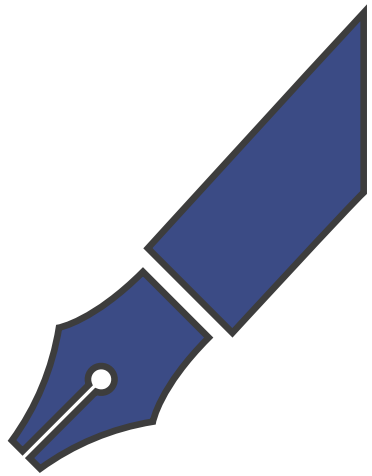
หน้าที่ในการแจ้งวัตถุประสงค์ ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

บทที่ 6

- บทนำ
- ความโปร่งใส
- ประกาศความเป็นส่วนตัว
- รายละเอียดข้อมูลที่แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ
- การเก็บรวบรวมข้อมูลส่วนบุคคลโดยตรงและโดยทางอื่น
- ข้อมูลที่ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบกรณีการเก็บข้อมูลโดยตรง
- กรณีมีการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น

• บทนำ

❑ บทนี้อธิบายหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในการให้ข้อมูลรายละเอียดการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคล



• ความโปร่งใส (Transparency)

ตามหลักความโปร่งใส ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งรายละเอียดต่าง ๆ ให้เจ้าของข้อมูลส่วนบุคคลทราบโดยในการแจ้งนั้น ควรแจ้งโดยใช้ข้อความที่ชัดเจน กระชับ และเข้าใจได้ง่าย โดยคำนึงถึงผู้รับฟังเป็นหลักด้วยว่าเป็นบุคคลกลุ่มใด ควรใช้ภาษาแบบใด โดยอาจทำด้วยวาจา หรือลายลักษณ์อักษรก็ได้ และให้เข้าถึงได้ง่าย เช่น การมีลิงก์ท้ายหน้าเว็บไซต์ทุกหน้าเพื่อเชื่อมโยงไปยังข้อมูลที่ต้องการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ

• ประกาศความเป็นส่วนตัว (Privacy Notice)

ประกาศความเป็นส่วนตัว คือ คำประกาศถึงเจ้าของข้อมูลส่วนบุคคลที่มีเนื้อหาอธิบายว่าองค์กรจะมีการดำเนินการการจัดเก็บ ใช้ รักษา เปิดเผย และทำลายข้อมูลส่วนบุคคลอย่างไร เนื่องจากข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบนั้นมีค่อนข้างมาก การจะแจ้งในรูปแบบที่กระชับจึงทำได้ยาก วิธีการที่สามารถใช้เพื่อให้การแจ้งข้อมูลนั้นกระชับ เช่น

- **การใช้การแจ้งแบบเป็นชั้น (layered privacy notices)** โดยการแจ้งข้อมูลในเบื้องต้นสั้น เกี่ยวกับองค์กรว่าเป็นใคร และจะมีการใช้ข้อมูลอย่างไรบ้าง โดยอาจมีลิงก์เพื่อขยายข้อความในแต่ละส่วนเพิ่มเติมเป็นชั้น ๆ ไป และอาจมีลิงก์เพื่อให้ข้อมูลเพิ่มเติมการใช้ข้อมูลในบางกรณี/สถานการณ์
- **การประกาศแบบทันเวลาพอดี (‘just-in-time’ notices)** เป็นการให้ข้อมูล ณ เวลาที่หรือก่อนที่เจ้าของข้อมูลส่วนบุคคลจะยอมรับการใช้บริการหรือ (ซื้อ) สินค้า หรืออาจใช้ในกรณีที่เป็นการแจ้งวัตถุประสงค์ในการใช้ข้อมูลเพิ่มเติมจากที่ได้เคยแจ้งไปก่อนหน้าแล้ว
- **-การใช้สัญรูปมาตรฐาน (standardized icons)** คือ การใช้สัญรูป (icon) ที่ทั้งคนและคอมพิวเตอร์สามารถเข้าใจได้ และสื่อความหมายที่ต้องการ เช่น ข้อมูลส่วนบุคคลทุกข้อมูลถูกเข้ารหัส

• รายละเอียดข้อมูลที่แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ

การเก็บรวบรวมข้อมูลส่วนบุคคลโดยตรงและโดยทางอื่น

แม้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งรายละเอียดการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนที่จะมีการเก็บข้อมูลส่วนบุคคล แต่ก็อาจไม่สามารถทำได้เสมอไป เพราะบางครั้งอาจมีการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น เช่น ข่าว หรือ รายการข้อมูลที่ถูกจดทะเบียนไว้กับทางราชการ

ดังนั้น ในกรณีนี้ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคคลให้ทราบหลังจากที่ได้ข้อมูลส่วนบุคคลมาแล้วภายใน 30 วันนับแต่ได้ข้อมูลส่วนบุคคลและได้เก็บรวบรวมข้อมูลส่วนบุคคล แต่ต้องก่อนการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลใด ๆ ทั้งนี้

ผู้ควบคุมข้อมูลส่วนบุคคลไม่ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบหากเข้ากรณียกเว้น เช่น กรณีที่เจ้าของข้อมูลส่วนบุคคลนั้นทราบข้อมูลอยู่แล้ว ทั้งนี้ กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลต้องการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลด้วยวัตถุประสงค์อื่นที่แตกต่างจากที่เคยแจ้งไว้ก่อนแล้วนั้น ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ใหม่นั้นและรายละเอียดอื่น ๆ ที่เกี่ยวข้องให้เจ้าของข้อมูลส่วนบุคคลทราบ ยกเว้นว่าจะมีกฎหมายบัญญัติไว้เป็นอย่างอื่น

• ข้อมูลที่ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบกรณีการเก็บข้อมูลโดยตรง

- วัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล
- กรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญา หรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล
- ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวม
- ระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคล
- ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย
- ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล พร้อมทั้งข้อมูลการติดต่อไปยังผู้ควบคุมข้อมูลส่วนบุคคลและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- สิทธิของเจ้าของข้อมูลส่วนบุคคล

• กรณีการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น

โดยหลักแล้ว พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่

(1) ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่เก็บรวบรวม และได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(2) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26

• กรณีการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น

ทั้งนี้ กฎหมายให้นำบทบัญญัติเกี่ยวกับการแจ้งวัตถุประสงค์ใหม่ตามมาตรา 21 และการแจ้งรายละเอียด ตามมาตรา 23 มาใช้บังคับกับการเก็บรวบรวมข้อมูลส่วนบุคคลที่ต้องได้รับความยินยอมตามวรรคหนึ่งโดยอนุโลม เว้นแต่กรณีดังต่อไปนี้

(1) เจ้าของข้อมูลส่วนบุคคลทราบวัตถุประสงค์ใหม่หรือรายละเอียดนั้นอยู่แล้ว

(2) ผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่าการแจ้งวัตถุประสงค์ใหม่หรือรายละเอียดดังกล่าวไม่สามารถทำได้หรือจะเป็นอุปสรรคต่อการใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ในกรณีนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิ เสรีภาพ และประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(3) การใช้หรือการเปิดเผยข้อมูลส่วนบุคคลต้องกระทำโดยเร่งด่วนตามที่กฎหมายกำหนดซึ่งได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(4) เมื่อผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้ซึ่งล่วงรู้หรือได้มาซึ่งข้อมูลส่วนบุคคลจากหน้าที่หรือจากการประกอบอาชีพหรือวิชาชีพและต้องรักษาวัตถุประสงค์ใหม่หรือรายละเอียดบางประการตามมาตรา 23 ไว้เป็นความลับตามที่กฎหมายกำหนด (เนื้อหาเป็นไปตาม ม. 25 วรรคสอง (4))

การแจ้งรายละเอียดข้างต้นนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบภายในสามสิบวันนับแต่วันที่เก็บรวบรวม เว้นแต่กรณีที่นำข้อมูลส่วนบุคคลไปใช้เพื่อการติดต่อกับเจ้าของข้อมูลส่วนบุคคลต้องแจ้งในการติดต่อครั้งแรก และกรณีที่จะนำข้อมูลส่วนบุคคลไปเปิดเผย ต้องแจ้งก่อนที่จะนำข้อมูลส่วนบุคคลไปเปิดเผยเป็นครั้งแรก

แบบทดสอบ บทที่ 6

ข้อที่ 1

Q : วิธีการใดบ้างจากตัวเลือกต่อไปนี้ที่สามารถนำมาใช้ได้เพื่อทำให้การแจ้งข้อมูลเป็นไปโดยกระชับ

ก. Standardized icons

ข. Key notices

ค. ‘Just-in-time’ notices

ง. Layered privacy notices

แบบทดสอบ บทที่ 6

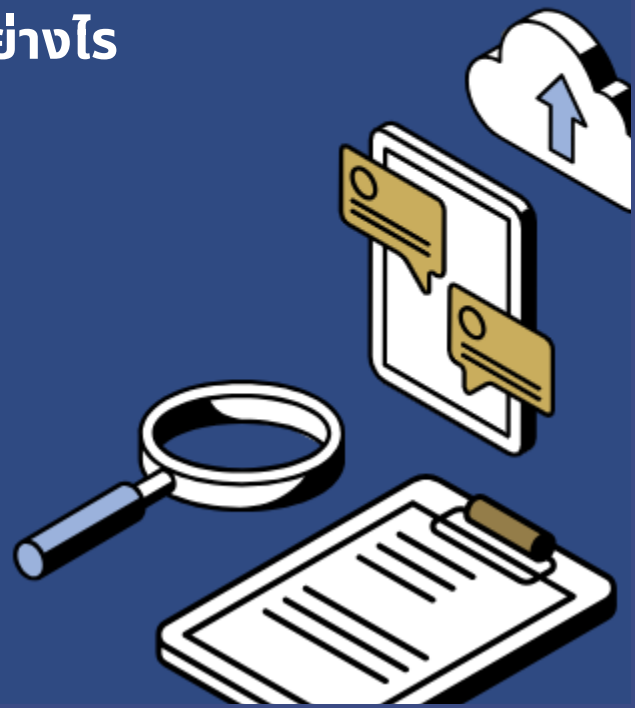
ข้อที่ 2

Q : ข้อมูลใดบ้างที่ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ เมื่อมีการเก็บรวบรวมข้อมูลส่วนบุคคล

แบบทดสอบ บทที่ 6

ข้อที่ 3

Q : การเก็บรวมรวมข้อมูลส่วนบุคคลโดยทางอื่นที่ไม่ใช่การเก็บโดยตรงจากเจ้าของข้อมูลส่วนบุคคลสามารถทำได้หรือไม่ อย่างไร



แบบทดสอบ บทที่ 6

ข้อที่ 4

Q : หน้าที่ในการแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เป็นหน้าที่ของบุคคลใด

ก. ผู้ควบคุมข้อมูลส่วนบุคคล

ข. ผู้ประมวลผลข้อมูลส่วนบุคคล

ค. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ง. คณะกรรมการผู้เชี่ยวชาญ

แบบทดสอบ บทที่ 6

ข้อที่ 5

Q : <u>จริงหรือเท็จ</u>

“กรณีการเก็บข้อมูลส่วนบุคคลจากแหล่งอื่น ต้องแจ้งการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า”

• เฉลยแบบทดสอบบทที่ 6

ข้อที่	เฉลย
1.	ก. ค. และ ง.
2.	(1) วัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล (2) กรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญา หรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล (3) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวม (4) ระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคล (5) ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย (6) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล พร้อมทั้งข้อมูลการติดต่อไปยังผู้ควบคุมข้อมูลส่วนบุคคลและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (7) สิทธิของเจ้าของข้อมูลส่วนบุคคล
3.	สามารถทำได้หาก (1) ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบภายในสามสิบวันนับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือ (2) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26

• เฉลยแบบทดสอบบทที่ 6

ข้อที่	เฉลย
4.	ก.
5.	จริง

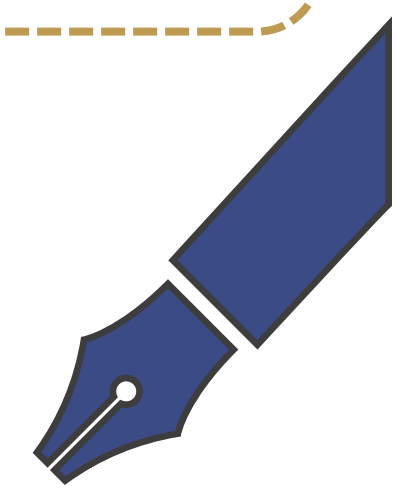
การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

บทที่ 7

- บทนำ
- หลักในการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ
- มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (Adequacy decisions)
- มาตรการคุ้มครองที่เหมาะสม (Appropriate safeguard)
- นโยบายคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ (Binding Corporate Rules - BCRs)
- ข้อยกเว้นตามกฎหมาย (Derogations)

• บทนำ

การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศเป็นประเด็นที่มีความสำคัญมากในยุคที่ข้อมูลสามารถเคลื่อนย้ายข้ามพรมแดนได้อย่างรวดเร็ว ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การโอนข้อมูลเช่นนี้ต้องปฏิบัติตามหลักเกณฑ์ที่กำหนด เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล และป้องกันไม่ให้ข้อมูลดังกล่าวถูกนำไปใช้ในทางที่ไม่เหมาะสมหรือเกิดความเสียหาย



• หลักการในการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

ในกรณีที่มีความจำเป็นต้องส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์กรระหว่างประเทศ ตามมาตรา 28 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ กำหนดหลักการในการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศดังนี้ คือ ผู้ควบคุมข้อมูลส่วนบุคคลในประเทศไทยสามารถส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้รับที่อยู่นอกประเทศไทยได้อย่างถูกต้องตามกฎหมายในกรณีดังต่อไปนี้

1. ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (Adequacy Decisions)
2. ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลมีมาตรการคุ้มครองที่เหมาะสม (Appropriate safeguard)
3. กรณีเข้าข้อยกเว้นตามกฎหมาย (Derogations)

• มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (Adequacy decisions)

มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีแนวคิดคล้ายกับเรื่อง Adequacy Decisions ตามข้อกำหนด GDPR ของสหภาพยุโรป ซึ่งมีพื้นฐานมาจากการประเมินกฎหมายของประเทศที่สามว่ามีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลหรือมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่เทียบเท่าหรือใกล้เคียงกับสหภาพยุโรปหรือไม่

คณะกรรมาธิการยุโรปเป็นผู้มีอำนาจในการตัดสินว่าประเทศใดมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ และตาม GDPR การตัดสินเรื่องความเพียงพอดังกล่าว จะได้รับการทบทวนทุก ๆ 4 ปี หากพบว่าประเทศใดไม่ปฏิบัติตามมาตรฐานที่กำหนด การตัดสินนั้นอาจถูกยกเลิก ระงับ หรือแก้ไขได้ ส่วนการตัดสินที่เคยทำไว้ภายใต้กฎหมายคุ้มครองข้อมูลเดิมจะยังคงมีผลบังคับใช้จนกว่าจะมีการแก้ไข เปลี่ยนแปลง หรือยกเลิก

• การพิจารณาว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอหรือไม่

ตามมาตรา 28 ของ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การพิจารณาว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอหรือไม่ จะต้องเป็นไปตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศตามมาตรา 28 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566 ซึ่งหลักเกณฑ์ดังกล่าวได้แก่

1. มีมาตรการหรือกลไกทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทางหรือองค์การระหว่างประเทศที่สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย โดยเฉพาะหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม มาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมและสามารถบังคับตามสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ และมาตรการเยียวยาทางกฎหมายที่มีประสิทธิภาพ

2. มีหน่วยงานหรือองค์กรที่มีหน้าที่และอำนาจในการบังคับใช้กฎหมายและกฎระเบียบเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในประเทศปลายทางหรือองค์การระหว่างประเทศ

• มาตรการคุ้มครองที่เหมาะสม (Appropriate safeguard)

ในกรณีที่ยังไม่มีคำวินิจฉัยเกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล อาจส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้ หากจัดให้มีมาตรการคุ้มครองที่เหมาะสม (Appropriate safeguard)

มาตรการคุ้มครองที่เหมาะสม สามารถนำมาใช้ในการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้โดยชอบด้วยกฎหมาย มาตรการคุ้มครองที่เหมาะสมเป็นเครื่องมือทางกฎหมายที่ออกแบบมาเพื่อให้มั่นใจว่าผู้รับข้อมูลส่วนบุคคลที่อยู่ต่างประเทศยังคงต้องคุ้มครองข้อมูลส่วนบุคคลตามมาตรฐานที่คล้ายคลึงกับของประเทศไทย

• การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

มาตรา 29 วรรคสาม บัญญัติเกี่ยวกับมาตรการคุ้มครองที่เหมาะสมว่าในกรณีที่ยังไม่มีคำวินิจฉัยของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามมาตรา 28 หรือยังไม่มีนโยบายในการคุ้มครองข้อมูลส่วนบุคคลตามมาตรา 29 วรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอาจส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้โดยได้รับยกเว้นไม่ต้องปฏิบัติตามมาตรา 28 เมื่อผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้จัดให้มีมาตรการคุ้มครองที่เหมาะสมสามารถบังคับตามสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ รวมทั้งมีมาตรการเยียวยาทางกฎหมายที่มีประสิทธิภาพ ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

ตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศตามมาตรา 29 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566 ได้กำหนดรูปแบบของมาตรการคุ้มครองที่เหมาะสม ดังนี้

1. ข้อสัญญาที่เป็นไปตามข้อสัญญาในการส่งหรือโอนข้อมูลส่วนบุคคลที่เป็นที่ยอมรับ ซึ่งเป็นข้อสัญญาในการคุ้มครองข้อมูลส่วนบุคคล ในส่วนที่เกี่ยวกับการส่งหรือโอนข้อมูลส่วนบุคคลข้ามพรมแดน หรือการส่งหรือโอนข้อมูลส่วนบุคคลระหว่างประเทศที่คณะกรรมการกำหนดให้ผู้ส่งหรือโอนข้อมูลส่วนบุคคลหรือผู้รับข้อมูลส่วนบุคคลใช้เพื่อกำหนดหน้าที่หรือเงื่อนไขของคู่สัญญาเพื่อให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม

2. การรับรอง (certification) เกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ในส่วนที่เกี่ยวกับการส่งหรือโอนข้อมูลส่วนบุคคลข้ามพรมแดน หรือการส่งหรือโอนข้อมูลส่วนบุคคลระหว่างประเทศ ว่ามีมาตรการคุ้มครองที่เหมาะสม โดยเป็นไปตามมาตรฐานที่เป็นที่ยอมรับ

3. ข้อกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลในตราสารหรือข้อตกลงที่มีผลผูกพันทางกฎหมายและสามารถใช้บังคับได้ระหว่างหน่วยงานของรัฐของประเทศไทยกับหน่วยงานของรัฐของประเทศอื่น ในกรณีการส่งหรือโอนข้อมูลส่วนบุคคลระหว่างหน่วยงานของรัฐของประเทศไทยกับหน่วยงานของรัฐของประเทศอื่นนั้น

• นโยบายคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ (Binding Corporate Rules - BCRs)

นโยบายคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ ถูกออกแบบมาเพื่อให้บริษัทข้ามชาติขนาดใหญ่สามารถนำนโยบายที่มีข้อกำหนดในการจัดการข้อมูลส่วนบุคคลที่มีผลผูกพันกับบริษัทมาใช้ หากหน่วยงานกำกับดูแลที่มีอำนาจอนุมัติข้อกำหนดเหล่านี้ บริษัทนั้นจะสามารถโอนข้อมูลส่วนบุคคลภายในองค์กรของตนทั่วโลกได้อย่างอิสระ

มาตรา 29 วรรคหนึ่ง บัญญัติเกี่ยวกับนโยบายคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการไว้ว่า ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักรได้กำหนดนโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการ หรือเครือธุรกิจเดียวกัน เพื่อการประกอบกิจการหรือธุรกิจร่วมกัน หากนโยบายในการคุ้มครองข้อมูลส่วนบุคคลดังกล่าวได้รับการตรวจสอบและรับรองจากสำนักงาน การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศที่เป็นไปตามนโยบายในการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการตรวจสอบและรับรองดังกล่าว ให้สามารถกระทำได้โดยได้รับยกเว้นไม่ต้องปฏิบัติตามมาตรา 28

• การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ออกประกาศเรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศตามมาตรา 29 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566 โดยมีการกำหนดเกี่ยวกับรายละเอียด หลักเกณฑ์การตรวจสอบและรับรองนโยบายดังกล่าวดังนี้

1. การมีผลและสภาพบังคับในทางกฎหมายของนโยบายในการคุ้มครองข้อมูลส่วนบุคคลดังกล่าวกับนิติบุคคลหรือบุคคลธรรมดาในเครือกิจการหรือเครือธุรกิจเดียวกัน ตลอดจนผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้อง ผู้ส่งหรือโอนข้อมูลส่วนบุคคล และผู้รับข้อมูลส่วนบุคคลที่อยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่เสนอนโยบายให้สำนักงานตรวจสอบและรับรอง ทั้งนี้ นโยบายดังกล่าวต้องสอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และต้องมีผลผูกพันต่อบุคลากร พนักงาน ลูกจ้าง หรือบุคคลที่เกี่ยวข้องกับผู้ส่งหรือโอนข้อมูลส่วนบุคคลและผู้รับข้อมูลส่วนบุคคล และการส่งหรือโอนข้อมูลส่วนบุคคลและการรับข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกันด้วย

2. ข้อกำหนดที่รับรองการคุ้มครองข้อมูลส่วนบุคคล สิทธิของเจ้าของข้อมูลส่วนบุคคลและการร้องเรียน สำหรับข้อมูลส่วนบุคคลที่ถูกส่งหรือโอนไปยังต่างประเทศ

3. มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลและมาตรการรักษาความมั่นคงปลอดภัยที่สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล โดยมาตรการรักษาความมั่นคงปลอดภัยจะต้องเป็นไปตามมาตรฐานขั้นต่ำตามที่กฎหมายกำหนด

• ข้อยกเว้นตามกฎหมาย (Derogations)

หากผู้ควบคุมข้อมูลส่วนบุคคลจำเป็นต้องส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทางหรือองค์การระหว่างประเทศ แต่ประเทศหรือองค์การระหว่างประเทศที่รับข้อมูลดังกล่าวไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ เช่น ประเทศปลายทางไม่มีกฎหมาย กฎเกณฑ์ องค์กร หรือพันธกรณีระหว่างประเทศที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ผู้ควบคุมข้อมูลส่วนบุคคลในประเทศไทยอาจพิจารณาข้อยกเว้นตามกฎหมายเพื่อดำเนินการโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทางต่อไป

มาตรา 28 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติเกี่ยวกับข้อยกเว้นตามกฎหมายอนุญาตให้สามารถส่งหรือโอนข้อมูลส่วนบุคคลได้ แม้ว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลดังกล่าวจะไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอก็ตาม ในกรณีดังนี้

1. เป็นการปฏิบัติตามกฎหมาย

2. ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว

3. เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น)

4. เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่น เพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

5. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล หรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้

6. เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

แบบทดสอบ บทที่ 7

ข้อที่ 1

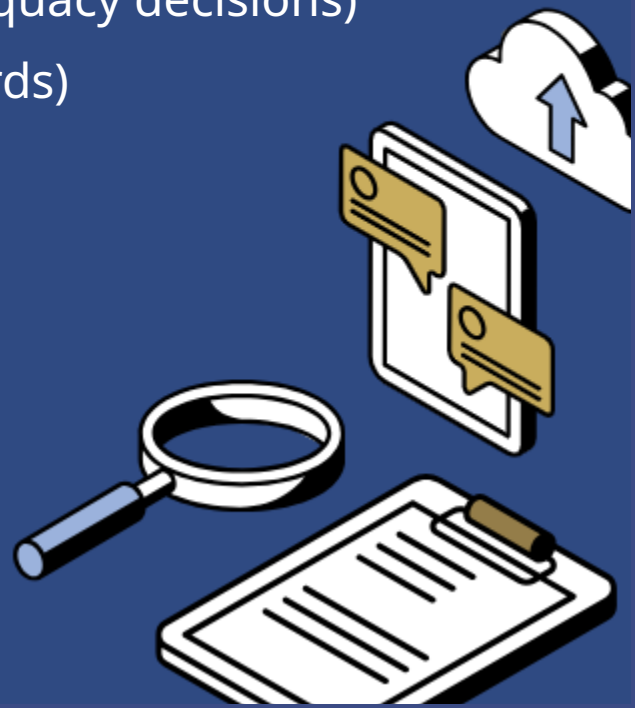
Q : ข้อใดคือหลักการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศที่ผู้ควบคุมข้อมูลส่วนบุคคลสามารถดำเนินการได้ตามกฎหมาย (ตอบได้มากกว่า 1 ข้อ)

ก. มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (Adequacy decisions)

ข. มาตรการคุ้มครองที่เหมาะสม (Appropriate safeguards)

ค. ข้อยกเว้นตามกฎหมาย (Derogations)

ง. นโยบายคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ (Binding Corporate Rules - BCRs)



แบบทดสอบ บทที่ 7

ข้อที่ 2

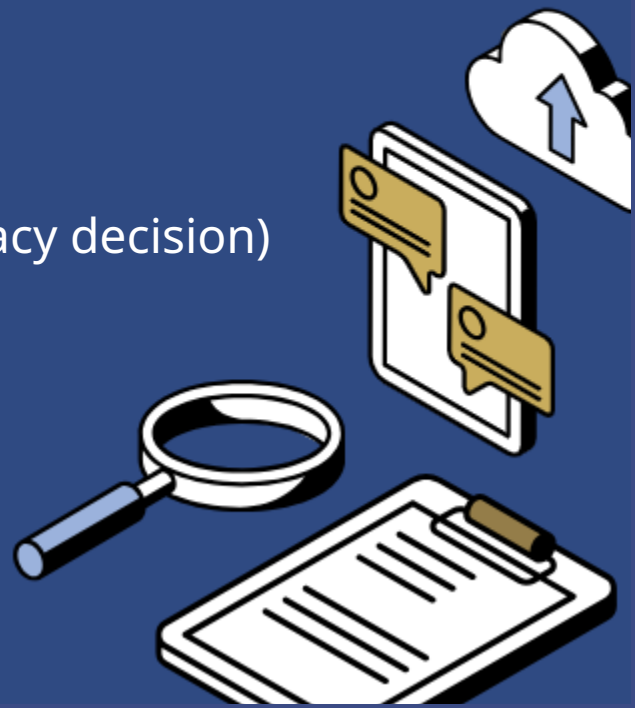
Q : ข้อใดต่อไปนี้เป็นตัวเลือกสำหรับการโอนข้อมูลระหว่างประเทศที่เป็นการตัดสินโดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลว่าประเทศที่สามมีการคุ้มครองข้อมูลส่วนบุคคลในระดับเดียวกับประเทศไทย

ก. มาตรการคุ้มครองที่เหมาะสม (Appropriate safeguard)

ข. ข้อยกเว้นตามกฎหมาย (Derogations)

ค. มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (Adequacy decision)

ง. นโยบายคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ (Binding Corporate Rules - BCRs)



แบบทดสอบ บทที่ 7

ข้อที่ 3

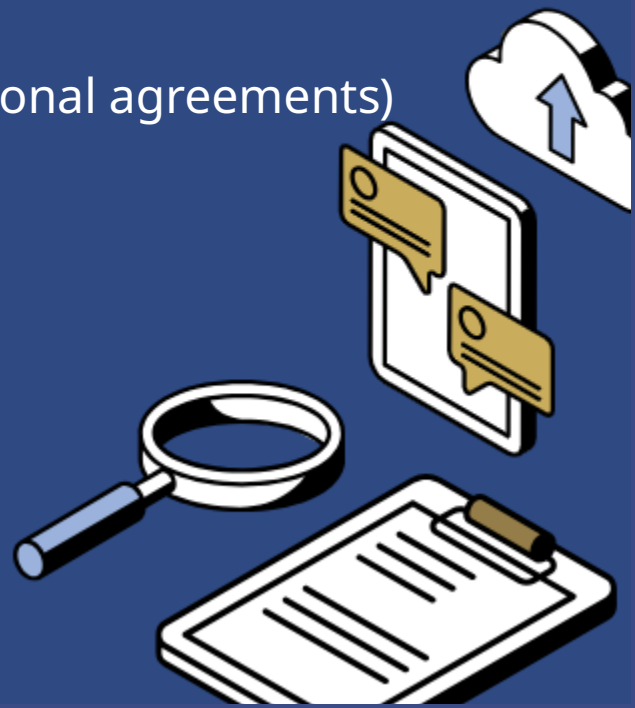
Q : มาตรการคุ้มครองที่เหมาะสมข้อใดที่อนุญาตให้บริษัทข้ามชาติขนาดใหญ่สามารถใช้นโยบายในการจัดการข้อมูลส่วนบุคคลได้

ก. ข้อสัญญาเฉพาะกิจ (Ad hoc contractual clauses)

ข. การอ้างอิงข้อตกลงระหว่างประเทศ (Reliance on international agreements)

ค. ข้อสัญญามาตรฐาน (Standard contractual clauses)

ง. นโยบายคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ (Binding corporate rules)



• เฉลยแบบทดสอบบทที่ 7

ข้อที่	เฉลย
1.	ก. ข. ค. และ ง.
2.	ค.
3.	ง.

แนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล

บทที่ 8

- บทนำ
- การคุ้มครองข้อมูลส่วนบุคคลในบริบทของนายจ้างและลูกจ้าง
- การเฝ้าระวัง (surveillance) และระบบกล้องวงจรปิด
- การตลาดแบบตรง
- เทคโนโลยีและความท้าทายด้านการคุ้มครองข้อมูลส่วนบุคคล
- แบบทดสอบ

บทนำ

แนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลในบทนี้จะเป็นการปรับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในบริบทต่าง ๆ ที่เกี่ยวข้องกับการดำเนินงานขององค์กร ตั้งแต่ความสัมพันธ์ระหว่างนายจ้างกับลูกจ้างในบริบทของการคุ้มครองข้อมูลส่วนบุคคล ข้อพิจารณาในกรณี Work From Home การบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในบริบทของการเฝ้าระวัง (surveillance) ระบบกล้องวงจรปิด (CCTV) ข้อมูลชีวภาพ ข้อมูลตำแหน่งที่ตั้ง การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรงโดยเฉพาะการโฆษณาตามพฤติกรรมออนไลน์ (online behavioural advertising) และการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในบริบทของปัญญาประดิษฐ์ คุกกี้ ระบบคลาวด์ และการจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล โดยใช้กรณีศึกษาที่เกิดขึ้นในต่างประเทศและเพื่อนำมาปรับใช้ภายใต้บริบทของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย

การคุ้มครองข้อมูลส่วนบุคคลในบริบทของนายจ้างและลูกจ้าง

การประมวลผลข้อมูลส่วนบุคคลของลูกจ้างในสถานประกอบการ

เมื่อกล่าวถึงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในบริบทของการจ้างแรงงาน หลายคนมักจะคำนึงถึงเฉพาะในขั้นตอนของการประมวลผลข้อมูลส่วนบุคคล (data processing) ของลูกจ้างหรือผู้สมัครเข้าทำงานในขั้นตอนของการคัดสรรหรือการเข้าทำสัญญาเท่านั้น แต่ในความเป็นจริง ในการบริหารองค์กรและบริหารงานบุคคลต้องมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกจ้างในหลายกระบวนการและมีความต่อเนื่องตลอดระยะเวลาของการจ้างงาน เช่น การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อประเมินความสามารถของพนักงาน เพื่อความปลอดภัยในสถานที่ทำงาน และเพื่อปกป้องทรัพย์สินในสถานที่ทำงาน เป็นต้น

ด้วยความก้าวหน้าของเทคโนโลยีในปัจจุบัน นายจ้างสามารถนำเทคโนโลยีหลาย ๆ อย่างมาใช้ในสถานประกอบการหรือแม้กระทั่งใช้ติดตามดูพฤติกรรมของลูกจ้างได้ตลอดเวลา (monitoring & tracing) ทั้งในและนอกสถานประกอบการ และในหรือนอกเวลาทำงาน อาทิ ระบบกล้องวงจรปิด ระบบตรวจสอบอัตลักษณ์ของบุคคล ระบบ GPS สมาร์ทโฟน และระบบคอมพิวเตอร์ ฯลฯ ซึ่งกิจกรรมเหล่านี้ล้วนเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามความหมายของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยการดำเนินกิจกรรมลักษณะนี้ มักมีความเข้าใจว่าในฐานะของนายจ้างย่อมสามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกจ้างของตนได้บนฐานความยินยอม (consent ground) แต่หากตีความตามความหมายของบทบัญญัติมาตรา 19 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่บัญญัติไว้ว่าการขอความยินยอมนั้นผู้ควบคุมข้อมูลส่วนบุคคลต้องคำนึงถึงอย่างที่สุดในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม (freely given consent) ความยินยอมที่บุคคลที่มีความไม่เท่าเทียมกันในทางเศรษฐกิจหรืออำนาจต่อรองได้ให้ไว้หรือจำต้องให้ในสถานะดังกล่าว (ลูกจ้าง) จึงอาจมีคำถามตามมาได้ว่า กรณีนี้จะถือเป็นความยินยอมที่ชอบด้วยกฎหมายหรือไม่

การคุ้มครองข้อมูลส่วนบุคคลในบริบทของนายจ้างและลูกจ้าง

เมื่อพิจารณาจากบริบทข้างต้นจะเห็นได้ว่าการขอความยินยอมเพื่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกจ้าง โดยนายจ้างนั้นอาจไม่สามารถทำบนฐานความยินยอมได้ในหลาย ๆ กรณี เนื่องจากนายจ้างและลูกจ้างมีอำนาจการต่อรองที่ต่างกัน (different position of power) ดังนั้น การให้ความยินยอมของลูกจ้างหรือผู้สมัครงานต่อนายจ้างโดยธรรมชาติมักเป็นการให้ความยินยอมโดยปราศจากความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคล เนื่องจากความกังวลต่อผลเสียที่อาจจะตามมา เช่น ผลต่อการรับเข้าทำงาน ขึ้นเงินเดือนหรือตำแหน่ง เป็นต้น ดังนั้น การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกจ้างในการบริหารงานบุคคลจึงเป็นการดำเนินการบนฐานเพื่อประโยชน์โดยชอบด้วยกฎหมายของนายจ้าง (legitimate interest) ตามนัยของมาตรา 24 (5) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยต้องเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีขอบเขตอย่างชัดเจนและโปร่งใส (limiting to the process & transparency) มิฉะนั้น การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อประโยชน์ในการบริหารของนายจ้างก็อาจเป็นการละเมิดสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของลูกจ้างได้

การกำหนดมาตรการต่าง ๆ เพื่อประโยชน์ทางการบริหารของนายจ้างจำเป็นอย่างยิ่งที่จะต้องพิจารณาถึง 4 ประเด็นหลักดังนี้

1) ความจำเป็น (Processing activity is necessary)
2) วัตถุประสงค์มีความเป็นธรรมต่อลูกจ้าง (Fair to employees)
3) ได้สัดส่วนกับความเสี่ยงที่อาจจะเกิดขึ้น (Proportionate to the concerns raised)
4) ความโปร่งใส (Transparent)

การคุ้มครองข้อมูลส่วนบุคคลในบริบทของนายจ้างและลูกจ้าง

ดังนั้น เพื่อให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในองค์กรไม่สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 องค์กรจึงควรต้องพิจารณาถึงประเด็นสำคัญ 4 ประการดังนี้

1) สิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (fundamental rights)
2) ฐานความจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย (legitimate interest)
3) ความโปร่งใสของการประมวลผลข้อมูลส่วนบุคคล (transparency)
4) หลักความจำเป็นและความได้สัดส่วน (data minimization & proportionality)

การคุ้มครองข้อมูลส่วนบุคคลในบริบทของนายจ้างและลูกจ้าง

ฐานทางกฎหมายในการการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกจ้าง

การให้ความยินยอมของลูกจ้างหรือผู้สมัครงานต่อนายจ้างโดยธรรมชาติมักเป็นการให้ความยินยอมโดยปราศจากความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคล เนื่องจากความกังวลต่อผลเสียที่อาจจะตามมาเช่น ผลต่อการรับเข้าทำงาน ขึ้นเงินเดือนหรือตำแหน่ง เป็นต้น ด้วยเหตุผลความต่างในอำนาจต่อรองนี้เอง (Imbalance of power between data subject & data controller) ในทางปฏิบัติองค์กรหรือนายจ้างจึงควรจะหลีกเลี่ยงการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกจ้างโดยอาศัยฐานความยินยอม เนื่องจากอาจทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นการขอความยินยอมที่ไม่เป็นไปตามเงื่อนไขในมาตรา 19 วรรคหนึ่ง และอาจมีผลให้การขอความยินยอมดังกล่าวของนายจ้างไม่มีผลผูกพันเจ้าของข้อมูลส่วนบุคคล (ลูกจ้าง) และทำให้ผู้ควบคุมข้อมูลส่วนบุคคล (นายจ้าง) ไม่สามารถทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกจ้างได้โดยชอบด้วยกฎหมาย

เมื่อพิจารณาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ฐานทางกฎหมาย (lawful basis for processing of personal data) สำหรับกรณีของนายจ้างอาจจะมีได้อย่างน้อย 4 กรณี กล่าวคือ

(1) ฐานสัญญา (Contract) ตามมาตรา 24(3)

(2) ฐานความยินยอม (Consent) ตามมาตรา 19

(3) ฐานเพื่อประโยชน์โดยชอบด้วยกฎหมาย (Legitimate interest) ตามมาตรา 24(5)

(4) ฐานการปฏิบัติหน้าที่ตามกฎหมาย (Legal obligations) ตามมาตรา 24(6)

การคุ้มครองข้อมูลส่วนบุคคลในบริบทของนายจ้างและลูกจ้าง

เพื่อเป็นการหลีกเลี่ยงความเสี่ยงทางกฎหมายอันเนื่องมาจากความไม่แน่นอนของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลโดยอาศัยฐานความยินยอมเท่านั้น นายจ้างในฐานะผู้ควบคุมข้อมูลส่วนบุคคลควรเลือกการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลบนฐานทางกฎหมายอื่นข้างต้นประกอบด้วย แต่หลักการสำคัญที่นายจ้างพึงต้องตระหนักเสมอ คือ แม้ในกรณีที่กฎหมายอนุญาตให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้โดยไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก็ตาม (มาตรา 24 (5)) กรณีดังกล่าวต้องเป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล และผู้ควบคุมข้อมูลส่วนบุคคลพึงตระหนักว่าการดำเนินการดังกล่าวควรใช้ความระมัดระวังเป็นพิเศษเพื่อปกป้องประโยชน์และป้องกันผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลโดยตรงและหลีกเลี่ยงการใช้ข้อมูลเกินความคาดหวังปกติในบริบทของการดำเนินการตามปกติ หรือความคาดหวังโดยสุจริตของลูกจ้าง

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยอ้างฐานความชอบด้วยกฎหมายนายจ้างจึงต้องคำนึงถึงหลักความได้สัดส่วน (Proportionate principle) ระหว่างประโยชน์โดยชอบด้วยกฎหมายของนายจ้างและสิทธิขั้นพื้นฐานของลูกจ้าง ซึ่งสิทธิในที่นี้หมายถึงสิทธิขั้นพื้นฐานและความเป็นอิสระของบุคคลเป็นสำคัญ และในทางปฏิบัติการกล่าวอ้างเพียงเพื่อประโยชน์ในการแข่งขันหรือประโยชน์ทางธุรกิจของนายจ้างเท่านั้น อาจจะไม่เพียงพอต่อการอ้างเพื่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 24 (5)

การคุ้มครองข้อมูลส่วนบุคคลในบริบทของนายจ้างและลูกจ้าง

ดังนั้น การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่กระทำโดยนายจ้างจึงต้องกระทำบนฐานความชอบด้วยกฎหมาย (Lawfulness) โดยเป็นธรรม (Fairness) และโปร่งใส (Transparency) ในการใช้เทคโนโลยีในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและการวางมาตรการเกี่ยวกับการกำกับดูแลลูกจ้างหรือกิจการใด ๆ ที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกจ้างต้องทำโดยมีวัตถุประสงค์ที่เหมาะสม ชัดเจนและได้สัดส่วนต่อความเสี่ยงหรือความต้องการของกิจการนั้น ๆ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยอาศัยฐานเพื่อประโยชน์โดยชอบด้วยกฎหมายนี้ลูกจ้างมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล หรือขอให้ผู้ควบคุมข้อมูลส่วนบุคคล (นายจ้าง) ดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้อีกด้วย (มาตรา 32 และ 33)

การคุ้มครองข้อมูลส่วนบุคคลในบริบทของนายจ้างและลูกจ้าง

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในบริบทของการจ้างงานนั้นถือเป็นประเด็นที่ละเอียดอ่อนและมีความซับซ้อนอย่างมาก โดย European Data Protection Board (EDPB) ได้แบ่งประเด็นและขั้นตอนต่าง ๆ ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่กระทำโดยนายจ้างไว้ถึง 9 กรณีดังต่อไปนี้

(1) ระหว่างการสรรหาพนักงาน
(2) ข้อมูลบนโซเชียลมีเดียของผู้สมัครงาน
(3) ข้อมูลการใช้งานในระบบเทคโนโลยีสารสนเทศของพนักงานในที่ทำงาน
(4) ข้อมูลการใช้งานบนระบบเทคโนโลยีสารสนเทศของพนักงานนอกสถานที่ทำงาน
(5) ข้อมูลเกี่ยวกับระยะเวลาและการเข้างาน
(6) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจากระบบกล้องวงจรปิด
(7) ข้อมูลเกี่ยวกับการใช้ยานพาหนะของพนักงาน
(8) การเปิดเผยข้อมูลของพนักงานต่อบุคคลที่สาม
(9) การส่งหรือโอนข้อมูลส่วนบุคคลของพนักงานไปยังต่างประเทศ

ในการใช้ฐานประโยชน์โดยชอบด้วยกฎหมายของนายจ้างในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกจ้าง ต้องเป็นไปตาม “หลักความได้สัดส่วน” ในบริบทของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยสามารถ (1) การชั่งน้ำหนักระหว่างประโยชน์สาธารณะอื่น ๆ (ถ้ามี) (2) ประโยชน์โดยชอบด้วยกฎหมายของนายจ้าง และ (3) การคุ้มครองสิทธิขั้นพื้นฐานของลูกจ้างที่มีความหมายกว้างกว่าการคุ้มครองความเป็นส่วนตัวของข้อมูลส่วนบุคคลเท่านั้น

การคุ้มครองข้อมูลส่วนบุคคลในบริบทของนายจ้างและลูกจ้าง

ความยินยอมของลูกจ้าง

หลักความชอบด้วยกฎหมาย ความเป็นธรรมและความโปร่งใสของการบริหารจัดการข้อมูล (Lawfulness, Fairness and Transparency) เป็นหนึ่งในหลักการพื้นฐานที่สำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคล หลักการดังกล่าวกำหนดให้องค์กรจะต้องมีฐานทางกฎหมายฐานใดฐานหนึ่ง มีวัตถุประสงค์ที่จำกัด มีการแจ้งวัตถุประสงค์โดยชอบด้วยกฎหมาย และแจ้งอย่างโปร่งใสและเป็นธรรมผ่านช่องทางของประกาศการคุ้มครองข้อมูลส่วนบุคคล (Privacy Notice) หรือวิธีการอื่น ๆ ที่เหมาะสม อีกทั้งต้องบันทึกฐานทางกฎหมายดังกล่าวไว้เพื่อการตรวจสอบด้วย

ความยินยอม (Consent) เป็นฐานทางกฎหมายหนึ่งในหลาย ๆ ฐานที่ถูกเข้าใจผิดบ่อย ๆ ว่าหากได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลแล้ว องค์กรจะสามารถดำเนินการต่าง ๆ กับข้อมูลส่วนบุคคลได้โดยปราศจากความรับผิด ซึ่งหากพิจารณาจากบทบัญญัติในมาตรา 19 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะพบว่าในบรรดาเงื่อนไขต่าง ๆ ของการขอและการได้มาซึ่งความยินยอมมีอยู่ประการหนึ่ง ได้แก่ “หลักความเป็นอิสระ” ที่กำหนดให้ความยินยอมจะชอบด้วยกฎหมายก็ต่อเมื่อเจ้าของข้อมูลส่วนบุคคลให้ความยินยอมโดยสมัครใจและอิสระ (freely given) โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม

การคุ้มครองข้อมูลส่วนบุคคลในบริบทของนายจ้างและลูกจ้าง

มาตรา 19 และแนวทางในการขอความยินยอมฯ ดังกล่าวตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สอดคล้องกับบทบัญญัติของ GDPR และ EDPB Guidelines 05/2020 โดยเฉพาะข้อจำกัดของการใช้ฐานความยินยอมสำหรับการดำเนินงานภาครัฐในส่วนที่เกี่ยวข้องกับการจัดทำบริการสาธารณะและความยินยอมในบริบทความสัมพันธ์ของนายจ้าง-ลูกจ้าง เนื่องจากการขาดองค์ประกอบของ “ความเป็นอิสระอย่างแท้จริง” ในการให้หรือไม่ให้ความยินยอมอันเนื่องมากจากความไม่เท่าเทียมกันของอำนาจในการต่อรอง (imbalance of power) EDPB Guidelines 05/2020 ยังให้ข้อสังเกตว่าการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลส่วนใหญ่ในบริบทของการจ้างงาน ฐานทางกฎหมายจึงไม่ควรใช้ “ความยินยอม”

ทั้งนี้ในทางปฏิบัติ นายจ้างสามารถกำกับตรวจสอบหรือใช้ข้อมูลต่าง ๆ ของลูกจ้างเพื่อให้บรรลุวัตถุประสงค์ตามสัญญาจ้างได้โดยอาศัยความผูกพันตามสัญญาจ้างแรงงาน หรือหากมีความจำเป็นต้องติดตามพฤติกรรมการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อวัตถุประสงค์ด้านความปลอดภัยในระบบสารสนเทศขององค์กรซึ่งเป็นประโยชน์โดยชอบด้วยกฎหมายขององค์กร เป็นต้น นายจ้างก็มีฐานทางกฎหมายในการดำเนินการแล้วโดยที่ไม้ต้องบังคับขอความยินยอม

การคุ้มครองข้อมูลส่วนบุคคลในบริบทของนายจ้างและลูกจ้าง

อย่างไรก็ตามมาตรา 19 วรรคสี่ ตอนท้ายกำหนดว่า ทั้งนี้ ในการเข้าทำสัญญาซึ่งรวมถึงการให้บริการใด ๆ ต้องไม่มีเงื่อนไขในการให้ความยินยอมเพื่อเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่มีความจำเป็นหรือเกี่ยวข้องสำหรับการเข้าทำสัญญาซึ่งรวมถึงการให้บริการนั้น ๆ ซึ่งหมายความว่าหากกรณีมีความจำเป็นตามสัญญาหรือการให้บริการใด ๆ ผู้ควบคุมข้อมูลส่วนบุคคลก็อาจจะขอความยินยอมแบบบังคับได้ ดังมีตัวอย่างในกรณีความเห็นของคณะอนุกรรมการเฉพาะกิจตอบข้อหารือฯ ในคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ในกรณีที่หน่วยงานของรัฐจัดสวัสดิการเกี่ยวกับการรักษาพยาบาลหรือสวัสดิการสุขภาพโดยใช้การประกันภัยแบบกลุ่ม (group insurance) และจะต้องเปิดเผยข้อมูลส่วนบุคคลเกี่ยวกับข้อมูลสุขภาพให้กับบริษัทตามกฎหมายว่าด้วยการประกันชีวิตหรือกฎหมายว่าด้วยการประกันวินาศภัย (“บริษัทประกันภัย”) ในฐานะที่บริษัทประกันภัยดังกล่าวเป็นผู้ควบคุมข้อมูลส่วนบุคคล เพื่อการเบิกจ่ายค่าใช้จ่ายที่เป็นสวัสดิการเกี่ยวกับการรักษาพยาบาลหรือสวัสดิการสุขภาพดังกล่าว การเปิดเผยข้อมูลส่วนบุคคลเกี่ยวกับข้อมูลสุขภาพดังกล่าวให้กับบริษัทประกันภัย และการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับสุขภาพของบริษัทประกันภัยนั้น จะไม่ได้รับยกเว้นการขอความยินยอมโดยชัดแจ้งตามมาตรา 26 (5) (ค) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และจะต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลตามมาตรา 26 เนื่องจากเป็นการเปิดเผยข้อมูลส่วนบุคคลเกี่ยวกับข้อมูลสุขภาพให้กับบุคคลอื่น (บริษัทประกันภัย) ที่มิใช่เป็นการจำเป็นในการปฏิบัติตามกฎหมายโดยตรง แต่การขอความยินยอมในกรณีการจัดสวัสดิการเกี่ยวกับการรักษาพยาบาลหรือสวัสดิการสุขภาพโดยใช้การประกันภัยแบบกลุ่ม (group insurance) ดังกล่าว อาจถือเป็นส่วนหนึ่งของการจัดสวัสดิการที่จำเป็นของหน่วยงานของรัฐที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลได้ ดังนั้น หากหน่วยงานนั้นเห็นว่ามีความจำเป็นและสมควร อาจกำหนดเงื่อนไขว่าในการเข้าทำสัญญาเป็นบุคลากรของหน่วยงาน หรือในการขอเบิกเงินสวัสดิการเกี่ยวกับการรักษาพยาบาลหรือสวัสดิการสุขภาพแต่ละครั้ง บุคลากรผู้มีสิทธิตามสวัสดิการดังกล่าว หรือบุคคลในครอบครัว จะต้องให้ความยินยอมเพื่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลให้กับ/โดยบริษัทประกันภัย เนื่องจากมีความจำเป็นหรือเกี่ยวข้องสำหรับการเข้าทำสัญญาหรือการเบิกจ่ายเงินสวัสดิการนั้น ซึ่งเป็นไปตามมาตรา 19 วรรคสี่ได้

การคุ้มครองข้อมูลส่วนบุคคลในบริบทของนายจ้างและลูกจ้าง

Work From Home กับมาตรการรักษาความมั่นคงปลอดภัยขององค์กร

Work from home (WFH) หรือการทำงานจากที่บ้านเป็นรูปแบบการทำงานที่บุคคลสามารถปฏิบัติงานได้จากที่พักอาศัยของตนเอง แทนที่จะต้องเดินทางไปที่สำนักงานหรือสถานที่ทำงานตามปกติ การทำงานในลักษณะนี้มักใช้เทคโนโลยีการสื่อสารเช่นอินเทอร์เน็ต อีเมล ซอฟต์แวร์ประชุมทางไกล เพื่อให้สามารถทำงานและติดต่อกับทีมงานหรือผู้เกี่ยวข้องได้อย่างต่อเนื่อง

การทำงานจากที่บ้านได้รับความนิยมมากขึ้น โดยเฉพาะในช่วงที่มีการแพร่ระบาดของ COVID-19 เนื่องจากช่วยลดการเดินทางและลดความเสี่ยงต่อการติดเชื้อ นอกจากนี้ยังช่วยให้มีความยืดหยุ่นในการจัดการเวลาและสถานที่ทำงานมากขึ้น จนถึงวันนี้ WFH เริ่มกลายเป็นภาวะปกติของการทำงานในหลายองค์กร ด้วยเทคโนโลยีที่พัฒนาก้าวหน้าอย่างรวดเร็ว ไม่ว่าจะเป็นการประชุมผ่านระบบวิดีโอ การพูดคุยแลกเปลี่ยนผ่านช่องทางสื่อสารออนไลน์ ส่งผลให้ WFH เป็นเรื่องที่มีความยืดหยุ่นและสร้างความสะดวกสบายสำหรับองค์กรและพนักงาน

การที่องค์กรมีนโยบายให้พนักงานสามารถ WFH ได้ นำมาซึ่งความท้าทายของการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลขององค์กร เพราะองค์กรยังคงมีหน้าที่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยเฉพาะอย่างยิ่งในส่วนหน้าที่ของการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสมเพื่อธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคลไม่ว่าข้อมูลเหล่านั้นจะถูกใช้จากภายในองค์กรหรือถูกใช้โดยรีโมทหรือเข้าถึงจากระบบภายนอกก็ตาม

การคุ้มครองข้อมูลส่วนบุคคลในบริบทของนายจ้างและลูกจ้าง

อย่างไรก็ตาม แม้องค์กรจะจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยซึ่งเป็นไปตามที่กล่าวมาแล้วข้างต้น แต่หากผู้บริหาร พนักงาน ลูกจ้าง หรือบุคลากรภายในองค์กรขาดซึ่งความตระรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย (Privacy and security awareness) การ WFH ก็ยังมีความเสี่ยงที่อาจก่อให้เกิดเหตุการละเมิดข้อมูลส่วนบุคคลและองค์กรยังคงมีความรับผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

การเฝ้าระวัง (surveillance) และระบบกล้องวงจรปิด

การเฝ้าระวังหรือการสอดแนม

Surveillance (การเฝ้าระวังหรือการสอดแนม) หมายถึง การติดตามหรือสังเกตการณ์พฤติกรรม กิจกรรม หรือข้อมูลของบุคคลหรือกลุ่มบุคคล ซึ่งมักทำเพื่อรวบรวมข้อมูลหรือเฝ้าระวังความปลอดภัย การเฝ้าระวังอาจมีรูปแบบหลายอย่าง เช่น การใช้กล้องวงจรปิด (CCTV) การติดตามการสื่อสารทางโทรศัพท์หรืออินเทอร์เน็ต การเฝ้าระวังทางกายภาพ หรือการรวบรวมข้อมูลส่วนบุคคลผ่านระบบดิจิทัล

การเฝ้าระวังสามารถทำได้โดยองค์กรของรัฐ บริษัทเอกชน หรือบุคคลทั่วไป และมีวัตถุประสงค์หลายอย่าง เช่น ป้องกันอาชญากรรม รักษาความปลอดภัย การสืบสวน หรือเพื่อวัตถุประสงค์ทางการตลาด ในขณะเดียวกันก็มีข้อกังวลเกี่ยวกับสิทธิในความเป็นส่วนตัวและเสรีภาพของบุคคลเนื่องจากการเฝ้าระวังที่มากเกินไป

การสอดส่องข้อมูลหรือการใช้มาตรการเฝ้าระวังโดยรัฐเป็นประเด็นที่อาจมีการพูดถึงและวิพากษ์วิจารณ์มาเป็นระยะเวลายาวนานโดยนักสิทธิมนุษยชน และมีการตรากฎหมายและตีความกฎหมายเพื่อกำหนดเงื่อนไขในการจำกัดอำนาจในการใช้มาตรการเฝ้าระวังหรือสอดแนมข้อมูลของปัจเจกชนโดยรัฐ โดยเฉพาะในประเทศตะวันตกที่ให้คุณค่าของความเป็นส่วนตัวมากกว่าในสังคมตะวันออก

การเฝ้าระวัง (surveillance) และระบบกล้องวงจรปิด

การเฝ้าติดตามพฤติกรรมของพนักงาน

ในปัจจุบัน แม้ว่านายจ้างหรือผู้ว่าจ้างมีเครื่องมือหลายอย่างในการตรวจสอบและติดตามการทำงานของลูกจ้างหรือผู้รับจ้างว่าเป็นไปตามเงื่อนไขของการจ้างหรือไม่ “การเฝ้าติดตามพฤติกรรมของพนักงาน” โดยการใช้ระบบกล้องวงจรปิดหรือเทคโนโลยีอื่น ๆ ก็อาจจำเป็นต้องมีการทบทวนถึงความชอบด้วยกฎหมายอีกครั้ง ซึ่งในยุโรปมีคดีที่เกี่ยวเนื่องกับการเฝ้าติดตามพฤติกรรมของพนักงานหลาย ๆ คดีที่อาจนำมาเป็นกรณีศึกษาสำหรับการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ โดยสองกรณีศึกษานี้เป็นคดีที่ตัดสินโดยศาลสิทธิมนุษยชนยุโรป (European Court of Human Rights, “ECtHR”) ตามมาตรา 8 ของอนุสัญญายุโรปว่าด้วยสิทธิมนุษยชน (European Convention on Human Rights, “ECHR”) เรื่องสิทธิในความเป็นส่วนตัว

การเฝ้าระวัง (surveillance) และระบบกล้องวงจรปิด

ระบบกล้องวงจรปิด

ระบบกล้องวงจรปิด (CCTV) ที่มีการบันทึกภาพและวิดีโอถือจึงถือว่าเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และต้องปฏิบัติให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อย่างน้อยดังต่อไปดังนี้

1) มีฐานทางกฎหมายในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ประโยชน์ที่ชอบด้วยกฎหมาย: องค์กรต้องมีเหตุผลที่ชัดเจนและชอบด้วยกฎหมายในการใช้ CCTV เช่น เพื่อความปลอดภัย หรือการป้องกันอาชญากรรม

ความจำเป็นและความเหมาะสม: การใช้ CCTV ต้องมีความจำเป็นสำหรับวัตถุประสงค์ที่กำหนด

2) ความโปร่งใสและการแจ้งเตือน

ป้ายแจ้งเตือน: ต้องติดตั้งป้ายที่ชัดเจนและมองเห็นได้ง่ายเพื่อแจ้งให้บุคคลทราบว่ามีการใช้ CCTV รวมถึงวัตถุประสงค์และข้อมูลการติดต่อของผู้ควบคุมข้อมูลส่วนบุคคล

ประกาศความเป็นส่วนตัว : ให้ข้อมูลที่เข้าถึงได้ง่ายเกี่ยวกับวิธีการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลจากระบบกล้องวงจรปิด

3) ขอบเขตของวัตถุประสงค์

การใช้เฉพาะเจาะจง: ใช้ข้อมูลจาก CCTV เฉพาะสำหรับวัตถุประสงค์ที่ระบุไว้เท่านั้น ห้ามนำไปใช้ในกิจกรรมอื่น ๆ โดยไม่ได้รับความยินยอม เว้นแต่เป็นกรณีที่มีกฎหมายอนุญาตให้กระทำได้

การเฝ้าระวัง (surveillance) และระบบกล้องวงจรปิด

4) การเก็บข้อมูลให้น้อยที่สุดเท่าที่จำเป็น (Data Minimization)

จำกัดพื้นที่การบันทึก: ติดตั้งกล้องเพื่อครอบคลุมเฉพาะพื้นที่ที่จำเป็น หลีกเลี่ยงการบันทึกพื้นที่ส่วนตัวหรือการครอบคลุมที่เกินความจำเป็นหลีกเลี่ยงการบันทึกเสียง: การบันทึกเสียงถือว่าละเมิดความเป็นส่วนตัวมากกว่าภาพวิดีโอ ควรหลีกเลี่ยงหากไม่จำเป็น

5) นโยบายการเก็บรักษาข้อมูลส่วนบุคคล

ระยะเวลาการเก็บรักษา: กำหนดและบันทึกระยะเวลาที่จะเก็บข้อมูลจาก CCTV ที่ชัดเจน เช่น 30 วัน และลบหรือทำให้ข้อมูลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้

การทบทวน: ประเมินความเหมาะสมของระยะเวลาเก็บรักษาอย่างสม่ำเสมอ

6) มาตรการรักษาความมั่นปลอดภัย

การควบคุมการเข้าถึง: จำกัดการเข้าถึงข้อมูลจาก CCTV เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น

มาตรการเชิงเทคนิค: ใช้การเข้ารหัสและมาตรการทางเทคโนโลยีเพื่อป้องกันการละเมิดข้อมูลข้อมูลส่วนบุคคล

7) สิทธิของเจ้าของข้อมูลส่วนบุคคล

สิทธิในการขอเข้าถึง: เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนเอง

สิทธิในการลบ: ภายใต้เงื่อนไขตามกฎหมาย เจ้าของข้อมูลส่วนบุคคลสามารถขอให้ลบข้อมูลส่วนบุคคลของตนได้

กระบวนการตอบสนอง: จัดทำขั้นตอนในการตอบสนองต่อคำขอของเจ้าของข้อมูลส่วนบุคคลภายในระยะเวลาที่กฎหมายกำหนด เช่น ภายใน 30 วัน ในกรณีการขอเข้าถึง และภายใน 90 วัน ในกรณีการขอให้ลบข้อมูลส่วนบุคคล

การเฝ้าระวัง (surveillance) และระบบกล้องวงจรปิด

8) ผู้ประมวลผลข้อมูลส่วนบุคคล

การปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562: ตรวจสอบให้แน่ใจว่าผู้ให้บริการและขอบเขตงานที่จ้างจำเป็นต้องจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคลหรือไม่

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล: ทำข้อตกลงที่ระบุความรับผิดชอบและข้อกำหนดตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

9) ความรับผิดชอบและการบันทึกข้อมูล

การเก็บบันทึกรายการกิจกรรม: รักษาบันทึกรายกิจกรรมเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลผลที่เกี่ยวข้องกับการใช้ CCTV

นโยบายและขั้นตอน: พัฒนานโยบายภายในที่ชัดเจนสำหรับการดำเนินงานของระบบ CCTV และการจัดการข้อมูลส่วนบุคคล

การปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับระบบ CCTV ต้องมีการพิจารณาอย่างรอบคอบเกี่ยวกับสิทธิความเป็นส่วนตัว การปฏิบัติที่โปร่งใส และมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

การเฝ้าระวัง (surveillance) และระบบกล้องวงจรปิด

ข้อมูลชีวภาพ

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 วรรคสอง “ข้อมูลชีวภาพ”หมายถึง ข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือข้อมูลจำลองลายนิ้วมือ

ตัวอย่างของข้อมูลชีวภาพ ได้แก่

(1) ข้อมูลจำลองลายนิ้วมือ: รูปแบบของลายบนปลายนิ้วที่เป็นเอกลักษณ์เฉพาะบุคคล

(2) ข้อมูลภาพจำลองใบหน้า: โครงสร้างและลักษณะของใบหน้าที่สามารถใช้ในการยืนยันตัวตน

(3) ข้อมูลจำลองม่านตา: รูปแบบของม่านตาหรือเรตินาที่ไม่ซ้ำกัน

(4) เสียง: ลักษณะของเสียงที่สามารถใช้ในการระบุบุคคล

(5) รูปแบบการเดิน: วิธีการเดินหรือการเคลื่อนไหวที่เป็นลักษณะเฉพาะ

การเฝ้าระวัง (surveillance) และระบบกล้องวงจรปิด

(1) กรณีศึกษาการใช้ข้อมูลภาพจำลองใบหน้า

Clearview AI ได้ชื่อว่าเป็นผู้ให้บริการ FRT ที่อาจเข้ามาเปลี่ยนแปลงชีวิตและความเป็นส่วนตัวของทุกคนอย่างมีนัยสำคัญ บริษัทนี้เป็นเจ้าของเทคโนโลยีการจดจำใบหน้าอัจฉริยะและการประมวลผลจาก big data บริษัทได้เข้ามามีบทบาทในการช่วยเจ้าหน้าที่ตำรวจในการค้นหาผู้กระทำความผิด โดยมีข้อมูลปรากฏว่ามีหน่วยงานในกระบวนการยุติธรรมทางอาญาและบังคับใช้กฎหมายรวมกว่า 2,200 องค์กร ใน 27 ประเทศทั่วโลก (ที่มา: BuzzFeed News Review) ได้นำเทคโนโลยีของ Clearview AI ไปใช้ในงานด้านการป้องกันและปราบปรามการกระทำความผิด

ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปหรือ GDPR “ข้อมูลภาพจำลองใบหน้า” ที่ทำโดยระบบคอมพิวเตอร์หรือ AI เข้าข่ายการเป็นข้อมูลกลุ่มพิเศษที่ GDPR และกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศในสหภาพยุโรปให้ความสำคัญอย่างมาก ในขณะที่กรอบนโยบายทางกฎหมายเฉพาะในส่วนที่เกี่ยวกับการบังคับใช้กฎหมายและกระบวนการยุติธรรมทางอาญาที่เกี่ยวเนื่องกับการประมวลผลข้อมูลส่วนบุคคลถูกกำหนดไว้ใน Law Enforcement Directive (Directive (EU) 2016/680) ซึ่งเป็นกฎหมายที่ออกมาพร้อมกับ GDPR ก็ยิ่งทำให้การใช้ประโยชน์จากเทคโนโลยีของ Clearview AI มีข้อจำกัดมากยิ่งขึ้น

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 บทบัญญัติห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับข้อมูลชีวภาพ (ซึ่งรวมถึงข้อมูลภาพจำลองใบหน้า) โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลเช่นเดียวกัน แต่มาตรา 4 (5) ได้กำหนดยกเว้นไม่ให้ใช้กฎหมายบังคับกับการดำเนินงานตามกระบวนการยุติธรรมทางอาญา เพียงแต่กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานด้วยเท่านั้น

การเฝ้าระวัง (surveillance) และระบบกล้องวงจรปิด

(2) การเฝ้าติดตามพฤติกรรมโดยใช้ข้อมูลภาพจำลองใบหน้า

กรณีการจับผิดตัวในสหรัฐอเมริกา

ในเดือนมกราคม 2563 ชายคนหนึ่งถูกตำรวจเมืองดีทรอยต์จับกุมเนื่องจากเป็นผู้ต้องสงสัยในคดีลักทรัพย์ที่เกิดขึ้นในปี 2561 ซึ่งสาเหตุการจับกุมดังกล่าวเกิดจากการที่ตำรวจใช้ FRT ในการช่วยประมวลหาภาพผู้ต้องสงสัยตามที่ปรากฏในระบบ CCTV ของร้านที่ถูกปล้น ซึ่งผลการจับคู่โดยระบบ FRT ซึ่งทางตำรวจเมืองดีทรอยต์นำมาใช้ประมวลผลโดยเทียบกับภาพถ่ายต่าง ๆ และพบว่าภาพใบอนุญาตขับขี่รถยนต์ของผู้ต้องสงสัยในคดีนี้ตรงกับภาพถ่ายของภาพผู้ต้องสงสัย เขาจึงถูกจับกุมและคุมขัง แต่ภายหลังการสอบสวนปรากฏว่าเป็นการจับผิดตัวเนื่องจากการทำงานผิดพลาดในการประมวลผลของระบบ FRT (false FRT match) เขาจึงได้รับการปล่อยตัวในที่สุด

การเฝ้าระวัง (surveillance) และระบบกล้องวงจรปิด

ดังนั้น ข้อมูลส่วนบุคคลซึ่งโดยธรรมชาติมีความอ่อนไหวโดยเฉพาะอย่างยิ่งที่เกี่ยวข้องกับสิทธิและเสรีภาพขั้นพื้นฐานของบุคคล (special categories of personal data/sensitive information) ควรได้รับการคุ้มครองที่เฉพาะเจาะจงมากขึ้น เนื่องจากบริบทของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเหล่านี้อาจก่อให้เกิดความเสี่ยงอย่างมีนัยสำคัญต่อสิทธิและเสรีภาพขั้นพื้นฐานของบุคคล ซึ่งข้อมูลส่วนบุคคลเหล่านี้ได้แก่ ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน เป็นต้น และสำหรับในยุคเทคโนโลยีเปลี่ยนโลก ข้อมูลพันธุกรรม ข้อมูลชีวภาพ ก็ได้ถูกจัดเข้ามาเป็นส่วนหนึ่งของข้อมูลที่ควรต้องได้รับการคุ้มครองเป็นพิเศษ และการเก็บรวบรวม ใช้ ข้อมูลเหล่านี้โดยไม่ชอบด้วยกฎหมาย ก็อาจนำมาซึ่งความเสียหายอย่างร้ายแรงต่อสิทธิและเสรีภาพของบุคคล ซึ่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ก็ได้บัญญัติรองรับหลักการดังกล่าวไว้ในมาตรา 26

อย่างไรก็ตาม มาตรา 4(5) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดยกเว้นไม่ให้นำบทบัญญัติแห่งพระราชบัญญัตินี้ไปใช้ในการดำเนินงานตามกระบวนการยุติธรรมทางอาญา แต่ยังคงกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลที่ได้รับยกเว้นดังกล่าวต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานด้วย

การเฝ้าระวัง (surveillance) และระบบกล้องวงจรปิด

ข้อมูลตำแหน่งที่ตั้ง (Geolocation)

เทคโนโลยีในการติดตามตำแหน่งที่ตั้งของบุคคล (Location tracking tools) เป็นที่ใช้กันอย่างแพร่หลายในการวิเคราะห์การตลาด และช่วยในการนำเสนอสินค้าหรือบริการได้อย่างตรงกลุ่มเป้าหมาย การใช้ข้อมูลตำแหน่งที่ตั้งของบุคคลในบางบริบทอาจสามารถระบุถึงตัวบุคคล (Individual) ได้และทำให้ข้อมูลนั้นมีสภาพเป็น “ข้อมูลส่วนบุคคล” ที่กฎหมายมุ่งคุ้มครอง

หากพิจารณาจากกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลไม่ว่าจะเป็น GDPR หรือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ฐานทางกฎหมาย (Lawful basis) ที่ทำให้องค์กรสามารถการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลประเภทข้อมูลตำแหน่งที่ตั้งได้โดยชอบนั้นอาจทำโดยอาศัยฐาน “ความยินยอม” (Consent base) เป็นหลัก

การเฝ้าระวัง (surveillance) และระบบกล้องวงจรปิด

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยอาศัยฐานความยินยอมนั้นถือว่าเป็นฐานที่ไม่ยุ่งยากและมีความซับซ้อนน้อยเมื่อเทียบกับการใช้ฐานทางกฎหมายอื่น ๆ ดังนั้น องค์กรจำนวนมากที่ต้องการการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตำแหน่งที่ตั้งของลูกค้าหรือผู้ใช้บริการจึงมักจะดำเนินการโดยจัดให้มีการขอความยินยอมบนหน้าเว็บไซต์หรือแอปพลิเคชันของตนและเพื่อเป็นการลดความเสี่ยงต่อการละเมิดกฎหมายคุ้มครองข้อมูลส่วนบุคคล อย่างไรก็ตาม ความยินยอมมีข้อจำกัดที่ต้องดำเนินการให้เหมาะสมดังนี้

1) เจ้าของข้อมูลส่วนบุคคลต้องให้ความยินยอมอย่างอิสระ กล่าวคือ การที่องค์กรรายใดรายหนึ่งในฐานะผู้ควบคุมข้อมูลส่วนบุคคลจะการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยอาศัยความยินยอมนั้น อำนาจในการต่อรองของทั้งสองฝ่ายควรมีเท่ากันและมีความอิสระในการเลือกตัดสินใจที่จะให้หรือไม่ให้ความยินยอม กรณีผู้ควบคุมข้อมูลส่วนบุคคลมีอำนาจต่อรองที่เหนือกว่าเจ้าของข้อมูลส่วนบุคคล (misbalancing power) เช่น ความสัมพันธ์ระหว่างนายจ้างกับลูกจ้าง นายจ้างในฐานะผู้ควบคุมข้อมูลส่วนบุคคลย่อมไม่สามารถอ้างฐานความยินยอมในการประมวลผลข้อมูลส่วนบุคคลของลูกจ้างได้ เนื่องจากโดยสภาพนายจ้างมีอำนาจต่อรองที่เหนือกว่าลูกจ้าง เพราะการตัดสินใจบางอย่างของลูกจ้างต่อนายจ้างอาจส่งผลต่อเรื่องของเงินเดือน รวมถึงสิทธิประโยชน์ต่าง ๆ ของตัวลูกจ้างในอนาคต ลูกจ้างจึงไม่อยู่ในฐานะที่จะให้หรือปฏิเสธการให้ความยินยอมต่อนายจ้างได้อย่างอิสระ ความสัมพันธ์ลักษณะนี้จึงไม่อาจใช้ฐานความยินยอมในการประมวลผลข้อมูลส่วนบุคคลได้

การเฝ้าระวัง (surveillance) และระบบกล้องวงจรปิด

2) การขอความยินยอมต้องทำอย่างเฉพาะเจาะจง การขอความยินยอมนั้นต้องระบุวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับมาจากการขอความยินยอมของเจ้าของข้อมูลส่วนบุคคลอย่างเฉพาะเจาะจงตามที่แจ้งไว้กับเจ้าของข้อมูลส่วนบุคคลเท่านั้น ตัวอย่างเช่น บริษัทประกันภัยทำการขอความยินยอมจากลูกค้าเพื่อใช้ข้อมูลส่วนบุคคลของลูกค้าในการประเมินความเสี่ยงเช่นนี้ บริษัทควรแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบด้วยว่าข้อมูลดังกล่าวจะถูกใช้เพื่อการนี้เท่านั้น รวมถึงผลกระทบจากการดำเนินการนี้อาจมีผลต่อการคิดคำนวณเบี้ยประกันรวมถึงสิทธิในกรมธรรม์ เป็นต้น

3) เจ้าของข้อมูลส่วนบุคคลควรได้รับการแจ้งรายละเอียดและวัตถุประสงค์ เจ้าของข้อมูลส่วนบุคคลต้องได้รับข้อมูลอย่างเพียงพอและชัดเจนเพื่อใช้ประกอบการตัดสินใจในการให้หรือไม่ให้ความยินยอมแก่ผู้ควบคุมข้อมูลส่วนบุคคล เป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลที่จะต้องให้ข้อมูลเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่จะเกิดขึ้นและวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น ๆ ซึ่งการแจ้งดังกล่าวจะสอดคล้องกับหลักความเป็นธรรมและโปร่งใส (fair & transparent processing) ที่ถือเป็นหลักการพื้นฐานของกฎหมายว่าด้วยการข้อมูลส่วนบุคคลทั้งในส่วนของ GDPR และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

การเฝ้าระวัง (surveillance) และระบบกล้องวงจรปิด

4) ภาษาที่ใช้ในการขอความยินยอมต้องมีความชัดเจนไม่คลุมเครือ เป็นลายลักษณ์อักษรสำหรับเจ้าของข้อมูลส่วนบุคคล และมีช่องทางในการจัดเก็บหรือทำบันทึกเพื่อให้สามารถใช้ในการยืนยันได้ว่าเจ้าของข้อมูลส่วนบุคคลที่ได้ให้ความยินยอมได้อ่านและทำความเข้าใจในเนื้อหาเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของตนแล้วจริง

5) การได้รับความยินยอมต้องถูกกระทำโดยได้รับการแถลงหรือยืนยันอย่างชัดเจน (consent must be granted in a “statement of a clear affirmative action”) การให้ความยินยอมของเจ้าของข้อมูลส่วนบุคคลนั้นต้องชัดเจนและมีความหมายไม่คลุมเครือ และช่องทางการให้ความยินยอมนั้นควรถูกออกแบบให้เจ้าของข้อมูลส่วนบุคคลเป็นผู้เลือกที่จะเข้าไปให้ความยินยอม (opt-in) ไม่ใช่การตั้งค่าไว้ให้เข้ามาถอนความยินยอม (opt-out)

นอกจากนี้ ในด้านการคุ้มครองความปลอดมั่นคงปลอดภัยของข้อมูลส่วนบุคคล การทำให้ข้อมูลตำแหน่งที่ตั้งเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ไม่ว่าจะโดยวิธีการทำให้เป็นข้อมูลแฝงหรือข้อมูลนิรนาม (pseudonymization / anonymization) จะช่วยทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นอยู่บนมาตรฐานด้านความมั่นคงปลอดภัยทางเทคนิคโดยวิธีการออกแบบมาตั้งแต่ต้น (privacy by design and by default) อีกด้วย ซึ่งเป็นประโยชน์ต่อทั้งองค์กรและเจ้าของข้อมูลส่วนบุคคล

การตลาดแบบตรง

การทำการตลาดแบบตรง

ให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

การทำการตลาดแบบตรงที่มีประสิทธิภาพมีความสำคัญอย่างยิ่งกับธุรกิจ โดยเมื่อองค์กรจะทำการตลาดแบบตรง องค์กรมีหน้าที่ต้องปฏิบัติให้สอดคล้องกับกฎหมายที่เกี่ยวข้อง อาทิ พระราชบัญญัติขายตรงและตลาดแบบตรง พ.ศ. 2545 พระราชบัญญัติคุ้มครองผู้บริโภค พ.ศ. 2522 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติขายตรงและตลาดแบบตรง พ.ศ. 2545 ให้บทนิยามของคำว่า **“ตลาดแบบตรง” คือ การทำตลาดสินค้าหรือบริการในลักษณะของการสื่อสารข้อมูลเพื่อเสนอขายสินค้าหรือบริการโดยตรงต่อผู้บริโภคซึ่งอยู่ห่างโดยระยะทางและมุ่งหวังให้ผู้บริโภคแต่ละรายตอบกลับเพื่อซื้อสินค้าหรือบริการจากผู้ประกอบธุรกิจตลาดแบบตรงนั้น**

การตลาดแบบตรง

ในการทำการตลาดแบบตรงให้สอดคล้องกับแนวทางสากลในการคุ้มครองข้อมูลส่วนบุคคล องค์กรอาจกำหนดการดำเนินการเป็น 4 ขั้นตอน ได้แก่

ขั้นตอนที่ 1 การระบุ (identify)

ขั้นตอนที่ 2 การวางแผน (plan)

ขั้นตอนที่ 3 การเก็บรวบรวม (collect)

ขั้นตอนที่ 4 การเคารพต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล (respect)

การตลาดแบบตรง

การกำหนดเป้าหมายการตลาดกับผู้ใช้สื่อสังคมออนไลน์

การให้บริการกำหนดกลุ่มเป้าหมาย (targeting service) โดยผู้ให้บริการสื่อสังคมออนไลน์ (social media providers) ทำให้องค์กรที่ต้องการกำหนดกลุ่มเป้าหมาย (targeters) สามารถสื่อสารข้อมูลต่าง ๆ ไปยังผู้ใช้บริการสื่อสังคมออนไลน์ (users) ได้อย่างมีประสิทธิภาพและตรงตามเป้าหมาย ไม่ว่าจะเป็นการสื่อสารข้อมูลด้านการตลาด ด้านการเมือง หรือวัตถุประสงค์อื่น ๆ ด้วยเทคโนโลยีและกระบวนการเพื่อช่วยในการกำหนดกลุ่มเป้าหมายมีความซับซ้อนและมีความแม่นยำมากขึ้นจากการเก็บรวบรวมข้อมูลส่วนบุคคลของผู้ใช้บริการโดยตรงผ่านการวิเคราะห์และการสังเคราะห์จากพฤติกรรมต่าง ๆ ที่ปรากฏในแพลตฟอร์มของผู้ให้บริการสื่อสังคมออนไลน์นั้นเองหรือโดยบุคคลที่สาม และผนวกเข้ากับข้อมูลส่วนบุคคลที่อาจจะได้มาจากแหล่งอื่น ๆ อาทิ จาก data brokers เป็นต้น

จากความแม่นยำของกระบวนการประมวลผลข้อมูลส่วนบุคคลดังกล่าวข้างต้น เมื่อพิจารณาในมิติของกฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้วอาจก่อให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของผู้ใช้บริการสื่อสังคมออนไลน์ได้อย่างกว้างขวาง ซึ่งความเสี่ยงส่วนใหญ่เกิดจากการประมวลผลข้อมูลส่วนบุคคลที่ขาดความโปร่งใสและปราศจากการควบคุมจากเจ้าของข้อมูลส่วนบุคคล (lack of transparency and users control of their personal data)

การตลาดแบบตรง

ในกระบวนการกำหนดเป้าหมายการตลาดกับผู้ใช้สื่อสังคมออนไลน์ อาจจำแนกกลุ่มบุคคลที่เข้ามาเกี่ยวข้องได้ 4 จำพวก ดังนี้

1) ผู้ใช้บริการสื่อสังคมออนไลน์ (users) ซึ่งมีสถานะเป็นเจ้าของข้อมูลส่วนบุคคลที่ข้อมูลถูกเก็บรวบรวม ใช้ หรือเปิดเผย

2) ผู้ให้บริการสื่อสังคมออนไลน์ (social media providers) ซึ่งเป็นเจ้าของแพลทฟอร์มผู้ให้บริการ ซึ่งนอกจากการให้บริการการเป็นสื่อสังคมออนไลน์โดยการมีระบบฐานข้อมูลสมาชิกแล้ว (account/profile) ผู้ให้บริการเหล่านี้ยังให้บริการในด้านการตลาดโดยการกำหนดเป้าหมายจากฐานข้อมูลของผู้ใช้สื่อสังคมออนไลน์อีกด้วย อาทิ Facebook, YouTube และ Twitter เป็นต้น

ผู้ให้บริการสื่อสังคมออนไลน์ สามารถการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ใช้บริการจากข้อมูลจำนวนมากที่เกี่ยวข้องกับเจ้าของข้อมูลส่วนบุคคลทั้งที่อาจได้รับมาโดยตรงหรือจากพฤติกรรมการใช้บริการ อาทิ การเลือกกดชื่นชอบ หรือการเลือกรับชมเนื้อหาต่าง ๆ ซึ่งผู้ให้บริการสื่อสังคมออนไลน์สามารถสร้างโปรไฟล์ลิ่ง (profiling) แล้วนำข้อมูลเหล่านี้ไปใช้ประมวลผลและสามารถกำหนดกลุ่มเนื้อหาที่ควรสื่อสาร (โฆษณา) ได้

3) Targeters อาจจะเป็นเจ้าของผลิตภัณฑ์โดยตรงหรืออาจจะเป็นตัวแทนด้านการโฆษณาของสินค้านั้น ๆ ก็ได้ โดย Targeters คือบุคคล/องค์กร ที่ต้องการสื่อสารข้อความใด ๆ ไปยังผู้ใช้บริการสื่อสังคมออนไลน์ตามค่าพื้นฐาน (parameter) หรือเกณฑ์เฉพาะบางประการที่กำหนดขึ้น

4) กลุ่มธุรกิจ Adtech ต่าง ๆ รวมถึงพวก data broker ต่าง ๆ

การตลาดแบบตรง

การโฆษณาตามพฤติกรรมออนไลน์ ปัญหา และข้อจำกัดทางกฎหมาย

(1) การโฆษณาออนไลน์

หน้าต่าง Pop-up ของหน้าเว็บไซต์ที่ขึ้นมาขณะกำลังเข้าใช้งานเว็บไซต์เพื่อให้กดยอมรับหรือไม่ยอมรับคุกกี้ ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลการกดยอมรับหรือไม่ยอมรับคุกกี้ก็คือการให้ความยินยอมประเภทหนึ่ง (Consent) ในขณะที่หลายคนอาจไม่เคยสังเกตว่าการให้ความยินยอมในการจัดเก็บคุกกี้ของผู้ให้บริการส่วนมากอาจจะยังไม่มีการให้ข้อมูลที่ชัดเจน เพียงพอและจัดให้เจ้าของข้อมูลส่วนบุคคลหรือผู้ใช้สามารถใช้สิทธิที่มีต่อข้อมูลส่วนบุคคลของตนได้ตามกฎหมาย

การตลาดแบบตรง

การขอความยินยอมและการใช้เทคโนโลยีการติดตามการใช้งานในอุตสาหกรรมการโฆษณาออนไลน์โดยเฉพาะอย่างยิ่งในการทำโฆษณาที่เรียกว่า Real time bidding (RTB) ที่ใช้การประมวลผลข้อมูลการใช้งานอินเทอร์เน็ตของลูกค้าเพื่อทำให้ผู้ซื้อพื้นที่โฆษณาสามารถเผยแพร่โฆษณาได้อย่างตรงความต้องการของกลุ่มเป้าหมายมากขึ้น (Targeted advertising) ยังเป็นเรื่องที่ขาดความเข้าใจและไม่มีแนวทางปฏิบัติที่เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลอย่างชัดเจนเพียงพอ โดย RTB นั้นอาจจะถูกฝังมากับคุกกี้ที่ลูกค้าหรือผู้ใช้บริการให้ความยินยอม ซึ่งตาม GDPR การใช้คุกกี้นั้นถูกควบคุมด้วยกฎหมาย 2 ฉบับ คือ ePrivacy Directive และ GDPR กล่าวคือ

1) การใช้งานคุกกี้ทุกประเภทต้องปฏิบัติตาม ePrivacy Directive
2) หากคุกกี้นั้นเป็น “ข้อมูลส่วนบุคคล” ต้องปฏิบัติตาม GDPR ด้วย กรณีนี้ก็ต้องใช้หลักเกณฑ์ตาม GDPR ประกอบกับ ePrivacy Directive

การตลาดแบบตรง

(2) สถานะทางกฎหมายของ Social Media Platform

ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปหรือ GDPR การเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือ Controller อาจเป็นคนเดียวหรือร่วมกันก็ได้ โดย GDPR ได้กำหนดบทนิยาม หน้าที่ และความความรับผิดของผู้ควบคุมข้อมูลส่วนบุคคลร่วมหรือ Joint Controller ไว้ในมาตรา 4 (7) ประกอบมาตรา 26 ของ GDPR และมีกรณีที่ศาลยุติธรรมแห่งสหภาพยุโรป (the Court of Justice of the European Union, CJEU) ได้เคยตัดสินและวางแนวบรรทัดฐานของการมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วมที่น่าสนใจในหลายคดี ซึ่งผู้เขียนจะนำมาเป็นกรณีศึกษา 2 คดีที่เกี่ยวข้องกับการมี Official Facebook Fanpage และการฝังปุ่ม “Like” ของ Facebook ในหน้าเว็บไซต์ และทั้ง 2 กรณีทำให้ Facebook กลายเป็น“ผู้ควบคุมข้อมูลส่วนบุคคลร่วม” หรือ Joint Controller โดยไม่รู้ตัว

การตลาดแบบตรง

ในส่วนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งเป็นกฎหมายที่กำหนดหน้าที่และความรับผิดชอบของบุคคลต่าง ๆ ที่เข้ามาเกี่ยวข้องในกระบวนการ “การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล” (รวมเรียกว่า “การประมวลผลข้อมูลส่วนบุคคล”) กำหนดว่า “ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยที่กฎหมายไม่ได้กำหนดว่าผู้ควบคุมข้อมูลส่วนบุคคลนั้นจะมีได้เพียงคนเดียว แต่ก็มิได้กำหนดนิยามของ Joint Controller ไว้เช่นเดียวกัน โดยคณะอนุกรรมการเฉพาะกิจตอบข้อหารือฯ ได้วางหลักการในประเด็นดังกล่าวไว้

การตลาดแบบตรง

ดังนั้น เพื่อเป็นการป้องกันการกระทำผิดพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 องค์กรที่มีหน้าที่หรือส่วนเกี่ยวของกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจึงมีหน้าที่ต้องศึกษาทำความเข้าใจในความหมายของสถานะต่าง ๆ ที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลรวมถึงบริบทและความสัมพันธ์กับคู่สัญญาหรือผู้เกี่ยวข้องฝ่ายต่าง ๆ อย่างละเอียดรอบคอบ เนื่องจากสถานะที่ต่างกันในบริบทของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เช่น ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลร่วม ผู้ประมวลผลข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลช่วง อาจมีหน้าที่และความรับผิดที่แตกต่างกันทั้งทางกฎหมายและตามสัญญา

การตลาดแบบตรง

(3) Facebook “Consent or Pay Model”

เมื่อวันที่ 17 เมษายน 2567 EDPB (European Data Protection Board) ได้เผยแพร่ความเห็นต่อกรณีการขอความยินยอมที่ชอบด้วยกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) ในโมเดลธุรกิจแบบ “Consent or Pay” ที่ผู้ใช้บริการต้องเลือกระหว่าง (1) “การให้ความยินยอม” ในการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการทำการตลาดตามกลุ่มเป้าหมาย (personalized advertising) หรือ (2) “การชำระเงิน” เพื่อไม่ให้ข้อมูลส่วนบุคคลถูกใช้เพื่อวัตถุประสงค์ในการทำการตลาดโดยแพลตฟอร์มออนไลน์ขนาดใหญ่ (Large Online Platforms) กล่าวคือเป็นการแลกเปลี่ยนกับการได้ใช้งานแบบ “ไม่มีโฆษณา” (no ads)

กรณีดังกล่าวสืบเนื่องจากการที่หน่วยงานกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคลของเนเธอร์แลนด์ นอร์เวย์ และเยอรมัน (ฮัมบูร์ก) ขอให้ EDPB พิจารณาให้ความเห็นเกี่ยวกับโมเดล “ยินยอมหรือชำระเงิน” ที่เกี่ยวข้องกับการโฆษณาตามพฤติกรรมว่าจะสามารถนำไปใช้ภายใต้สถานการณ์และเงื่อนไขใด โดยคำนึงถึงอำนาจเหนือตลาดของแพลตฟอร์มออนไลน์ขนาดใหญ่ประกอบด้วย

การตลาดแบบตรง

(4) IG ข้อมูลส่วนบุคคลของผู้เยาว์

เมื่อวันที่ 15 กันยายน 2565 Ireland Data Protection Commission (“DPC”) ได้เผยแพร่คำสั่งลงโทษปรับ Meta Platforms Ireland Limited (Instagram) เป็นเงินรวม 405 ล้านยูโรต่อกรณีการประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์ที่ใช้ Instagram ในสหภาพยุโรปโดยไม่ชอบด้วยกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป หรือ General Data Protection Regulation (“GDPR”) โดยการไต่สวนการกระทำความผิดดังกล่าวเริ่มต้นขึ้นในวันที่ 21 กันยายน 2563 โดยมี DPC เป็นผู้มีอำนาจหลักในการดำเนินการไต่สวนและกำหนดมาตรการลงโทษ Meta Platforms Ireland Limited เนื่องจากเป็นประเทศที่ถือว่า Meta มีสำนักงานใหญ่ตั้งอยู่ในสภาพยุโรป

การตลาดแบบตรง

อย่างไรก็ตาม DPC ภายหลังการวินิจฉัยตัดสินของ EDPB ให้ความเห็นว่าการเปิดเผยข้อมูลการติดต่อของผู้เยาว์ไม่ถือว่าเป็นส่วนหนึ่งที่เป็นองค์ประกอบที่จำเป็นของการดำเนินการตาม Instagram Term of Use แม้ว่าจะมีข้อตกลง/สัญญาระหว่างกัน แต่ข้อตกลงดังกล่าวไม่ครอบคลุมถึงการที่ต้องเปิดเผยข้อมูลการติดต่อของผู้เยาว์ Meta Ireland จึงไม่สามารถกล่าวอ้างได้ว่าเพราะมีความผูกพันตามสัญญาจึงสามารถใช้สิทธิในการเปิดเผยข้อมูลการติดต่อ การตีความการดำเนินการใด ๆ ต่อข้อมูลส่วนบุคคลเพื่อให้สามารถบรรลุวัตถุประสงค์ตามสัญญาต้องเป็นการดำเนินการที่มีความจำเป็นอย่างแท้จริง

การตลาดแบบตรง

กรณีศึกษาการตลาดผ่านทางโทรศัพท์ (Telemarketing)

Telemarketing คือ การตลาดผ่านทางโทรศัพท์ ซึ่งธุรกิจหรือองค์กรใช้การโทรศัพท์เพื่อสื่อสารและเสนอขายสินค้าหรือบริการให้กับลูกค้าเป้าหมาย โดยอาจมีวัตถุประสงค์ทั้งเพื่อการขายโดยตรง การแจ้งข้อมูลข่าวสาร หรือการสำรวจความคิดเห็น การตลาดผ่านโทรศัพท์นี้สามารถทำได้ทั้งแบบโทรออกเพื่อเข้าถึงลูกค้า (outbound) หรือการรับสายจากลูกค้าที่ติดต่อเข้ามาเอง (inbound)

(1) Vodafone Italia SpA

(2) Leads Work Limited

เทคโนโลยีและความท้าทายด้านการคุ้มครองข้อมูลส่วนบุคคล

ปัญญาประดิษฐ์

(1) การสอน AI ด้วยข้อมูลส่วนบุคคล

ความฉลาดของ AI ขึ้นอยู่กับปริมาณและคุณภาพของข้อมูลที่ใช้ในการสอนอย่างการสร้างแบบจำลอง และแหล่งข้อมูลหนึ่งที่ถูกใช้ในการสร้างชุดข้อมูลเพื่อการสอน AI คือ ข้อมูลจากเว็บไซต์ต่าง ๆ โดยวิธีการหนึ่งซึ่งนิยมแพร่หลาย คือ web scraping ซึ่งเป็นวิธีการคัดลอกหรือดูดข้อมูลต่าง ๆ จากหน้าเว็บไซต์ที่เปิดเผยต่อสาธารณะ เช่น พฤติกรรม ข้อความ รูปภาพ ข้อมูลติดต่อ และอื่น ๆ ตามรูปแบบที่กำหนด เพื่อนำข้อมูลไปวิเคราะห์ตามจุดประสงค์ต่าง ๆ ซึ่งในการดูดหรือคัดลอกอาจมีทั้งข้อมูลส่วนบุคคลทั่วไปและข้อมูลส่วนบุคคลตามมาตรา 26 การสร้างชุดข้อมูลเพื่อการสอน AI จาก web scraping จึงจำเป็นต้องปฏิบัติให้สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลด้วย

เทคโนโลยีและความท้าทายด้านการคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นกฎหมายที่มีหลักการทำนองเดียวกันกับ GDPR ของสหภาพยุโรป ที่มุ่งประสงค์กำกับกระบวนการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลให้สอดคล้องกับหลักเกณฑ์ตามที่กฎหมายกำหนด Dataset ที่เก็บรวบรวมมาโดยไม่ถูกต้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยเฉพาะการการเก็บรวบรวมโดยไม่มีฐานทางกฎหมาย หากมีการนำไปใช้ต่อโดยนักพัฒนา นักพัฒนาก็ย่อมมีความเสี่ยงในด้านการคุ้มครองข้อมูลส่วนบุคคลเช่นเดียวกัน การนำเข้าข้อมูลจากแหล่งสาธารณะต่าง ๆ เพื่อการสอน AI จึงเป็นประเด็นท้าทายในทางกฎหมายและการพัฒนาเทคโนโลยี AI อย่างยิ่งว่าจะสร้างสมดุลได้อย่างไร

ดังนั้น เมื่อพิจารณาถึงลักษณะของการคัดลอกข้อมูลจากเว็บไซต์จากกรณีศึกษาข้างต้น การขอความยินยอม ความโปร่งใสในการแจ้งรายละเอียดเกี่ยวกับการประมวลผล และสิทธิในการคัดค้าน จึงถือเป็นหลักการที่ยากต่อการนำไปปฏิบัติ โดยเฉพาะหากเป็นการดำเนินการเพื่อวัตถุประสงค์ในการสอน AI หรือพัฒนาชุดข้อมูลขนาดใหญ่เพื่อการสอน AI ด้วยเหตุนี้ การมี Regulatory Sandbox เพื่อให้มีการกำกับดูแลที่เหมาะสมสำหรับการพัฒนา AI ด้วยข้อมูลส่วนบุคคลจึงอาจมีความจำเป็นอย่างยิ่งหากต้องการส่งเสริมการพัฒนาระบบ AI ของประเทศ

เทคโนโลยีและความท้าทายด้านการคุ้มครองข้อมูลส่วนบุคคล

(2) ChatGPT

Generative AI อาจให้ข้อมูลที่ผิดพลาดหรือไม่ตรงกับความเป็นจริงได้ ดังนั้น ผู้ใช้งานโมเดลภาษาขนาดใหญ่ (LLM: Larger language models) จึงต้องมีความตระหนักรู้ในข้อจำกัดของเทคโนโลยีประกอบด้วย โดยข้อมูลที่ผิดพลาดอาจจะเป็นข้อเท็จจริงพื้นฐาน หรืออาจจะเป็นข้อมูลเกี่ยวกับบุคคลก็ได้

หาก Generative AI ให้ข้อมูลที่ไม่ถูกต้องเกี่ยวกับบุคคล เช่น “วันเดือนปีเกิด” ผู้ใช้งานหรือเจ้าของข้อมูลส่วนบุคคลที่ไม่ถูกต้อง และโดยเฉพาะอย่างยิ่งหากมีการให้ข้อมูลที่ไม่ถูกต้องที่อาจสร้างความเสื่อมเสียต่อเจ้าของข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคลจะมีสิทธิตามกฎหมายอย่างไรบ้างหรือไม่เพื่อจะทำให้ข้อมูลส่วนบุคคลของตนที่ถูกประมวลผล หรือแสดงผลโดย Generative AI นั้นถูกต้อง หรือขอให้ลบข้อมูลเหล่านั้นออกจากการประมวลผลหรือการแสดงผลลัพธ์

เทคโนโลยีและความท้าทายด้านการคุ้มครองข้อมูลส่วนบุคคล

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดหน้าที่ของผู้ให้บริการ Generative AI ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล และผู้ใช้บริการในฐานะเจ้าของข้อมูลส่วนบุคคล ไว้ดังนี้

(1) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ใช้บังคับการประมวลผลข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลที่อยู่นอกราชอาณาจักร (extra territorial) หากมีการเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าจะมีการชำระเงินของเจ้าของข้อมูลส่วนบุคคลหรือไม่ก็ตาม ดังนั้น ผู้ให้บริการ Generative AI ที่ให้บริการในประเทศไทย แม้ว่าจะไม่ได้จดทะเบียนจัดตั้งหรือมีสาขาในประเทศไทย ก็อาจต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 5 วรรคสอง)

(2) เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม (มาตรา 30)

(3) ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด และเจ้าของข้อมูลส่วนบุคคลสามารถร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการให้ข้อมูลส่วนบุคคลของตนถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิดได้ (มาตรา 35 และมาตรา 36)

(4) เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ (มาตรา 33)

เทคโนโลยีและความท้าทายด้านการคุ้มครองข้อมูลส่วนบุคคล

(3) Clearview AI

เมื่อวันที่ 16 พฤษภาคม 2567 Dutch DPA ซึ่งเป็นหน่วยงานบังคับใช้กฎหมาย GDPR ในประเทศเนเธอร์แลนด์ได้มีคำสั่งกำหนดค่าปรับและคำสั่งลงโทษเพิ่มเติมในกรณีที่ไม่ปฏิบัติตามคำสั่งดังกล่าวต่อกรณีการกระทำผิดของ Clearview AI ซึ่งเป็นผู้ให้บริการข้อมูลภาพจำลองใบหน้า (fascial recognition) สัญชาติอเมริกันเป็นเงินจำนวน 30,500,000 ยูโร

Clearview AI บริษัทสัญชาติอเมริกันที่ไม่มีสำนักงานในยุโรป โดยเป็นเจ้าของเทคโนโลยีการจดจำใบหน้าอัจฉริยะและการประมวลผลจาก big data โดยมีฐานข้อมูลภาพใบหน้าของบุคคลจำนวนมากกว่า 30 พันล้านภาพ ซึ่งบริษัทเก็บรวบรวมมาจากข้อมูลต่าง ๆ ที่เผยแพร่และเข้าถึงได้ทางอินเทอร์เน็ต โดยใช้เทคนิคที่เรียกว่า Crawler (หรือ Web Crawler) โดยการใช้โปรแกรมหรือบอทที่ถูกออกแบบมาให้ท่องเว็บไซต์ต่าง ๆ โดยอัตโนมัติเพื่อเก็บข้อมูล โดยเฉพาะในบริบทของเครื่องมือค้นหา (Search Engines) เช่น Google, Bing, หรือ Yahoo! บอทเหล่านี้จะทำการค้นหาและจัดเก็บข้อมูลจากหน้าเว็บไซต์ต่าง ๆ เพื่อนำมาใช้ในการสร้างดัชนี (Indexing) เพื่อให้เครื่องมือค้นหาสามารถแสดงผลลัพธ์ของการค้นหาได้อย่างมีประสิทธิภาพ โดย Crawlers จะทำงานโดยการเริ่มต้นจากหน้าเว็บไซต์หนึ่ง และจากนั้นติดตามลิงก์ต่าง ๆ ที่ปรากฏในหน้านั้นเพื่อไปยังหน้าอื่น ๆ ต่อไป โดยกระบวนการนี้จะดำเนินการไปอย่างต่อเนื่องเพื่อให้ครอบคลุมหน้าเว็บที่กว้างขวางมากที่สุด

เทคโนโลยีและความท้าทายด้านการคุ้มครองข้อมูลส่วนบุคคล

(4) Twitter AI

Grok AI เป็นของบริษัท xAI ซึ่งก่อตั้งโดย Elon Musk ในปี 2023 xAI พัฒนา Grok เป็นส่วนหนึ่งของโครงการปัญญาประดิษฐ์ โดยมีจุดมุ่งหมายเพื่อเป็นทางเลือกแทนแชทบอท AI อื่น ๆ เช่น ChatGPT ของ OpenAI โดย Grok ได้ถูกรวมเข้ากับแพลตฟอร์มโซเชียลมีเดีย X (เดิมคือ Twitter) ของ Musk และถูกออกแบบให้มีบุคลิกที่ตลกขบขันและ “ขบถ” มากขึ้น สะท้อนถึงวิสัยทัศน์ของ Musk ในการสร้าง AI ที่ให้การสนทนาแบบไม่จำกัดมากขึ้น โดยชื่อ “Grok” มาจากหนังสือไซไฟชื่อดังเรื่อง Stranger in a Strange Land โดย Robert A. Heinlein ซึ่งหมายถึงการเข้าใจบางสิ่งอย่างถ่องแท้ทั้งในเชิงตรรกะและอารมณ์ ปัจจุบัน Grok 2 AI Assistant เปิดให้ใช้งานได้เฉพาะผู้ใช้บริการ X/Twitter ที่สมัครสมาชิกแบบ Premium หรือ Premium+ เท่านั้น

เทคโนโลยีและความท้าทายด้านการคุ้มครองข้อมูลส่วนบุคคล

Cookies

คุกกี้ (cookie) เป็นเครื่องมือสำคัญที่ช่วยให้องค์กรที่มีการใช้หน้าเว็บไซต์สามารถวิเคราะห์ข้อมูลเชิงลึกเกี่ยวกับกิจกรรมออนไลน์เพื่อทราบถึงพฤติกรรมต่าง ๆ ของผู้บริโภคที่เข้ามายังหน้าเว็บไซต์และนำไปใช้ในการกำหนดกลยุทธ์ทางธุรกิจได้อย่างมีประสิทธิภาพ ปัจจุบันจึงจะเห็นได้ว่าเว็บไซต์ต่าง ๆ ดำเนินการเก็บคุกกี้เพื่อวัตถุประสงค์ทางด้านการวิเคราะห์พฤติกรรมของผู้บริโภคอย่างแพร่หลาย อย่างไรก็ตาม คุกกี้บางประเภทที่หน้าเว็บไซต์ต่าง ๆ ใช้นั้นอาจเป็นข้อมูลที่สามารถระบุหรือบ่งบอกถึงตัวบุคคลของผู้ใช้บริการที่เข้ามาเยี่ยมชมเว็บไซต์ได้ ดังนั้น คุกกี้บางประเภทจึงอาจจัดเป็นข้อมูลส่วนบุคคลตามความหมายของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

เทคโนโลยีและความท้าทายด้านการคุ้มครองข้อมูลส่วนบุคคล

คุกกี้คืออะไร

Privacy and Electronic Communication Regulations (PECR) หรือกฎหมายว่าด้วยสิทธิความเป็นส่วนตัวที่เกี่ยวข้องกับการสื่อสารโดยช่องทางอิเล็กทรอนิกส์ของประเทศอังกฤษ (เป็นกฎหมายที่อนุมัติตาม ePrivacy Directive ของสหภาพยุโรป) ได้ให้ความหมายของคุกกี้ไว้ว่า คุกกี้เป็นข้อมูลตัวอักษรเล็ก ๆ (text file) ที่ถูกดาวน์โหลดและจัดเก็บไว้ในอุปกรณ์ เช่น เครื่องคอมพิวเตอร์หรือสมาร์ทโฟนของผู้ที่เข้ามาเยี่ยมชมหน้าเว็บไซต์ (terminal equipment) โดยคุกกี้จะสามารถจดจำอุปกรณ์ของผู้เข้าชมเว็บไซต์และจัดเก็บข้อมูลบางประเภทเกี่ยวกับความต้องการของผู้บริโภค (user's preferences) และประวัติการเข้าชมบนหน้าเว็บไซต์ (past actions)

หากพิจารณาถึงลักษณะการทำงานของคุกกี้บางประเภทจะเห็นได้ว่า คุกกี้บางประเภทนั้นสามารถใช้ระบุถึงตัวตนของบุคคลใดบุคคลหนึ่งได้ภายใต้เงื่อนไขของการเก็บรวบรวม ใช้ และเปิดเผย ("การประมวลผล") ที่กำหนดในกิจกรรมการประมวลผลหนึ่ง ๆ คุกกี้ (หรือ cookie IDs) ลักษณะดังกล่าวจึงเป็น "ข้อมูลส่วนบุคคล" ซึ่งแนวทางการตีความว่า cookie IDs บางประเภทเป็นข้อมูลส่วนบุคคลสอดคล้องกับ GDPR แนวทางการวินิจฉัยของศาลสหภาพยุโรปในคดี Fashion ID (C-40/17) และ Planet49 (C-673/17) และคำแนะนำของ European Data Protection Board (2020)

เทคโนโลยีและความท้าทายด้านการคุ้มครองข้อมูลส่วนบุคคล

ดังนั้น การใช้คุกกี้บนหน้าเว็บไซต์จึงต้องคำนึงถึงฐานความชอบด้วยกฎหมายในการประมวลผลข้อมูลส่วนบุคคลด้วย ซึ่งโดยทั่วไปฐานความชอบด้วยกฎหมายที่สอดคล้องกับการประมวลผลคุกกี้จะอยู่ในฐานของ “ความยินยอม” (PDPA มาตรา 19 ประกอบมาตรา 24) ซึ่ง “Cookie Consent” ที่ชอบด้วยกฎหมายจำเป็นต้องพิจารณาประกอบกับเงื่อนไขด้านวัตถุประสงค์ การแจ้งที่ชอบด้วยกฎหมาย และการได้รับความยินยอม

ประเภทของคุกกี้จำแนกตามวัตถุประสงค์ของการใช้งาน อาจจำแนกได้เป็น 4 ประเภท

1) คุกกี้ที่จำเป็น (strictly necessary cookie)

2) คุกกี้เพื่อการทำงานของเว็บไซต์ (functional cookie)

3) คุกกี้ข้อมูลสถิติ (statistics cookie)

4) คุกกี้เพื่อการตลาด (marketing cookie)

เทคโนโลยีและความท้าทายด้านการคุ้มครองข้อมูลส่วนบุคคล

ระบบคลาวด์

ผู้ให้บริการระบบคลาวด์ (cloud computing service provider) หมายความว่า ผู้ให้บริการเก็บรักษาข้อมูลหรือเก็บพักข้อมูลแก่บุคคลอื่นในรูปแบบชั่วคราวหรือถาวร โดยมีระบบที่บริหารจัดการข้อมูลบนอินเทอร์เน็ต โดยอาจให้บริการในรูปแบบต่าง ๆ เช่น ผู้ให้บริการโครงสร้างพื้นฐานหลัก (Infrastructure as a Service: IaaS) ผู้ให้บริการแพลตฟอร์ม (Platform as a Service: PaaS) ผู้ให้บริการซอฟต์แวร์ (Software as a Service: SaaS) ผู้ให้บริการระบบจัดเก็บข้อมูล (Data Storage as a Service: DSaaS) และผู้ให้บริการระบบบริหารจัดการข้อมูลแบบ Serverless Computing หรือผู้ให้บริการฟังก์ชัน (Function as a Service: FaaS) เป็นต้น

เทคโนโลยีและความท้าทายด้านการคุ้มครองข้อมูลส่วนบุคคล

(1) ความปลอดภัยของระบบคลาวด์

แม้ว่าหลายองค์กรได้นำการประมวลผลแบบคลาวด์มาใช้แล้วหรือกำลังอยู่ในขั้นตอนการเปลี่ยนไปใช้โซลูชันระบบคลาวด์ แต่อีกหลายองค์กรก็ยังลังเลกับการนำระบบคลาวด์ไปใช้ ในยุโรปมีการเปิดเผยว่าผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) ที่ยังไม่ได้นำการประมวลผลแบบคลาวด์มาใช้ มีเรื่องกังวลดังนี้

- ความมั่นคงปลอดภัยของข้อมูลไม่เพียงพอและความเสี่ยงของข้อมูล
- การปฏิบัติตามข้อกำหนดและประเด็นทางกฎหมาย
- ความเสี่ยงในการกำกับดูแลหรือควบคุมข้อมูล

เทคโนโลยีและความท้าทายด้านการคุ้มครองข้อมูลส่วนบุคคล

(2) ระบบคลาวด์และการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

เมื่อวันที่ 1 ธันวาคม 2564 ศาลปกครองแห่งเมืองวีสบาเดิน ประเทศเยอรมนี ได้มีคำสั่งระหว่างพิจารณาเกี่ยวกับการใช้ Cookie Management Platform ในประเด็นของการโอนข้อมูลไปยังต่างประเทศ (นอกสหภาพยุโรป) โดยคดีดังกล่าวสืบเนื่องจากการที่มหาวิทยาลัยแห่งหนึ่งในประเทศเยอรมนีได้นำ Cookie Management Platform มาใช้ในการประมวลผลข้อมูลส่วนบุคคล ซึ่งบริษัทที่ให้บริการ Cookie Management Platform เป็นบริษัทที่จดทะเบียนและมีสำนักงานแห่งใหญ่อยู่ในประเทศเดนมาร์ก แต่ได้ใช้บริการของผู้ให้บริการระบบคลาวด์ซึ่งอยู่ในประเทศสหรัฐอเมริกาเพื่อจัดเก็บข้อมูลที่ได้จากการประมวลผลผ่าน Cookie Management Platform

เทคโนโลยีและความท้าทายด้านการคุ้มครองข้อมูลส่วนบุคคล

(3) การจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล

เพื่อให้การดำเนินการบรรลุวัตถุประสงค์ตามสัญญาให้บริการในธุรกิจให้บริการทางเทคโนโลยีไม่ว่าจะเป็นลักษณะของการให้บริการซอฟต์แวร์และแอปพลิเคชัน (Software as a Service, SaaS) การให้บริการด้านแพลตฟอร์ม (Platform as a Service, PaaS) และบริการเฉพาะโครงสร้างพื้นฐาน (Infrastructure as a Service) ผู้ให้บริการดังกล่าวย่อมมีหน้าที่เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในฐานะ “ผู้ประมวลผลข้อมูลส่วนบุคคล” (Data Processor) ตามคำสั่งหรือในนามของผู้รับบริการ ซึ่งมีฐานะเป็น “ผู้ควบคุมข้อมูลส่วนบุคคล” (Data Controller) ซึ่งหากข้อมูลดังกล่าวนั้นถือเป็นข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผู้ให้บริการย่อมมีหน้าที่และความรับผิดตามพระราชบัญญัติดังกล่าว

แบบทดสอบ บทที่ 8

ข้อที่ 1

Q : ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ฐานทางกฎหมายข้อใดที่นายจ้างอาจนำมาใช้ในการส่งข้อมูลส่วนบุคคลของพนักงานอันประกอบด้วยข้อมูลเกี่ยวกับการหักภาษี ณ ที่จ่ายและฐานอัตราเงินเดือนของลูกจ้าง ซึ่งเป็นข้อมูลทางการเงินไปยังกรมสรรพากรได้

ก. ความยินยอมโดยชัดแจ้งของพนักงาน

ข. การปฏิบัติตามกฎหมายของนายจ้าง

ค. ประโยชน์สาธารณะ

ง. ประโยชน์สาธารณะที่สำคัญ

แบบทดสอบ บทที่ 8

ข้อที่ 2

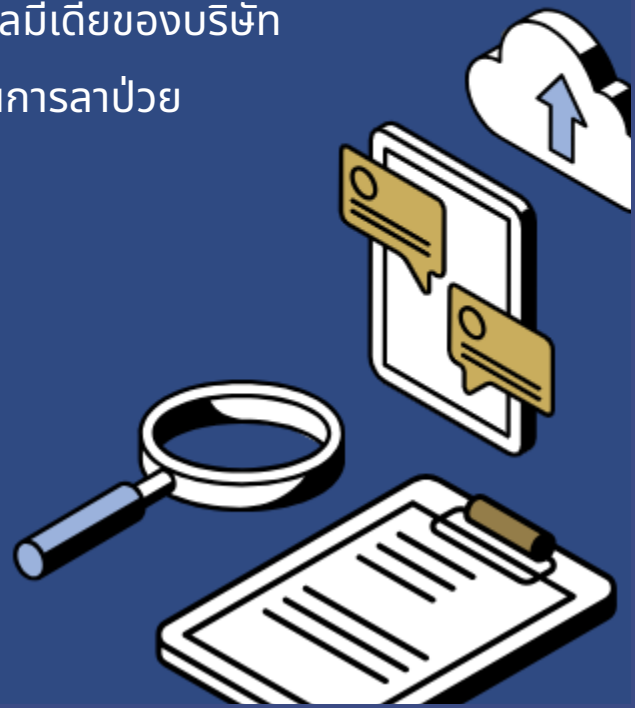
Q : หากนายจ้างจะขอความยินยอมจากลูกจ้างได้โดยชอบด้วยกฎหมาย ข้อใดถูกต้องที่สุด

ก. โพสต์ภาพถ่ายกิจกรรมการแข่งขันจักรยานของพนักงานบนโซเชียลมีเดียของบริษัท

ข. การดำเนินการเกี่ยวกับใบรับรองสุขภาพของพนักงานเพื่อใช้สิทธิในการลาป่วย

ค. การติดตั้งและใช้ระบบกล้องวงจรปิดในบริเวณพื้นที่ของบริษัท

ง. การประเมินเพื่อขอเลื่อนตำแหน่งหรือกำหนดคุณวุฒิที่สูงขึ้น



แบบทดสอบ บทที่ 8

ข้อที่ 3

Q : ข้อใดต่อไปนี้ไม่ถูกต้องเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคลด้วยระบบกล้องวงจรปิด

ก. ผู้ควบคุมข้อมูลส่วนบุคคลอาจใช้ฐานประโยชน์โดยชอบด้วยกฎหมายในการเก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าว

ข. ผู้ควบคุมข้อมูลส่วนบุคคลอาจไม่ต้องแจ้งรายละเอียดเกี่ยวกับวัตถุประสงค์ของการเก็บรวบรวมเพื่อการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผย หากเจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

ค. ติดตั้งกล้องเพื่อให้ครอบคลุมพื้นที่สาธารณะได้มากที่สุด หากระบบกล้องวงจรปิดมีประสิทธิภาพมากเพียงพอ

ง. บุคคลที่ข้อมูลถูกบันทึกในระบบกล้องวงจรปิดอาจไม่มีสิทธิในการขอให้ลบข้อมูลส่วนบุคคลที่เกี่ยวกับตนเอง หากเป็นการเก็บรักษาไว้เพื่อประโยชน์ในการใช้สิทธิทางศาลของบุคคลอื่น

แบบทดสอบ บทที่ 8

ข้อที่ 4

Q : ข้อใดต่อไปนี้ไม่ถูกต้องเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง

ก. เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรงเมื่อใดก็ได้

ข. ในกรณีที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้าน ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อไปได้ และต้องยุติการให้บริการตามสัญญาต่าง ๆ ที่มีกับเจ้าของข้อมูลส่วนบุคคลที่ใช้สิทธิคัดค้านโดยทันที

ค. ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติโดยแยกส่วนข้อมูลส่วนบุคคลที่ถูกคัดค้านออกจากข้อมูลอื่นอย่างชัดเจนในทันทีเมื่อเจ้าของข้อมูลส่วนบุคคลได้แจ้งการคัดค้านให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบ

ง. การส่งข้อความประชาสัมพันธ์และเชิญชวนให้ซื้อหน่วยลงทุนไปยังผู้ใช้บริการทุกคนของแอปพลิเคชันด้วยข้อความเดียวกัน ไม่ใช่การตลาดแบบตรง

แบบทดสอบ บทที่ 8

ข้อที่ 5

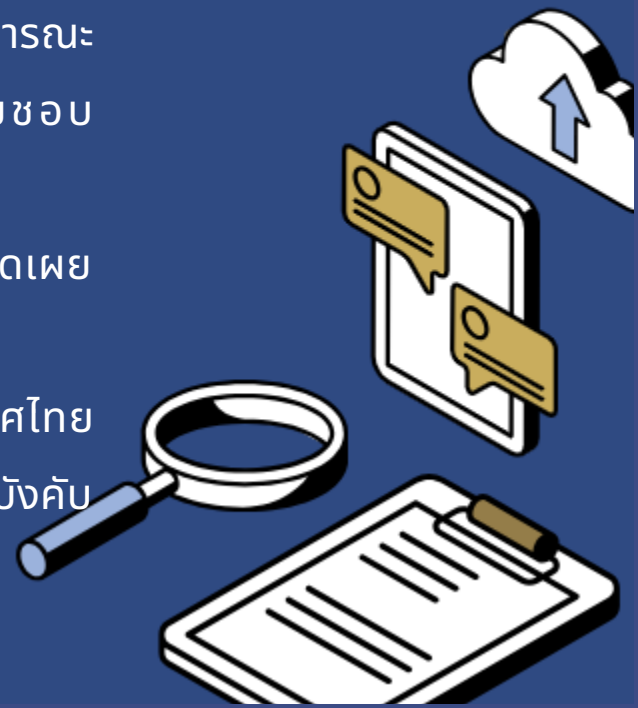
Q : ในกรณีที่ท่านเป็นผู้ใช้งาน (end user) ของ Generative AI ข้อใดต่อไปนี้ถูกต้องที่สุด

ก. ผู้ใช้งานเป็นผู้ควบคุมข้อมูลส่วนบุคคล และผู้ให้บริการ Generative AI เป็นผู้ประมวลผลข้อมูลส่วนบุคคล

ข. ผู้ให้บริการ Generative AI สามารถเก็บรวบรวมข้อมูลเกี่ยวกับสุขภาพของบุคคลที่มีการโพสต์หรือแชร์ในโซเชียลมีเดียที่มีการตั้งค่าเป็นสาธารณะเพื่อนำมาใช้ในการฝึกอบรม AI เนื่องจากเป็นประโยชน์โดยชอบด้วยกฎหมายของผู้ให้บริการ Generative AI

ค. ผู้ใช้งานสามารถขอใช้สิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนเองเพื่อนำใช้ในการฝึกอบรม AI ได้

ง. ผู้ให้บริการ Generative AI หากไม่มีการแต่งตั้งตัวแทนในประเทศไทย หรือมิได้มีการจดทะเบียนเป็นนิติบุคคลในประเทศไทย จะไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



• เฉลยแบบทดสอบบทที่ 8

ข้อที่	เฉลย
1.	ข.
2.	ก.
3.	ค.
4.	ข.
5.	ค.

การรักษาความมั่นคงปลอดภัย ของข้อมูลส่วนบุคคล

บทที่ 9

- บทนำ
- มาตรการเชิงองค์กรและเชิงเทคนิคที่เหมาะสม
  - หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล
  - การกำหนดมาตรการรักษาความมั่นคงปลอดภัย
- หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล
- การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล
- แบบทดสอบ

บทนำ

มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสามารถช่วยคุ้มครองข้อมูลส่วนบุคคล เพื่อให้สอดคล้องกับการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ เนื่องจากปัญหาส่วนใหญ่ที่เกิดขึ้นเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลมักเป็นเหตุการณ์เกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ในบทนี้จะครอบคลุมแนวปฏิบัติที่ดีเพื่อป้องกันไม่ให้เกิดเหตุที่จะกระทบความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล รวมถึงหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลในการปฏิบัติตามกฎหมายในเรื่องความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

มาตรการเชิงองค์กรและเชิงเทคนิคที่เหมาะสม

ความมั่นคงปลอดภัยเป็นประเด็นที่สำคัญมากในการคุ้มครองข้อมูลส่วนบุคคล นอกจากโทษทางกฎหมายและการชดเชยค่าเสียหายแล้ว หากมีการละเมิดข้อมูลส่วนบุคคลเกิดขึ้น ก็เป็นเหตุให้ชื่อเสียงและภาพลักษณ์ขององค์กรเสียหายอีกด้วย

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลไว้ในมาตรา 37 (1) ให้ผู้ควบคุมข้อมูลส่วนบุคคลนั้นต้อง “จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็น หรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด”

นอกจากนี้ ตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ได้กำหนดมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

การกำหนดมาตรการรักษาความมั่นคงปลอดภัย

การกำหนดมาตรการรักษาความมั่นคงปลอดภัยช่วยเสริมความมั่นใจว่าระบบข้อมูลสารสนเทศมีความมั่นคงปลอดภัย โดยที่มาตรการต่าง ๆ ที่กำหนดนั้น ต้องสามารถใช้งานได้ และต้องมีระบบแจ้งเตือนหากมีข้อผิดพลาดเกิดขึ้น

องค์ประกอบของมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลนั้นประกอบด้วย 3 ด้านได้แก่

1) Confidentiality - “การธำรงไว้ซึ่งความลับ” ซึ่งหมายความถึง ความสามารถในการรักษาความลับของระบบ โดยการควบคุมการเข้าถึงข้อมูล ให้เข้าถึงโดยบุคคลที่มีอำนาจ และรู้เท่าที่จำเป็นต้องรู้
2) Integrity - “ความถูกต้องครบถ้วน” หมายความถึง ความถูกต้องและความสมบูรณ์ของข้อมูล ซึ่งถูกต้องสมบูรณ์เสมอจากต้นฉบับ และหากจะเปลี่ยนแปลงแก้ไข ก็ต้องทำโดยผู้ที่ได้รับสิทธิเท่านั้น ดังนั้น ระบบต้องสามารถป้องกันการโจมตี แก้ไขหรือเปลี่ยนแปลงข้อมูลโดยผู้ที่ไม่มีสิทธิได้
3) Availability – “สภาพพร้อมใช้งาน” หมายความถึง ความสามารถของระบบที่จะคงอยู่ ให้บริการหรือทำงานได้ตลอดเวลาจากคนที่มีสิทธิ ดังนั้น ระบบต้องมีมาตรการสำรองเตรียมพร้อมไว้เสมอ เพื่อให้ระบบยังคงดำเนินการได้แม้มีเหตุไม่คาดคิดเกิดขึ้น

การกำหนดมาตรการรักษาความมั่นคงปลอดภัย

ในทางปฏิบัติ องค์กรควรมองภาพแบบองค์รวม โดยอาจพิจารณาในเรื่องต่าง ๆ ดังต่อไปนี้ด้วย

-การส่งเสริมความตระหนักในเรื่องความเสี่ยงและความสำคัญของการให้ความคุ้มครองข้อมูลส่วนบุคคลแก่บุคลากรทุกคน

-การมีระบบจัดการข้อมูลสารสนเทศ โดยมีข้อมูลขององค์กรทั้งหมดเกี่ยวกับกฎเกณฑ์ต่าง ๆ ในเรื่องการรักษาความลับและความมั่นคงปลอดภัยของข้อมูล โดยประกอบด้วยวัตถุประสงค์และขอบเขตของการรักษาความมั่นคงปลอดภัย หลักการในการรักษาความมั่นคงปลอดภัย มาตรฐานและกฎหมายที่ต้องปฏิบัติตาม และบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้อง นอกจากนี้ องค์กรควรสื่อสารนโยบายเกี่ยวกับการจัดการความมั่นคงปลอดภัยของข้อมูลไปยังบุคลากรทุกคนรวมถึงบุคคลภายนอกที่เกี่ยวข้อง และมีการทบทวนอย่างสม่ำเสมอ

-การจัดการสิ่งแวดล้อมทางกายภาพ เช่น ระบบการเข้าถึงข้อมูลที่ซับซ้อน การติดตั้งกล้องวงจรปิด การต้องมีกุญแจล็อคสถานที่ที่ใช้เก็บข้อมูล

-มาตรการทางเทคนิคต่าง ๆ ซึ่งรวมถึงกลไกการคุ้มครองข้อมูลส่วนบุคคล เช่น การเข้ารหัสข้อมูล การมีเทคโนโลยีป้องกันไวรัสและสแปมไฟร์วอล ระบบการจัดการการเข้าถึงและระบุตัวตน ระบบตรวจจับการเกิดเหตุการละเมิดข้อมูล การป้องกันข้อมูลสูญหาย การยืนยันสองขั้นตอน (two-factor authentication) ระบบเก็บข้อมูลประวัติการเข้าใช้งาน (logging and audit trails) ระบบการจัดการความเสี่ยง การทบทวนรหัสความมั่นคงปลอดภัยอย่างสม่ำเสมอ

-มาตรการเชิงองค์กร โดยเป็นการใช้เพื่อสนับสนุนมาตรการทางเทคนิค ซึ่งรวมถึงกระบวนการสรรหาและอบรมบุคลากรที่เป็นผู้มีความเหมาะสมในการดำเนินการต่าง ๆ กับข้อมูลส่วนบุคคล โดยเฉพาะกรณีเป็นข้อมูลส่วนบุคคลตามมาตรา 26 การมีมาตรการเพื่อให้มั่นใจว่าจะมีการจัดการข้อมูลอย่างเหมาะสมผ่านการธรรมาภิบาลข้อมูล (data governance) การจำแนกข้อมูล กระบวนการแบ่งปันข้อมูล (Data Sharing) ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล

หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” คือ บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล โดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลไว้ในมาตรา 40 ดังนี้

(1) ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

(2) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

(3) จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล

ทั้งนี้ เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมาย โดยเฉพาะในมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับผู้ประมวลผลข้อมูลส่วนบุคคลด้วย (Data Processing Agreement) โดยอาจจัดทำในรูปแบบลายลักษณ์อักษรหรือในรูปแบบอิเล็กทรอนิกส์ก็ได้ โดยต้องมีรายละเอียดอย่างน้อยดังนี้

1. กำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคล
2. ระบุให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
3. ระบุให้ผู้ประมวลผลข้อมูลส่วนบุคคลแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมง นับแต่ผู้ประมวลผลข้อมูลส่วนบุคคลทราบเหตุเท่าที่จะสามารถกระทำได้
4. กำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

นอกจากนี้ผู้ควบคุมข้อมูลส่วนบุคคลอาจกำหนดรายละเอียดดังต่อไปนี้เพิ่มเติมตามความเหมาะสมด้วยก็ได้

1. ข้อตกลงการรักษาความลับ
2. การช่วยเหลือผู้ควบคุมข้อมูลส่วนบุคคลตามสมควรเมื่อเจ้าของข้อมูลใช้สิทธิของตน
3. การลบ/ทำลาย/ส่งคืนข้อมูลมายังผู้ควบคุมข้อมูลส่วนบุคคลเมื่อหมดความจำเป็น
4. ข้อกำหนดในการจ้างผู้ประมวลผลข้อมูลส่วนบุคคลช่วง หากมี

การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

การละเมิดข้อมูลส่วนบุคคลนั้น หมายถึง “การละเมิดมาตรการรักษาความมั่นคงปลอดภัยที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่อง หรืออุบัติเหตุ หรือเหตุอื่นใด” โดยอาจแบ่งประเภทของการละเมิดได้เป็นสามประเภท ดังนี้

(1) **การละเมิดความลับของข้อมูลส่วนบุคคล (Confidentiality Breach)** คือ มีการเข้าถึง หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่อง หรืออุบัติเหตุ

(2) **การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล (Integrity Breach)** ได้แก่ การเปลี่ยนแปลง แก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่อง หรืออุบัติเหตุ

(3) **การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล (Availability Breach)** ซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลส่วนบุคคล ทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่พร้อมใช้งานได้ตามปกติ

การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

เมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคลขึ้น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น และกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) โดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล แต่ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย มาตรา 40 วรรคแรก (2)

การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

ทั้งนี้ เมื่อผู้ควบคุมข้อมูลส่วนบุคคลได้รับแจ้งข้อมูลไม่ว่าจะโดยทางใดว่ามีหรือน่าจะมีเหตุการละเมิดข้อมูลส่วนบุคคลเกิดขึ้น ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการ ดังต่อไปนี้

1. ประเมินความน่าเชื่อถือของข้อมูล และตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิด โดยตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล รวมถึงการประเมินความเสี่ยงจากการละเมิดข้อมูลส่วนบุคคล

2. หากประเมินความเสี่ยงแล้วพบว่า การละเมิดดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ดำเนินการป้องกัน ระงับ หรือแก้ไขเพื่อให้การละเมิดดังกล่าวสิ้นสุด หรือไม่ให้การละเมิดส่งผลกระทบเพิ่มเติม โดยทันทีเท่าที่จะทำได้

3. เมื่อพิจารณาแล้วเห็นว่า มีเหตุอันควรเชื่อว่ามีการละเมิดเกิดขึ้นจริง ให้แจ้งเหตุดังกล่าวแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่จะทำได้ เว้นแต่เป็นกรณีไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล แต่ในกรณีที่เหตุการณ์ละเมิดดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเหตุละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบ พร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย

4. ดำเนินการตามมาตรการที่จำเป็น เหมาะสม เพื่อระงับ ตอบสนอง แก้ไขเหตุละเมิด และป้องกันเหตุละเมิด และผลกระทบที่อาจเกิดในลักษณะเดียวกันในอนาคต รวมถึงการทบทวนมาตรการรักษาความมั่นคงปลอดภัยให้เหมาะสม โดยคำนึงถึงปัจจัยต่าง ๆ เช่น ระดับความเสี่ยง บริบท สภาพแวดล้อม ลักษณะการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และทรัพยากรที่ต้องใช้

การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

การประเมินความเสี่ยงสำหรับการละเมิดข้อมูลส่วนบุคคลว่าจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลเพียงใด ผู้ควบคุมข้อมูลส่วนบุคคลอาจพิจารณาจากปัจจัยดังต่อไปนี้

1. ลักษณะและประเภทของการละเมิด
2. ลักษณะและประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับเหตุละเมิด
3. ปริมาณของข้อมูลที่เกี่ยวข้องกับการละเมิด โดยพิจารณาจำนวนข้อมูล จำนวนรายการที่เกี่ยวข้อง
4. ลักษณะ ประเภท สถานะของเจ้าของข้อมูลส่วนบุคคลว่าเป็นบุคคลกลุ่มใด
5. ความร้ายแรงของผลกระทบ และความเสียหายที่จะเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล และประสิทธิภาพของมาตรการป้องกัน ระงับแก้ไขเหตุละเมิด หรือการเยียวยาความเสียหาย
6. ผลกระทบในวงกว้างต่อธุรกิจ หรือการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล หรือต่อสาธารณะ
7. ลักษณะของระบบเก็บข้อมูลที่เกี่ยวกับการละเมิด และมาตรการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ทั้งที่เป็นมาตรการเชิงองค์กร (organizational measures) มาตรการเชิงเทคนิค (technical measures) รวมถึงมาตรการทางกายภาพ (physical measures)
8. สถานะทางกฎหมาย รวมทั้งขนาดและลักษณะของกิจการของผู้ควบคุมข้อมูลส่วนบุคคล

การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

นอกจากนี้ ตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 นั้น ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคล ต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษร หรือแจ้งโดยผ่านวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดตามที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด โดยในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลนั้น ต้องระบุสาระสำคัญดังต่อไปนี้เท่าที่จะสามารถกระทำได้

1) ข้อมูลโดยสังเขปเท่าที่จะสามารถระบุได้เกี่ยวกับลักษณะและประเภทของการละเมิดข้อมูลส่วนบุคคล
2) ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในกรณีที่มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือชื่อ สถานที่ติดต่อ และวิธีการติดต่อของบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายให้ทำหน้าที่ประสานงานและให้ข้อมูลเพิ่มเติม
3) ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นจากเหตุการละเมิดข้อมูลส่วนบุคคล
4) ข้อมูลเกี่ยวกับมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหาย

การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

ทั้งนี้ กรณีที่เหตุการละเมิดข้อมูลส่วนบุคคลมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเหตุละเมิดแก่เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบด้วยโดยไม่ชักช้าในรายละเอียดดังต่อไปนี้

1) ข้อมูลโดยสังเขปเกี่ยวกับลักษณะของการละเมิดข้อมูลส่วนบุคคล
2) ช่องทางติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือบุคคลที่ได้รับมอบหมายให้ประสานงาน
3) ผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล
4) แนวทางเยียวยาความเสียหาย มาตรการที่จะป้องกัน ระงับ แก้ไขเหตุละเมิด รวมถึงข้อแนะนำเกี่ยวกับมาตรการที่เจ้าของข้อมูลส่วนบุคคล อาจดำเนินการได้ เพื่อป้องกัน ระงับ แก้ไข เยียวยาความเสียหาย

แบบทดสอบ บทที่ 9

ข้อที่ 1

Q : CIA ย่อมาจากคำว่าอะไรบ้าง

แบบทดสอบ บทที่ 9

ข้อที่ 2

Q : ปัจจัยใดบ้างที่ผู้ควบคุมข้อมูลส่วนบุคคลต้องคำนึงถึงในการดำเนินการจัดให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคล

แบบทดสอบ บทที่ 9

ข้อที่ 3

Q : <u>จริงหรือเท็จ</u>

(3.1) “เทคโนโลยีที่ทันสมัยที่สุดเป็นตัวเลือกที่ดีที่สุดเสมอสำหรับการรักษาความมั่นคงปลอดภัย”

(3.2) ผู้ประมวลผลข้อมูลส่วนบุคคลต้องใช้มาตรการเชิงองค์กรและเชิงเทคนิคที่เหมาะสมเพื่อรักษาความมั่นคงปลอดภัยของข้อมูล

แบบทดสอบ บทที่ 9

ข้อที่ 4

Q : ให้ระบุรายละเอียดที่ต้องมีในข้อตกลงการประมวลผลข้อมูลส่วนบุคคล

แบบทดสอบ บทที่ 9

ข้อที่ 5

Q : ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคลในกรณีใด

แบบทดสอบ บทที่ 9

ข้อที่ 6

Q : ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเจ้าของข้อมูลส่วนบุคคล
เมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคลในกรณีใด

• เฉลยแบบทดสอบบทที่ 9

ข้อที่	เฉลย
1.	Confidentiality, Integrity และ Availability
2.	ปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน
3.	3.1 เท็จ 3.2 จริง
4.	(1) การกำหนดให้ดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับ (2) การกำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม (3) ระบุให้ผู้ประมวลผลข้อมูลส่วนบุคคลแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ผู้ประมวลผลข้อมูลส่วนบุคคลทราบเหตุเท่าที่จะสามารถกระทำได้ (4) กำหนดให้ทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

• เฉลยแบบทดสอบบทที่ 9

ข้อที่	เฉลย
5.	เมื่อเหตุการละเมิดข้อมูลส่วนบุคคลดังกล่าวมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพเจ้าของข้อมูลส่วนบุคคล
6.	เมื่อเหตุการละเมิดข้อมูลส่วนบุคคลดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

ความรับผิดชอบ

บทที่ 10

- บทนำ
- นิยามความรับผิดชอบ
- การคุ้มครองข้อมูลส่วนบุคคลโดยการออกแบบและโดยค่าเริ่มต้น
- การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล
- นโยบายการคุ้มครองข้อมูลส่วนบุคคล
- บันทึกกิจกรรมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- แบบทดสอบ

บทนำ

ความรับผิดชอบ (accountability) ในที่นี้หมายถึง ความสามารถในการแสดงว่าได้มีการดำเนินการเพื่อการคุ้มครองข้อมูลส่วนบุคคลและสอดคล้องกับที่กฎหมายกำหนด เนื้อหาในบทนี้จะกล่าวถึงความรับผิดชอบ รวมถึง ระบบการบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล นโยบายการคุ้มครองข้อมูลส่วนบุคคล และบทบาทของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

นิยามความรับผิดชอบ

กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็น หรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยต้องประกอบด้วยมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการละเมิดข้อมูลส่วนบุคคล ทั้งต้องคำนึงถึงการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัย ตั้งแต่การระบุความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้นกับทรัพย์สินสารสนเทศ (information assets) ที่สำคัญ การป้องกันความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้น การตรวจสอบและเฝ้าระวังภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล รวมถึงการที่จะต้องคำนึงถึงความสามารถในการธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคลไว้ได้อย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

นิยามความรับผิดชอบ

ดังนี้ จะเห็นได้ว่า การดำเนินการดังกล่าวใช้ฐานความเสี่ยง (risk-based approach) ในการคุ้มครองข้อมูลส่วนบุคคล และส่งผลให้ใช้มาตรการทางเทคนิคและมาตรการอื่น ๆ ซึ่งสามารถแสดงให้เห็นว่าได้มีการดำเนินการตามกฎหมาย นอกจากนี้ยังมีการกำหนดให้ทำบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคลอีกด้วย และแม้ในกรณีที่กฎหมายจะกำหนดหน้าที่ความรับผิดชอบบางอย่างแก่ผู้ควบคุมข้อมูลส่วนบุคคลแต่เพียงฝ่ายเดียวโดยไม่กำหนดแก่ผู้ประมวลผลข้อมูลส่วนบุคคลด้วยก็ตาม แต่ผู้ประมวลผลข้อมูลส่วนบุคคลก็มีหน้าที่ในการที่จะต้องสนับสนุนผู้ควบคุมข้อมูลส่วนบุคคลเพื่อให้ปฏิบัติตามกฎหมายได้ด้วย

ดังนี้ ในทางปฏิบัติ อาจสรุปได้ว่าต้องมีการดำเนินการดังนี้

- **การให้ความคุ้มครองการคุ้มครองข้อมูลส่วนบุคคลโดยการออกแบบและโดยค่าเริ่มต้น**
- **ดำเนินการการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment – DPIA)**
- **การทำบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล**
- **การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด**

การคุ้มครองข้อมูลส่วนบุคคลโดยการออกแบบและโดยค่าเริ่มต้น

การคุ้มครองข้อมูลส่วนบุคคลโดยการออกแบบ (Data Protection by Design) เป็นการคุ้มครองข้อมูลส่วนบุคคลตั้งแต่กระบวนการออกแบบ ซึ่งในการวางแผนจะต้องครอบคลุมตั้งแต่ขั้นตอนแรกจนไปถึงขั้นตอนสุดท้ายของการออกแบบระบบ และการคุ้มครองจะเริ่มตั้งแต่ก่อนมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและนำเข้าข้อพิจารณาการคุ้มครองข้อมูลส่วนบุคคลในการวางแผน โดยต้องนำมาตรการป้องกันที่เหมาะสมเข้าไปใช้ด้วย เช่น การใช้นามแฝง (Data pseudonymization) การจัดเก็บเฉพาะเท่าที่จำเป็น (Data minimization)

การคุ้มครองข้อมูลส่วนบุคคลโดยค่าเริ่มต้น (Data Protection by Default) เป็นแนวทางในการออกแบบกระบวนการให้มีการคุ้มครองข้อมูลส่วนบุคคลอย่างอัตโนมัติ โดยนำเกณฑ์ที่เจ้าของข้อมูลส่วนบุคคลได้เลือกไว้ไปใช้ในขั้นตอนการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งในการจำกัดการเก็บรวบรวม ใช้ การเก็บรักษา และการเข้าถึงข้อมูลส่วนบุคคล ทั้งนี้ การตั้งค่าที่จำเป็นที่สุดเพื่อการคุ้มครองข้อมูลส่วนบุคคล นั้นควรถูกตั้งเป็นค่าเริ่มต้น และให้เจ้าของข้อมูลส่วนบุคคลสามารถเลือกในการตั้งค่าที่อาจทำให้เกิดความเสี่ยงแก่ข้อมูลส่วนบุคคลของตนเองสูงขึ้น ซึ่งข้อคำนึงในการพิจารณา เช่น วัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จำนวนข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม ขอบเขตการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ระยะเวลาการเก็บข้อมูล และการเข้าถึงข้อมูล

การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment – DPIA) หรืออาจเรียกว่า การประเมินผลกระทบด้านความเป็นส่วนตัว (privacy impact assessment) มีประโยชน์ในการช่วยองค์กรในการพิจารณานำการคุ้มครองข้อมูลส่วนบุคคลไปใช้ในการวางแผนการดำเนินการคุ้มครองข้อมูลส่วนบุคคลขององค์กร และสามารถแสดงแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลให้ทราบถึงการปฏิบัติขององค์กรที่สอดคล้องกับกฎหมาย

การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

เนื่องจากการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลจึงจำเป็นต้องจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลเพื่อช่วยให้สามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปในทิศทางเดียวกันกับเงื่อนไขและข้อกำหนดของกฎหมายในประเด็นต่าง ๆ ดังนี้

(1) ในกรณีผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธการเข้าถึงข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งให้เจ้าของข้อมูลทราบถึงผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น

(2) ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อเทคโนโลยีมีการเปลี่ยนแปลง

(3) แจ้งเหตุละเมิดข้อมูลส่วนบุคคลพร้อมกับแนวทางการเยียวยาแก่เจ้าของข้อมูลส่วนบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล

(4) ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องจัดให้มีบันทึกรายการในกรณีที่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

(5) ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องจัดให้มีคำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 39 และ 40

การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

ทั้งนี้ หากอ้างอิงตามข้อบังคับในกฎหมายของสหภาพยุโรปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ความเป็นส่วนตัว (General Data Protection Regulation - GDPR) แล้ว ในการทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลนั้น ต้องครอบคลุม 3 ประเด็นสำคัญดังต่อไปนี้

1) รายละเอียดการประมวลผลข้อมูลส่วนบุคคล โดยรวมถึงวัตถุประสงค์และฐานทางกฎหมายที่ใช้

2) ความจำเป็นในการประมวลผล ความได้สัดส่วน ความเสี่ยงที่อาจเกิดขึ้นแก่เจ้าของข้อมูลส่วนบุคคล

3) มาตรการในการลดหรือจัดการความเสี่ยงที่เหมาะสม

กล่าวโดยสรุป นอกจากความจำเป็นที่ต้องทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลภายใต้กฎหมายแล้ว การจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลเป็นเครื่องมือที่มีประโยชน์ในการประเมินผลกระทบต่อสิทธิเสรีภาพของบุคคลที่เกิดจากการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อที่องค์กรจะได้สามารถปรับปรุงโครงสร้างการดำเนินงานอย่างเป็นระบบและมีความปลอดภัยในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

นโยบายการคุ้มครองข้อมูลส่วนบุคคล

นโยบายภายในด้านการคุ้มครองข้อมูลส่วนบุคคลอาจเป็นเครื่องมือที่เป็นประโยชน์ขององค์กรเพื่อให้มั่นใจว่า บุคลากรขององค์กรได้รับการอบรมที่เหมาะสมเพื่อจะได้สามารถปฏิบัติตามกฎหมายได้ จุดประสงค์ของนโยบายการคุ้มครองข้อมูลส่วนบุคคลคือการอธิบายแก่บุคลากรว่าในการดำเนินการใด ๆ กับข้อมูลส่วนบุคคลนั้น มีสิ่งใดบ้างที่สามารถทำได้และมีสิ่งใดบ้างที่ไม่สามารถทำได้ และยังช่วยกำหนดขั้นตอนการดำเนินการรวมถึงผลที่จะเกิดตามมาหากมีการฝ่าฝืนนโยบาย ในการออกแบบนโยบายการคุ้มครองข้อมูลส่วนบุคคลนั้น ควรคำนึงถึงประเด็นดังต่อไปนี้

- มีข้อความกระชับ และเข้าใจได้ง่าย
- ต้องให้แน่ใจว่าสามารถดำเนินการได้จริง และภายในเวลาที่ทันท่วงที

บันทึกกิจกรรมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

บันทึกการประมวลผลข้อมูลส่วนบุคคลเป็นวิธีหนึ่งที่ช่วยในการแสดงได้ว่า องค์กรได้ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แล้ว ซึ่งเป็นวิธีการแสดงออกถึงความรับผิดชอบอย่างหนึ่ง โดยจะทำบันทึกเป็นหนังสือหรือในรูปแบบระบบอิเล็กทรอนิกส์ก็ได้

ทั้งนี้ ตามมาตรา 39 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกรายการอย่างน้อยดังต่อไปนี้

(1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

(2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

(3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

(4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

(6) การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับการยกเว้นไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(7) การปฏิเสธคำขอหรือการคัดค้านของเจ้าของข้อมูลส่วนบุคคล

(8) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย

ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนดไม่จำเป็นต้องทำบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล เว้นแต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26

บันทึกกิจกรรมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ในส่วนของผู้ประมวลผลข้อมูลส่วนบุคคลนั้น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดไว้ในมาตรา 40 ให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด ซึ่งตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 3 ได้กำหนดให้การทำบันทึกดังกล่าวต้องทำเป็นลายลักษณ์อักษร โดยจะจัดทำเป็นหนังสือหรือในรูปแบบอิเล็กทรอนิกส์ก็ได้ โดยต้องมีรายละเอียดที่ต้องทำการบันทึก ดังนี้

(1) ชื่อและข้อมูลเกี่ยวกับผู้ประมวลผลข้อมูลส่วนบุคคล และตัวแทนของผู้ประมวลผลข้อมูลส่วนบุคคลในกรณีที่มีการแต่งตั้งตัวแทน

(2) ชื่อและข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลที่ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลนั้น และตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลในกรณีที่มีการแต่งตั้งตัวแทน

(3) ชื่อและข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล รวมถึงสถานที่ติดต่อและวิธีการติดต่อ ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(4) ประเภทหรือลักษณะของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งรวมถึงข้อมูลส่วนบุคคลและวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล

(5) ประเภทของบุคคลหรือหน่วยงานที่ได้รับข้อมูลส่วนบุคคล ในกรณีที่มีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

(6) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล คือ บุคคลผู้ที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลแต่งตั้งขึ้น เพื่อให้มั่นใจว่าการดำเนินการปฏิบัติกับข้อมูลส่วนบุคคลขององค์กรนั้นเป็นไปตามที่กฎหมายกำหนด โดยผู้ที่ได้รับการแต่งตั้งเป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลนั้น ควรเป็นผู้ที่มีความรู้ความเชี่ยวชาญทั้งด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคลและการคุ้มครองข้อมูลส่วนบุคคลในทางปฏิบัติ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 41 กำหนดผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ดังนี้

1) หน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด เช่น กระทรวงต่าง ๆ สถาบันอุดมศึกษาของรัฐที่มีสถานพยาบาลในสังกัด
2) กรณีผู้ควบคุมข้อมูลส่วนบุคคลมีกิจกรรมหลัก เป็นการประมวลผลข้อมูลซึ่งมีการติดตามเจ้าของข้อมูลจำนวนมาก อย่างสม่ำเสมอ และเป็นระบบตามที่คณะกรรมการประกาศกำหนด
3) กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีกิจกรรมหลักเป็นการประมวลผลข้อมูลส่วนบุคคลตามมาตรา 26

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

อนึ่ง ตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 (2) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566 ข้อ 6 การดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นส่วนหนึ่งของกิจกรรมหลักที่มีข้อมูลส่วนบุคคลเป็นจำนวนมาก (on a large scale) ให้พิจารณาจากปัจจัย ดังต่อไปนี้

(1) จำนวนเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง หรือสัดส่วนของจำนวนเจ้าของข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม ใช้ หรือเปิดเผย เมื่อเทียบกับจำนวนเจ้าของข้อมูลส่วนบุคคลทั้งหมดที่อาจเป็นไปได้

(2) ปริมาณ ประเภท หรือลักษณะของข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม ใช้ หรือเปิดเผย

(3) ระยะเวลา (duration) หรือความคงอยู่ (permanence) ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อประโยชน์ในการดำเนินกิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

(4) ขอบเขตการใช้ข้อมูลส่วนบุคคลขององค์กร หรือตามขนาดพื้นที่หรือจำนวนประเทศที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ทั้งนี้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในกรณีดังต่อไปนี้ ให้ถือเป็นกรณีที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากด้วย

(1) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ซึ่งเป็นส่วนหนึ่งของกิจกรรมหลัก โดยมีจำนวนเจ้าของข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตั้งแต่ 100,000 รายขึ้นไป

(2) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ด้านการโฆษณาตามพฤติกรรม (behavioral advertising) ผ่านโปรแกรมค้นหา (search engine) หรือสื่อสังคมออนไลน์ (social media) ที่มีผู้ใช้งานอย่างกว้างขวาง

(3) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกค้าหรือผู้รับบริการตามการดำเนินงานปกติโดยบริษัทตามกฎหมายว่าด้วยประกันชีวิต บริษัทตามกฎหมายว่าด้วยประกันวินาศภัย ผู้ประกอบธุรกิจสถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน ทั้งนี้ ไม่รวมถึงการดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

(4) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกค้าหรือผู้รับบริการโดยผู้รับใบอนุญาตประกอบกิจการโทรคมนาคมแบบที่สามตามกฎหมายว่าด้วยการประกอบกิจการโทรคมนาคม

(5) กรณีอื่นตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

มาตรา 42 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไว้ดังต่อไปนี้

(1) ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

(2) ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลรวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

(3) ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลรวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

(4) รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ในกรณีที่มีปัญหาในการปฏิบัติหน้าที่ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องสามารถรายงานไปยังผู้บริหารสูงสุดของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลโดยตรงได้

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

นอกจากนี้ กฎหมายยังกำหนดให้ ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยจัดหาเครื่องมือหรืออุปกรณ์อย่างเพียงพอ รวมทั้งอำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคลเพื่อการปฏิบัติหน้าที่

ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจะให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลออกจากงานหรือเลิกสัญญาการจ้างด้วยเหตุที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลปฏิบัติหน้าที่ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลไม่ได้

อย่างไรก็ดี แม้จะไม่ใช่ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจำเป็นต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายกำหนดก็ตาม ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลก็อาจเลือกที่จะแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลก็ได้ เพื่อช่วยในการออกแบบการจัดการคุ้มครองข้อมูลส่วนบุคคลและจะได้มั่นใจว่าได้ปฏิบัติถูกต้องตามกฎหมาย

แบบทดสอบ บทที่ 10

ข้อที่ 1

Q : <u>จริงหรือเท็จ</u>

4.1) ทั้งผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต่างก็มีหน้าที่ความรับผิดชอบภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

4.2) การคุ้มครองข้อมูลส่วนบุคคลโดยการออกแบบ (Data Protection by Design) เป็นการคุ้มครองข้อมูลส่วนบุคคลซึ่งเริ่มตั้งแต่ก่อนมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และนำเข้าข้อพิจารณาการคุ้มครองข้อมูลในขั้นตอนการวางแผน

4.3) กฎหมายกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องติดต่อหน่วยงานกำกับดูแลหลังจากดำเนินการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลและก่อนการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลทุกครั้ง

4.4) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องเป็นผู้ที่มีความเชี่ยวชาญทั้งด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคลและการดำเนินการคุ้มครองข้อมูลส่วนบุคคลในทางปฏิบัติ

แบบทดสอบ บทที่ 10

ข้อที่ 2

Q : ประโยชน์ที่สำคัญหลัก ๆ ของการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลคือประการใดบ้าง

ก. การนำข้อพิจารณาปัจจัยการคุ้มครองข้อมูลเข้ามาในการวางแผนเชิงองค์กร

ข. กำหนดวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

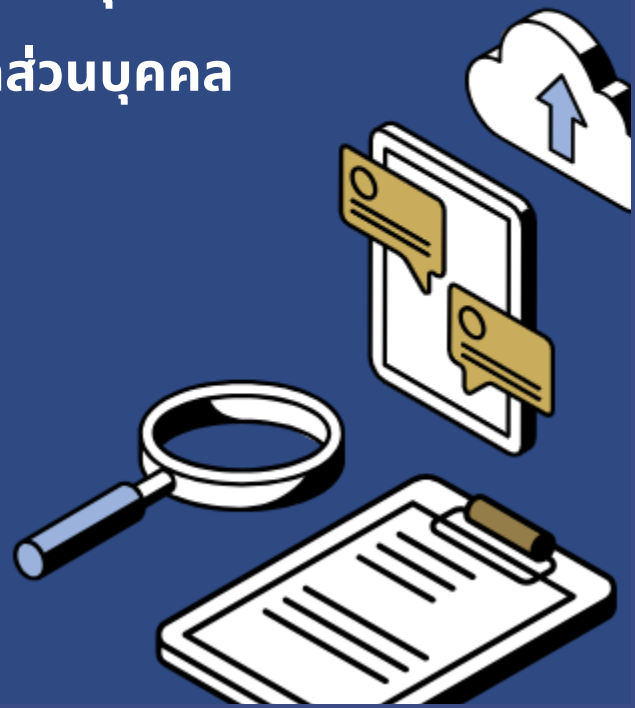
ค. แสดงให้เห็นถึงการปฏิบัติตามกฎหมายต่อหน่วยงานกำกับดูแล

ง. กำหนดวิธีการของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

แบบทดสอบ บทที่ 10

ข้อที่ 3

Q : รายการใดซึ่งกฎหมายกำหนดให้ต้องมีอยู่ในบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคล แต่ไม่จำเป็นต้องมีในบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูลส่วนบุคคล



แบบทดสอบ บทที่ 10

ข้อที่ 4

Q : กรณีใดบ้างที่ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

• เฉลยแบบทดสอบบทที่ 10

ข้อที่	เฉลย
1.	1.1 จริง 1.2 จริง 1.3 เท็จ 1.4 จริง
2.	ก. และ ค.
3.	(1) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล (2) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น (3) การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับการยกเว้นไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (4) การปฏิเสธคำขอหรือการคัดค้านของเจ้าของข้อมูลส่วนบุคคล
4.	(1) หน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด เช่น กระทรวงต่าง ๆ สถาบันอุดมศึกษาของรัฐที่มีสถานพยาบาลในสังกัด (2) กรณีผู้ควบคุมข้อมูลส่วนบุคคลมีกิจกรรมหลัก เป็นการประมวลผลข้อมูลซึ่งมีการติดตามเจ้าของข้อมูลส่วนบุคคลจำนวนมาก อย่างสม่ำเสมอ และเป็นระบบตามที่คณะกรรมการประกาศกำหนด (3) กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีกิจกรรมหลักเป็นการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว

การกำกับดูแลและบังคับใช้กฎหมาย

บทที่ 11

- บทนำ
- คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- กลไกการคุ้มครองข้อมูลส่วนบุคคล ความรับผิดและบทกำหนดโทษ
- แบบทดสอบ

บทนำ

ในบทนี้จะกล่าวถึงกลไกการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และหน่วยงานที่เกี่ยวข้องในกระบวนการกำกับดูแลและการบังคับใช้กฎหมายซึ่งได้แก่ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และคณะกรรมการผู้เชี่ยวชาญซึ่งมีอำนาจในการพิจารณาออกคำสั่งลงโทษปรับทางปกครองตามที่กฎหมายกำหนด มาตรการเพื่อบังคับการให้เป็นไปตามกฎหมายได้แก่ ความรับผิดทางแพ่ง โทษทางอาญา และโทษทางปกครอง

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

หรือ กคส. ประกอบด้วยกรรมการโดยตำแหน่งและโดยการสรรหา ดังต่อไปนี้

(1) ประธานกรรมการ

(2) ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (รองประธานกรรมการ)

(3) กรรมการโดยตำแหน่ง จำนวน 5 คน ได้แก่ ปลัดสำนักนายกรัฐมนตรี เลขาธิการคณะกรรมการกฤษฎีกา เลขาธิการคณะกรรมการคุ้มครองผู้บริโภค อธิบดีกรมคุ้มครองสิทธิและเสรีภาพ และอัยการสูงสุด

(4) กรรมการผู้ทรงคุณวุฒิ จำนวน 9 คน

(5) เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (กคส.) มีหน้าที่และอำนาจดังต่อไปนี้

(1) จัดทำแผนแม่บทการดำเนินงานด้านการส่งเสริม และการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับนโยบาย ยุทธศาสตร์ชาติ และแผนระดับชาติที่เกี่ยวข้อง เพื่อเสนอต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติตามกฎหมายว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

(2) ส่งเสริมและสนับสนุนหน่วยงานของรัฐและภาคเอกชน ดำเนินกิจกรรมตามแผนแม่บทตาม (1) รวมทั้งจัดให้มีการประเมินผลการดำเนินงานตามแผนแม่บทดังกล่าว

(3) กำหนดมาตรการหรือแนวทางการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

(4) ออกประกาศหรือระเบียบเพื่อให้การดำเนินการเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

(5) ประกาศกำหนดหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

(6) ประกาศกำหนดข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลเป็นแนวทางให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติ

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(7) เสนอแนะต่อคณะรัฐมนตรีให้มีการตราหรือปรับปรุงกฎหมายหรือกฎที่ใช้บังคับอยู่ในส่วนที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

(8) เสนอแนะต่อคณะรัฐมนตรีในการตราพระราชกฤษฎีกาหรือทบทวนความเหมาะสมของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อย่างน้อยทุกรอบห้าปี

(9) ให้คำแนะนำและคำปรึกษาเกี่ยวกับการดำเนินการใด ๆ เพื่อให้ความคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐและภาคเอกชนในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

(10) ตีความและวินิจฉัยชี้ขาดปัญหาที่เกิดจากการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

(11) ส่งเสริมและสนับสนุนให้เกิดทักษะการเรียนรู้และความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้แก่ประชาชน

(12) ส่งเสริมและสนับสนุนการวิจัย เพื่อพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

(13) ปฏิบัติการอื่นใดตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือกฎหมายอื่นกำหนดให้เป็นหน้าที่และอำนาจของคณะกรรมการ

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้จัดตั้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลขึ้น โดยมีวัตถุประสงค์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งส่งเสริมและสนับสนุนให้เกิดการพัฒนาด้านการคุ้มครองข้อมูลส่วนบุคคลของประเทศ โดยให้มีสถานะเป็นหน่วยงานของรัฐ มีฐานะเป็นนิติบุคคล นอกจากหน้าที่และอำนาจในการดำเนินการให้เป็นไปตามวัตถุประสงค์ดังกล่าวข้างต้นแล้ว ให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมีหน้าที่ปฏิบัติงานวิชาการและงานธุรการให้แก่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการผู้เชี่ยวชาญ และคณะอนุกรรมการ รวมทั้งให้มีหน้าที่และอำนาจดังต่อไปนี้

(1) จัดทำร่างแผนแม่บทการดำเนินงานด้านการส่งเสริม และการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับนโยบาย ยุทธศาสตร์ชาติ และแผนระดับชาติที่เกี่ยวข้อง รวมทั้งร่างแผนแม่บทและมาตรการแก้ไขปัญหาอุปสรรคการปฏิบัติการตามนโยบาย ยุทธศาสตร์ชาติ และแผนระดับชาติดังกล่าว เพื่อเสนอต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(2) ส่งเสริมและสนับสนุนการวิจัย เพื่อพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

(3) วิเคราะห์และรับรองความสอดคล้องและความถูกต้องตามมาตรฐานหรือตามมาตรการหรือกลไกการกำกับดูแลที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งตรวจสอบและรับรองนโยบายในการคุ้มครองข้อมูลส่วนบุคคลตามมาตรา 29

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(4) สำรวจ เก็บรวบรวมข้อมูล ติดตามความเคลื่อนไหวของสถานการณ์ด้านการคุ้มครองข้อมูลส่วนบุคคล และแนวโน้มการเปลี่ยนแปลงด้านการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งวิเคราะห์และวิจัยประเด็นทางด้านการคุ้มครองข้อมูลส่วนบุคคลที่มีผลต่อการพัฒนาประเทศเพื่อเสนอต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(5) ประสานงานกับส่วนราชการ รัฐวิสาหกิจ ราชการส่วนท้องถิ่น องค์การมหาชน หรือหน่วยงานอื่นของรัฐเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

(6) ให้คำปรึกษาแก่หน่วยงานของรัฐและหน่วยงานของเอกชนเกี่ยวกับการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

(7) เป็นศูนย์กลางในการให้บริการทางวิชาการหรือให้บริการที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแก่หน่วยงานของรัฐ หน่วยงานของเอกชน และประชาชน รวมทั้งเผยแพร่และให้ความรู้ความเข้าใจในเรื่องการคุ้มครองข้อมูลส่วนบุคคล

(8) กำหนดหลักสูตรและฝึกอบรมการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง หรือประชาชนทั่วไป

(9) ทำความตกลงและร่วมมือกับองค์การหรือหน่วยงานทั้งในประเทศและต่างประเทศในกิจการที่เกี่ยวกับการดำเนินการตามหน้าที่และอำนาจของสำนักงาน เมื่อได้รับความเห็นชอบจากคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(10) ติดตามและประเมินผลการปฏิบัติพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

(11) ปฏิบัติหน้าที่อื่นตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการผู้เชี่ยวชาญ หรือคณะอนุกรรมการมอบหมาย หรือตามที่กฎหมายกำหนด

กลไกการคุ้มครองข้อมูลส่วนบุคคล ความรับผิดและบทกำหนดโทษ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดหน้าที่ขององค์กรในฐานะผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องปฏิบัติไว้หลายประการ พร้อมทั้งได้กำหนดมาตรการเพื่อบังคับการให้เป็นไปตามกฎหมายไว้ด้วยกล่าวคือ กำหนดให้องค์กรอาจมีความรับผิดทางแพ่ง โทษทางอาญา และโทษทางปกครอง ในกรณีที่องค์กรปฏิบัติฝ่าฝืนกฎหมาย ซึ่งเป็นการบัญญัติที่สอดคล้องกับกฎหมายอีกหลาย ๆ ฉบับที่ต้องการให้มีมาตรการบังคับเพื่อให้เป็นไปตามกฎหมาย

ความรับผิดทางแพ่ง

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนด “**ความรับผิดทางแพ่ง**” ไว้ในมาตรา 77 และมาตรา 78 ดังนี้

มาตรา 77 ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลอันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะพิสูจน์ได้ว่า

(1) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง

(2) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย

ค่าสินไหมทดแทนตามวรรคหนึ่ง ให้หมายความรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย

ความรับผิดทางแพ่ง

มาตรา 78 ให้ศาลมีอำนาจสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจ่ายค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มขึ้นจากจำนวนค่าสินไหมทดแทนที่แท้จริงที่ศาลกำหนดได้ตามที่ศาลเห็นสมควร แต่ไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริงนั้น ทั้งนี้ โดยคำนึงถึงพฤติการณ์ต่าง ๆ เช่น ความร้ายแรงของความเสียหายที่เจ้าของข้อมูลส่วนบุคคลได้รับ ผลประโยชน์ที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้รับ สถานะทางการเงินของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล การที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้บรรเทาความเสียหายที่เกิดขึ้น หรือการที่เจ้าของข้อมูลส่วนบุคคลมีส่วนในการก่อให้เกิดความเสียหายด้วย

สิทธิเรียกร้องค่าเสียหายอันเกิดจากการละเมิดข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้เป็นอันขาดอายุความเมื่อพ้นสามปีนับแต่วันที่ผู้เสียหายรู้ถึงความเสียหายและรู้ตัวผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องรับผิด หรือเมื่อพ้นสิบปีนับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล

ความรับผิดทางแพ่ง

จากบทบัญญัติดังกล่าว หลักการสำคัญเกี่ยวกับความรับผิดทางแพ่งตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีดังต่อไปนี้

(1) นำหลักความรับผิดโดยเคร่งครัด (Strict Liability) มาใช้บังคับ กล่าวคือ

ก. ผู้ควบคุมข้อมูลส่วนบุคคลหรือประมวลผลข้อมูลส่วนบุคคล

ข. ฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ค. ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล

ง. ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล

จ. ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม

ฉ. เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะพิสูจน์ได้ว่า

1) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง

2) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย

ดังนั้น ภาระการพิสูจน์จึงเป็นของผู้ควบคุมข้อมูลส่วนบุคคลหรือประมวลผลข้อมูลส่วนบุคคลที่จะต้องพิสูจน์ให้ได้การกระทำของตนว่าเข้าเงื่อนไขตาม 1) หรือ 2) เท่านั้น หากพิสูจน์ไม่ได้ ก็จะมีความรับผิดทางแพ่งตามที่กฎหมายกำหนด

ความรับผิดทางแพ่ง

(2) ค่าสินไหมทดแทน รวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย

(3) ศาลมีอำนาจกำหนดค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มขึ้นจากจำนวนค่าสินไหมทดแทนที่แท้จริงที่ศาลกำหนดได้ตามที่ศาลเห็นสมควรแต่ไม่เกิน 2 เท่าของค่าสินไหมทดแทนที่แท้จริงนั้น (ผู้เสียหายจะได้รับ “ค่าสินไหมทดแทนที่แท้จริง” และ “ค่าสินไหมทดแทนเพื่อการลงโทษอีกไม่เกิน 2 เท่าของค่าสินไหมทดแทนที่แท้จริง”)

(4) อายุความการฟ้องคดีเพื่อเรียกค่าเสียหายภายใน 3 ปีนับแต่วันที่ผู้เสียหายรู้ถึงความเสียหายและรู้ตัวผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องรับผิด แต่ไม่เกิน 10 ปีนับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล

(5) ความรับผิดทางแพ่งตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผู้เสียหายอาจดำเนินคดีแบบกลุ่ม (Class Action) ได้ตามประมวลกฎหมายวิธีพิจารณาความแพ่ง

โทษทางปกครอง

ความรับผิดทางปกครองและมาตรการบังคับทางปกครองถือเป็นกลไกสำคัญในการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยกฎหมายกำหนดให้แต่งตั้ง **คณะกรรมการผู้เชี่ยวชาญ** ให้มีหน้าที่และอำนาจ ดังต่อไปนี้

(1) พิจารณาเรื่องร้องเรียนตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

(2) ตรวจสอบการกระทำใด ๆ ของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับข้อมูลส่วนบุคคลที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล

(3) ไกล่เกลี่ยข้อพิพาทเกี่ยวกับข้อมูลส่วนบุคคล

(4) ปฏิบัติการอื่นใดตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้เป็นหน้าที่และอำนาจของคณะกรรมการผู้เชี่ยวชาญหรือตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมอบหมาย

โทษทางปกครอง

โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือประกาศที่ออกตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยการยื่นการไม่รับเรื่อง การยุติเรื่อง การพิจารณา และระยะเวลาในการพิจารณาคำร้องเรียนให้เป็นไปตามระเบียบที่คณะกรรมการประกาศกำหนด โดยคำนึงถึงการกำหนดให้ไม่รับเรื่องร้องเรียนหรือยุติเรื่องในกรณีที่มีผู้มีอำนาจพิจารณาในเรื่องนั้นอยู่แล้วตามกฎหมายอื่นด้วย

คำร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญให้ยื่นโดยวิธีการใดวิธีการหนึ่ง ดังต่อไปนี้

(1) ยื่นโดยตรงต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(2) ยื่นผ่านทางไปรษณีย์มายังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(3) ยื่นผ่านทางช่องทางอิเล็กทรอนิกส์หรือช่องทางอื่นใดตามที่สำนักงานสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

โทษทางปกครอง

ในการพิจารณาออกคำสั่งลงโทษปรับทางปกครอง หรือใช้มาตรการบังคับทางปกครองเพื่อลงโทษปรับทางปกครองกับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลหรือบุคคลอื่นที่เกี่ยวข้อง คณะกรรมการผู้เชี่ยวชาญต้องคำนึงถึงปัจจัย ดังต่อไปนี้

(1) รายละเอียดความผิดที่เกิดขึ้น โดยเฉพาะกรณีที่เป็นการกระทำผิดโดยเจตนาหรือจงใจหรือประมาทเลินเล่ออย่างร้ายแรงหรือขาดความระมัดระวังตามสมควร

(2) ความร้ายแรงของพฤติกรรมที่กระทำผิด

(3) ขนาดของกิจการของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

(4) ผลของมาตรการลงโทษปรับทางปกครองที่จะบังคับว่าได้ช่วยบรรเทาความเสียหาย หรือความเดือดร้อนแก่เจ้าของข้อมูลส่วนบุคคลหรือไม่ เพียงใด

(5) ประโยชน์ที่เจ้าของข้อมูลส่วนบุคคลจะได้รับจากมาตรการลงโทษทางปกครอง และผลกระทบต่อผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลหรือบุคคลที่กระทำผิดและผลกระทบในวงกว้างต่อธุรกิจหรือกิจการอื่นที่เกี่ยวข้อง

โทษทางปกครอง

(6) มูลค่าความเสียหายและความร้ายแรงที่เกิดจากการกระทำผิดนั้น

(7) ระดับโทษปรับทางปกครองและมาตรการลงโทษทางปกครองที่เคยใช้กับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลรายอื่นในความผิดทำนองเดียวกัน (ถ้ามี)

(8) ประวัติการถูกลงโทษทางปกครองของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล และในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นนิติบุคคล ให้หมายความรวมถึงประวัติการถูกลงโทษปรับทางปกครองของบุคคลที่เกี่ยวข้องกับการกระทำของนิติบุคคลนั้น

(9) ระดับความรับผิดชอบและมาตรฐานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลขณะที่มีการกระทำความผิด

(10) การดำเนินการตามประมวลจริยธรรม แนวปฏิบัติทางธุรกิจ หรือมาตรฐานในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลขณะที่มีการกระทำความผิด

(11) การเยียวยาและบรรเทาความเสียหายของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเมื่อทราบเหตุที่กระทำความผิด

(12) การชดใช้ค่าสินไหมทดแทนเพื่อเยียวยาความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล

(13) ข้อเท็จจริงอื่น ๆ ที่เกี่ยวข้อง

โทษทางปกครอง

ในการพิจารณาออกคำสั่งลงโทษปรับทางปกครอง ให้คณะกรรมการผู้เชี่ยวชาญพิจารณาออกคำสั่งตามระดับความร้ายแรงของการกระทำความผิดและความเหมาะสมในการปรับใช้มาตรการลงโทษ ดังนี้

(1) กรณีไม่ร้ายแรง

ให้คณะกรรมการผู้เชี่ยวชาญมีคำสั่งให้แก้ไขหรือตักเตือนในเบื้องต้นก่อนโดยอาจดำเนินการ ดังนี้

(ก) ตักเตือนหรือสั่งให้ปฏิบัติ หรือดำเนินการแก้ไข หยุด ระงับ ละเว้น หรืองดเว้นการกระทำที่ฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายให้ถูกต้องภายในระยะเวลาที่กำหนด โดยคำสั่งดังกล่าวต้องมีรายละเอียด เหตุผล และวัตถุประสงค์ของคำสั่งอย่างชัดเจนว่าจะต้องแก้ไขและดำเนินการให้ถูกต้องตามกฎหมายอย่างไร

(ข) สั่งห้ามกระทำการที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลหรือให้กระทำการใดเพื่อระงับความเสียหายนั้นภายในระยะเวลาที่กำหนด

(ค) สั่งจำกัดการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีการกระทำผิดไว้เพื่อระงับความเสียหายนั้นภายในระยะเวลาที่กำหนด

คำสั่งตาม (ก) (ข) หรือ (ค) อาจกำหนดเงื่อนไขหรือวิธีการปรับปรุงบุคลากร กระบวนการ หรือเทคโนโลยี ให้มีประสิทธิภาพและความเหมาะสมตามที่คณะกรรมการผู้เชี่ยวชาญเห็นสมควร

โทษทางปกครอง

(2) กรณีร้ายแรง หรือคำสั่งตักเตือนหรือให้แก้ไขไม่เป็นผล

กฎหมายกำหนดให้คณะกรรมการผู้เชี่ยวชาญมีคำสั่งลงโทษปรับทางปกครองแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลหรือบุคคลที่เกี่ยวข้อง โดยคำนึงถึงความร้ายแรงและพฤติการณ์อื่นในการลงโทษปรับทางปกครองตามที่เห็นสมควร และอาจมีคำสั่งตาม (1) (ก) (ข) หรือ (ค) ด้วยก็ได้

คำสั่งของคณะกรรมการผู้เชี่ยวชาญให้เป็นที่สุด แต่ทั้งนี้ไม่เป็นการตัดสิทธิคู่กรณีที่จะฟ้องเพิกถอนคำสั่งทางปกครองของคณะกรรมการผู้เชี่ยวชาญต่อศาลปกครอง ภายในระยะเวลา 90 วันนับแต่วันที่รู้หรือควรรู้ถึงเหตุแห่งการฟ้องคดีตามเงื่อนไขที่กฎหมายกำหนด

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดโทษปรับทางปกครองไว้ในอัตราต่าง ๆ กัน ขึ้นอยู่กับลักษณะของการกระทำความผิด ตัวอย่างเช่น

(1) ต้องระวางโทษปรับทางปกครองไม่เกิน 1,000,000 บาท ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่ปฏิบัติตามมาตรา 23 มาตรา 30 วรรคสี่ มาตรา 39 วรรคหนึ่ง มาตรา 41 วรรคหนึ่ง หรือมาตรา 42 วรรคสองหรือวรรคสาม หรือไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนดตามมาตรา 19 วรรคสาม หรือไม่แจ้งผลกระทบจากการถอนความยินยอมตามมาตรา 19 วรรคหก หรือไม่ปฏิบัติตามมาตรา 23 ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 25 วรรคสอง

โทษทางปกครอง

(2) ต้องระวางโทษปรับทางปกครองไม่เกิน 3,000,000 บาท ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา 21 มาตรา 22 มาตรา 24 มาตรา 25 วรรคหนึ่ง มาตรา 27 วรรคหนึ่งหรือวรรคสอง มาตรา 28 มาตรา 32 วรรคสอง หรือมาตรา 37 หรือขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ หรือไม่ปฏิบัติตามมาตรา 21 ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 25 วรรคสอง หรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม

(3) ต้องระวางโทษปรับทางปกครองไม่เกิน 5,000,000 บาท ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลฝ่าฝืนมาตรา 26 วรรคหนึ่งหรือวรรคสาม หรือฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง หรือมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 หรือส่งหรือโอนข้อมูลส่วนบุคคลตามมาตรา 26 โดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม

(4) ต้องระวางโทษปรับทางปกครองไม่เกิน 3,000,000 บาท ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลไม่ปฏิบัติตามมาตรา 40 โดยไม่มีเหตุอันควร หรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม หรือไม่ปฏิบัติตามมาตรา 37 (5) ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 38 วรรคสอง

โทษทางอาญา

มาตรการลงโทษหนึ่งที่ถูกกำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่มักถูกกล่าวถึงเสมอคือ **“โทษทางอาญา”** ของผู้บริหารนิติบุคคลซึ่งกฎหมายกำหนดขึ้นเพื่อให้ผู้บริหารของนิติบุคคลปฏิบัติหน้าที่ตามกฎหมายว่าด้วยความรับผิดชอบ (accountability) หากมีหน้าที่ในฐานะผู้นำขององค์กรควรสั่งการหรือกระทำการให้สอดคล้องกับกฎหมายก็พึงต้องกระทำ ในขณะเดียวกันก็ต้องไม่เพิกเฉยหรือละเลย ละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิดอีกด้วย ซึ่งกฎหมายหลาย ๆ ฉบับก็มีมาตรการบังคับในทำนองเดียวกัน ตัวอย่างเช่น มาตรา 77 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งเป็นกฎหมายที่ตราขึ้นในช่วงเวลาเดียวกัน เป็นต้น

ขณะที่ในบริบทของสังคมโลก ก็มีการนำมาตรการลงโทษทางอาญามาใช้เพื่อบังคับการให้เป็นไปตามกฎหมายเช่นเดียวกัน ในโอกาสนี้ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ขอยกกรณีศึกษาของ 2 ประเทศ อาทิ ประเทศเยอรมนี และประเทศสิงคโปร์ เป็นต้น

โทษทางอาญา

ประเทศเยอรมนี ตาม GDPR นั้นจะไม่มีบทกำหนดโทษทางอาญา มีแต่ค่าปรับทางปกครองในอัตราที่สูงมาก โดยค่าปรับในอัตราสูงสุดจะอยู่ที่ร้อยละ 4 ของผลประกอบการรวมจากทั่วโลก (ไม่ใช่เฉพาะแต่ผลประกอบการในสหภาพยุโรป) แต่การที่ GDPR ไม่มีบทกำหนดโทษทางอาญาไม่ใช่ว่าสหภาพยุโรปจะเห็นว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลไม่ควรมีโทษทางอาญา แต่เพราะว่า “การลงโทษทางอาญา” ไม่อยู่ในขอบอำนาจของสหภาพยุโรป ดังนั้น กฎหมายของสหภาพยุโรป “จึงไม่มีโทษทางอาญา”

อย่างไรก็ตาม การกำหนดโทษทางอาญายังคงเป็นอำนาจของรัฐสมาชิก รัฐสมาชิกสามารถกำหนดมาตรการเพิ่มเติมเท่าที่ไม่ขัดหรือแย้งกับ GDPR เพื่อให้กฎหมายมีผลใช้บังคับได้ ในประเทศเยอรมนีที่มีการตรา Federal Data Protection Act 2017 (BDSG) ขึ้นก็มีการกำหนดโทษทางอาญาไว้ในมาตรา 42 ของกฎหมายดังกล่าวโดยกำหนดโทษจำคุกไว้ไม่เกิน 3 ปีหรือปรับในกรณีที่กระทำผิดเงื่อนไขเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

โทษทางอาญา

ประเทศสิงคโปร์ ได้มีการแก้ไขกฎหมายคุ้มครองข้อมูลส่วนบุคคลตาม Personal Data Protection (Amendment) Act 2020 (No. 40 of 2020) มีผลใช้บังคับเมื่อวันที่ 1 กุมภาพันธ์ 2564 โดยเพิ่มเติมบทบัญญัติว่าด้วยความรับผิดทางอาญาไว้ 3 กรณี ได้แก่

(1) การเปิดเผยข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย (Singapore PDPA section 48D)

(2) การใช้ข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมายและทำให้ได้มาซึ่งผลประโยชน์หรือทำให้เกิดความเสียหายต่อบุคคล (Singapore PDPA section 48E)

(3) การระบุกับอัตลักษณ์ของบุคคล (re-identification) โดยไม่ชอบด้วยกฎหมาย (Singapore PDPA section 48F)

นอกจากนี้ ในการแก้ไขดังกล่าวยังได้กำหนดด้วยว่าในกรณีที่การกระทำความผิดตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลเกิดจากการกระทำความผิดของนิติบุคคล ให้กรรมการหรือผู้บริหารของนิติบุคคลมีความรับผิดด้วยหากการกระทำผิดนั้นเกิดจากการกระทำหรือการงดเว้นกระทำของกรรมการหรือผู้มีอำนาจ (SG PDPA section 52) โดยความรับผิดทางอาญานั้นมีโทษปรับไม่เกิน 5,000 เหรียญสิงคโปร์ หรือโทษจำคุกไม่เกิน 2 ปี หรือทั้งจำทั้งปรับ

โทษทางอาญา

ความรับผิดทางอาญาตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

มาตรา 79 บัญญัติว่า ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง หรือไม่ปฏิบัติตามมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง หรือไม่ปฏิบัติตามมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งล้านบาท หรือทั้งจำทั้งปรับ

ความผิดตามมาตรานี้เป็นความผิดอันยอมความได้

โทษทางอาญา

กรณีของการบังคับใช้มาตรา 79 นั้น คณะอนุกรรมการเฉพาะกิจตอบข้อหารือและให้คำแนะนำหน่วยงานของรัฐเพื่อรองรับการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลพิจารณาแล้ว มีความเห็นไว้ในหลายกรณี ซึ่งอาจสรุปได้ดังนี้

(1) การใช้หรือการเปิดเผยข้อมูลส่วนบุคคลที่จะเป็นความผิดทางอาญาตามมาตรา 79 วรรคหนึ่ง ต้องเกิดขึ้นจากการที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26 ได้แก่ ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ฯลฯ โดยฝ่าฝืนไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลและกระทำการดังกล่าวไม่เข้าข้อยกเว้นอื่นตามมาตรา 26 ประกอบมาตรา 27 วรรคหนึ่ง หรือเป็นกรณีที่บุคคลที่ได้รับข้อมูลส่วนบุคคลตามมาตรา 26 มาจากการเปิดเผยของผู้ควบคุมข้อมูลส่วนบุคคล แต่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลในการขอรับข้อมูลส่วนบุคคลนั้นตามมาตรา 27 วรรคสองโดยประการที่น่าจะทำให้ผู้อื่นเสียหายเสียชื่อเสียงถูกดูหมิ่นถูกเกลียดชังหรือได้รับความอับอาย หรือกรณีที่ข้อเท็จจริงปรากฏในคดีว่าผู้กระทำความผิดเป็นนิติบุคคลและการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินการของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วยตามความในมาตรา 81

โทษทางอาญา

(2) การเป็นผู้ควบคุมข้อมูลส่วนบุคคลดังกล่าว เมื่อพิจารณาจากบทบัญญัติแห่งกฎหมายที่กำหนดหน้าที่และความรับผิดไว้หลายประการ เช่น การกำหนดให้การเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องมีฐานทางกฎหมายตามมาตรา 24 หรือมาตรา 26 แล้วแต่กรณี หน้าที่ในการแจ้งวัตถุประสงค์และรายละเอียดเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคลตามมาตรา 23 ข้อกำหนดและเงื่อนไขเกี่ยวกับการส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศตามมาตรา 28 และมาตรา 29 หน้าที่ในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมและการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ในกรณีที่มีการละเมิดมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 37 (1) และ 37 (4) หน้าที่ในการตอบสนองต่อคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 30 ถึง 36 หน้าที่ในการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 และหน้าที่ในการจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอมปรากฏรายละเอียดตามมาตรา 37

(3) บทบัญญัติและเจตนารมณ์แห่งกฎหมายดังกล่าวมุ่งประสงค์จะใช้บังคับแก่บุคคลหรือนิติบุคคลที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล อย่างเป็นระบบหรือเป็นประจำสม่ำเสมอเพื่อวัตถุประสงค์อย่างใดอย่างหนึ่งขององค์กรหรือของบุคคลนั้น โดยกำหนดหลักการที่สำคัญประการหนึ่งเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ว่าต้องมีฐานทางกฎหมายตามที่กำหนดไว้ในมาตรา 24 หรือมาตรา 26 แล้วแต่กรณี และหากไม่มีฐานทางกฎหมายอื่นได้เพื่อใช้ในการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ตามหลักเกณฑ์ในมาตรา 19 และมาตรา 20 แห่งพระราชบัญญัติดังกล่าว และได้กำหนดหน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคลไว้ตั้งแต่ขั้นตอนการเก็บรวบรวมจนกระทั่งการลบหรือทำลายข้อมูลส่วนบุคคล ประกอบกับมาตรา 4 (1) แห่งพระราชบัญญัติดังกล่าวได้กำหนดข้อยกเว้นไม่ให้นำพระราชบัญญัตินี้ไปใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคล เพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น

โทษทางอาญา

จากบทบัญญัติในมาตรา 79 และแนวทางการตอบข้อหารือข้างต้น อาจสรุปได้ว่ากฎหมายกำหนดความรับผิดทางอาญาไว้สองกรณี ดังนี้

(1) ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสองหรือไม่ปฏิบัติตามมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

(2) ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสองหรือไม่ปฏิบัติตามมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งล้านบาท หรือทั้งจำทั้งปรับ

ในการวินิจฉัยในประเด็นดังกล่าว คณะอนุกรรมการเฉพาะกิจฯ ได้วางกรอบแนวทางไว้ ดังนี้

(1) พฤติกรรมตามข้อหารือเป็น “การใช้เพื่อประโยชน์ส่วนตน” อันเป็นข้อยกเว้นการใช้บังคับกฎหมายตามมาตรา 4 (1) หรือไม่

(2) องค์ประกอบความรับผิดทางอาญาตามมาตรา 79

โทษทางอาญา

การใช้เพื่อประโยชน์ส่วนตน (Private Use)

คณะอนุกรรมการเฉพาะกิจฯ เห็นว่า บทบัญญัติและเจตนารมณ์ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มุ่งประสงค์จะใช้บังคับแก่บุคคลหรือนิติบุคคลที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล อย่างเป็นระบบหรือเป็นประจำสม่ำเสมอ เพื่อวัตถุประสงค์อย่างใดอย่างหนึ่งขององค์กรหรือของบุคคลนั้น โดยกำหนดหลักการที่สำคัญประการหนึ่งเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ว่าต้องมีฐานทางกฎหมายตามที่กำหนดไว้ในมาตรา 24 หรือมาตรา 26 แล้วแต่กรณี และหากไม่มีฐานทางกฎหมายอื่นใดเพื่อใช้ในการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ตามหลักเกณฑ์ในมาตรา 19 และมาตรา 20 แห่งพระราชบัญญัติดังกล่าว และได้กำหนดหน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคลไว้ตั้งแต่ขั้นตอนการเก็บรวบรวมจนกระทั่งการลบหรือทำลายข้อมูลส่วนบุคคล ประกอบกับมาตรา 4 (1) แห่งพระราชบัญญัติดังกล่าวได้กำหนดข้อยกเว้นไม่ให้นำพระราชบัญญัตินี้ไปใช้บังคับแก่การเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคล เพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น และกรณีดังต่อไปนี้ คณะอนุกรรมการเฉพาะกิจฯ เห็นว่าอาจเป็นการใช้เพื่อประโยชน์ส่วนตน

ตัวอย่างการใช้เพื่อประโยชน์ส่วนตน

(1) การโพสต์ภาพใบสำคัญการหย่าในติ๊กต๊อก (TikTok) ที่มีชื่อและนามสกุลของผู้กล่าวหาทำให้ได้รับความเสียหาย

(2) กรณีนำข้อมูลที่สามารถระบุตัวบุคคลได้อันเป็นข้อมูลส่วนบุคคลและยังเป็นข้อมูลเกี่ยวกับประวัติอาชญากรรมของผู้เสียหายที่ผู้เสียหายถูกกล่าวหาว่าได้กระทำความผิดต่อกฎหมายไปโพสต์ลงบนเฟสบุ๊กของผู้ต้องหา

(3) ผู้ต้องหาว่าจ้างผู้เสียหายซึ่งเป็นผู้รับเหมาต่อเติมบ้าน แต่ผู้ต้องหาเห็นว่าผู้รับเหมาทำงานไม่ดีจึงโพสต์ภาพผลงาน ความเห็นและภาพสำเนาบัตรประจำตัวประชาชนของผู้รับเหมาลงในเฟสบุ๊กของผู้ต้องหาออกสู่สาธารณะ

(4) คัดลอกภาพถ่ายใบหน้าผู้เสียหายกับครอบครัว ซึ่งเป็นภาพโปรไฟล์ (Facebook) ของผู้เสียหายไปโพสต์ในเฟสบุ๊กของผู้ต้องหาในลักษณะนำไปโพสต์ประจานเรื่องไม่ชำระหนี้แก่ผู้ต้องหาโดยผู้เสียหายไม่ได้อนุญาต

(5) กรณีที่บุคคลธรรมดาได้รับข้อมูลส่วนบุคคลของบุคคลอื่น เช่น ภาพถ่ายบุคคล มาจากผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่มีอำนาจตามกฎหมาย และนำภาพถ่ายบุคคลดังกล่าวมาเผยแพร่ในแอพพลิเคชั่นเฟสบุ๊กพร้อมข้อความอันเป็นการหมิ่นประมาทเจ้าของข้อมูลส่วนบุคคลดังกล่าว โดยไม่ได้รับอนุญาตจากเจ้าของข้อมูลส่วนบุคคล

โทษทางอาญา

องค์ประกอบความรับผิดทางอาญาตามมาตรา 79

การใช้หรือการเปิดเผยข้อมูลส่วนบุคคลที่จะเป็นความผิดทางอาญาตามมาตรา 79 วรรคหนึ่ง ต้องเกิดขึ้นจากการที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26 ได้แก่ ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ ฯลฯ ด้วยเหตุนี้องค์ประกอบความรับผิดที่สำคัญ คือ การกระทำผิดที่กล่าวอ้างนั้น ต้องมีข้อมูลส่วนบุคคลตามมาตรา 26 (sensitive data) ประกอบด้วยเสมอ ดังนั้น ภาพถ่ายโดยทั่วไป ชื่อ-สกุล ข้อมูลการติดต่อ หรือข้อมูลทางการเงิน ไม่ใช่ข้อมูลตามมาตรา 26 การใช้หรือการเปิดเผยข้อมูลส่วนบุคคลดังกล่าวจึงไม่อาจมีความรับผิดทางอาญาได้

แต่อย่างไรก็ดี หากการกระทำของผู้ต้องหาหรือผู้ที่ถูกกล่าวหาว่ากระทำผิดมีลักษณะเป็นการละเมิดสิทธิในความเป็นส่วนตัวของบุคคลอื่นเกินสมควร ผู้กระทำอาจมีความรับผิดตามกฎหมายอื่น ๆ ได้ เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม หรือประมวลกฎหมายอาญาในความผิดฐานหมิ่นประมาท หรืออาจเป็นการละเมิดตามมาตรา 420 แห่งประมวลกฎหมายแพ่งและพาณิชย์ เป็นต้น

โทษทางอาญา

ส่วนมาตรา 81 กำหนดว่า ในกรณีที่ผู้กระทำความผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการ หรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย

ดังนั้น การที่กรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคล จะมีความรับผิดทางอาญาตามมาตรา 81 จึงต้องมีองค์ประกอบความรับผิด ดังนี้

(1) นิติบุคคลที่เป็น “ผู้ควบคุมข้อมูลส่วนบุคคล” มีความรับผิดทางอาญาตามมาตรา 79

(2) ผู้ที่จะมีความรับผิดตามมาตรานี้ต้องเป็น กรรมการ ผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น

(3) การกระทำความผิดนั้นต้องเกิดจากการที่บุคคลตามข้อ (2) มีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด

แบบทดสอบ บทที่ 11

ข้อที่ 1

Q : ข้อใดต่อไปนี้อาจเป็นโทษทางอาญาตามมาตรา 79

ก. สามีโพสต์ภาพใบสำคัญการหย่าในติ๊กต๊อกที่มีชื่อและนามสกุลของภรรยา ทำให้ภรรยาได้รับความเสียหาย และอับอาย

ข. กรรมการตรวจรับของบริษัทเอกชนแห่งหนึ่งนำข้อมูลเกี่ยวกับผู้ชนะการประกวดราคาไปเผยแพร่ในโซเชียลมีเดียของตนเอง

ค. นายแพทย์ ค เจ้าของคลินิกเปิดเผยข้อมูลเกี่ยวกับการรักษาพยาบาลของคนไข้รายหนึ่งผ่านเพจของคลินิกทำให้คนไข้รายดังกล่าวเสื่อมเสียชื่อเสียงและได้รับความอับอาย เนื่องจากคนรอบตัวรู้ถึงอาการโรคติดต่ออันเป็นที่น่ารังเกียจของสังคม

ง. นาย ก ว่าจ้างนาย ข ซึ่งเป็นผู้รับเหมาต่อเติมบ้าน ว่าผู้รับเหมาทำงานไม่ดีจึงโพสต์ภาพผลงาน ความเห็นและภาพสำเนาบัตรประจำตัวประชาชนของผู้รับเหมาลงในเฟสบุ๊กของตนเอง

แบบทดสอบ บทที่ 11

ข้อที่ 2

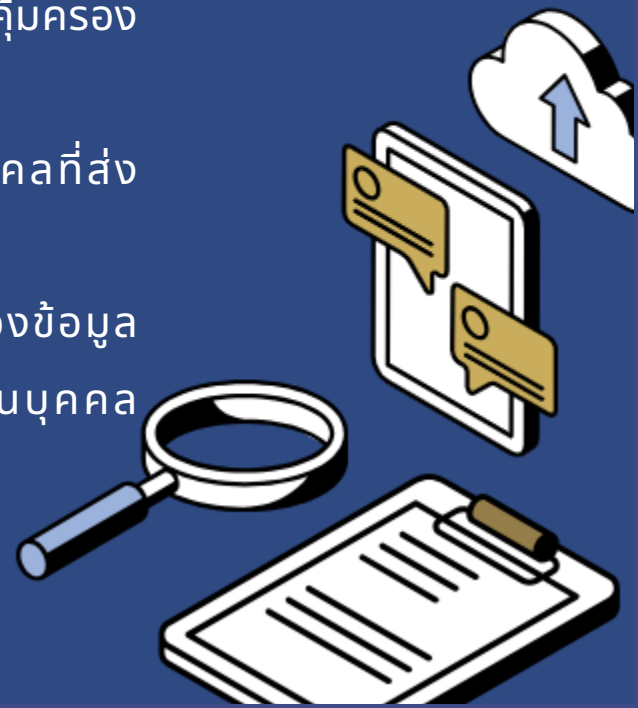
Q : ข้อใดต่อไปนี้ ไม่ใช่หน้าที่และอำนาจของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ก. การกำหนดนโยบายการบริหารงาน และให้ความเห็นชอบแผนการดำเนินงานของสำนักงาน

ข. ตีความและวินิจฉัยชี้ขาดปัญหาที่เกิดจากการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ค. ประกาศกำหนดหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

ง. กำหนดมาตรการหรือแนวทางการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



แบบทดสอบ บทที่ 11

ข้อที่ 3

Q : ข้อใดต่อไปนี้ไม่ถูกต้องเกี่ยวกับความรับผิดทางแพ่งตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ก. ผู้เสียหายจะได้รับค่าสินไหมทดแทนที่แท้จริงและค่าสินไหมทดแทนเพื่อการลงโทษอีกไม่เกิน 2 เท่าของค่าสินไหมทดแทนที่แท้จริง

ข. ค่าสินไหมทดแทนไม่รวมถึงค่าใช้จ่ายที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย

ค. ในกรณีที่ผู้เสียหายรู้ถึงความเสียหายและรู้ตัวผู้ควบคุมข้อมูลส่วนบุคคลที่ต้องรับผิด อายุความการฟ้องคดีจะไม่เกิน 3 ปีนับจากวันที่รู้

ง. ผู้ควบคุมข้อมูลส่วนบุคคลอาจไม่มีความรับผิดทางแพ่งหากพิสูจน์ได้ว่าความเสียหายนั้นเกิดจากการละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง

แบบทดสอบ บทที่ 11

ข้อที่ 4

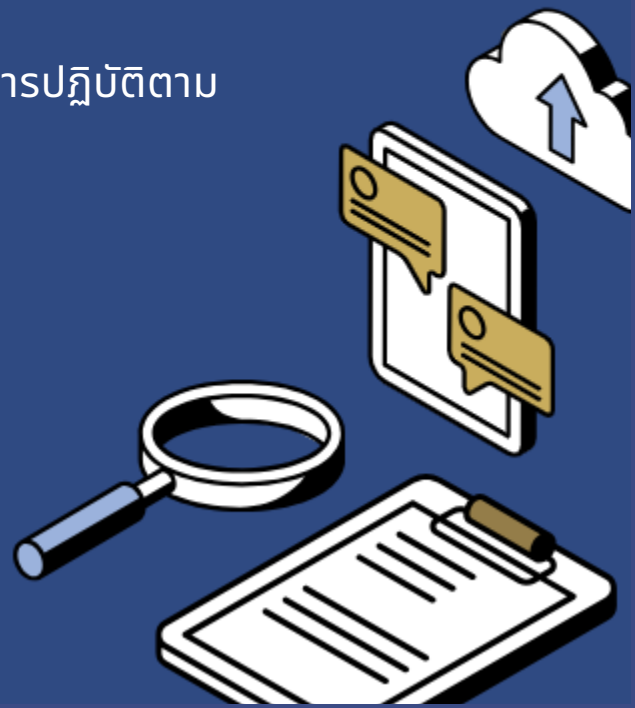
Q : ข้อใดต่อไปนี้ ไม่ใช่หน้าที่และอำนาจของคณะกรรมการผู้เชี่ยวชาญ

ก. พิจารณาเรื่องร้องเรียนตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ข. ตรวจสอบการกระทำใดของผู้ควบคุมข้อมูลส่วนบุคคลเกี่ยวกับข้อมูลส่วนบุคคล ที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล

ค. ให้คำปรึกษาแก่หน่วยงานของรัฐและหน่วยงานของเอกชนเกี่ยวกับการปฏิบัติตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ง. ไกล่เกลี่ยข้อพิพาทเกี่ยวกับข้อมูลส่วนบุคคล



แบบทดสอบ บทที่ 11

ข้อที่ 5

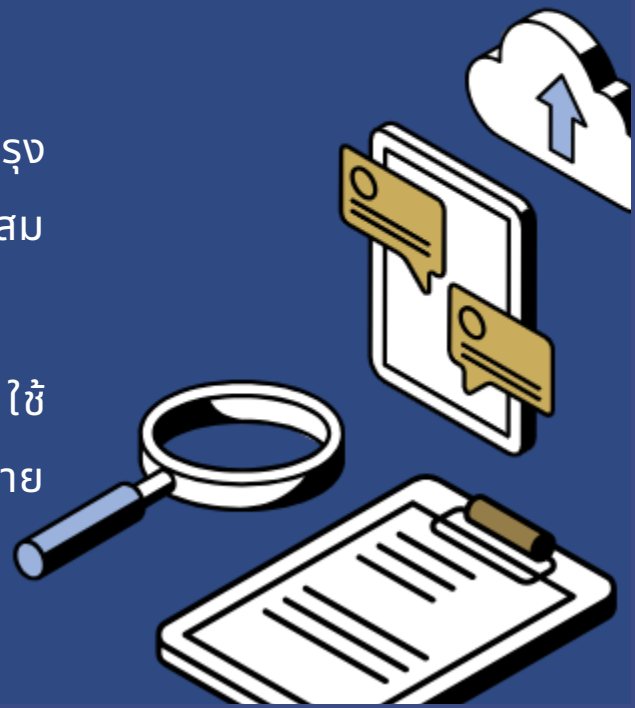
Q : ในการออกคำสั่งลงโทษทางปกครอง หากคณะกรรมการผู้เชี่ยวชาญพิจารณาเห็นว่าเป็นกรณี “ร้ายแรง” ข้อใดต่อไปนี้ไม่ใช่มาตรการที่ คณะกรรมการผู้เชี่ยวชาญจะมีคำสั่งได้

ก. สั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลหยุดกระทำการที่ฝ่าฝืนกฎหมายเท่านั้น

ข. มีคำสั่งลงโทษปรับทางปกครอง

ค. มีคำสั่งลงโทษปรับทางปกครองและกำหนดเงื่อนไขหรือวิธีการปรับปรุงบุคลากร กระบวนการหรือเทคโนโลยี ให้มีประสิทธิภาพและความเหมาะสมตามที่คณะกรรมการผู้เชี่ยวชาญเห็นสมควร

ง. มีคำสั่งลงโทษปรับทางปกครองและสั่งจำกัดการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีการกระทำผิดไว้เพื่อระงับความเสียหายนั้นภายในระยะเวลาที่กำหนด



• เฉลยแบบทดสอบบทที่ 11

ข้อที่	เฉลย
1.	ค.
2.	ก.
3.	ข.
4.	ค.
5.	ก.