Thai Financial Planners Association
สมาคมนักวางแผนการเงินไทย

Guideline on Personal Data Protection for

Thai Financial Planners Association (TFPA)

แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลสำหรับ
สมาคมนักวางแผนการเงินไทย

คำสงวนสิทธิ์ : *สมาคมนักวางแผนการเงินไทยจัดทำแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ เพื่อใช้เป็นข้อเสนอแนะสำหรับท่านพิจารณาเป็นแนวปฏิบัติเบื้องต้นตามที่เห็นสมควรเพื่อรองรับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ต่อไป ทั้งนี้ สมาคมนักวางแผนการเงินไทยขอสงวนสิทธิในการแก้ไขปรับปรุงแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลสำหรับสมาคมนักวางแผนการเงินไทยดังกล่าวได้ ในกรณีที่มีการแก้ไขกฎหมายหรือมีการประกาศใช้กฎหมายลำดับรอง หรือมีการแก้ไขเปลี่ยนแปลงแนวทางการปฏิบัติภายในภาคธุรกิจ เพื่อให้แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลของสมาคมนักวางแผนการเงินไทยมีความสมบูรณ์ และท่านสามารถนำไปพิจารณาปรับใช้ได้อย่างมีประสิทธิภาพ”*

สารบัญ

1. บทนำ

1.1 การคุ้มครองข้อมูลส่วนบุคคลกับสมาคมนักวางแผนการเงินไทย

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (“พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล”) มีผลบังคับใช้อย่างสมบูรณ์ในวันที่ 1 มิถุนายน พ.ศ. 2564 ซึ่งสมาคมนักวางแผนการเงินไทย (Thai Financial Planners Association (TFPA)) ได้เห็นถึงความสำคัญ ของการกำหนดแนวทางในการดำเนินงานการคุ้มครองข้อมูลส่วนบุคคลในกลุ่มนักวางแผนทางการเงิน (“ท่าน”) เพื่อให้เป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กฎหมายลำดับรอง และประกาศอื่น ๆ ที่เกี่ยวข้องกับพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (รวมเรียกว่า “กฎหมายคุ้มครองข้อมูลส่วนบุคคล”) เอกสารฉบับนี้จึงได้มีการนำกฎหมายคุ้มครองข้อมูลส่วนบุคคลมาปรับใช้ รวมถึงมีการยกตัวอย่างเพื่อให้ผู้อ่านสามารถเข้าใจถึงการนำตัวบทกฎหมายไปปฏิบัติได้ดียิ่งขึ้น

มาตรการในการคุ้มครองข้อมูลส่วนบุคคล มีการมุ่งเน้นถึงหน้าที่และความรับผิดชอบของผู้ประกอบการ (ทั้งบุคคลธรรมดา และนิติบุคคล) ในการกระทำการใดๆ ที่เกี่ยวกับข้อมูลส่วนบุคคล อันเนื่องมาจากในประเทศไทย มีผู้ประกอบการจำนวนมากทำการติดต่อและรับส่งข้อมูลส่วนบุคคลกัน ทั้งการรับส่งภายในกันเองภายในองค์กรและภายนอกองค์กร อีกทั้งยังมีการส่งข้อมูลส่วนบุคคลออกนอกประเทศ มีการนำข้อมูลไปเผยแพร่เพื่อประโยชน์ส่วนตนโดยไม่ได้รับอนุญาต หรือมีการติดต่อไปยังเจ้าของข้อมูลส่วนบุคคลมากจนเกินความจำเป็น จนอาจเป็นการรบกวนความเป็นส่วนตัว ซึ่งข้อมูลดังกล่าวมีทั้งข้อมูลที่เป็นข้อมูลทางธุรกิจ และข้อมูลส่วนบุคคล (นั่นก็คือ ข้อมูลที่เกี่ยวข้องโดยตรงกับบุคคลที่ทำให้สามารถระบุตัวตนได้ ไม่ว่าทางตรงหรือทางอ้อม) การกระทำใดๆ กับข้อมูลส่วนบุคคลนั้นอาจมีความเสี่ยงที่จะเป็นการกระทำอันละเมิดหรือกระทบต่อสิทธิและเสรีภาพของบุคคลได้ ดังนั้น จึงมีความจำเป็นจำเป็นต้องมีกฎหมาย กฎเกณฑ์ต่าง ๆ มาควบคุมและจำกัดการใช้ข้อมูลส่วนบุคคล รวมถึงบทลงโทษสำหรับการละเมิดกฎข้อบังคับต่าง ๆ เพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งสิทธิความเป็นส่วนตัวให้ดียิ่งขึ้น ผู้ประกอบการจึงต้องมีการใช้ข้อมูลอย่างระมัดระวังมากขึ้น มิให้การประมวลผลข้อมูลส่วนบุคคลเป็นการละเมิดสิทธิเสรีภาพและความเป็นส่วนตัวของบุคคล ซึ่งเป็นหน้าที่ของผู้ประกอบการที่ต้องจัดให้มีมาตรการที่ทำให้มั่นใจว่าข้อมูลส่วนบุคคลได้รับการคุ้มครอง มีการบริหารจัดการข้อมูลอย่างเหมาะสม

1.2 เป้าหมายและวัตถุประสงค์ของเอกสารฉบับนี้

แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของสมาคมนักวางแผนการเงินไทย (Guideline on Personal Data Protection for Thai Financial Planners Association (TFPA)) มีวัตถุประสงค์เพื่อให้มั่นใจว่าท่านตระหนักและเข้าใจถึงการคุ้มครองข้อมูลส่วนบุคคล และเพื่อเป็นแนวทางในการนำกฎหมาย

คุ้มครองข้อมูลส่วนบุคคล ไปถือปฏิบัติโดยให้เป็นมาตรฐานเดียวกันในกลุ่มสมาชิกสมาคมนักวางแผนการเงินไทย เอกสารฉบับนี้มีกลุ่มเป้าหมายให้กับผู้จัดทำนโยบายของท่าน เพื่อให้ง่ายต่อการนำไปพัฒนาเป็นร่างนโยบายและวิธีปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของท่านให้เหมาะสมและสอดคล้องกับความเสี่ยงและวิธีการดำเนินธุรกิจของท่านได้อย่างเหมาะสม

1.3 การใช้แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของสมาคมนักวางแผนการเงินไทยฉบับนี้ สามารถสรุปเนื้อหาหลัก ได้ดังต่อไปนี้

1) หลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคล (Principle Relating to Personal Data Protection)
2) แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล แบ่งตามวงจรชีวิตของข้อมูล (Data Life Cycle) ได้แก่ การเก็บรวบรวมข้อมูลส่วนบุคคล (Data Collection), การใช้และเปิดเผยข้อมูลส่วนบุคคล (Data Usage/Disclose/Transfer), การเก็บข้อมูลส่วนบุคคลและระยะเวลาในการเก็บรักษา (Data Retention) และการลบหรือทำลายข้อมูลส่วนบุคคล (Data Deletion or Data Destruction)
3) สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights)
4) แนวปฏิบัติเกี่ยวกับหน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (Data Controller and Data Processor Obligation) รวมทั้งหน้าที่และความรับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer Roles and Responsibilities)
5) ภาคผนวก

1.4 ข้อจำกัดในการปฏิบัติงานและข้อจำกัดของเอกสารฉบับนี้

บริษัท ดีล้อย ทู้ช โธมัทสุ ไชยยศ ที่ปรึกษา จำกัด (“บริษัทที่ปรึกษา”) มีข้อจำกัดในการปฏิบัติงานเพื่อจัดทำแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของสมาคมนักวางแผนการเงินไทย ดังต่อไปนี้

- เอกสารฉบับนี้อ้างอิงตามข้อกำหนดของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
- เอกสารฉบับนี้ มีขอบเขตการศึกษา วิเคราะห์ และตีความ จากประสบการณ์และจากฐานข้อมูลที่น่าเชื่อถือ ทั้งในเรื่องของการคุ้มครองข้อมูลส่วนบุคคลและผลิตภัณฑ์หรือบริการที่เกี่ยวข้องของท่าน อย่างไรก็ตาม ข้อมูลอ้างอิงดังกล่าวเป็นข้อมูลที่มี ณ เวลาใดเวลาหนึ่ง และท่านควรตระหนักด้วยว่าการคุ้มครองข้อมูลส่วนบุคคลเป็นเรื่องที่กำลังพัฒนาและมีการปรับปรุงเปลี่ยนแปลงอยู่อย่างรวดเร็ว ดังนั้น เนื้อหาหลายประการอาจมีความล้าสมัยหรือไม่เหมาะสมในหลายสถานการณ์เมื่อเวลาผ่านไป หรือรายการอ้างอิง

ใดๆ ของเนื้อหาอาจมีการเปลี่ยนแปลง สูญหายได้เมื่อถึงเวลาที่ท่านได้อ่านเอกสารฉบับนี้ ดังนั้น ท่านจึงอาจจำเป็นต้องได้รับคำปรึกษาจากผู้เชี่ยวชาญในเรื่องดังกล่าวโดยตรง

- บริษัทที่ปรึกษาไม่ได้ปฏิบัติงานด้านการให้คำปรึกษาทางกฎหมาย ดังนั้นจึงไม่สามารถรับรองความถูกต้องของครบถ้วนของเนื้อหา รวมถึงไม่สามารถให้คำรับรองหรือรับประกันใดๆทั้งสิ้นของเนื้อหาในเอกสารฉบับนี้ได้ และบริษัทที่ปรึกษาจะไม่รับผิดชอบต่อความสูญเสีย หรือเสียหายใดๆ ที่อ้างว่าเกิดขึ้นจากการปฏิบัติตามเนื้อหาของเอกสารฉบับนี้ ไม่ว่ากรณีใดๆ ทั้งสิ้น

2. คำนิยาม

รายการ	คำอธิบายรายการ
ท่าน	หมายถึง สมาชิกสมาคมนักวางแผนการเงินไทย ได้แก่ นักวางแผนการเงิน CFP และปรึกษาการเงิน AFPT หรือผู้ใช้เครื่องหมาย CFP/AFPT
การประมวลผลข้อมูลส่วนบุคคล (Processing of Personal Data)	หมายถึง การดำเนินการหรือชุดการดำเนินการใดๆ กับข้อมูลส่วนบุคคล เช่น การจัดเก็บ รวบรวม การบันทึก การจัดระบบ จัดโครงสร้าง การอัปเดตหรือการแก้ไข การดึงข้อมูล การใช้ การเปิดเผยด้วยการส่งต่อ เผยแพร่ หรือ การกระทำใดๆ เพื่อให้พร้อมใช้งาน การใช้ การรวม การบล็อก การลบหรือการทำลายข้อมูล
การรั่วไหลของข้อมูลส่วนบุคคล (Personal Data Breach)	หมายถึง การรั่วไหลหรือละเมิดมาตรการความมั่นคงปลอดภัยต่อข้อมูลส่วนบุคคลทำให้เกิด ความเสียหาย สูญหาย เปลี่ยนแปลง เปิดเผยโดยไม่ได้รับอนุญาต
การลบข้อมูล (Data Deletion)	หมายถึง การทำให้ข้อมูลส่วนบุคคลนั้นถูกลบออกระบบและไม่อาจกู้คืนได้โดยตัวเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล ทั้งนี้ ไม่ว่าในเวลาใด ๆ
การทำข้อมูลนิรนาม (Data Anonymization)	หมายถึง กระบวนการแปลงข้อมูลส่วนบุคคลให้เป็นข้อมูลที่ไม่สามารถใช้เพื่อระบุตัวตนของบุคคลใดบุคคลหนึ่งได้
ข้อมูลนิรนาม (Anonymized Data)	หมายถึง ข้อมูลที่ไม่สามารถใช้เพื่อระบุตัวตนของบุคคลใดบุคคลหนึ่งได้
ข้อมูลส่วนบุคคล (Personal Data)	หมายถึง ข้อมูลที่เกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ตามคำนิยามของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
ข้อมูลอ่อนไหว (Sensitive Personal Data)	หมายถึง ข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวของเจ้าของข้อมูลส่วนบุคคล และมีความละเอียดอ่อนและมีความสุ่มเสี่ยงต่อการถูกใช้ใน

รายการ	คำอธิบายรายการ
	การเลือกปฏิบัติอย่างไม่เป็นธรรม หรือเป็นข้อมูลอื่นใดซึ่งอาจทำให้เกิดผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
คณะกรรมการ (Personal Data Protection Committee)	หมายถึง คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
เจ้าของข้อมูลส่วนบุคคล (Data Subject)	หมายถึง บุคคลใดๆ ที่ข้อมูลใดๆทำให้สามารถระบุตัวตนนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม
โปรไฟลิ่ง (Profiling)	หมายถึง รูปแบบการประมวลผลข้อมูลส่วนบุคคลใดๆ ซึ่งมีการใช้ข้อมูลส่วนบุคคลในการประเมินลักษณะเกี่ยวกับบุคคลบางประการโดยเฉพาะอย่างยิ่งเพื่อวิเคราะห์หรือคาดการณ์เกี่ยวกับบุคคลในเรื่องประสิทธิภาพในการทำงาน สถานะทางเศรษฐกิจ สุขภาพของบุคคล ความชื่นชอบส่วนบุคคล สถานะทางการเงินของบุคคล สุขภาพของบุคคล พฤติกรรมของบุคคล ความน่าเชื่อถือของบุคคล ตำแหน่งทางภูมิศาสตร์ หรือความเคลื่อนไหวของบุคคล
บริการวางแผนการเงิน (Financial Planning Services)	หมายถึง การบริการวางแผนการเงิน และการแนะนำผลิตภัณฑ์ทางการเงินทุกประเภท ที่อยู่ภายใต้การกำกับของหน่วยงานอื่น เช่น ตราสารหนี้ กองทุนรวม ประกันวินาศภัย และประกันชีวิต
ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	หมายถึง บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล [เอกสารฉบับนี้อาจมีการใช้คำว่า ผู้ควบคุมข้อมูลแทนคำว่าผู้ควบคุมข้อมูลส่วนบุคคล]
ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)	หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล [เอกสารฉบับนี้อาจมีการใช้คำว่าผู้ประมวลผลข้อมูลแทนคำว่าผู้ประมวลผลข้อมูลส่วนบุคคล]
ลูกค้า (Customer)	หมายถึง บุคคลธรรมดาและนิติบุคคลซึ่งใช้บริการวางแผนการเงินอยู่ในปัจจุบันและให้หมายความรวมถึงผู้ติดต่อสอบถามข้อมูล ผู้ที่

รายการ	คำอธิบายรายการ
	รับทราบการบริการวางแผนการเงินผ่านสื่อต่าง ๆ และผู้ที่ได้รับการเสนอหรือชักชวนจากผู้ให้บริการเพื่อให้รับบริการวางแผนการเงิน
สำนักงานคุ้มครองข้อมูลส่วนบุคคล	หมายถึง สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Office of the Personal Data Protection Committee)

3. ขอบเขตของข้อมูลส่วนบุคคลและการจำแนกข้อมูลส่วนบุคคล (Personal Data Scope and Classification)

3.1 การระบุข้อมูลส่วนบุคคล (Identifying Personal Identifiable Information)

“ข้อมูลส่วนบุคคล” (Personal Data) ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“เจ้าของข้อมูลส่วนบุคคล” (Data Subject) หมายความว่า บุคคลผู้ที่ข้อมูลส่วนบุคคลสามารถระบุไปถึง

ความสามารถในการระบุไปยังเจ้าของข้อมูลส่วนบุคคลสามารถแบ่งได้เป็น 3 ลักษณะ

I. **การแยกแยะ (Distinguishability)** คือการที่ข้อมูลมีความสามารถในการระบุแยกแยะตัวบุคคลออกจากกันได้ ตัวอย่างเช่น ในชุดข้อมูล มี ชื่อ หมายเลขหนังสือเดินทาง หมายเลขประกันสังคม หรือข้อมูล Biometric ซึ่งข้อมูลดังกล่าวสามารถระบุตัวของเจ้าของข้อมูลได้ ในทางตรงกันข้าม หากชุดข้อมูลระบุเพียงคะแนนเครดิต (Credit score) นั้นไม่สามารถระบุไปยังตัวบุคคลได้ จำเป็นจะต้องมีข้อมูลเกี่ยวกับตัวบุคคลเพิ่มเติมจึงจะสามารถแยกแยะตัวบุคคลได้
II. **การติดตาม (Traceability)** คือการที่ข้อมูลสามารถถูกใช้ในการติดตาม เพื่อระบุลักษณะจำเพาะของบุคคลนั้นได้ ยกตัวอย่างเช่น พฤติกรรม กิจกรรมที่บุคคลนั้นกระทำ สถานะหรือการบันทึกการกระทำของผู้ใช้งานระบบที่ทำให้สามารถใช้ในการติดตามกิจกรรมของแต่ละบุคคลได้
III. **การเชื่อมโยง (Linkability)** คือการที่ข้อมูลมีคุณสมบัติในการเชื่อมโยงกันและระบุไปยังตัวบุคคลได้ ซึ่งแบ่งออกเป็น 2 ประเภท
    - ข้อมูลที่ถูกเชื่อมโยงแล้ว (Linked Information) คือกรณีที่ข้อมูลที่เกี่ยวข้องกับเจ้าของข้อมูลส่วนบุคคลคนละชุด เมื่อใช้ข้อมูลทั้งสองชุดประกอบกันแล้วจะมีความสามารถในการระบุตัวเจ้าของข้อมูลส่วนบุคคลได้ เช่น ข้อมูล PII สองชุดที่มีองค์ประกอบ PII ต่างกัน เมื่อมีบุคคลที่สามารถเข้าถึงชุดข้อมูลทั้งสองชุดได้ ก็จะสามารถเชื่อมโยงข้อมูลดังกล่าวในการระบุตัวเจ้าของข้อมูลส่วนบุคคลได้ รวมถึงกรณีที่การเข้าถึงข้อมูลอื่นที่เกี่ยวข้องกับเจ้าของข้อมูลส่วนบุคคล หากฐานข้อมูลทั้งสองชุดอยู่ในระบบเดียวกันหรือระบบที่เกี่ยวข้องกันอย่างใกล้ชิด และไม่มีควบคุมการเข้าถึงอย่างมีประสิทธิภาพ กรณีนี้ถือเป็นข้อมูลที่ถูกเชื่อมโยงแล้วได้

- ข้อมูลที่อาจถูกเชื่อมโยงได้ (Linkable Information) คือกรณีที่ หากมีชุดข้อมูลที่หากใช้ร่วมกันกับข้อมูลอื่นแล้วก็จะสามารถระบุตัวบุคคลได้ โดยที่ข้อมูลอื่นที่จะนำมาใช้ร่วมนั้นมาจากแหล่งข้อมูลอื่น โดยไม่อยู่ในระบบเดียวกันหรือระบบที่เกี่ยวข้องกันอย่างใกล้ชิด มีอยู่ในอินเทอร์เน็ต หรือแหล่งอื่น กรณีนี้เป็นข้อมูลที่ อาจถูกเชื่อมโยงได้

3.1.1 ตัวอย่างของข้อมูลที่เป็นข้อมูลส่วนบุคคล

รายการต่อไปนี้คือตัวอย่างของข้อมูลที่อาจถูกพิจารณาเป็นข้อมูลส่วนบุคคล

- ชื่อ นามสกุล ชื่อกลาง
- เลขประจำตัวประชาชน หมายเลขประกันสังคม หมายเลขหนังสือเดินทางหมายเลขใบขับขี่ หมายเลขประจำตัวผู้เสียภาษี เลขบัญชีธนาคาร เลขบัตรเครดิต
- ข้อมูลที่อยู่ อีเมล หมายเลขโทรศัพท์
- ข้อมูลอุปกรณ์ เช่น เลข IP address, MAC address, Cookie ID
- ข้อมูลที่เป็นลักษณะเฉพาะ เช่น รูปภาพใบหน้า
- ข้อมูลทางชีวมิติ (Biometric) ซึ่งเป็นข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว (Sensitive Personal Data) เช่น ข้อมูลแบบจำลองใบหน้า ข้อมูลแบบจำลองลายนิ้วมือ ฟิล์มเอกซเรย์ข้อมูลสแกนม่านตา ข้อมูลอัตลักษณ์เสียง ข้อมูลพันธุกรรม เป็นต้น
- ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์ โฉนดที่ดิน
- ข้อมูลเกี่ยวกับบุคคลที่เชื่อมโยงหรือถูกเชื่อมโยงกับหนึ่งในข้างต้น เช่น วันเกิด สถานที่เกิด น้ำหนัก ส่วนสูง ข้อมูลตำแหน่งทางภูมิศาสตร์ (Location)
- เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ ซึ่งเป็นข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว (Sensitive Personal Data)
- ข้อมูลการจ้างงาน ข้อมูลการศึกษา ข้อมูลทางการเงิน

3.1.2 ตัวอย่างของข้อมูลที่ไม่เป็นข้อมูลส่วนบุคคล

รายการต่อไปนี้คือตัวอย่างของข้อมูลที่ไม่ถูกพิจารณาเป็นข้อมูลส่วนบุคคล

- ข้อมูลจดทะเบียนบริษัท, ข้อมูลติดต่อทางธุรกิจ ที่ไม่ได้ระบุถึงตัวบุคคล เช่น ที่อยู่สำนักงาน, อีเมลบริษัท, หมายเลขโทรศัพท์สำนักงาน, หมายเลขแฟกซ์สำนักงาน
- ข้อมูลที่ไม่สามารถระบุถึงตัวบุคคลได้ เช่น ข้อมูลนิรนาม (Anonymized Data)

- ข้อมูลผู้ถึงแก่กรรม

3.2 แนวปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security)

3.2.1 ความมั่นคงปลอดภัย

ความมั่นคงปลอดภัย หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

3.2.2 มาตรการรักษาความมั่นคงปลอดภัย

หากท่านอยู่ในสถานะผู้ควบคุมข้อมูลส่วนบุคคล ท่านมีหน้าที่ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าวต้องมีการดำเนินการอย่างน้อยดังต่อไปนี้

1) ต้องครอบคลุมการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ไม่ว่าข้อมูลส่วนบุคคลนั้นจะอยู่ในรูปแบบเอกสาร อิเล็กทรอนิกส์ หรือในรูปแบบอื่นใด
2) ต้องประกอบด้วยมาตรการเชิงองค์กร (organizational measures) เช่น องค์กรควรมีการจัดทำนโยบายความมั่นคงปลอดภัยภายใน (Internal Security Policy) เพื่อให้พนักงานหรือลูกจ้างปฏิบัติตาม รวมถึงการสร้างความรับรู้ (Awareness) เรื่องการคุ้มครองข้อมูลส่วนบุคคลแก่บุคลากรเหล่านั้น และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม เช่น องค์กรอาจเลือกใช้วิธีการทางเทคนิคที่เหมาะสมด้วยการเข้ารหัส (Encryption) การแฝงข้อมูล (Pseudonymization) หรือการทำข้อมูลให้เป็นนิรนาม (Anonymization) การควบคุมการเข้าถึง (Access Control) รวมถึงการตรวจสอบติดตามกิจกรรมเกี่ยวกับข้อมูลส่วนบุคคลที่เกิดขึ้น (Log) ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย โดยคำนึงถึงระดับความเสี่ยง ตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
3) ต้องคำนึงถึงการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยตั้งแต่การระบุความเสี่ยงที่สำคัญที่อาจเกิดขึ้นกับทรัพย์สินสารสนเทศ (information assets) ที่สำคัญ การป้องกันความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้น การตรวจสอบและเฝ้าระวังภัย

คุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล และการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามหรือเหตุการณ์ละเมิดข้อมูลส่วนบุคคลด้วย ทั้งนี้ เท่าที่จำเป็นเหมาะสม และเป็นไปได้ตามระดับความเสี่ยง

4) ต้องคำนึงถึงความสามารถในการธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคลไว้ได้อย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน

5) สำหรับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องครอบคลุมส่วนประกอบต่าง ๆ ของระบบสารสนเทศที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล เช่น ระบบและอุปกรณ์จัดเก็บข้อมูลส่วนบุคคล เครื่องคอมพิวเตอร์แม่ข่าย (servers) เครื่องคอมพิวเตอร์ลูกข่าย (clients) และอุปกรณ์ต่าง ๆ ที่ใช้ ระบบเครือข่าย ซอฟต์แวร์และแอปพลิเคชัน อย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงหลักการป้องกันเชิงลึก (defense in depth) ที่ควรประกอบด้วยมาตรการป้องกันหลายชั้น (multiple layers of security controls) เพื่อลดความเสี่ยงในกรณีที่มาตรการบางมาตรการมีข้อจากัดในการป้องกันความมั่นคงปลอดภัยในบางสถานการณ์

6) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว ในส่วนที่เกี่ยวกับการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล อย่างน้อยต้องประกอบด้วยการดำเนินการดังต่อไปนี้อย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงความจำเป็นในการเข้าถึงและใช้งานตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล การรักษาความมั่นคงปลอดภัยตามระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

   (ก) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศที่สำคัญ (access control) ที่มีการพิสูจน์และยืนยันตัวตน (identity proofing and authentication) และการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงและใช้งาน (authorization) ที่เหมาะสม โดยคำนึงถึงหลักการให้สิทธิเท่าที่จำเป็น (need-to-know basis) ตามหลักการให้สิทธิที่น้อยที่สุดเท่าที่จำเป็น (principle of least privilege)

(ข) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่เหมาะสมซึ่งอาจรวมถึง

- การลงทะเบียนและการถอนสิทธิผู้ใช้งาน (user registration and de-registration)
- การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (user access provisioning)
- การบริหารจัดการสิทธิการเข้าถึงตามสิทธิ (management of privileged access rights)
- การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (management of secret authentication information of users)
- การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) และ
- การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (removal or adjustment of access rights)

(ค) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ซึ่งรวมถึงกรณีที่เป็นการกระทำนอกเหนือบทบาทหน้าที่ที่ได้รับมอบหมาย ตลอดจนการลักลอบทำสำเนาข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และการลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

(ง) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง แก้ไข หรือลบข้อมูลส่วนบุคคล (audit trails) ที่เหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

7) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องรวมถึงการสร้างเสริมความตระหนักรู้ด้านความสาคัญของการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย (privacy and security awareness) และการแจ้งนโยบาย แนวปฏิบัติ และมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคลอย่างเหมาะสม ให้บุคลากร พนักงาน ลูกจ้าง หรือบุคคลอื่นที่เป็นผู้ใช้งาน (user) หรือเกี่ยวข้องกับการเข้าถึง เก็บรวบรวม ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล ทราบและถือปฏิบัติ รวมทั้งกรณีที่มีการปรับปรุงแก้ไขนโยบาย แนวปฏิบัติ และมาตรการดังกล่าวด้วย โดยคำนึงถึงลักษณะและ

วัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

ผู้ควบคุมข้อมูลส่วนบุคคลต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัยดังกล่าวข้างต้นเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสาหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน เมื่อมีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ให้ถือว่าผู้ควบคุมข้อมูลส่วนบุคคลมีความจำเป็นต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัย เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ตามกฎหมายอื่นในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามกฎหมายนั้น แต่มาตรการรักษาความมั่นคงปลอดภัยดังกล่าวของผู้ควบคุมข้อมูลส่วนบุคคลจะต้องเป็นไปตามมาตรฐานขั้นต่ำที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด

ทั้งนี้ ในกรณีที่ท่านเป็นผู้ควบคุมข้อมูลส่วนบุคคล และมีคู่สัญญาอีกฝ่ายเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ท่านต้องจัดให้มีข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล และท่านต้องพิจารณากำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

3.2.3 แนวปฏิบัติเกี่ยวกับการจำแนกข้อมูล (Data Classification)

"การจำแนกข้อมูล" (Data Classification) หมายถึงกระบวนการที่เกี่ยวข้องกับการประเมินชุดข้อมูลกับการรักษาความปลอดภัยของข้อมูล อันได้แก่ ข้อมูลความลับ ข้อมูลอ่อนไหว ข้อมูลที่ต้องจัดให้มีเพื่อพร้อมใช้งาน และข้อมูลที่ต้องเปิดเผยตามข้อกำหนดของกฎหมาย เพื่อให้สามารถใช้ข้อมูล และกำหนดระดับการเปิดเผยอย่างเหมาะสม รวมถึงระดับการป้องกันความปลอดภัยของข้อมูล เพื่อเพิ่มความมั่นคงและความปลอดภัยของข้อมูล

การจำแนกข้อมูลเป็นกระบวนการที่ช่วยให้องค์กรรักษาความปลอดภัยของข้อมูลที่มีความอ่อนไหว หรือสำคัญให้อยู่ในระดับที่เหมาะสม ไม่ว่าข้อมูลจะถูกนำไปใช้งานหรือถูกเก็บในที่ใดก็ตาม การจำแนกข้อมูลถือเป็นจุดเริ่มต้นและเป็นพื้นฐานในการรักษาความเป็นส่วนตัวของ

ข้อมูล ซึ่งองค์กรต้องทำการตัดสินใจเกี่ยวกับการกระทำใด ๆ กับข้อมูล บนพื้นฐานของความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับองค์กร จะช่วยให้องค์กรประเมินความเสี่ยงในแต่ละประเภทของข้อมูลได้อย่างเหมาะสมยิ่งขึ้น ตัวอย่างการรักษาความปลอดภัยของข้อมูลในแต่ละประเภท เช่น ข้อมูลประเภทที่ “ถูกจำกัด” (Restricted) ควรได้รับการดูแลด้วยมาตรฐานที่สูงกว่าข้อมูลที่ “ไม่ถูกจำกัด” (Unrestricted) ที่ทุกคนในองค์กรสามารถเข้าถึงได้ เนื่องจากหากข้อมูลที่ถูกจำกัดเกิดการรั่วไหล อาจทำให้เกิดผลกระทบร้ายแรงต่อเจ้าของข้อมูลส่วนบุคคลและองค์กรมากกว่าข้อมูลที่ไม่ถูกจำกัด

ในการกำหนดวัตถุประสงค์ด้านความปลอดภัย (Security Objective) ของข้อมูลแบ่งออกเป็น 3 ด้าน ได้แก่

1) **การรักษาความลับของข้อมูล (Confidentiality)** คือ การจำกัดการเข้าถึงและการเปิดเผยข้อมูล รวมถึงการปกป้องความเป็นส่วนตัวและสิทธิของข้อมูล
2) **ความถูกต้องสมบูรณ์ของข้อมูล (Integrity)** คือ การรักษาความปลอดภัยของข้อมูลจากการดัดแปลงหรือถูกทำลายโดยไม่เหมาะสม รวมถึงการทำให้มั่นใจว่าข้อมูลมีความถูกต้อง
3) **ความพร้อมใช้งานของข้อมูล (Availability)** คือ การทำให้มั่นใจว่า สามารถเข้าถึงข้อมูลและใช้งานได้อย่างทันเวลาและเชื่อถือได้

องค์กรมีความจำเป็นที่ต้องจัดให้มีการบริหารความเสี่ยงอย่างเหมาะสม จากการจำแนกข้อมูลตามความเสี่ยงและผลกระทบ โดยการกำหนดระดับความเสี่ยงของข้อมูลส่วนบุคคลในชุดต่าง ๆ (Data Risk Level) และผลกระทบที่อาจเกิดขึ้น (Impact) กับองค์กรหรือบุคคล หากถูกละเมิดความปลอดภัย สามารถแบ่งได้เป็น 3 ระดับ ได้แก่

1) **ผลกระทบระดับต่ำ (Low)** กรณีที่ผลกระทบจากการสูญเสียการรักษาความลับของข้อมูล (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) มีแนวโน้มที่จะมีผลกระทบอย่างจำกัด (Limited Adverse Effect) ต่อองค์กร ทรัพย์สินขององค์กรและบุคคล เช่น
   - ทำให้ความสามารถในการปฏิบัติภารกิจลดลงในขอบเขตและระยะเวลาที่องค์กรสามารถปฏิบัติหน้าที่หลักได้ แต่ประสิทธิภาพระบบสารสนเทศลดลงอย่างสังเกตเห็นได้
   - ส่งผลให้เกิดความเสียหายเล็กน้อยต่อทรัพย์สินขององค์กร
   - ส่งผลให้เกิดความเสียหายทางการเงินเล็กน้อย
   - ส่งผลให้เกิดผลกระทบเล็กน้อยต่อบุคคล เช่น ทำให้ต้องเปลี่ยนเลขหมายโทรศัพท์

2) **ผลกระทบระดับกลาง (Moderate) กรณีที่ผลกระทบจากการสูญเสียการรักษาความลับของข้อมูล (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) มีแนวโน้มที่จะมีผลกระทบอย่างมาก (Serious Adverse Effect) ต่อองค์กร ทรัพย์สินขององค์กรและบุคคล เช่น**
   - ทำให้เกิดการลดลงอย่างมีนัยสำคัญในความสามารถในการปฏิบัติภารกิจในระดับและระยะเวลาที่องค์กรสามารถปฏิบัติหน้าที่หลักได้ แต่ประสิทธิภาพของระบบสารสนเทศจะลดลงอย่างมีนัยสำคัญ
   - ส่งผลให้เกิดความเสียหายอย่างมีนัยสำคัญต่อทรัพย์สินขององค์กร
   - ส่งผลให้เกิดการสูญเสียทางการเงินอย่างมีนัยสำคัญ
   - ส่งผลให้เกิดอันตรายอย่างมีนัยสำคัญต่อบุคคล แต่ไม่ถึงกับการสูญเสียชีวิตหรือได้รับบาดเจ็บร้ายแรงถึงชีวิต เช่น ทำให้เกิดความเสียหายทางการเงินเพราะถูกสวมรอยบุคคลหรือถูกปฏิเสธไม่ให้ประโยชน์บางอย่าง ทำให้ต้องอับอายแก่สาธารณะ ทำให้ถูกเลือกปฏิบัติ ทำให้ถูกแบล็คเมล์
3) **ผลกระทบระดับสูง (High) กรณีที่ผลกระทบจากการสูญเสียการรักษาความลับของข้อมูล (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) มีแนวโน้มที่จะมีผลกระทบอย่างร้ายแรงหรือหายนะ (Severe or Catastrophic Adverse Effect) ต่อองค์กร ทรัพย์สินขององค์กรและบุคคล เช่น**
   - ทำให้เกิดความเสื่อมโทรมอย่างรุนแรงในหรือสูญเสียความสามารถในการปฏิบัติภารกิจในขอบเขตและระยะเวลาที่องค์กรไม่สามารถปฏิบัติหน้าที่หลักอย่างน้อยหนึ่งอย่าง
   - ส่งผลให้เกิดความเสียหายอย่างใหญ่หลวงต่อทรัพย์สินขององค์กร
   - ส่งผลให้เกิดการสูญเสียทางการเงินที่สำคัญ
   - ส่งผลให้เกิดอันตรายอย่างรุนแรงต่อความปลอดภัยของชีวิตหรือได้รับบาดเจ็บร้ายแรงถึงชีวิต

ทั้งนี้ การจำแนกข้อมูลสามารถกำหนดระดับการจำแนกข้อมูลได้หลากหลายระดับ ขึ้นอยู่กับความเหมาะสมขององค์กร

4. หลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Principles)

ในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้น มีหลักการพื้นฐานที่สำคัญซึ่งเป็นสิ่งที่พึงระลึกก่อนทำการประมวลผลข้อมูลส่วนบุคคล และท่านควรทำความเข้าใจหลักการที่สำคัญเหล่านี้จะช่วยให้เข้าใจถึงหลักการและข้อจำกัดในการประมวลข้อมูลส่วนบุคคล เพื่อที่จะสามารถพิจารณาความเหมาะสมในการประมวลผลข้อมูลในกรณีอื่นได้ ดังรายละเอียดต่อไปนี้

4.1 หลักการที่ 1 : หลักการประมวลผลโดยชอบด้วยกฎหมาย เป็นธรรม และโปร่งใสต่อเจ้าของข้อมูลส่วนบุคคล (“Lawfulness, Fairness, and Transparency”)

ข้อมูลส่วนบุคคลจะต้องถูกประมวลผลโดยชอบด้วยกฎหมาย มีความเป็นธรรมและโปร่งใส

- **“Lawfulness”** หมายถึงในการประมวลผลข้อมูลส่วนบุคคลโดยชอบด้วยกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องสามารถระบุ “ฐานทางกฎหมาย” (Lawful Basis) ในการประมวลผลข้อมูลส่วนบุคคลท่านจะต้องระบุฐานในการประมวลผลให้ได้ฐานใดฐานหนึ่ง และจะต้องมีความระมัดระวังมากขึ้นในการประมวลผลข้อมูลอ่อนไหว (Sensitive Personal Data) ซึ่งถ้าหากผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถระบุฐานทางกฎหมายในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ จะเป็นการขัดต่อหลักการข้อนี้ รวมทั้งอาจเป็นการขัดต่อกฎหมาย ซึ่งเจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะขอให้ผู้ควบคุมข้อมูลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุถึงเจ้าของข้อมูลส่วนบุคคลได้
- **“Fairness”** หมายถึงความเป็นธรรม ในการประมวลผลข้อมูลส่วนบุคคลจะต้องทำในลักษณะที่สมเหตุสมผลตามความคาดหมายของเจ้าของข้อมูลส่วนบุคคล มีความยุติธรรมและไม่เป็นการละเมิดสิทธิและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
- **“Transparency”** หมายถึงความโปร่งใส โดยทั่วไปแล้วความโปร่งใสนั้นเชื่อมโยงกับความเป็นธรรม เนื่องจากการประมวลผลข้อมูลส่วนบุคคลอย่างโปร่งใส ผู้ควบคุมข้อมูลจะต้องแสดงรายละเอียดในการประมวลผลข้อมูลโดยชัดเจน เพื่อให้เจ้าของข้อมูลส่วนบุคคลเข้าใจถึงการประมวลผลข้อมูลของตนได้ ตัวอย่างเช่น เริ่มต้นจากผู้เก็บรวบรวมข้อมูลส่วนบุคคลแสดงตนว่าใครคือผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล มีการประมวลผลข้อมูลส่วนบุคคลอย่างไร รวมทั้งสามารถเปิดเผยให้แก่เจ้าของข้อมูลส่วนบุคคลทราบและตรวจสอบได้ นอกจากนั้นควรแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบด้วยภาษาที่ง่ายต่อความเข้าใจ ไม่ซับซ้อนหรือไม่ทำเกิดความเข้าใจผิดได้ง่าย

4.2 หลักการที่ 2 : หลักการประมวลผลโดยจำกัดด้วยวัตถุประสงค์ (“Purpose Limitation”)

การเก็บรวบรวมข้อมูลส่วนบุคคล จะต้องเก็บเฉพาะที่เกี่ยวข้อง จำเป็น เพื่อประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์อันชอบด้วยกฎหมายที่ระบุไว้อย่างชัดเจน และชอบธรรม อีกทั้งผู้ควบคุมข้อมูลส่วนบุคคลจะต้องไม่นำไปประมวลผลต่อในลักษณะที่ไม่สอดคล้องกับวัตถุประสงค์เหล่านั้นและไม่สามารถนำไปใช้กับวัตถุประสงค์ใหม่ที่นอกเหนือจากวัตถุประสงค์ในการเก็บรวบรวมที่ระบุไว้ในตอนแรก สำหรับการใช้ข้อมูลในบริบทนี้ หมายความรวมถึง การใช้ เปิดเผย และการโอนข้อมูลส่วนบุคคลด้วย

4.3 หลักการที่ 3 : หลักการประมวลผลข้อมูลส่วนบุคคลอย่างน้อยที่สุด (“Data Minimisation”)

ในการประมวลผลข้อมูลส่วนบุคคล ตั้งแต่กระบวนการเก็บรวบรวม ใช้ หรือเปิดเผย รวมถึงระยะเวลาในการเก็บ ผู้ควบคุมข้อมูลส่วนบุคคลควรจะดำเนินการเท่าที่จำเป็น เกี่ยวข้อง และจำกัดตามวัตถุประสงค์ในการประมวลผลข้อมูล และผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยให้เจ้าของข้อมูลส่วนบุคคลทราบ

4.4 หลักการที่ 4 : หลักความถูกต้องของเจ้าของข้อมูลส่วนบุคคล (“Accuracy”)

ข้อมูลส่วนบุคคลควรมีความถูกต้อง สมบูรณ์และเป็นปัจจุบัน ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการเพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลที่ไม่ถูกต้องจะถูกลบหรือแก้ไขโดยไม่ล่าช้า

4.5 หลักการที่ 5 : หลักการเก็บรักษาข้อมูลอย่างจำกัด (“Storage Limitation”)

ข้อมูลส่วนบุคคลจะต้องไม่เก็บเกินความจำเป็นตามระยะเวลาที่เหมาะสมเพื่อวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลหรือเก็บตามระยะเวลาที่กฎหมายกำหนด

4.6 หลักการที่ 6 : หลักการรักษาความลับและความถูกต้องของข้อมูลส่วนบุคคล (“Integrity and Confidentiality”)

ในการประมวลผลข้อมูลส่วนบุคคลจะต้องมีมาตรการที่ทำให้มั่นใจว่ามีการรักษาความปลอดภัยของข้อมูลส่วนบุคคล และข้อมูลส่วนมีความสมบูรณ์ถูกต้อง โดยจัดให้มีมาตรการทั้งในเชิงบริหารจัดการและเชิงเทคนิคที่มีความเหมาะสม และมีการป้องกันการประมวลผลจากบุคคลที่ไม่ได้รับอนุญาตหรือการประมวลผลอันมิชอบด้วยกฎหมาย มีการป้องกันการสูญหาย เสียหาย หรือการถูกทำลาย โดยไม่ได้ตั้งใจ

4.7 หลักการที่ 7 : หลักความรับผิดชอบ (“Accountability”)

ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่และความรับผิดชอบในการประมวลผลข้อมูลให้เป็นไปตามหลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Principles)

5. การเก็บรวบรวมข้อมูลส่วนบุคคล

5.1 วัตถุประสงค์ในการเก็บรวบรวมข้อมูล

5.1.1 ท่านจะต้องทำการแจ้งให้แก่เจ้าของข้อมูลส่วนบุคคลทราบถึงวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ว่าข้อมูลส่วนบุคคลของลูกค้าจะถูกนำไปใช้อย่างไร เพื่อวัตถุประสงค์ใด อีกทั้งความจำเป็นที่ต้องใช้ข้อมูลเหล่านี้ ในกรณีที่มีความจำเป็นที่จะต้องเปิดเผยข้อมูลส่วนบุคคลให้กับบุคคลภายนอกก็ต้องสามารถระบุวัตถุประสงค์ได้ว่าเพื่อวัตถุประสงค์อะไรรวมทั้งประเภทของบุคคลหรือหน่วยงานที่ข้อมูลอาจถูกเปิดเผย ซึ่งท่านจะต้องทำการดำเนินการแจ้งลูกค้าผ่านช่องทางและวิธีการที่เหมาะสม เช่น ประกาศความเป็นส่วนตัว ผ่านทางเว็บไซต์ของท่าน เป็นต้น โดยวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลนั้นมีความสัมพันธ์กับหลักพื้นฐานชองกฎหมายคุ้มครองข้อมูลส่วนบุคคล คือ หลักการจำกัดวัตถุประสงค์ (Purpose limitation) และสิทธิในการรับรู้เจ้าของข้อมูลส่วนบุคคล

5.1.2 ท่านจะต้องเก็บรวบรวมข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลเท่าที่จำเป็นภายใต้วัตถุประสงค์โดยชอบด้วยกฎหมาย โดยต้องพิจารณาจากองค์ประกอบ 3 ประการ คือ เพียงพอ เกี่ยวข้อง และจำกัด เพื่อป้องกันการเก็บรวบรวมข้อมูลมากเกินไป ซึ่งเป็นไปตามหลักการใช้ข้อมูลของเจ้าของข้อมูลส่วนบุคคลให้น้อยที่สุดเท่าที่จำเป็น (Data minization) อีกทั้งประการสำคัญ คือ “ความโปร่งใส” ในการประมวลผลข้อมูลส่วนบุคคลที่ต้องคำนึงถึง “ความเป็นธรรม” ต่อเจ้าของข้อมูลส่วนบุคคลด้วย

5.1.3 ในการระบุวัตถุประสงค์ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล ท่านไม่จำเป็นต้องระบุถึงขั้นตอนหรือกระบวนการปฏิบัติงานทุก ๆ กิจกรรม แต่ให้ระบุถึงวัตถุประสงค์ที่เกี่ยวข้องในการประมวลผลข้อมูลส่วนบุคคล เหตุผลที่เกี่ยวข้องหรือประโยชน์อันใดที่เกี่ยวข้อง รวมถึงฐานในการประมวลผลข้อมูลส่วนบุคคล หากลูกค้ามีข้อสงสัยในการเก็บรวบรวมข้อมูล ใช้ เปิดเผยข้อมูลส่วนบุคคล ท่านต้องจัดให้มีช่องทางในการร้องขอหรือจัดให้มีข้อมูลติดต่อท่านอย่างชัดเจนไปยัง DPO หรือบุคคลที่ท่านกำหนดให้ทำหน้าที่ในการรับเรื่อง เพื่อให้เจ้าของข้อมูลส่วนบุคคลใช้สิทธิร้องขอได้

5.1.4 ในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล ท่านต้องกระทำเท่าที่จำเป็นตามวัตถุประสงค์อันชอบด้วยกฎหมาย ซึ่งในแต่ละกิจกรรมการประมวลผลข้อมูล ท่านจะต้องสามารถระบุ “ฐานทางกฎหมาย” (Lawful Basis) ที่เหมาะสมในการประมวลผลให้ได้ฐานใดฐานหนึ่ง

5.2 แนวปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคล

การประมวลผลข้อมูลส่วนบุคคลโดยชอบด้วยกฎหมาย ท่านจะต้องสามารถระบุฐานในการประมวลผลตามกฎหมาย (Lawful basis) ในแต่ละกิจกรรมการประมวลผลข้อมูลให้ได้ฐานใดฐานหนึ่งตามที่จะกล่าวดังต่อไปนี้และจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงฐานในการประมวลผลข้อมูล รวมถึงสิทธิของเจ้าของข้อมูลส่วนบุคคลและข้อจำกัดในแต่ละฐานที่แตกต่างกันด้วย

5.2.1 ฐานความยินยอม (Consent)

ท่านสามารถใช้ฐานความยินยอมในการประมวลผลข้อมูลได้ ในกรณีที่เจ้าของข้อมูลส่วนบุคคลสมัครใจ และให้ความยินยอมอย่างชัดแจ้ง (Explicit Consent) ที่จะให้ทำการประมวลผลข้อมูลส่วนบุคคลได้ตามวัตถุประสงค์ที่แจ้งแก่เจ้าของข้อมูลส่วนบุคคล อย่างไรก็ตาม ฐานความยินยอมเหมาะสมเมื่อต้องการขอความยินยอมเพื่อประมวลผลข้อมูลส่วนบุคคลในเรื่องที่ไม่จำเป็นในการปฏิบัติตามสัญญาและไม่สามารถอ้างฐานอื่นใดในการประมวลผลข้อมูลทางกฎหมายได้ นอกจากนั้นในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลต้องคำนึงถึงความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคล ซึ่งความเป็นอิสระนั้นต้องอยู่บนพื้นฐานของการมีทางเลือกอย่างแท้จริง (Real choice) ดังนั้น การขอความยินยอมจะต้องเป็นสิ่งที่เจ้าของข้อมูลส่วนบุคคลทำการเลือกว่าจะให้ความยินยอมหรือปฏิเสธได้ และการปฏิเสธดังกล่าวจะต้องไม่มีผลกระทบต่อการได้รับบริการตามสัญญา ซึ่งผลของความยินยอมที่ไม่อิสระย่อมส่งผลให้ความยินยอมนั้นไม่มีผลผูกพันกับเจ้าของข้อมูลส่วนบุคคล ทำให้ท่านในฐานะผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถอ้างฐานความยินยอมนั้นเป็นฐานในการประมวลผลข้อมูลส่วนบุคคลได้ สำหรับเงื่อนไขและรายละเอียดการขอความยินยอมภายใต้ฐานความยินยอมโปรดดูรายละเอียดเพิ่มเติมในหัวข้อ “ความยินยอม (Consent)”

5.2.2 ฐานสัญญา (Contract)

ท่านสามารถใช้ฐานสัญญาในการประมวลผลข้อมูลส่วนบุคคล ในกรณีที่การประมวลผลข้อมูลจำเป็นต่อการให้บริการตามสัญญาที่ตกลงกันไว้ระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคล หรือเมื่อจำเป็นต้องประมวลผลข้อมูลส่วนบุคคลเพื่อปฏิบัติตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนที่จะเข้าสู่การทำสัญญา หากใช้สัญญาดังกล่าวเป็นฐานในการประมวลผลแล้วก็ไม่ต้องขอความยินยอมเพิ่มเติม ฐานนี้ใช้ได้กับข้อมูลส่วนบุคคลทั่วไปเท่านั้น ไม่สามารถใช้ฐานสัญญาในการประมวลผลข้อมูลอ่อนไหว (Sensitive Personal Data) สำหรับ

รายละเอียดและเงื่อนไขในการประมวลผลข้อมูลอ่อนไหวโปรดดูรายละเอียดเพิ่มเติมในหัวข้อ “ข้อมูลอ่อนไหว (Sensitive Personal Data)”

กรณีที่ท่านมีความจำเป็นที่จะต้องเปิดเผยข้อมูลของลูกค้าไปยังบุคคลที่สาม หากการเปิดเผยนั้นไม่ใช่เพื่อวัตถุประสงค์ทางการตลาด สำหรับกรณีนี้หากลูกค้าไม่ให้ความยินยอมจะกระทบต่อการดำเนินงานของท่านอย่างมีนัยสำคัญ หรือไม่สามารถให้บริการอย่างเป็นธรรมและต่อเนื่องได้ เช่น การเปิดเผยข้อมูลแก่ผู้ให้บริการภายนอก หรือตัวแทนของผู้ให้บริการ หรือผู้รับจ้างช่วงงานต่อ เพื่อสนับสนุนการให้บริการของผู้ให้บริการ การเปิดเผยข้อมูลให้หน่วยงานราชการตามกฎหมาย และการเปิดเผยข้อมูลให้กับบริษัทพันธมิตรในลักษณะ Co-brand เป็นต้น ท่านสามารถกำหนดให้การเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลที่สามดังกล่าวเป็นส่วนหนึ่งของเงื่อนไขในการขอใช้บริการได้

ตัวอย่าง ลูกค้าขอรับบริการวางแผนทางการเงินจากท่าน โดยท่านมีความจำเป็นต้องขอข้อมูลส่วนบุคคล เช่น ชื่อ นามสกุล ที่อยู่ ข้อมูลทางการเงิน เพื่อใช้สำหรับการให้บริการดังกล่าว ท่านควรใช้ฐานสัญญาในการประมวลผลข้อมูลส่วนบุคคลเพื่อให้บริการแก่ลูกค้าตามข้อกำหนดและเงื่อนไขการให้บริการ ที่ลูกค้าได้ตกลงตามข้อผูกพันดังกล่าว

5.2.3 ฐานประโยชน์สำคัญต่อชีวิต (Vital Interest)

กรณีที่การประมวลผลข้อมูลจำเป็นต่อการปกป้องผลประโยชน์ที่สำคัญของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น โดยเป็นการป้องกันอันตรายอันเกิดต่อสุขภาพและชีวิต ผู้ควบคุมข้อมูลส่วนบุคคลสามารถใช้ฐานการประมวลผลข้อมูลส่วนบุคคลนี้ได้ หากเจ้าของข้อมูลส่วนบุคคลอยู่ในสภาพที่ไม่สามารถให้ได้ความยินยอมได้ ทั่วไปใช้กับทางการแพทย์

ตัวอย่างที่**ไม่ควร**ใช้ฐานประโยชน์สำคัญต่อชีวิต ตัวอย่าง 1 ในกรณีที่ท่านทำการเก็บรวบรวมข้อมูลส่วนบุคคลของพนักงาน เช่น หมายเลขโทรศัพท์ของผู้ที่สามารถติดต่อได้ในกรณีฉุกเฉิน เพื่อใช้ติดต่อในกรณีฉุกเฉิน ซึ่งท่านสามารถทำการเก็บรวบรวมข้อมูลภายใต้ฐานสัญญาที่ทำระหว่างพนักงานและท่านในการรับเข้าทำงาน ตัวอย่าง 2 ท่านต้องการเก็บรวบรวมข้อมูลที่เป็นข้อมูลอ่อนไหวของพนักงาน เช่น ข้อมูลกรุ๊ปเลือดของพนักงาน หรือข้อมูลเกี่ยวกับสุขภาพของพนักงาน เพื่อไว้ใช้ในกรณีฉุกเฉินหากเกิดอันตรายต่อชีวิตของพนักงาน ในกรณีนี้ข้อมูลที่ท่านต้องการเก็บรวบรวมเป็นข้อมูลอ่อนไหว หากก่อนหรือขณะทำการเก็บรวบรวมข้อมูล พนักงานอยู่ในสภาพที่สามารถให้ความยินยอมได้ ท่านสามารถเก็บรวบรวมข้อมูลดังกล่าวได้ภายใต้ฐานความยินยอมแต่ไม่สามารถอ้างฐาน

ประโยชน์สำคัญต่อชีวิตได้เนื่องจาก จะใช้ได้เฉพาะกรณีที่เจ้าของข้อมูลส่วนบุคคลอยู่ในสภาพที่ไม่สามารถให้ได้ความยินยอมได้เท่านั้น

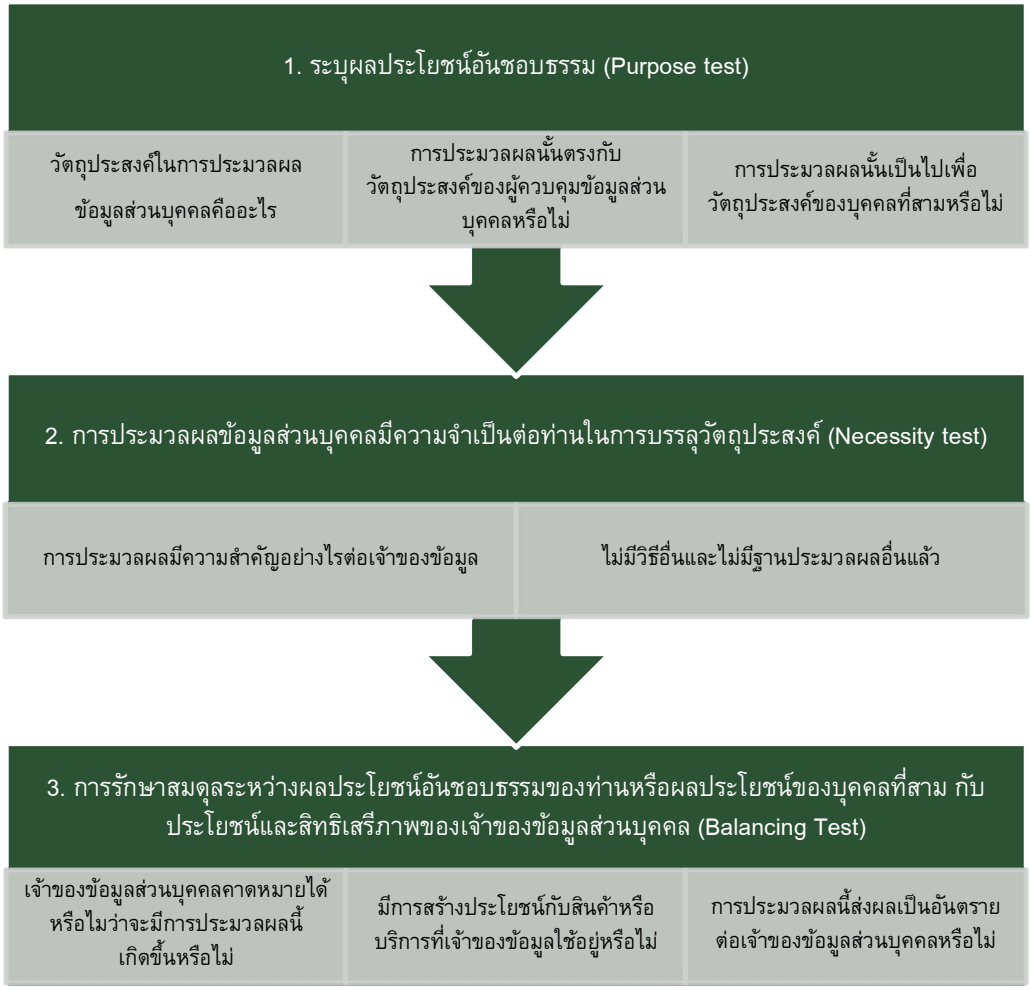
5.2.4 ฐานภารกิจของรัฐ (Public Task)

กรณีที่การประมวลผลเป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะหรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบหมายให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล โดยส่วนใหญ่ผู้ที่จะประมวลผลข้อมูลตามฐานนี้ได้มักเป็นเจ้าหน้าที่หรือองค์กรของภาครัฐ เช่น ศาล รัฐสภา หรือเจ้าหน้าที่ของกระทรวงต่างๆ ที่ปฏิบัติภารกิจตามกฎหมาย ซึ่งการประมวลผลโดยฐานดังกล่าวจะต้องสามารถอ้างอิงได้อย่างชัดเจนว่ากระทำภายใต้กฎหมายใดที่ให้อำนาจในการประมวลผลข้อมูล ซึ่งการใช้ฐานภารกิจของรัฐนั้นยังจำเป็นต้องมีการรักษาความปลอดภัยของข้อมูล เช่นเดียวกันกับฐานอื่น แต่เจ้าของข้อมูลส่วนบุคคลไม่สามารถ ใช้สิทธิในการ ลบ หรือโอนย้ายข้อมูลได้ แต่ยังมีสิทธิในการคัดค้านการประมวลผลได้

ตัวอย่าง ท่านมีหน้าที่ในการจัดทำการยื่นภาษีให้กับกรมสรรพากร ซึ่งกรมสรรพากรอาจขอให้ท่านเปิดเผยข้อมูลค่าใช้จ่ายเงินเดือนพนักงาน เพื่อทำการตรวจสอบความถูกต้องของข้อมูลในการคำนวณภาษีที่ท่านยื่นต่อกรมสรรพากร กรณีนี้ท่านสามารถเปิดเผยข้อมูลให้กับกรมสรรพากรภายใต้ฐานการปฏิบัติตามกฎหมาย และกรมสรรพากรทำการประมวลผลข้อมูลที่ได้รับจากท่านภายใต้ฐานภารกิจของรัฐ

5.2.5 ฐานประโยชน์อันชอบธรรม (Legitimate Interest)

การใช้ฐานประโยชน์อันชอบธรรมเป็นหนึ่งในฐานกฎหมายที่มีความยืดหยุ่นมากที่สุดในการประมวลผลข้อมูลส่วนบุคคล แต่อย่างไรก็ตามฐานนี้ก็ไม่ได้เป็นฐานที่เหมาะสมที่สุดเสมอไป จะเหมาะสมเมื่อท่านประมวลผลข้อมูลส่วนบุคคลในแบบที่เจ้าของข้อมูลส่วนบุคคลสามารถคาดหมายได้อย่างสมเหตุสมผล อีกทั้งมีผลกระทบต่อความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลเพียงเล็กน้อย หรือในกรณีที่ท่านมีเหตุผลในการประมวลผลข้อมูลอย่างสมเหตุสมผลซึ่งท่านเองจะต้องอธิบายได้ หากท่านเลือกที่จะประมวลผลภายใต้ฐานประโยชน์อันชอบธรรม ท่านจะมีหน้าที่และความรับผิดชอบเพิ่มขึ้นในการใช้ดุลพินิจอย่างมากในการประมวลผลข้อมูลส่วนบุคคล และการคุ้มครองสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล เนื่องจากท่านจะต้องคำนึงถึงประโยชน์ของ 2 ฝั่ง อันได้แก่ผลประโยชน์อันชอบธรรมของท่านเองกับสิทธิและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ซึ่งการได้ประโยชน์อันชอบธรรมดังกล่าวจะต้องไม่เป็นการละเมิดหรือกระทบต่อสิทธิขั้นพื้นฐานและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะอย่างยิ่งกับผู้เยาว์



ตารางแสดงการประเมินการใช้ฐานผลประโยชน์อันชอบธรรม

Legitimate interest Assessment (LIA)

ในการประเมินการใช้ฐานผลประโยชน์อันชอบธรรม สามารถทำได้โดยพิจารณา 3 องค์ประกอบ ที่ช่วยในการตัดสินใจอย่างเหมาะสมในการใช้ฐานดังกล่าว ซึ่งจะต้องทำก่อนการประมวลผลข้อมูลส่วนบุคคล อันได้แก่

1. ระบุผลประโยชน์อันชอบธรรม (Purpose test)

การประมวลผลข้อมูลส่วนบุคคลภายใต้ผลประโยชน์อันชอบธรรมอาจเป็นผลประโยชน์ของท่านเองหรือผลประโยชน์ของบุคคลที่สาม รวมถึงผลประโยชน์เชิงพาณิชย์ และผลประโยชน์แก่สาธารณะ

2. การประมวลผลข้อมูลส่วนบุคคลมีความจำเป็นต่อท่านในการบรรลุวัตถุประสงค์ (Necessity test)

การประมวลผลข้อมูลส่วนบุคคลจะต้องมีความจำเป็น หากท่านสามารถบรรลุวัตถุประสงค์เดียวกันได้อย่างสมเหตุสมผลด้วยวิธีการที่จะมีผลกระทบต่อความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลที่น้อยกว่า ท่านควรประมวลผลโดยใช้ฐานอื่น

3. การรักษาสมดุลระหว่างผลประโยชน์อันชอบธรรมของท่านหรือผลประโยชน์ของบุคคลที่สาม กับประโยชน์และสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล (Balancing test)

ท่านจะต้องชั่งน้ำหนักระหว่างผลประโยชน์อันชอบธรรมของท่านกับสิทธิเสรีภาพ/ประโยชน์ของเจ้าของข้อมูลส่วนบุคคล หากการประมวลผลนั้นไม่เป็นไปตามความคาดหมายอย่างสมเหตุสมผลแก่เจ้าของข้อมูลส่วนบุคคลหรืออาจก่อให้เกิดความไม่เป็นธรรม ท่านจะต้องให้ ประโยชน์และสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคลแทนที่ผลประโยชน์อันชอบธรรมของท่าน นั่นคือการให้สิทธิในการคัดค้านการประมวลผลข้อมูลของเจ้าของข้อมูลส่วนบุคคล อย่างไรก็ตามประโยชน์อันชอบธรรมของท่านไม่จำเป็นต้องสอดคล้องกับประโยชน์ของเจ้าของข้อมูลส่วนบุคคลเสมอไป หากมีข้อโต้แย้งเกี่ยวกับสิทธิเสรีภาพ/ประโยชน์ของเจ้าของข้อมูลส่วนบุคคลเกิดขึ้น ท่านยังสามารถประมวลผลได้เพื่อประโยชน์อันชอบธรรมดังกล่าวของท่านตราบเท่าที่ท่านจะแสดงให้เห็นอย่างสมเหตุสมผลและชัดเจนในเรื่องของผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล

<u>ตัวอย่างคำถามที่ใช้ประกอบการพิจารณาการทำ Balancing Test</u>

- ท่านมีความสัมพันธ์อย่างไรกับเจ้าของข้อมูลส่วนบุคคล
- มีการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลที่เป็นข้อมูลอ่อนไหวหรือข้อมูลส่วนบุคคลหรือไม่
- ลูกค้ามีความคาดหวังเกี่ยวกับกิจกรรมการประมวลผลของท่านในลักษณะนี้หรือไม่
- ท่านมีความเต็มใจและสามารถที่จะอธิบายเกี่ยวกับการประมวลผลให้ลูกค้าทราบหรือไม่
- ท่านคาดว่าลูกค้ามีแนวโน้มจะคัดค้านกิจกรรมการประมวลผลหรือพบว่าเป็นการละเมิด/รุกล้ำความเป็นส่วนตัวหรือไม่
- ผลกระทบที่เป็นไปได้ต่อบุคคลเป็นอย่างไรและจะมีผลกระทบมากน้อยเพียงใด
- ท่านกำลังประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์หรือไม่
- ท่านสามารถใช้มาตรการในการป้องกันเพื่อลดผลกระทบที่อาจเกิดขึ้นได้หรือไม่
- ท่านสามารถให้ลูกค้าทำการคัดค้านการประมวลผลได้หรือไม่

นอกจากนั้นท่านจะต้องทำการเก็บบันทึกประเมินการใช้ฐานผลประโยชน์อันชอบธรรม (LIA) เพื่อให้มั่นใจว่าการประมวลผลมีความจำเป็นและมีความสมเหตุสมผลในการใช้ฐานดังกล่าวเพื่อใช้แสดงแก่สำนักงานคุ้มครองข้อมูลส่วนบุคคลหากมีความจำเป็น และท่านจะต้องทำการระบุกิจกรรมการประมวลผล (Data Processing Activities) ที่ใช้ฐานผลประโยชน์อันชอบธรรมไว้ในนโยบายความเป็นส่วนตัวของท่าน (Privacy Notice) เพื่อเป็นการแจ้งให้ทราบแก่บุคคล

ในทางปฏิบัติท่านสามารถใช้ฐานการประมวลผลอันชอบธรรมได้ในกรณีต่อไปนี้

- ท่านสามารถประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ทางการตลาดได้ หากท่านสามารถแสดงให้เห็นถึงความเหมาะสมในการใช้ข้อมูล และมีผลกระทบเพียงเล็กน้อยต่อความเป็นส่วนตัวของบุคคล และบุคคลสามารถคาดหมายต่อกิจกรรมเหล่านั้นของท่านได้ หรือบุคคลไม่มีแนวโน้มที่จะคัดค้านกิจกรรมการประมวลผลเหล่านั้นได้
- ท่านสามารถประมวลผลข้อมูลของผู้เยาว์ภายใต้ฐานประโยชน์อันชอบธรรมได้ แต่จะต้องกระทำอย่างระมัดระวังเป็นพิเศษเพื่อให้แน่ใจว่าสิทธิและผลประโยชน์ของผู้เยาว์นั้นได้รับการคุ้มครองอย่างเหมาะสม โดยเฉพาะอย่างยิ่งการทำโปรไฟล์ลิ่งข้อมูลของผู้เยาว์ ที่เกี่ยวกับการวิเคราะห์ข้อมูลเพื่อวัตถุประสงค์ทางการตลาด สำหรับกรณีนี้ ท่านอาจต้องพิจารณาการจัดทำ DPIA เพื่อประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการประมวลผลข้อมูลและแนวทางในการจัดการกับความเสี่ยงดังกล่าว โปรดดูรายละเอียดการจัดทำ DPIA เพิ่มเติมในหัวข้อ “แนวปฏิบัติเกี่ยวกับการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA)”

<u>ตัวอย่างการใช้ฐานผลประโยชน์อันชอบธรรม</u>

<u>ตัวอย่าง 1</u> ท่านทำการประมวลผลข้อมูลส่วนบุคคล เพื่อการป้องกันระบบเศรษฐกิจการเงินในการจัดการอาชญากรรม การระงับเหตุ การสืบสวน การเรียกคืนความเสียหาย ลดความเสี่ยงทุจริตที่อาจเกิดการกระทำที่ผิดกฎหมายต่าง ๆ เพื่อป้องกันนักลงทุนและคุ้มครองสิทธิประโยชน์อันชอบธรรมของลูกค้าจากกลุ่มมิจฉาชีพที่แอบแฝงเข้าก่อความเสียหายต่อประชาชนทั้งทางตรงและทางอ้อมอันส่งผลถึงเศรษฐกิจโดยรวมของประเทศ เพื่อเสถียรภาพและความเชื่อมั่นต่อการจัดการอาชญากรรมทางเศรษฐกิจ ซึ่งรวมถึงการแบ่งปันข้อมูลส่วนบุคคลเพื่อยกระดับมาตรฐานการทำงานของกลุ่มสถาบันการเงินธุรกิจท่าน ในการป้องกันระงับเหตุ ลดความเสี่ยงทุจริตและกฎหมายอาญาข้างต้น เช่น การตรวจสอบป้องกันการทุจริต (Fraud Prevention and Investigation) ท่านอาจมีการเปิดเผยข้อมูลของบุคคลที่มี

ความเสี่ยงหรือบุคคลเฝ้าระวังที่เกี่ยวข้องกับการทุจริตหรือมีประวัติการทุจริตให้กับสมาชิกสมาคมนักวางแผนการเงินไทย รวมถึงการจัดเก็บและรวบรวมข้อมูล Fraud Risk ซึ่งอยู่ภายใต้ วัตถุประสงค์และนโยบายของกลุ่มธุรกิจท่าน หรือภายใต้วัตถุประสงค์และนโยบายในการคุ้มครองข้อมูลส่วนบุคคลของท่าน เพื่อทำการประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ข้างต้น

ตัวอย่าง 2 ท่านทำการบันทึกภาพบรรยากาศและบันทึกวีดีโอ ของผู้ที่มาเข้าร่วมการอบรมหรืองานสัมมนาต่างๆ ซึ่งการบันทึกดังกล่าวอาจมีการเปิดเผยหรือเผยแพร่ให้แก่บุคคลภายนอกเพื่อวัตถุประสงค์ในการประชาสัมพันธ์ อย่างไรก็ตามสำหรับกรณีนี้ท่านจะต้องทำการติดประกาศในบริเวณงานเพื่อเป็นการแจ้งให้ทราบแก่บุคคลที่มาร่วมงาน ว่าจะมีการบันทึกภาพในงานและอาจมีการเผยแพร่เพื่อการประชาสัมพันธ์

ตัวอย่าง 3 ท่านทำการประมวลผลข้อมูลส่วนบุคคลเพื่อการรักษาความสัมพันธ์กับลูกค้า เช่น การจัดการข้อร้องเรียน การเสนอสิทธิประโยชน์พิเศษโดยไม่มีวัตถุประสงค์ทางการตลาดให้แก่ลูกค้า เป็นต้น

ตัวอย่าง 4 ท่านทำการบันทึกภาพผู้ที่มาติดต่อทำธุรกรรมกับสำนักงานของท่านลงบน CCTV รวมถึง การแลกบัตรก่อนเข้าอาคาร เพื่อการรักษาความปลอดภัยภายในบริเวณอาคารของท่าน อย่างไรก็ตามสำหรับกรณีนี้ท่านจะต้องทำการติดประกาศ ในบริเวณที่สามารถเห็นได้ง่ายของอาคาร เพื่อเป็นการแจ้งให้ทราบ

ตัวอย่าง 5 ท่านทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อการบริหารความเสี่ยง/การกำกับตรวจสอบ/การบริหารจัดการภายในองค์กร เช่น ข้อมูลบุคคลล้มละลาย, ข้อมูลบุคคลที่มีความเสี่ยงในการทุจริต Fraud Risk, ข้อมูลรายชื่อลูกค้าเฝ้าระวัง Suspect risk

5.2.6 ฐานการปฏิบัติตามกฎหมาย (Legal Obligation)

ฐานการปฏิบัติตามกฎหมาย ผู้ควบข้อมูลส่วนบุคคลสามารถใช้ฐานดังกล่าวได้ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ประมวลผลข้อมูลตามที่กฎหมายกำหนด และจะต้องสามารถระบุได้อย่างชัดเจนว่ากำลังปฏิบัติหน้าที่ตามบทบัญญัติใดของกฎหมาย หรือทำตามคำสั่งของหน่วยงานใด สำหรับกรณีนี้ แม้ว่าเจ้าของข้อมูลส่วนบุคคลจะมีสิทธิในการคัดค้านการประมวลผลข้อมูล อย่างไรก็ตามหากการประมวลผลดังกล่าวเป็นไปตามฐานการปฏิบัติตามกฎหมาย ท่านสามารถปฏิเสธคำร้องขอการคัดค้านการประมวลผลได้ โดยการระบุเหตุแห่งการปฏิเสธประกอบด้วย

ตัวอย่าง 1 ท่านมีหน้าที่ในการจัดทำการยื่นภาษีให้กับกรมสรรพากร ซึ่งกรมสรรพากรอาจขอให้ท่านเปิดเผยข้อมูลค่าใช้จ่ายเงินเดือนพนักงาน เพื่อทำการตรวจสอบความถูกต้องของข้อมูลในการคำนวณภาษีที่ท่านยื่นต่อกรมสรรพากร กรณีนี้ท่านสามารถเปิดเผยข้อมูลให้กับกรมสรรพากรภายใต้ฐานการปฏิบัติตามกฎหมาย

ตัวอย่าง 2 ในกรณีที่ท่านมีความจำเป็นจะต้องเปิดเผยข้อมูลส่วนบุคคลของลูกหนี้แก่ศาล เพื่อดำเนินการฟ้องล้มละลายภายใต้พระราชบัญญัติล้มละลาย

5.2.7 ฐานเอกสารประวัติศาสตร์ จดหมายเหตุและการศึกษาวิจัยหรือสถิติ (Research)

กรณีที่ท่านมีความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือสาธารณประโยชน์อื่น ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น สำหรับการประมวลผลโดยฐานนี้ GDPR กำหนดให้จะต้องใช้ฐานอื่นประกอบการประมวลผลโดยฐานนี้เสมอ ไม่สามารถอ้างฐานนี้เพียงอย่างเดียวเพื่อใช้ในการประมวลผลได้นอกจากนั้นการประมวลผลบนฐานนี้มีความจำเป็นที่จะต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ตามที่คณะกรรมการประกาศกำหนด เนื่องจากการประมวลผลข้อมูลภายใต้ฐานนี้จำเป็นจะต้องมีมาตรการที่ความสอดคล้องกับมาตรฐานจริยธรรม และระเบียบในการจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุและการศึกษาวิจัยหรือสถิติด้วย

5.3 ความยินยอม (Consent)

5.3.1 เงื่อนไขในการใช้ฐานความยินยอมมีดังต่อไปนี้

- ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนจึงจะเก็บรวบรวม ใช้ เปิดเผยข้อมูลนั้นๆ ได้
- เจ้าของข้อมูลส่วนบุคคลสามารถถอนความยินยอมเมื่อใดก็ได้
- การใช้ฐานความยินยอมนั้น จะต้องให้สิทธิเจ้าของข้อมูลส่วนบุคคลสามารถปฏิเสธไม่ให้ความยินยอมได้
- การขอความยินยอมจะต้องกระทำอย่างชัดเจนไม่คลุมเครือ ดังนั้น ท่านจึงควรออกแบบแบบฟอร์มการขอความยินยอมที่ทำให้เจ้าของข้อมูลส่วนบุคคลสามารถเห็นได้อย่างชัดเจนว่า ท่านขอความยินยอมในการประมวลผลข้อมูลเพื่อวัตถุประสงค์ใดบ้าง

- ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องคำนึงถึงอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม ทั้งนี้การขอความยินยอมจะต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน ไม่นำมารวมอยู่ในเงื่อนไขการให้บริการ (Terms & Conditions) หรือข้อความในสัญญา
- การขอความยินยอมจะทำในรูปแบบเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ก็ได้

5.3.2 การใช้ฐานความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เป็นฐานในการประมวลผลที่เจ้าของข้อมูลส่วนบุคคลสามารถเลือกที่จะจัดการกับข้อมูลส่วนบุคคลของตนเองได้อย่างเต็มที่ ซึ่งท่านจะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลในการประมวลผล ยกเว้นกรณีการประมวลผลข้อมูลส่วนบุคคลเป็นการประมวลผลภายใต้ฐานกฎหมายอื่น

5.3.3 ท่านควรเลือกใช้ฐานในการประมวลผลให้เหมาะสมกับวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล เนื่องจากฐานความยินยอมไม่สามารถใช้ได้กับทุกกรณี เว้นแต่กรณีที่ต้องขอความยินยอมตามข้อกำหนดของกฎหมายอื่น ฐานความยินยอมจะเหมาะสมเมื่อการประมวลผลข้อมูลไม่ได้มีความจำเป็นตามเงื่อนไขของสัญญา นอกจากนั้นการให้ความยินยอมจะต้องเป็นสิ่งที่ให้เจ้าของข้อมูลส่วนบุคคลทำการเลือกว่าจะให้หรือปฏิเสธได้ และการปฏิเสธจะต้องไม่มีผลกระทบต่อการได้รับบริการตามสัญญา การขอความยินยอมจะต้องกระทำโดยชอบด้วยกฎหมายเป็นธรรม และโปร่งใส โดยท่านจะต้องไม่ใช้ข้อความที่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ และจะต้องคำนึงถึงความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการตัดสินใจให้ความยินยอม โดยการให้ความยินยอมจะต้องเป็นการสมัครใจ ดังนั้นการขอความยินยอมจะต้องระบุวัตถุประสงค์ในการประมวลผลข้อมูลอย่างชัดเจนว่าจะขอความยินยอมในเรื่องใด

5.3.4 ท่านต้องไม่นำฐานความยินยอมและฐานสัญญามาปะปนกัน ต้องแยกให้ได้ว่าข้อมูลใดจำเป็นสำหรับการปฏิบัติตามสัญญาก็ควรจะระบุอยู่ในสัญญา ซึ่งการขอความยินยอมจะต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน ไม่นำมารวมอยู่ในเงื่อนไขการให้บริการ (Terms & Conditions) เนื่องจากการกระทำดังกล่าวอาจทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดว่าหากไม่ให้ความยินยอมแล้วจะไม่ได้รับบริการหรือมีผลต่อการใช้บริการของท่าน

5.3.5 นอกจากนั้นการใช้ฐานความยินยอมอาจเหมาะสมในสถานการณ์ที่จะประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เฉพาะเจาะจงมากกว่า และท่านไม่สามารถ

ประมวลผลตามวัตถุประสงค์ที่เพิ่มเติมขึ้นมาใหม่เองได้ โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ท่านจะต้องทำการขอความยินยอมใหม่หากต้องการประมวลผลเพื่อวัตถุประสงค์อื่นที่นอกเหนือจากที่เคยได้รับความยินยอมไปแล้ว เว้นแต่หากพิจารณาแล้วว่าการประมวลผลเพื่อวัตถุประสงค์อื่นนั้น สามารถทำได้ภายใต้ฐานกฎหมายฐานอื่น

5.3.6 การขอความยินยอม สามารถทำได้หลายวิธี เช่น

- การยินยอมจากการเลือกยินยอม (Opt-in Consent) ผู้ควบคุมข้อมูลส่วนบุคคลได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลอย่างชัดเจน เป็นลายลักษณ์อักษร หรือทำโดยผ่านระบบอิเล็กทรอนิกส์ ท่านควรออกแบบให้เจ้าของข้อมูลส่วนบุคคลต้องมีการกระทำให้ความยินยอมอย่างชัดเจน (Clear Affirmative Action) และมีอิสระบนพื้นฐานของการมีทางเลือกอย่างแท้จริง (Real choice) เช่น การทำเป็นช่องเช็คถูก (Check Box) โดยให้เจ้าของข้อมูลส่วนบุคคลกด/เขียนเช็คเองได้ (Signatures or Ticks Indicating Consent)
- กรณีที่โดยสภาพไม่อาจขอความยินยอมรูปแบบหนังสือ หรือทำโดยผ่านระบบอิเล็กทรอนิกส์ได้ ท่านอาจสามารถขอความยินยอมในรูปแบบวาจา (Verbal Consent) สำหรับรูปแบบการขอความยินยอมนี้ใช้ในกรณีที่มีการบันทึกความยินยอมในรูปแบบเสียง (Voice Record) ด้วยระบบดิจิทัล เช่น บันทึกผ่านการติดต่อกับเจ้าของข้อมูลส่วนบุคคลทาง Contact Center หรือผ่านทางระบบ Interactive Voice Response (IVR) โดยขอให้เจ้าของข้อมูลส่วนบุคคลกดปุ่มยืนยันการให้ความยินยอม เป็นต้น ซึ่งท่านจะต้องมีกระบวนการพิสูจน์และยืนยันตัวตนของเจ้าของข้อมูลส่วนบุคคลก่อนทำการขอความยินยอมเพื่อให้มั่นใจว่าคู่สนทนาเป็นเจ้าของข้อมูลส่วนบุคคลของท่านจริง นอกจากนั้นท่านควรให้ข้อมูลแก่เจ้าของข้อมูลส่วนบุคคลอย่างเพียงพอต่อการตัดสินใจ มีทางเลือก และเนื้อหาชัดเจนไม่ก่อให้เกิดความเข้าใจผิด และให้เจ้าของข้อมูลส่วนบุคคลสามารถให้ความยินยอมหรือไม่ให้ความยินยอมก็ได้โดยสมัครใจ ไม่เป็นการบังคับ
- การถอนความยินยอม (Withdraw of Consent)
  เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะขอเพิกถอนความยินยอม (“Right to Withdraw of Consent”) ที่จะให้ไว้กับท่านในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลเมื่อใดก็ได้ และท่าน

จะต้องดำเนินการหยุดการประมวลผลข้อมูลที่เจ้าของข้อมูลส่วนบุคคลเคยได้ให้ความยินยอมไว้หากท่านไม่มีฐานโดยชอบด้วยกฎหมายอื่นที่จะทำการเก็บรวบรวมใช้หรือเปิดเผยต่อไปให้ท่านดำเนินการลบข้อมูลออก

การใช้สิทธิถอนความยินยอม ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีช่องทางที่เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิกระทำได้ง่ายในระดับเดียวกับการให้ความยินยอม

5.3.7 กรณีการเก็บรวบรวมข้อมูลส่วนบุคคลที่ท่านสามารถทำได้โดยได้รับการยกเว้นไม่ต้องขอความยินยอม ในกรณีดังนี้

- เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุหรือเพื่อประโยชน์สาธารณะ
- เพื่อการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสม
- เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล
- เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น
- เพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของท่านหรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ท่าน
- เป็นการจำเป็นเพื่อประโยชน์อันชอบด้วยกฎหมายของท่านหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ท่าน เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล
- เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

<u>ตัวอย่างการประมวลผลข้อมูลที่ควรใช้ฐานความยินยอม</u>

<u>ตัวอย่าง</u> ท่านจะต้องทำการขอความยินยอม เพื่อใช้ในการเปิดเผยข้อมูลส่วนบุคคล หรือข้อมูลทางการเงินอื่น ๆ ของลูกค้าที่ได้ให้ไว้แก่ท่านหรือที่ท่านอาจเข้าถึงได้จากแหล่งอื่น ไปยังพันธมิตรทางธุรกิจของท่าน เพื่อการบริการวางแผนทางการเงิน แนะนำผลิตภัณฑ์ทางการเงิน และเพื่อประชาสัมพันธ์เกี่ยวกับบริการต่าง ๆ (Marketing Purpose) ของบุคคลดังกล่าว สำหรับกรณีนี้ท่านต้องขอความยินยอมจากลูกค้า

ตัวอย่างกรณีการขอความยินยอมที่ไม่ควรนำมารวมอยู่ในเงื่อนไขของการให้บริการ

ตัวอย่าง ท่านไม่สามารถกำหนดเงื่อนไขให้ลูกค้าต้องเลือกซื้อผลิตภัณฑ์หรือใช้บริการตามที่ท่านกำหนดเท่านั้นโดยไม่สามารถตัดสินใจเลือกผลิตภัณฑ์หรือใช้บริการเป็นอย่างอื่นได้เป็นเงื่อนไขในการเข้ารับบริการวางแผนทางการเงิน

ตัวอย่าง แบบฟอร์มการขอความยินยอม (Consent form)

หนังสือให้ความยินยอมในการเก็บรวบรวม/ใช้/เปิดเผยข้อมูลส่วนบุคคล (PDPA)

เรียน ลูกค้าคนสำคัญ

(เลือกระบุ (1) นักวางแผนการเงิน CFP / ระบุชื่อบริษัทของนักวางแผนการเงิน CFP ("นักวางแผนการเงิน CFP") หรือ (2) ที่ปรึกษาการเงิน AFPT / ระบุชื่อบริษัทของที่ปรึกษาการเงิน AFPT ("ที่ปรึกษาการเงิน AFPT")) มีความมั่นใจเป็นอย่างยิ่งว่าจะนำพาลูกค้าไปสู่ความมั่นคงทางการเงินและยังคงนำเสนอผลิตภัณฑ์และบริการที่เหมาะสมกับลูกค้ามากที่สุด ให้สอดคล้องกับกฎหมายและกฎระเบียบข้อบังคับ (เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) จึงได้จัดทำหนังสือขออนุญาตจากลูกค้าในการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลของลูกค้า ได้แก่ [โปรดระบุข้อมูลส่วนบุคคลที่ท่านทำการประมวลผล (เก็บรวบรวม, ใช้, เปิดเผย) ข้อมูลส่วนบุคคล] ที่ได้ให้แก่ (เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) หรือที่ (เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) อาจเข้าถึงได้จากแหล่งอื่น

เพื่อวัตถุประสงค์ดังต่อไปนี้:

- [ระบุวัตถุประสงค์ในการประมวลผล (เก็บรวบรวม, ใช้, เปิดเผย) ข้อมูลส่วนบุคคล]
- [ระบุวัตถุประสงค์ในการประมวลผล (เก็บรวบรวม, ใช้, เปิดเผย) ข้อมูลส่วนบุคคล]

โดยเปิดเผยไปยังบุคคลดังต่อไปนี้[1]:

- [ระบุบริษัทที่ท่านเปิดเผยข้อมูลส่วนบุคคล]
- [ระบุบริษัทที่ท่านเปิดเผยข้อมูลส่วนบุคคล]

ท่านสามารถดูรายละเอียดเพิ่มเติมที่เผยแพร่ภายใต้ ประกาศความเป็นส่วนตัว (Privacy Notice) บนเว็บไซต์ของ (เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) <webpage URL> (เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) จะทำการเก็บข้อมูลส่วนบุคคลและการให้ความยินยอมของลูกค้าไว้ตามประกาศความเป็นส่วนตัวของ (เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)

[1] หากท่านไม่มีการเปิดเผยข้อมูลไปยังบุคคลอื่น ท่านสามารถพิจารณาตัดข้อความในส่วนดังกล่าวออกได้

หากลูกค้าประสงค์จะเพิกถอนความยินยอมนี้ หรือทำการยื่นข้อร้องเรียนใดๆที่เกี่ยวกับการละเมิดสิทธิของลูกค้า สามารถดำเนินการผ่านทาง ABC Contact Center หมายเลข 1234 หรือช่องทางที่ระบุไว้ในเว็บไซต์ของ (เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) นอกจากนี้ลูกค้ายังสามารถรายงานหรือยื่นข้อเรื่องร้องเรียนใดๆ ที่เกี่ยวข้องกับการละเมิดสิทธิของลูกค้า ได้ที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่ DPO@abc.com

วันที่.....

ชื่อ-นามสกุล.....

เลขประจำตัวประชาชน.....

☐ ยินยอม ☐ ไม่ยินยอม

ลงชื่อ ..... เจ้าของข้อมูลส่วนบุคคล

(.....)

5.3.8 การขอความยินยอมจากผู้เยาว์

ในการขอความยินยอมจากผู้เยาว์ (ผู้เยาว์ หมายถึง ผู้มีอายุไม่ครบ 20 ปีบริบูรณ์ หรือ ไม่ได้จดทะเบียนสมรสกันก่อนอายุ 20 ปีโดยอายุไม่ต่ำกว่า 17 ปี) ท่านต้องกระทำโดยระมัดระวังเป็นพิเศษ เนื่องจากความสามารถในการเข้าใจวัตถุประสงค์ของผู้เยาว์นั้นไม่เท่ากับผู้ที่บรรลุนิติภาวะแล้ว ดังนั้นการขอความยินยอมจากผู้เยาว์ต้องทำอย่างถูกต้อง เป็นธรรมและโปร่งใส ("Lawfulness, Fairness, and Transparency") โดยใช้ภาษาที่ง่าย มีความเหมาะสมกับระดับความเข้าใจของผู้เยาว์ มีความชัดเจน ไม่ก่อให้เกิดความเข้าใจผิดได้ง่าย

ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลได้ให้หลักการในเรื่องของการให้ความยินยอมของผู้เยาว์ว่า หากเจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ซึ่งยังไม่บรรลุนิติภาวะโดยการสมรสหรือไม่มีฐานะเสมือนดังบุคคลซึ่งบรรลุนิติภาวะแล้วตามมาตรา 27 แห่งประมวลกฎหมายแพ่งและพาณิชย์ การขอความยินยอมจากผู้เยาว์นั้นจะต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำแทนผู้เยาว์ด้วย เว้นแต่ เป็นไปตาม มาตรา 22 23 และ 24* แห่งประมวลกฎหมายแพ่งและพาณิชย์ ผู้เยาว์จึงจะสามารถให้ความยินยอมตามลำพังได้

ในกรณีที่ผู้เยาว์มีอายุไม่เกินสิบปี ให้ขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

(* มาตรา 22 แห่งประมวลกฎหมายแพ่งและพาณิชย์ ผู้เยาว์อาจทำการใดๆ ได้ทั้งสิ้น หากเป็นเพียงเพื่อจะได้ไปซึ่งสิทธิอันใดอันหนึ่ง หรือเป็นการเพื่อหลุดพ้นจากหน้าที่อันใดอันหนึ่ง

มาตรา 23 แห่งประมวลกฎหมายแพ่งและพาณิชย์ ผู้เยาว์อาจทำการใดๆ ได้ทั้งสิ้น ซึ่งเป็นการต้องทำเองเฉพาะตัว

มาตรา 24 แห่งประมวลกฎหมายแพ่งและพาณิชย์ ผู้เยาว์อาจทำการใดๆ ได้ทั้งสิ้น ซึ่งเป็นการสมแก่ฐานานุรูปแห่งตน และเป็นการอันจำเป็นในการดำรงชีพอันสมควร)

สำหรับการถอนความยินยอมของผู้เยาว์ที่ไม่ใช่เพื่อการใด ๆ ตามประมวลกฎหมายแพ่งและพาณิชย์มาตรา 22 23 และ 24 จะต้องได้รับความยินยอมจากผู้มีอำนาจปกครองที่มีอำนาจกระทำแทนด้วย ในกรณีที่ผู้เยาว์มีอายุไม่เกินสิบปี ให้ผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ใช้สิทธิในการถอนความยินยอมกระทำการแทนผู้เยาว์

หากท่านมีความจำเป็นที่ต้องประมวลผลข้อมูลของผู้เยาว์ ท่านควรจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment : DPIA) ก่อนการประมวลผล โปรดดูรายละเอียดในหัวข้อ “แนวปฏิบัติเกี่ยวกับการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA)” เพื่อประเมินผลกระทบที่อาจเกิดขึ้น และหาวิธีการลดความเสี่ยงจากการประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์ต่อไป นอกจากนั้นท่านต้องคำนึงถึงการคุ้มครองสิทธิของผู้เยาว์ด้วย

5.3.9 การขอความยินยอมในการเก็บคุกกี้ (Cookie Consent)

“คุกกี้ (Cookie)” หมายถึง ข้อความขนาดเล็กที่เว็บไซต์ทำการเก็บไว้ ซึ่งคุกกี้จะถูกจัดเก็บลงในอุปกรณ์คอมพิวเตอร์ หรือเครื่องมือสื่อสารที่เข้าใช้งานของผู้ใช้งานเว็บไซต์หรือแอปพลิเคชัน ซึ่งคุกกี้จะถูกนำมาใช้เพื่อทำให้ผู้ใช้งานเว็บไซต์หรือแอปพลิเคชันสามารถใช้งานได้อย่างต่อเนื่อง อย่างไรก็ตาม คุกกี้บางประเภทอาจส่งผลกระทบกับความเป็นส่วนตัวของผู้ใช้งาน เช่น ใช้ในการวิเคราะห์ความสนใจลูกค้า พฤติกรรมการเยี่ยมชม เพื่อนำเสนอสื่อให้เหมาะสมกับความสนใจของ

ลูกค้า รวมถึงอาจมีการติดตามการใช้งานเว็บไซต์หรือแอปพลิเคชันที่ผู้ใช้งานเยี่ยมชมได้

ท่านสามารถใช้ข้อมูลคุกกี้ประเภทที่มีความจำเป็นต่อการใช้งานเว็บไซต์หรือแอปพลิเคชัน (Necessary Cookies) ได้โดยไม่ต้องขอความยินยอม สำหรับคุกกี้ประเภทอื่น ๆ เช่น คุกกี้ที่ใช้ในการวิเคราะห์ข้อมูล (Analytic Cookies) คุกกี้ที่ใช้ในการโฆษณา (Targeting Cookies) เป็นต้น ท่านควรทำการขอความยินยอมในการใช้งานคุกกี้ประเภทที่ไม่ได้จำเป็นต่อการใช้งานเว็บไซต์ดังกล่าวก่อนการใช้คุกกี้นั้น ๆ หรือท่านอาจจัดให้ลูกค้าสามารถจัดการฟังก์ชันคุกกี้เองได้ กล่าวคือ ลูกค้าจะสามารถเลือกเปิดหรือปิดค่าคุกกี้แต่ละประเภทในหน้าเว็บไซต์ได้ ในการขอความยินยอมคุกกี้ ผู้ใช้งานจะต้องสามารถยอมรับหรือปฏิเสธคุกกี้ได้และการปฏิเสธไม่ให้ความยินยอมของผู้ใช้งานจะต้องไม่ส่งผลกระทบต่อการใช้งานเว็บไซต์หรือแอปพลิเคชัน

5.4 ข้อมูลอ่อนไหว (Sensitive Personal Data)

ข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว “Sensitive Personal Data” คือ ข้อมูลส่วนบุคคลที่สามารถพิจารณาได้ว่าเป็นเรื่องส่วนตัวของเจ้าของข้อมูลส่วนบุคคล และมีความละเอียดอ่อนและมีความสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม จึงจำเป็นต้องดำเนินการอย่างระมัดระวังเป็นพิเศษในการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว เช่น เชื้อชาติ เผ่าพันธุ์ ประวัติอาชญากรรม ความเห็นทางการเมือง ความเชื่อ ลัทธิ ศาสนา ปรัชญา พฤติกรรมทางเพศ ข้อมูลสุขภาพ ข้อมูลความพิการ ข้อมูลสุขภาพจิต ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ ข้อมูลอื่นใดซึ่งกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

ท่านห้ามเก็บข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว หากไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล (Explicit Consent) เว้นแต่ในกรณีที่ได้รับการยกเว้นตามกฎหมายไม่ได้ต้องขอความยินยอม ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว ได้แก่

- เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม
- เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคมหรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอก

- เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล
- เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
- เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ ประโยชน์สาธารณะด้านการสาธารณสุข การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่นที่สำคัญ โดยต้องกระทำเพื่อบรรลุวัตถุประสงค์เท่าที่จำเป็น และจัดให้มีมาตรการในการคุ้มครองข้อมูลที่เหมาะสม

ตัวอย่าง 1 ในกรณีที่ลูกค้าเข้ารับบริการวางแผนการเงินกับท่าน ท่านอาจมีความจำเป็นที่ต้องทำการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว เช่น ข้อมูลสุขภาพของลูกค้าในปัจจุบัน ประวัติสุขภาพ ในกรณีเหล่านี้ท่านจำเป็นต้องได้รับความยินยอมอย่างชัดแจ้งจากลูกค้าก่อนหรือขณะเก็บรวบรวมข้อมูล

ตัวอย่าง 2 ในกรณีที่ท่านต้องทำการเก็บข้อมูลจากบัตรประจำตัวประชาชน ซึ่งมีข้อมูลอ่อนไหวคือ ศาสนา และ/หรือ กรุ๊ปเลือด เพื่อวัตถุประสงค์ในการเข้ารับบริการวางแผนการเงินกับท่าน และเพื่อการบริหารจัดการบัญชี ซึ่งเกิดขึ้นบ่อยครั้งในรูปแบบของ การขอถ่ายสำเนาบัตรประจำตัวประชาชนจากลูกค้า และเก็บสำเนาของข้อมูลลูกค้าไว้

หากท่านจะทำการเก็บรวบรวมข้อมูลศาสนา ท่านจะต้องได้รับความยินยอมอย่างชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลก่อน หรือหากท่านไม่ประสงค์จะขอความยินยอมจากลูกค้า ก็จะต้องมีกระบวนการในการจัดเก็บข้อมูลบัตรประจำตัวประชาชน โดยไม่มีการเก็บข้อมูลศาสนา และ/หรือ กรุ๊ปเลือด เช่นการขีดทึบข้อมูลดังกล่าวในสำเนาบัตรประจำตัวประชาชน

ตัวอย่าง 3 กรณีที่ท่านเก็บรวบรวมข้อมูลอ่อนไหว อันได้แก่ลายนิ้วมือของพนักงาน เพื่อใช้ในการเช็คเวลาเข้างานหรือเลิกงาน หรือ ใช้การสแกนลายนิ้วมือเพื่อเข้าตึกสำนักงานของท่าน ท่านจะต้องทำการขอความยินยอมอย่างชัดแจ้งในการเก็บข้อมูลลายนิ้วมือ เมื่อพนักงานเข้าทำงานกับท่าน สำหรับข้อมูลลายนิ้วมือที่มีการเก็บอยู่ก่อนแล้วให้ท่านทำการขอความยินยอมใหม่

ตัวอย่าง 4 กรณีลูกจ้างลาป่วยติดต่อกันเกิน 3 วัน ลูกจ้างจะต้องแสดงใบรับรองแพทย์ตามกฎหมายคุ้มครองแรงงาน ในกรณีนี้นายจ้าง (ท่าน) สามารถทำการเก็บรวบรวมข้อมูลอ่อนไหวได้ ในที่นี้คือข้อมูลสุขภาพที่ระบุอยู่ในใบรับรองแพทย์โดยไม่ต้องขอความยินยอม เนื่องจากเป็นกรณียกเว้นไม่ต้อง

ขอความยินยอมในการประมวลผลข้อมูลอ่อนไหว หากการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการคุ้มครองแรงงาน

5.5 การประกาศความเป็นส่วนตัว (Privacy Notice)

ประกาศความเป็นส่วนตัวเป็นข้อความหรือรายละเอียด ที่ท่านจะต้องแสดงกับเจ้าของข้อมูลส่วนบุคคล เพื่ออธิบายเกี่ยวกับรายละเอียดในการประมวลผลข้อมูล ประกาศความเป็นส่วนตัวจะช่วยเพิ่มความโปร่งใสในการประมวลผลข้อมูลส่วนบุคคลของท่านเอง ตามหลักการการประมวลผลข้อมูลส่วนบุคคลโดยชอบด้วยกฎหมาย เป็นธรรมและโปร่งใส ซึ่งเป็นหลักการที่สำคัญสำหรับเรื่องนี้ ซึ่งจะช่วยให้เจ้าของข้อมูลส่วนบุคคลมั่นใจได้ว่า ท่านปฏิบัติอย่างไรกับข้อมูลของเจ้าของข้อมูลส่วนบุคคล อีกทั้งเพื่อให้ความเชื่อมั่นแก่เจ้าของข้อมูลส่วนบุคคล ว่าข้อมูลที่เจ้าของข้อมูลส่วนบุคคล ได้ให้ไว้กับท่านหรือที่ท่านได้มาจากแหล่งอื่นนั้น จะไม่ถูกนำไปประมวลผลนอกเหนือจากรายละเอียดตามที่ระบุไว้ในประกาศความเป็นส่วนตัว ดังนั้น ท่านจึงต้องอธิบายในรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลทั้งหมด ในภาษาที่เข้าใจได้ง่าย เพื่อเป็นการแจ้งให้กับเจ้าของข้อมูลส่วนบุคคลทราบว่าท่านกำลังเก็บรวบรวมข้อมูลส่วนบุคคลอะไรบ้าง เพื่อบรรลุวัตถุประสงค์อะไร และมีการเปิดเผยข้อมูลส่วนบุคคลให้แก่ประเภทของบุคคลหรือหน่วยงานใดบ้าง และจะทำการเก็บข้อมูลไว้เป็นระยะเวลาเท่าใด รวมถึงสิทธิของเจ้าของข้อมูลส่วนบุคคล เป็นต้น นอกจากนั้นท่านจะต้องทำการแจ้งประกาศความเป็นส่วนตัวแก่ลูกค้า ด้วยวิธีการหรือช่องทางที่ลูกค้าสามารถเข้าถึงได้ง่าย ซึ่งอาจทำในรูปแบบเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ก็ได้

ในการเก็บรวบรวมข้อมูลส่วนบุคคล ท่านจะต้องแจ้งเจ้าของข้อมูลส่วนบุคคลก่อน หรือขณะเก็บรวบรวม เกี่ยวกับรายละเอียดในการประมวลผลข้อมูลส่วนบุคคลไว้ในประกาศความเป็นส่วนตัว ซึ่งจะต้องแสดงรายละเอียดของประกาศความเป็นส่วนตัวในหัวข้อดังต่อไปนี้

1) ข้อมูลของผู้ควบคุมข้อมูลส่วนบุคคล และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) ให้ท่านแจ้งรายละเอียดการติดต่อท่านและรายละเอียดการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (หากมี) ให้ชัดเจนเพื่อให้เจ้าของข้อมูลส่วนบุคคลติดต่อได้ เช่น ชื่อบริษัท สถานที่ติดต่อ ช่องทางการติดต่อ เช่น หมายเลขโทรศัพท์ อีเมล
2) ข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวม ให้ท่านแสดงรายการข้อมูลส่วนบุคคลที่ต้องการเก็บรวบรวม ใช้ และเปิดเผยเพื่อแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล ให้เจ้าของข้อมูลส่วนบุคคลทราบ
3) ข้อความแสดงวัตถุประสงค์ เป็นการบอกวัตถุประสงค์ของการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคล ซึ่งในประกาศความเป็นส่วนตัวจะต้องมีการระบุวัตถุประสงค์ใน

การเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลข้อมูลส่วนบุคคลไว้อย่างชัดเจน และครอบคลุมทุกวัตถุประสงค์ของกิจกรรมการประมวลผล โดยไม่ควรกล่าวอย่างกว้างเกินไป หรือกล่าวอย่างคลุมเครือ เพื่อให้เจ้าของข้อมูลส่วนบุคคลเข้าใจว่าข้อมูลส่วนบุคคลจะถูกนำไปประมวลผลอย่างไร

4) ฐานการประมวลผลข้อมูลส่วนบุคคล ท่านต้องระบุฐานในการประมวลผลข้อมูลโดยพิจารณาฐานที่ใช้ในการประมวลผลตามหัวข้อ “แนวปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคล” โดยท่านจะต้องระบุฐานในการประมวลผลให้ได้ฐานใดฐานหนึ่ง และท่านจะต้องแจ้งให้ทราบถึงความจำเป็นที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญา หรือมีความจำเป็นที่ต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา และแจ้งผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล โดยระบุรายละเอียดไว้ในฐานการประมวลผลตามกฎหมาย
5) คำอธิบายการประมวลผลข้อมูลส่วนบุคคล ท่านทำการแจ้งรายละเอียดในการประมวลผลข้อมูลส่วนบุคคล อันได้แก่ การเก็บรวบรวมข้อมูลส่วนบุคคล การใช้ข้อมูล และประเภทของบุคคลหรือหน่วยงานที่ข้อมูลส่วนบุคคลอาจถูกทำการเปิดเผย โดยให้ระบุอย่างชัดเจน ซึ่งอาจระบุรวมไว้กับวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกค้าและเหตุผลในการประมวลผลข้อมูลตามวัตถุประสงค์
6) ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล ท่านต้องทำการระบุระยะเวลาในการเก็บรักษาข้อมูลไว้อย่างชัดเจน ตามเกณฑ์ที่ท่านใช้ในการพิจารณาระยะเวลาในการเก็บข้อมูลส่วนบุคคล เช่น ภาระผูกพันตามกฎหมายที่ต้องเก็บตามระยะเวลาที่กำหนด อาทิ กฎหมายว่าด้วยภาษีอากร กฎหมายว่าด้วยการบัญชี ซึ่งท่านอาจระบุวิธีการทำลายข้อมูลส่วนบุคคลหรือการทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวตนได้เมื่อสิ้นสุดระยะเวลาในการเก็บข้อมูล
7) สิทธิของเจ้าของข้อมูลส่วนบุคคล ท่านต้องอธิบายสิทธิของเจ้าของข้อมูลส่วนบุคคลทั้งหมดอย่างชัดเจน และรายละเอียดการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือบุคคลที่ทำหน้าที่รับผิดชอบต่อการจัดการข้อมูลส่วนบุคคลเพื่อให้เจ้าของข้อมูลส่วนบุคคลทำการร้องขอได้ ท่านสามารถดูรายละเอียดเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ในหัวข้อ “แนวปฏิบัติเกี่ยวกับการดำเนินการตามสิทธิของเจ้าของข้อมูลส่วนบุคคล”

5.5.1 ตัวอย่างประกาศความเป็นส่วนตัว (Privacy Notice)

<u>ประกาศความเป็นส่วนตัว (Privacy Notice)</u>

(เลือกระบุ (1) นักวางแผนการเงินไทย CFP / ระบุชื่อบริษัทของนักวางแผนการเงิน CFP (“นักวางแผนการเงิน CFP”) หรือ (2) ที่ปรึกษาการเงิน AFPT / ระบุชื่อบริษัทของที่

ปรึกษาการเงิน AFPT (“ที่ปรึกษาการเงิน AFPT”)) มุ่งเน้นที่จะให้บริการที่ดีที่สุดให้แก่ลูกค้าคนสำคัญ ซึ่งการได้รับความไว้วางใจและความเชื่อมั่นจากเจ้าของข้อมูลส่วนบุคคลในฐานะลูกค้าของ (เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) (“ลูกค้า”) เป็นสิ่งที่สำคัญอย่างยิ่ง (เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) มีความตระหนักถึงความสำคัญในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าจึงมีระบบในการรักษาความปลอดภัยของข้อมูล และขั้นตอนการดำเนินงานที่รัดกุม อีกทั้งมาตรการในการรักษาความปลอดภัยของข้อมูล เพื่อป้องกันการเข้าถึง เปิดเผย นำไปใช้หรือเปลี่ยนแปลงข้อมูลโดยมิได้รับอนุญาต ดังนั้น(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)จึงจัดทำประกาศฉบับนี้ขึ้นเพื่อชี้แจง รายละเอียดเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ระยะเวลาในการเก็บข้อมูล การทำลายข้อมูล อีกทั้งสิทธิของเจ้าของข้อมูลส่วนบุคคล ซึ่งลูกค้าสามารถศึกษารายละเอียดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลได้ดังต่อไปนี้

1. **ข้อมูลที่(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) ทำการเก็บรวบรวม ใช้ หรือเปิดเผย** ได้แก่
   - 1.1 ข้อมูลส่วนบุคคลทั่วไปที่เป็นข้อมูลแสดงตัวตนของลูกค้า (Identity Data) ซึ่งหมายถึงข้อมูลที่เกี่ยวกับบุคคลธรรมดาที่ทำให้สามารถระบุตัวตนลูกค้ารายนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ/นามสกุล เลขประจำตัวประชาชน เลขหนังสือเดินทาง วัน/เดือน/ปีเกิด รวมถึงข้อมูลอ่อนไหว เช่น ข้อมูลชีวภาพ (ลายนิ้วมือ ข้อมูลใบหน้า) ข้อมูลสุขภาพ เป็นต้น
   - 1.2 ข้อมูลติดต่อของลูกค้า (Contact Data) เช่น ที่อยู่ อีเมล หมายเลขโทรศัพท์
   - 1.3 ข้อมูลทางการเงินหรือข้อมูลการทำธุรกรรมของลูกค้ากับ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) (Financial and Transaction Data) เช่น ข้อมูลรายได้ รายจ่าย สินทรัพย์ หนี้สิน กรมธรรม์ เครดิตบูโร ข้อมูลจากฐานข้อมูล หมายเลขบัญชีเงินฝาก/เงินลงทุน เป็นต้น
   - 1.4 ข้อมูลความชื่นชอบของลูกค้าในการค้นหาข้อมูลจากอินเทอร์เน็ต (Technical and Usage Data) เช่น การค้นหาข้อมูลผลิตภัณฑ์ของลูกค้า (Website Browsing) จากการใช้ Cookies หรือการเชื่อมต่อเว็บไซต์อื่นๆ ที่ลูกค้าเข้าไปค้นหาข้อมูล เป็นต้น
   - 1.5 ข้อมูลการติดต่อกับ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) (Communication Data) เช่น เทปบันทึกในกรณีที่ลูกค้า เข้ามาติดต่อผ่านทาง Contact Center ซึ่งอาจเป็นภาพหรือเสียง เป็นต้น และไม่ว่าลูกค้าได้ให้ข้อมูลไว้หรือมีอยู่กับ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่

ปรึกษาการเงิน AFPT) หรือ ที่(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)ได้รับ หรือ เข้าถึงได้จากแหล่งอื่นที่น่าเชื่อถือ เช่น หน่วยงานราชการ บริษัทพันธมิตรของ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) หรือที่ปรึกษาของ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)

2. วัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกค้า

(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)ทำการเก็บรวบรวมข้อมูล เพื่อประโยชน์ของลูกค้าในการทำธุรกรรมและ/หรือใช้บริการกับ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) เพื่อปฏิบัติตามกฎหมายและกฎระเบียบที่เกี่ยวข้อง และ/หรือเพื่อประโยชน์อื่นใดที่ลูกค้าได้ให้ความยินยอมไว้แก่(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) โดย(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)จะเก็บรักษาข้อมูลของลูกค้าตามมาตรการรักษาความปลอดภัย โดยลูกค้าสามารถศึกษารายละเอียดได้ดังต่อไปนี้

1.1 การปฏิบัติตามสัญญาระหว่างลูกค้ากับ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) เช่น การใช้ผลิตภัณฑ์หรือบริการต่างๆ ของลูกค้า การรับ-ส่งเอกสารติดต่อระหว่างลูกค้ากับ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)

2.2 การปฏิบัติตามกฎหมาย เช่น การป้องกันและตรวจจับความผิดปกติของธุรกรรมที่นำไปสู่กิจกรรมที่ผิดกฎหมาย การรายงานข้อมูลของลูกค้าต่อกรมสรรพากร การรายงานข้อมูลส่วนบุคคลต่อหน่วยงานราชการ เช่น กรมสรรพากร หรือ เมื่อได้รับหมายเรียก หมายอายัดจากหน่วยงานราชการ หรือ ศาล เป็นต้น

2.3 ประโยชน์อันชอบด้วยกฎหมายของ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) เช่น

- การบันทึกภาพผู้ที่มาติดต่อทำธุรกรรมกับสำนักงานของ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)ลงบน CCTV รวมถึง การแลกบัตรก่อนเข้าอาคาร เพื่อการรักษาความปลอดภัยภายในบริเวณอาคารของ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)
- การบริหารความเสี่ยง/การกำกับตรวจสอบ/การบริหารจัดการภายในองค์กร

- การตรวจสอบการรับส่งอีเมลหรือการใช้อินเทอร์เน็ตของพนักงานกับลูกค้าเพื่อป้องกันการเปิดเผยข้อมูลลับของ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)ต่อบุคคลภายนอก
- การวิเคราะห์ข้อมูลเพื่อใช้ในการนำเสนอผลิตภัณฑ์/บริการในประเภทเดียวกันกับที่ลูกค้ามีอยู่กับ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) ให้แก่ลูกค้า อย่างเหมาะสมกับความต้องการของลูกค้าและ/หรือในการทำวิจัยทางการตลาด เพื่อพัฒนาการให้บริการของ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)
- การรักษาความสัมพันธ์กับลูกค้า เช่น การจัดการข้อร้องเรียน การเสนอสิทธิประโยชน์พิเศษโดยไม่มีวัตถุประสงค์ทางการตลาดให้แก่ลูกค้า เป็นต้น

ทั้งนี้ หากลูกค้าไม่ให้ข้อมูลส่วนบุคคลกับ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)อาจส่งผลกระทบต่อลูกค้าในการไม่ได้รับการให้ บริการไม่ได้รับความสะดวก หรือไม่ได้รับการปฏิบัติตามสัญญาและลูกค้าอาจได้รับความเสียหาย/เสียโอกาสและอาจส่งผลกระทบต่อการปฏิบัติตามกฎหมายใดๆ ที่ลูกค้าหรือ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)ต้องปฏิบัติตาม และอาจมีบทกำหนดโทษที่เกี่ยวข้อง

2. การเปิดเผยข้อมูลส่วนบุคคล

(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)จะทำการเปิดเผยข้อมูลให้แก่บุคคลภายนอกในกรณีดังต่อไปนี้

- เป็นการเปิดเผยข้อมูลส่วนบุคคลให้แก่ (โปรดระบุข้อมูลเพิ่มเติม)
- เปิดเผยข้อมูลให้แก่บุคคลภายนอกตามที่(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)ได้รับความยินยอมจากลูกค้า
- เปิดเผยข้อมูลเพื่อการทำธุรกรรม และ/หรือ การใช้บริการตามความประสงค์ของลูกค้า
- เปิดเผยแก่ผู้บริการภายนอก (Outsource/Service Provider) ที่นักวางแผนทางการเงินเป็นคู่สัญญา ทั้งในประเทศไทยและต่างประเทศ เช่น (โปรดระบุข้อมูลเพิ่มเติม)
- เปิดเผยให้แก่หน่วยงานราชการหรือหน่วยงานกำกับดูแล เพื่อปฏิบัติตามกฎหมายหรือเป็นไปตามคำสั่งของหน่วยงานรัฐ เช่น (โปรดระบุข้อมูลเพิ่มเติม)

3. ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

ในกรณีที่ลูกค้ายุติความสัมพันธ์ทางธุรกิจกับ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)ไปแล้ว (เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)จะจัดเก็บข้อมูลส่วนบุคคลของลูกค้าตามที่กฎหมายกำหนดและตามนโยบายแนวปฏิบัติต่างๆ ในเรื่องการจัดเก็บ ทำลายเอกสารต่างๆ ของ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) และเมื่อสิ้นสุดระยะเวลาในการเก็บแล้ว(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)จะทำลายข้อมูลส่วนบุคคลดังกล่าว

4. สิทธิของลูกค้าเกี่ยวกับข้อมูลส่วนบุคคล

นักวางแผนทางการเงินคำนึงถึงสิทธิส่วนบุคคลของลูกค้า ซึ่งสิทธิของลูกค้าในข้อนี้เป็นสิทธิตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ลูกค้าควรทราบ ได้แก่

4.1 สิทธิในการถอนความยินยอม (“Right to Withdraw of Consent”)
ลูกค้ามีสิทธิขอเพิกถอนความยินยอมที่จะให้ไว้กับ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกค้าเมื่อใดก็ได้ เว้นแต่การเพิกถอนความยินยอมจะมีข้อจำกัดโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่ลูกค้า

4.2 สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (“Right to Access”)
ลูกค้ามีสิทธิขอทราบและขอรับสำเนาข้อมูลส่วนบุคคลของลูกค้าซึ่งอยู่ในความรับผิดชอบของ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) หรือ ขอให้(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) เปิดเผยการได้มาซึ่งข้อมูลที่ลูกค้าไม่ได้ให้ความยินยอมได้

4.3 สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (“Right to Rectification”)
ลูกค้ามีสิทธิขอให้(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)ดำเนินการแก้ไขเพื่อให้ข้อมูลถูกต้อง เป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิด

4.4 สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล (“Right to Data Portability”)
ลูกค้ามีสิทธิขอรับข้อมูลที่เกี่ยวกับลูกค้าจาก(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) ในกรณีที่(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) ได้ทำให้ข้อมูลนั้นอยู่ในรูปแบบที่สามารถอ่าน หรือ ใช้งานโดยทั่วไปได้ด้วยเครื่องมือ หรือ อุปกรณ์ที่ทำงานได้

โดยอัตโนมัติและสามารถใช้หรือเปิดเผยได้ด้วยวิธีการอัตโนมัติ รวมทั้ง (ก) มีสิทธิขอให้(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)ส่งหรือโอนข้อมูลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นเมื่อสามารถทำได้ด้วยวิธีการอัตโนมัติ หรือ (ข) ขอรับข้อมูลที่(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)ส่งหรือโอนข้อมูลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยตรง เว้นแต่สภาพทางเทคนิคไม่สามารถทำได้

4.5 สิทธิในการลบข้อมูลส่วนบุคคล (“Right to Deletion”)

ลูกค้ามีสิทธิขอให้(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)ลบ หรือ ทำลาย หรือ ทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลว่าเป็นลูกค้าได้ ในกรณีดังนี้

- ข้อมูลส่วนบุคคลดังกล่าวไม่มีความจำเป็นสำหรับวัตถุประสงค์ในการเก็บรวบรวมหรือประมวลผลข้อมูลส่วนบุคคลอีกต่อไป
- เจ้าของข้อมูลส่วนบุคคล ทำการถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคลและ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)ไม่มีอำนาจตามกฎหมายที่จะทำการประมวลผลได้
- เจ้าของข้อมูลส่วนบุคคล คัดค้านการประมวลผลเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง
- เป็นการประมวลผลข้อมูลส่วนบุคคลอันมิชอบด้วยกฎหมาย
- เจ้าของข้อมูลส่วนบุคคล คัดค้านการประมวลผลข้อมูล (นอกเหนือจากที่เกี่ยวข้องกับการคัดค้านการประมวลผลเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง) และ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)ไม่มีเหตุแห่งการอ้างการประมวลผลโดยประโยชน์อันชอบธรรม

4.6 สิทธิในการห้ามมิให้ประมวลผลข้อมูลส่วนบุคคล (“Right to Restriction of Processing”)

ลูกค้ามีสิทธิในการห้ามมิให้ประมวลผลข้อมูลส่วนบุคคลของตน เมื่อเข้าเงื่อนไขดังต่อไปนี้

- การประมวลผลไม่จำเป็นอีกต่อไป แต่การเก็บรักษาข้อมูลส่วนบุคคลยังคงมีความจำเป็นเพื่อการใช้สิทธิเรียกร้องทางกฎหมาย

- เป็นการประมวลผลข้อมูลส่วนบุคคลอันมิชอบด้วยกฎหมาย แต่เจ้าของข้อมูลส่วนบุคคลนั้นต้องการห้ามมิให้มีการประมวลผลโดยแทนการลบหรือทำลายข้อมูลส่วนบุคคลของตน
- เมื่ออยู่ในระหว่างการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลตามที่ลูกค้าร้องขอ
- เมื่อ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)อยู่ในระหว่างการพิสูจน์ให้เห็นถึงเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า

4.7 สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล (“Right to Object”)

ลูกค้ามีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลที่เกี่ยวกับลูกค้า ในกรณีดังนี้

- กรณีที่เป็นการเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง
- กรณีที่เป็นการเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ เว้นแต่การจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะของ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)
- กรณีที่เป็นข้อมูลที่เก็บรวบรวมได้ด้วยเหตุจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะของ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) หรือ เหตุจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) เว้นแต่(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)แสดงให้เห็นถึงเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า หรือเป็นไปเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตาม หรือ การใช้สิทธิเรียกร้องตามกฎหมาย หรือ การยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

4.8 สิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ เมื่อพบว่านักวางแผนทางการเงิน ลูกจ้างหรือ ผู้รับจ้างของนักวางแผนทางการเงิน กระทำการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย (Right to Lodge a Complaint)

5. การทบทวนและปรับปรุงแก้ไขประกาศ

(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)สงวนสิทธิ์ในการแก้ไขเปลี่ยนแปลงประกาศความเป็นส่วนตัว โดยไม่ต้องแจ้งให้ทราบล่วงหน้า ทั้งนี้ (เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)จะทำการเปิดเผยไว้บนเว็บไซต์ของ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) หรือช่องทางอื่นใดของ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)

6. ข้อมูลการติดต่อ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)

หากลูกค้าต้องการติดต่อหรือมีข้อสงสัยหรือต้องการสอบถามรายละเอียดเพิ่มเติมเกี่ยวกับเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล การใช้สิทธิของลูกค้า หรือมีข้อร้องเรียนใดๆ ลูกค้าสามารถติดต่อ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) ได้ดังช่องทางต่อไปนี้

- ศูนย์บริการลูกค้า (Contact Center) โทร 1234
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)
  (นาย ข. email: dpo@abc.com)
- เว็บไซต์ www.abc.com
- สถานที่ติดต่อ (ระบุที่อยู่ในการติดต่อ)

6. การใช้และเปิดเผยข้อมูลส่วนบุคคล (Data Usage and Data Disclosure)

หลังจากที่ท่านทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลแล้ว ท่านอาจมีความจำเป็นที่ต้องใช้หรือเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลอื่นที่เกี่ยวข้อง ซึ่งการเปิดเผยข้อมูล ท่านสามารถทำได้เพื่อบรรลุวัตถุประสงค์ในการประมวลผลข้อมูล หรือการเปิดเผยมีความเกี่ยวข้องโดยตรงกับวัตถุประสงค์ดังกล่าว หรือเป็นการเปิดเผยเพื่อปฏิบัติตามกฎหมายหรือเป็นไปตามคำสั่งของหน่วยงานใด ซึ่งโดยหลักการแล้วหากต้องมีการเปิดเผยข้อมูลส่วนบุคคล ท่านต้องมีการแจ้งกับเจ้าของข้อมูลส่วนบุคคลไว้ในประกาศความเป็นส่วนตัว (Privacy Notice) ซึ่งจะต้องแจ้งก่อนหรือขณะเก็บรวบรวมข้อมูลจากเจ้าของข้อมูลส่วนบุคคล ถึงความจำเป็นในการใช้หรือเปิดเผยข้อมูลเพื่อวัตถุประสงค์ใด อีกทั้งต้องระบุประเภทของบุคคลหรือหน่วยงานที่ข้อมูลส่วนบุคคลอาจถูกทำการเปิดเผยอย่างชัดเจน

ตัวอย่าง แนวปฏิบัติในการใช้หรือเปิดเผยข้อมูลไปยังบุคคลหรือหน่วยงานต่าง ๆ

ตัวอย่างแนวปฏิบัติในการเปิดเผยข้อมูลเพื่อการทำธุรกรรม และ/หรือ การใช้บริการตามความประสงค์ของลูกค้า

ตัวอย่าง ท่านทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกค้า เพื่อวัตถุประสงค์ในการบริการวางแผนทางการเงินให้กับลูกค้า ท่านมีความจำเป็นที่จะต้องเก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าวเพื่อใช้ประกอบการวิเคราะห์ และวางแผนทางการเงินให้แก่ลูกค้า

ตัวอย่างแนวปฏิบัติในการเปิดเผยข้อมูลให้แก่หน่วยงานราชการหรือหน่วยงานกำกับดูแล เพื่อปฏิบัติตามกฎหมายหรือเป็นไปตามคำสั่งของหน่วยงานรัฐ

ตัวอย่าง เพื่อปฏิบัติตามกฎหมายหรือเป็นไปตามคำสั่งของหน่วยงานรัฐ ท่านสามารถเปิดเผยข้อมูลให้แก่หน่วยงานราชการหรือหน่วยงานกำกับดูแลได้ เช่น กรมสรรพากร สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ศาล รวมทั้งผู้สอบบัญชี บริษัทข้อมูลเครดิต เป็นต้น

6.1 การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ (Cross-border data transfer)

ท่านอาจมีความจำเป็นจะต้องส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ หรือองค์การระหว่างประเทศ ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล กำหนดให้ประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ และเป็นไปตามประกาศกำหนดหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ อย่างไรก็ตามปัจจุบันคณะกรรมการ

คุ้มครองข้อมูลส่วนบุคคลยังมิได้มีการกำหนดรายละเอียดหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศไว้

ในกรณีที่จำเป็นต้องมีการโอนหรือส่งข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศท่านสามารถทำได้ในกรณีดังต่อไปนี้

6.1.1 ประเทศหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

แนวทางการพิจารณาความเพียงพอของมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศที่รับโอนข้อมูลส่วนบุคคล (Adequacy of the Level of Protection) สามารถพิจารณาได้โดย

1) พิจารณาจากกฎหมายของประเทศดังกล่าว ว่ามีการคุ้มครองสิทธิมนุษยชนและสิทธิขั้นพื้นฐาน จากกฎหมายที่เกี่ยวข้องทั้งในภาพรวมหรือกฎหมายเฉพาะ รวมถึงการรักษาความมั่นคงของชาติ กฎหมายอาญา การเข้าถึงข้อมูลส่วนบุคคลของหน่วยงานรัฐ การบังคับใช้กฎหมาย กฎเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคล กฎเกณฑ์ของผู้ประกอบวิชาชีพ มาตรการในการรักษาความปลอดภัยของข้อมูล กฎเกณฑ์ในการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ ความมีประสิทธิภาพในการบังคับใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล มาตรการเยียวยาแก่เจ้าของข้อมูลส่วนบุคคลหากข้อมูลส่วนบุคคลที่ถูกโอนนั้นถูกละเมิด
2) การมีอยู่และการทำงานขององค์กร/หน่วยงานอิสระในต่างประเทศหรือหน่วยงานระหว่างประเทศที่รับโอนข้อมูลส่วนบุคคล ว่ามีอำนาจหน้าที่ในการบังคับใช้กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล และอำนาจหน้าที่ในการให้ความช่วยเหลือเจ้าของข้อมูลส่วนบุคคล ในการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลและอำนาจหน้าที่ในการร่วมมือกับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของราชอาณาจักรไทย
3) ข้อผูกพันระดับนานาชาติของประเทศหรือองค์การระหว่างประเทศที่รับโอนข้อมูลส่วนบุคคล เกิดจากการที่ประเทศหรือองค์กรระหว่างประเทศผู้รับโอนได้เข้าผูกพันทางกฎหมาย โดยเฉพาะที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล เช่น อนุสัญญาที่มีผลบังคับผูกพันทางกฎหมาย หรือ การเข้าร่วมในระบบพหุภาคีหรือภูมิภาค

ตัวอย่างการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

ท่านซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลในประเทศไทยเก็บรวบรวมข้อมูลส่วนบุคคลของพนักงานและมีความประสงค์ที่จะส่งข้อมูลดังกล่าวไปยังบริษัทแม่ที่ตั้งอยู่ที่ประเทศสหรัฐอเมริกา การส่งข้อมูลส่วนบุคคลดังกล่าวจะเริ่มต้นจากการที่ข้อมูลถูกแปลงให้กลายเป็นหน่วยย่อย และถูกส่งจากเครื่องคอมพิวเตอร์ของผู้ส่งโดยผ่านเครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่ทำหน้าที่ให้บริการรับหรือส่ง และจัดเก็บอีเมลของบุคคลหรือองค์กร (mail server) ไปยังเครื่องคอมพิวเตอร์ของผู้รับ ถือเป็นการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ เนื่องจากผู้รับข้อมูลซึ่งตั้งอยู่ต่างประเทศนั้นสามารถเข้าถึงข้อมูลส่วนบุคคลที่ส่งผ่านอีเมลและเครือข่ายอินเทอร์เน็ตได้ ทั้งนี้ แม้ว่าจะเป็นการส่งและรับข้อมูลของบริษัทในเครือธุรกิจเดียวก็ตาม

6.1.2 กรณีที่ได้รับการยกเว้นตามกฎหมาย

ท่านสามารถโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศได้ แม้ว่ามาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทางไม่เพียงพอหากเข้ากรณียกเว้นตามกฎหมายดังต่อไปนี้

1) เป็นการปฏิบัติตามกฎหมาย
2) ได้รับการยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยท่านได้แจ้งให้เจ้าของข้อมูลส่วนบุคคล ทราบถึงมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือ องค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว
3) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น
4) เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่นเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
5) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้
6) เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

6.1.3 กรณีที่มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (Transfers Subject to Appropriate Safeguards)

กรณีที่คณะกรรมการมาตรการคุ้มครองข้อมูลส่วนบุคคลยังไม่มีประกาศหลักเกณฑ์ในการให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ หรือยังไม่มีนโยบายในการคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ ท่านสามารถใช้มาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมอื่น ๆ ที่สามารถบังคับสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ ได้แก่

- ข้อสัญญาที่เกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล (Standard Data Protection Clauses) ที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอนุมัติ
- หลักปฏิบัติด้านจรรยาบรรณ (Code of Conduct) ที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอนุมัติ หลักปฏิบัติด้านจรรยาบรรณ ดังกล่าวต้องมีผลผูกพันและบังคับใช้กับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในต่างประเทศหรือองค์การระหว่างประเทศ ในการจัดให้มีมาตรการคุ้มครองข้อมูลอย่างเหมาะสม รวมถึงการบังคับใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
- คำรับรองเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Certification Mechanism) ที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอนุมัติ ซึ่งคำรับรองดังกล่าวต้องมีผลผูกพันและบังคับใช้กับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในต่างประเทศหรือองค์การระหว่างประเทศ ในการจัดให้มีมาตรการคุ้มครองข้อมูลอย่างเหมาะสม รวมถึงการบังคับใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
- ข้อสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (Contractual Clauses) ผู้ประมวลผลหรือผู้รับข้อมูลส่วนบุคคลในประเทศปลายทางที่ได้รับอนุมัติจาก คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอนุมัติ
- ข้อบัญญัติเพิ่มเติม ในข้อตกลงการบริหารงานระหว่างหน่วยงานสาธารณะ (Provision to be Inserted into Administrative Arrangements Between Public Authorities) ที่ได้รับอนุมัติจาก คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอนุมัติ ซึ่งมีผลบังคับใช้ การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

7. การเก็บข้อมูลส่วนบุคคลและระยะเวลาในการเก็บ (Data Retention)

ท่านสามารถทำการเก็บข้อมูลส่วนบุคคล ตามระยะเวลาในการเก็บรักษาเฉพาะเท่าที่จำเป็นตามที่ต้องบรรลุวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลหรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือเก็บตามข้อกำหนดของกฎหมายที่ท่านจำเป็นต้องปฏิบัติ เมื่อสิ้นสุดระยะเวลาในการเก็บรักษาแล้วให้ท่านดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล ทั้งนี้ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวมข้อมูลนั้น ๆ

7.1 แนวปฏิบัติเกี่ยวกับระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

ท่านจะต้องเก็บรักษาข้อมูลส่วนบุคคล เท่าที่จำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลเพื่อเป็นการปฏิบัติตามหลักการในการคุ้มครองข้อมูลส่วนบุคคล และท่านจะต้องมีการระบุระยะเวลาในการเก็บรักษาตามเกณฑ์ที่ท่านใช้ในการพิจารณาระยะเวลาในการเก็บข้อมูลส่วนบุคคล เช่น ภาระผูกพันตามกฎหมายที่ต้องเก็บตามระยะเวลาที่กำหนด ไว้ในนโยบายความเป็นส่วนตัวหรือนโยบายคุ้มครองข้อมูลส่วนบุคคล และท่านจะต้องจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา

สำหรับการพิจารณาเพื่อกำหนดระยะเวลาในการเก็บรักษา ควรพิจารณาถึงความจำเป็นของระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อันชอบด้วยกฎหมายในการประมวลผลข้อมูล เนื่องจากความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลแต่ละกรณี อาจมีข้อกำหนดของระยะเวลาการเก็บรักษาที่แตกต่างกัน ท่านจึงต้องพิจารณาถึงความเหมาะสมของระยะเวลาการเก็บข้อมูลเป็นรายกรณีหรือรายวัตถุประสงค์ในการประมวลผลข้อมูล ซึ่งควรกำหนดไว้ในนโยบายการเก็บรักษา (Retention Policy) หรือแนวปฏิบัติต่าง ๆ อย่างชัดเจน รวมถึงควรระบุวิธีการจัดเก็บ และวิธีการทำลายเอกสารต่าง ๆ เนื่องจากการเก็บข้อมูลส่วนบุคคลเกินความจำเป็นนั้นจะเป็นผลลบต่อท่านเอง จะเป็นการเพิ่มความเสี่ยงในการรั่วไหลของข้อมูล อีกทั้งการเก็บข้อมูลจำนวนมากนั้นจะเป็นการเพิ่มค่าใช้จ่ายในการเก็บรักษาข้อมูล

เมื่อสิ้นสุดความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล หรือเจ้าของข้อมูลส่วนบุคคลดำเนินการร้องขอใช้สิทธิในการลบข้อมูลส่วนบุคคล หรือถอนความยินยอม ท่านจะต้องดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลนั้น เว้นแต่เป็นไปตามข้อยกเว้นตามกฎหมาย ที่กำหนดให้ท่านสามารถเก็บรักษาไว้เพื่อวัตถุประสงค์ดังต่อไปนี้ได้

- การใช้เสรีภาพในการแสดงความคิดเห็น

- การเก็บรักษาไว้เพื่อการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ หรือเกี่ยวกับการศึกษาวิจัยหรือสถิติเพื่อประโยชน์สาธารณะที่มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
- การจำเป็นเพื่อปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะ
- การจำเป็นเพื่อปฏิบัติตามกฎหมายให้บรรลุวัตถุประสงค์เกี่ยวกับเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ หรือประโยชน์สาธารณะด้านสาธารณสุข
- ใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย
- การใช้ข้อมูลเพื่อฟ้องร้องหรือต่อสู้คดี
- การปฏิบัติตามกฎหมายอื่น

ตัวอย่างระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลตามวัตถุประสงค์ทางกฎหมาย

ตัวอย่าง 1 ท่านจะต้องทำการเก็บรักษาเอกสาร หลักฐานการประกอบการลงบัญชี ตามกฎหมายว่าด้วยการบัญชี (พ.ร.บ.การบัญชี พ.ศ. 2543) ไว้เป็นเวลาไม่น้อยกว่า 5 ปี นับแต่วันที่ปิดบัญชี หรือการเก็บข้อมูลเพื่อการดำเนินคดี

ตัวอย่าง 2 ท่านจะต้องเก็บรักษาเอกสารเกี่ยวกับการแสดงตน และเอกสารเกี่ยวกับการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าเป็นเวลา 10 ปีนับแต่วันที่มีการปิดบัญชีหรือยุติความสัมพันธ์กับลูกค้าตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน เว้นแต่จะได้รับแจ้งเป็นหนังสือจากพนักงานเจ้าหน้าที่ให้ปฏิบัติเป็นอย่างอื่น

ตัวอย่าง 3 ท่านจะต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วันก็ได้แต่มิให้เกินกว่า 2 ปี หรือตามคำสั่งของพนักงานเจ้าหน้าที่ นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ ตามข้อกำหนดของ พ.ร.บ.ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

ตัวอย่าง 4 ท่านต้องเก็บและรักษารายงานเกี่ยวกับภาษีมูลค่าเพิ่ม ใบกำกับภาษี และสำเนาใบกำกับภาษี พร้อมทั้งเอกสารประกอบการรายงานหรือเอกสารอื่นที่อธิบดีกรมสรรพากรกำหนดไว้ ณ สถานประกอบการหรือสถานที่อื่นที่อธิบดีกรมสรรพากรกำหนดเป็นเวลาไม่น้อยกว่า 5 ปีนับแต่วันที่ได้ยื่นแบบแสดงรายการภาษีหรือวันทำรายงานแล้วแต่กรณี แต่ไม่เกิน 7 ปี ตามประมวลรัษฎากร

8. การลบหรือทำลายข้อมูลส่วนบุคคล (Data Deletion or Data Destruction)

เมื่อพ้นกำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล หรือไม่เกี่ยวข้องเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล ท่านจะต้องทำการลบหรือทำลายข้อมูลส่วนบุคคล ("การลบ" หมายถึง การทำให้ข้อมูลส่วนบุคคลนั้นถูกลบออกระบบและไม่อาจกู้คืนได้โดยตัวเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ทั้งนี้ ไม่ว่าในเวลาใด ๆ) หรือทำให้ข้อมูลส่วนบุคคลอยู่ในลักษณะที่ไม่สามารถระบุตัวบุคคลของเจ้าของข้อมูลส่วนบุคคลได้ ดังนั้น ท่านจึงต้องจัดให้มีระบบการตรวจสอบข้อมูลเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล เมื่อสิ้นสุดความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล หรือเจ้าของข้อมูลส่วนบุคคลดำเนินการร้องขอใช้สิทธิในการลบข้อมูลส่วนบุคคล หรือถอนความยินยอม เว้นแต่เป็นกรณีที่ได้รับยกเว้นตามกฎหมาย โปรดดูรายละเอียดเพิ่มเติมในหัวข้อ "แนวปฏิบัติเกี่ยวกับระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล"

ท่านจึงมีความจำเป็นที่จะต้องมีการบริหารจัดการข้อมูลส่วนบุคคล ซึ่งในการตัดสินใจเลือกใช้วิธีการในการประมวลผลข้อมูลส่วนบุคคลที่เหมาะสมนั้นจะต้องมีมาตรการเชิงเทคนิคหรือมาตรการเชิงบริหารจัดการ เพื่อเพิ่มมาตรฐานในการรักษาความปลอดภัยของข้อมูลส่วนบุคคล เช่น ดำเนินการออกแบบระบบให้รองรับการปฏิบัติงานของท่านให้เป็นไปได้อย่างราบรื่น ในขณะเดียวกันก็ต้องมีการคุ้มครองข้อมูลอย่างเหมาะสมและมีประสิทธิภาพ ระบบสามารถทำการตรวจสอบได้ว่าข้อมูลจะต้องถูกลบและทำลายภายใต้เงื่อนไขใด เช่น เมื่อสิ้นสุดระยะเวลาในการเก็บ ท่านอาจทำข้อมูลให้อยู่ในรูปของข้อมูลนิรนาม (Anonymization) ซึ่งเป็นวิธีการที่จะทำให้ข้อมูลไม่สามารถระบุตัวตนได้ขณะเดียวกันท่านจะต้องพิจารณาทั้งต้นทุนในการติดตั้งระบบที่ใช้ในการประมวลผลให้เพียงพอกับผลกระทบที่อาจเกิดขึ้นต่อเจ้าของข้อมูลส่วนบุคคล (Impact) และโอกาสที่อาจเกิดขึ้น (Likelihood) จากการถูกละเมิดข้อมูลส่วนบุคคล

อย่างไรก็ดีหากท่านมีการเก็บข้อมูลที่อยู่ในรูปของเอกสาร Hard file การลบหรือทำลายอาจต้องใช้เครื่องทำลายเอกสาร หรือจัดจ้างบริษัททำลายเอกสารเพื่อทำลาย โดยท่านต้องมั่นใจว่าบริษัทที่ถูกจัดจ้างมีมาตรการในการรักษาความปลอดภัยทุกขั้นตอนก่อนถูกทำลาย เพื่อป้องกันการเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคลแก่ผู้ที่ไม่ได้รับอนุญาต สำหรับเอกสารในรูปแบบ Soft file หรือการจัดเก็บข้อมูลในระบบของท่าน ในทางปฏิบัติอาจเป็นเรื่องยากที่จะทำการลบหรือทำลายข้อมูลให้หายไปและไม่สามารถกู้คืนได้อีก เอกสารฉบับนี้จึงจะเน้นถึงการทำข้อมูลส่วนบุคคลให้เป็นข้อมูลที่ไม่สามารถระบุตัวตนของเจ้าของข้อมูลส่วนบุคคลได้ ซึ่งการกระทำดังกล่าวเป็นวิธีการที่ทำให้ข้อมูลส่วนบุคคลไม่ใช่ข้อมูลส่วนบุคคลอีกต่อไป เป็นหนึ่งในการบริหารความเสี่ยงของท่าน มีเทคนิคหลากหลายวิธี ดังที่จะกล่าวรายละเอียดในหัวข้อถัดไป

8.1 แนวปฏิบัติเกี่ยวกับการทำข้อมูลนิรนาม (Data Anonymization)

โดยทั่วไปแล้วการจัดทำข้อมูลนิรนาม หมายถึง กระบวนการในการทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวบุคคลได้ คำศัพท์ที่ใช้ในแต่ละแหล่งอ้างอิงอาจแตกต่างกันไป ตัวอย่างเช่น บ้างใช้คำว่าการทำข้อมูลนิรนาม (Anonymization) และการขจัดตัวตน (De-Identification) สลับกัน บ้างก็ใช้คำว่า de-identification ว่าเป็นการอธิบายกระบวนการในการทำให้ข้อมูลไม่สามารถระบุตัวตนได้ และใช้คำว่า anonymization เพื่อแสดงถึงความจำเพาะของประเภทการ De-Identification ที่จะทำให้ไม่สามารถนำกลับมาระบุตัวบุคคลได้อีกครั้ง ไม่ว่าจะเป็นข้อมูลที่เป็นข้อมูลเดียวหรือข้อมูลที่ต้องนำไปรวมกับข้อมูลอื่นที่มีอยู่อีก

สำหรับวัตถุประสงค์หลักของแนวปฏิบัติฉบับนี้ คำว่า "Anonymization" หมายถึงกระบวนการแปลงข้อมูลส่วนบุคคลให้เป็นข้อมูลที่ไม่สามารถใช้เพื่อระบุตัวตนของบุคคลใดบุคคลหนึ่งได้ ทั้งนี้ข้อมูลที่ถูกทำการนิรนามทางกฎหมายจะไม่ถือเป็นข้อมูลส่วนบุคคลอีก ในกรณีที่ข้อมูลจะสามารถย้อนกลับมาเพื่อระบุตัวตนได้หรือย้อนกลับไม่ได้ การทำให้ข้อมูลกลับมาระบุตัวตนของบุคคลได้นั้นเป็นสิ่งที่องค์กรต้องพิจารณาในการจัดการกับความเสี่ยงของข้อมูลที่สามารถกลับมาระบุตัวตนได้

เหตุผลในการทำข้อมูลให้อยู่ในรูปของข้อมูลนิรนาม (Anonymized Data) เพื่อให้ข้อมูลมีความเหมาะสมสำหรับการใช้งานมากกว่าสถานะเดิมของข้อมูลที่ถูกคุ้มครองภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล ตัวอย่างเช่น ข้อมูลที่ไม่สามารถระบุตัวตนได้ อาจถูกใช้เพื่อการทำวิจัยและการวิเคราะห์ข้อมูลจำนวนมาก ซึ่งการกระทำดังกล่าวไม่มีความจำเป็นที่จะต้องใช้ข้อมูลเพื่อการระบุตัวตน ดังนั้นชุดข้อมูลของ Anonymized Data ถือเป็นมาตรการในการบริหารความเสี่ยง ลดผลกระทบที่อาจเกิดขึ้นจากการถูกละเมิดความปลอดภัยของข้อมูล

ตัวอย่าง มาตรการเชิงเทคนิคในการรักษาความและปลอดภัยของข้อมูล

i. การแฝงข้อมูล (Pseudonymisation) คือการแทนที่สิ่งที่ระบุตัวบุคคลของเจ้าของข้อมูลส่วนบุคคล ด้วยการอ้างอิงอื่น ๆ ตัวอย่างเช่น การแทนที่ชื่อบุคคล ด้วย รหัสหรือหมายเลขอ้างอิงที่สร้างขึ้นแบบสุ่ม ซึ่งข้อมูลทั้งสองชุดจะต้องถูกลดความสามารถในการเชื่อมโยงกัน ซึ่งเป็นหนึ่งในมาตรการในการรักษาความปลอดภัยของข้อมูล เพื่อลดความเสี่ยงและผลกระทบจากเหตุการณ์ถูกละเมิดข้อมูล
   การแฝงข้อมูลเป็นการประมวลผลข้อมูลส่วนบุคคลในลักษณะที่ข้อมูลส่วนบุคคลไม่สามารถระบุตัวเจ้าของข้อมูลได้หากปราศจากการใช้ข้อมูลเพิ่มเติมประกอบ ทั้งนี้ข้อมูลเพิ่มเติมนี้มีการเก็บรักษาไว้แยกออกจากกันและอยู่ภายใต้มาตรการเชิงเทคนิคและมาตรเชิงบริหารจัดการเพื่อประกันว่าข้อมูลส่วนบุคคลจะไม่สามารถระบุไปถึงบุคคลธรรมดาได้

ii. การรวมกลุ่มข้อมูล (Aggregation) แสดงค่าเป็นผลรวม ดังนั้นจึงไม่มีการแสดงค่าแต่ละค่าที่สามารถระบุตัวบุคคลได้ ตัวอย่างเช่นกำหนดชุดข้อมูลที่มีอายุแปดคน (เช่น 33, 35, 34, 37, 42, 45, 37, 40) แสดงผลรวมของอายุแต่ละบุคคลของจำนวนบุคคลทั้งหมดในกลุ่ม (เช่น 303) มากกว่าอายุของแต่ละบุคคลที่เป็นตัวแทนในชุดข้อมูลนี้

iii. การแทนที่ (Replacement) เป็นการแทนที่ค่าหรือเซตย่อยของค่าด้วยค่าเฉลี่ยที่คำนวณ ตัวอย่างเช่นแทนที่บุคคลด้วยอายุ 15, 18 และ 20 ด้วยค่าอายุ 17 เพื่อลดความแตกต่างของข้อมูล หากในกรณีที่อายุที่แท้จริงไม่ได้เป็นวัตถุประสงค์ในการใช้ข้อมูล

iv. การสกัดกั้นข้อมูล (Data Suppression) คือลบค่าที่ไม่จำเป็นสำหรับวัตถุประสงค์ในการใช้ข้อมูล ตัวอย่างเช่นการลบฟิลด์ "เชื้อชาติ" ออกจากชุดของข้อมูลส่วนบุคคล

v. การกล่าวอย่างกว้าง (Data recoding or generalization) คือการจัดกลุ่มหมวดหมู่เป็นหมวดหมู่ที่กว้างขึ้น การกล่าวเป็นช่วงของข้อมูล ตัวอย่างเช่นการจัดกลุ่มของระดับการศึกษาที่แน่นอน (เช่น ชั้นประถมศึกษา3 ชั้นมัธยมศึกษา2) ออกเป็นหมวดหมู่ที่กว้างขึ้น (เช่น ระดับ ประถมศึกษา มัธยมศึกษา ระดับปริญญาตรี) หรือซ่อนค่าภายในช่วงที่กำหนด (เช่นแทนที่อายุ 43 ' ด้วยช่วง '40 -50 ')

vi. การสับเปลี่ยนข้อมูล (Data Shuffling) คือการผสมหรือแทนที่ค่ากับชนิดเดียวกันเพื่อให้ข้อมูลมีลักษณะคล้ายกัน แต่ไม่เกี่ยวข้องกับรายละเอียดที่แท้จริง ตัวอย่างเช่น นามสกุลในฐานข้อมูลลูกค้าสามารถถูกทำให้ไม่สามารถระบุตัวตนได้ โดยการแทนที่ด้วยนามสกุลที่มาจากฐานข้อมูลอื่น

vii. การบังข้อมูล (Masking) คือลบรายละเอียดบางอย่างในขณะที่รักษารูปลักษณ์ของข้อมูล ตัวอย่างเช่นการแสดงข้อมูลตัวเลขพาสปอร์ตเป็น ‘#####567A’ แทนที่จะแสดง ‘S1234567A’ หรือการ บังข้อมูลหมายเลขโทรศัพท์เป็น ‘081xxxx678 แทนที่จะแสดง ‘0812345678’

อย่างไรก็ตาม กฎหมายมิได้กำหนดให้ใช้วิธีการใดวิธีการหนึ่งโดยเฉพาะหรือรับรองการใช้เทคนิคใด ๆ ท่านจึงควรประเมินสถานการณ์และลักษณะการดำเนินธุรกิจเองและนำเทคนิคการรักษาความมั่นคงและปลอดภัยที่เหมาะสมที่มาใช้กับการดำเนินธุรกิจ

9. แนวปฏิบัติเกี่ยวกับการดำเนินการตามสิทธิของเจ้าของข้อมูลส่วนบุคคล

หากท่านได้รับการติดต่อจากเจ้าของข้อมูลส่วนบุคคล ในการร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล ท่านอาจจัดให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือหน่วยงานรับเรื่องร้องเรียน หรือ Contact Center ของท่านทำหน้าที่ในการรับเรื่องร้องขอก็ได้

ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลกำหนดให้สิทธิของเจ้าของข้อมูลส่วนบุคคล มีดังต่อไปนี้

- สิทธิในการถอนความยินยอม (“Right to Withdraw of Consent”)
- สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (“Right to Access”)
- สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (“Right to Rectification”)
- สิทธิในการลบข้อมูลส่วนบุคคล (“Right to Deletion”)
- สิทธิในการห้ามมิให้ประมวลผลข้อมูลส่วนบุคคล (“Right to Restriction of Processing”)
- สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล (“Right to Object”)
- สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล (“Right to Data Portability”)
- สิทธิในการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ (“Right to Lodge a Complaint”)

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิตามกฎหมายในการร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามที่ร้องขอ ซึ่งในรายละเอียดของการดำเนินการตามสิทธิที่ร้องขอของเจ้าของข้อมูลส่วนบุคคลจะกล่าวถึงในรายละเอียดดังต่อไปนี้

9.1 สิทธิในการถอนความยินยอม (“Right to Withdraw of Consent”)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะขอเพิกถอนความยินยอมที่จะให้ไว้กับผู้ควบคุมข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลเมื่อใดก็ได้ และผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการหยุดการประมวลผลข้อมูลที่เจ้าของข้อมูลส่วนบุคคลเคยได้ให้ความยินยอมไว้ หากผู้ควบคุมข้อมูลส่วนบุคคลไม่มีฐานโดยชอบด้วยกฎหมายอื่น ที่จะทำการเก็บรวบรวม ใช้ หรือเปิดเผยต่อไป ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบข้อมูลออก

การใช้สิทธิถอนความยินยอม ผู้ควบคุมข้อมูลส่วนบุคคลควรดำเนินการโดยไม่ล่าช้านับแต่ที่ได้ทราบถึงการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล โดยระยะเวลาในการปฏิตามสิทธิให้เป็นไปตามนโยบายที่เหมาะสมของผู้ควบคุมข้อมูลส่วนบุคคล และผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีช่องทางที่เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิกระทำได้ง่ายในระดับเดียวกับการให้ความยินยอม

9.2 สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (“Right to Access”)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มา ซึ่งข้อมูลดังกล่าวที่เจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอม เพื่อเป็นการยืนยันจากผู้ควบคุมข้อมูลส่วนบุคคลว่า ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมไว้นั้นกำลังถูกประมวลผลหรือไม่อย่างไร เมื่อได้รับคำร้องขอแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการตามคำร้องขอ โดยไม่ชักช้าภายใน 30 วัน นับแต่วันที่ได้รับการร้องขอ และผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดเตรียมข้อมูลที่เกี่ยวข้อง ข้อมูลส่วนบุคคลและการประมวลผล กล่าวคือ

1) คำรับรองว่าท่านได้ประมวลผลข้อมูลส่วนบุคคลนั้น และเปิดเผยการได้มาซึ่งข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอม
2) สำเนาข้อมูลส่วนบุคคลดังกล่าวให้แก่เจ้าของข้อมูล และ
3) ข้อมูลประกอบที่เกี่ยวข้อง ดังต่อไปนี้
    - วัตถุประสงค์ในการประมวลผลข้อมูล
    - ประเภทของข้อมูลส่วนบุคคล
    - ผู้รับข้อมูลหรือประเภทของผู้รับข้อมูลส่วนบุคคลที่ได้รับหรือจะได้รับข้อมูลโดยเฉพาะอย่างยิ่ง ผู้รับข้อมูลที่อยู่ในประเทศที่สามหรือองค์การระหว่างประเทศ
    - ระยะเวลาที่จะจัดเก็บข้อมูลส่วนบุคคล หรือ เกณฑ์ในการกำหนดระยะเวลาจัดเก็บข้อมูล
    - สิทธิในการแก้ไขข้อมูล ลบข้อมูล ห้ามหรือคัดค้านมิให้ประมวลผลข้อมูลส่วนบุคคล
    - สิทธิในการยื่นคำร้องทุกข์ต่อหน่วยงานกำกับดูแล
    - แหล่งที่มาของข้อมูลส่วนบุคคล (กรณีได้รับมาจากแหล่งอื่น)
    - รายละเอียดที่เกี่ยวข้องกับการตัดสินใจอัตโนมัติ และโปรไฟลิ่ง (profiling) รวมถึงตรรกะเหตุผลที่ใช้ และผลที่คาดว่าจะเกิดขึ้นจากการประมวลผลด้วยวิธีการดังกล่าว

    ทั้งนี้ ข้อมูลข้างต้นที่จะต้องส่งให้แก่เจ้าของข้อมูลควรเป็นข้อมูลที่มีอยู่ในขณะที่ส่งข้อมูลให้แก่เจ้าของข้อมูล (แม้ว่าจะมีการแก้ไขข้อมูลในระหว่างที่ได้รับคำร้องขอกับการดำเนินการแจ้งข้อมูลตามคำร้องขอก็ตาม)

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล อาจกำหนดหลักเกณฑ์เกี่ยวกับการเข้าถึงและการขอรับสำเนาหรือขยายระยะเวลาในการดำเนินการตามคำร้องขอตามความเหมาะสมได้ ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลมีสิทธิที่จะปฏิเสธคำร้องขอจากเจ้าของข้อมูลส่วนบุคคลได้ ในกรณีต่อไปนี้ และให้บันทึกการปฏิเสธคำร้องขอพร้อมด้วยเหตุผลตามที่ระบุในหัวข้อ 10.2.10

1. เป็นการปฏิเสธตามกฎหมาย หรือ ตามคำสั่งศาล
2. หากการใช้สิทธิในการเข้าถึงและการขอรับสำเนาข้อมูลส่วนบุคคลนั้น จะส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น หากข้อมูลที่เก็บรวบรวมมีข้อมูลส่วนบุคคลของบุคคลที่สามรวมเกี่ยวข้องอยู่ด้วย ผู้ควบคุมข้อมูลส่วนบุคคลสามารถปฏิเสธที่จะไม่เปิดเผยข้อมูลเฉพาะของบุคคลที่สามได้ แต่ไม่สามารถปฏิเสธการเข้าถึงข้อมูลและขอรับสำเนาของเจ้าของข้อมูลส่วนบุคคลได้

ในการดำเนินการตามคำร้องขอของเจ้าของข้อมูลส่วนบุคคลนั้น ผู้ควบคุมข้อมูลส่วนบุคคลไม่ควรเรียกเก็บค่าธรรมเนียมใด ๆ ในการใช้สิทธิ เว้นแต่เจ้าของข้อมูลบุคคลมีการขอรับสำเนาเพิ่มเติมมากจนเกินความจำเป็น ท่านอาจพิจารณาเรียกเก็บค่าธรรมเนียมในการจัดการได้ตามสมควรแก่กรณี

การใช้สิทธิในการเข้าถึงข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล ท่านควรพิจารณาให้มีช่องทางการร้องขอใช้สิทธิที่สาขาหรืออิเล็กทรอนิกส์ได้ตามสมควรแก่กรณี และการดำเนินการตามสิทธินั้นควรพิจารณาการให้ข้อมูลทางสาขาหรือทางอิเล็กทรอนิกส์ได้ตามสมควรด้วยเช่นกัน เพื่อให้ง่ายต่อการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

9.3 สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (“Right to Rectification”)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลแก้ไขข้อมูลส่วนบุคคลของตนที่ให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิด อันได้แก่

i. กรณีที่ข้อมูลไม่สมบูรณ์ คือการที่ข้อมูลที่ผู้ควบคุมข้อมูลส่วนบุคคลมีอยู่นั้นถูกต้องแต่ได้รับข้อมูลมาไม่ครบถ้วน ไม่เพียงพอต่อการนำไปประมวลผลตามวัตถุประสงค์
ii. กรณีที่ข้อมูลไม่ถูกต้อง คือการที่ข้อมูลไม่ตรงกับความจริง

ทั้งสองกรณี ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการแก้ไขโดยไม่ชักช้า ในระหว่างการดำเนินการแก้ไขนั้น เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการประมวลผลชั่วคราวในระหว่างการตรวจสอบความถูกต้องของข้อมูล และดำเนินการแก้ไขข้อมูลส่วนบุคคลก่อนประมวลผลอีกครั้ง อย่างไรก็ตามเพื่อป้องกันผลกระทบจากการประมวลผลข้อมูลส่วนบุคคลที่ไม่ถูกต้องผู้ควบคุมข้อมูลส่วนบุคคลควรระงับการประมวลผลแม้ว่าเจ้าของข้อมูลส่วนบุคคลจะใช้สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการประมวลผลข้อมูลส่วนบุคคลหรือไม่ก็ตาม นอกจากนั้น ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องทำการแจ้งแก่บุคคลที่สามที่ข้อมูลส่วนบุคคลถูกเปิดเผย เช่น ผู้ประมวลผลข้อมูลส่วนบุคคลของท่าน ให้ทราบถึงการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลข้อมูลจะพิสูจน์ได้ว่าเป็นไปไม่ได้หรือเกินความพยายามตามสมควร

ทั้งนี้ หากผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามคำร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคล พร้อมด้วยเหตุผลตามที่ระบุในหัวข้อ 10.2.10

ในการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลในแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง ท่านอาจกำหนดหลักเกณฑ์ในการพิสูจน์ความถูกต้องของข้อมูลส่วนบุคคล เช่น ให้เจ้าของข้อมูลส่วนบุคคลนำหลักฐานที่เกี่ยวข้องมาประกอบการพิจารณา อย่างไรก็ตาม แม้เจ้าของข้อมูลส่วนบุคคลจะมีสิทธิในการแก้ไข แต่ท่านยังคงมีหน้าที่ ที่ต้องดำเนินการตามหลักการในการประมวลผลข้อมูลส่วนบุคคลอย่างถูกต้อง เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลควรมีความถูกต้อง สมบูรณ์และเป็นปัจจุบัน ไม่ก่อให้เกิดความเข้าใจผิด และข้อมูลที่ไม่ถูกต้องจะต้องถูกลบหรือได้รับการแก้ไข ท่านควรตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลในขณะเก็บรวบรวมข้อมูลส่วนบุคคล เพื่อลดความเสี่ยงและผลกระทบที่อาจทำให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลและกับท่านเอง

9.4 สิทธิในการลบหรือทำลายข้อมูลส่วนบุคคล (“Right to Deletion”)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการขอให้ลบหรือทำลายข้อมูลส่วนบุคคลของตน ท่านจะต้องดำเนินการดังกล่าว หากมีเหตุดังต่อไปนี้

- ข้อมูลส่วนบุคคลดังกล่าวหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอีกต่อไป
- เจ้าของข้อมูลส่วนบุคคล ทำการถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและท่านไม่มีอำนาจตามกฎหมายที่จะทำการเก็บรวบรวม ใช้ หรือเปิดเผยอีกต่อไป
- เจ้าของข้อมูลส่วนบุคคลคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ในกรณีที่เป็นข้อมูลส่วนบุคคลที่ท่านเก็บรวบรวม ไว้โดยได้รับยกเว้นไม่ต้องขอความยินยอม ภายใต้ฐานภารกิจของรัฐ หรือ ฐานประโยชน์อันชอบธรรม และท่านไม่สามารถพิสูจน์ได้ว่ามีเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า ประโยชน์ สิทธิเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล หรือเป็นไปเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
- เจ้าของข้อมูลส่วนบุคคลคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล เพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง
- เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันมิชอบด้วยกฎหมาย

หากเกิดเหตุข้างต้น ท่านจะต้องทำการลบหรือทำลายหรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้อีกโดยไม่ล่าช้า หากท่านได้ทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่เปิดเผยแก่สาธารณะ และท่านได้รับคำ

ร้องขอใช้สิทธิดังกล่าว ท่านจะต้องรับผิดชอบดำเนินการทั้งในทางเทคโนโลยีและค่าใช้จ่ายเพื่อให้เป็นไปตามคำร้องขอ โดยจะต้องทำการแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลอื่น ๆ ทราบถึงการใช้สิทธิในการลบของเจ้าของข้อมูลส่วนบุคคล เพื่อดำเนินการลบหรือทำลายหรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้

อย่างไรก็ตามท่านสามารถปฏิเสธคำร้องขอการใช้สิทธิในการลบหรือทำลายได้ หากพิสูจน์ได้ว่าการประมวลผลข้อมูลนั้นมีความจำเป็นในเรื่องดังต่อไปนี้

- ท่านพิสูจน์ได้ว่า การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลนั้นได้แสดงให้เห็นถึงเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า ประโยชน์ สิทธิ เสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล
- เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
- เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น
- เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
- เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะ หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ท่าน
- เป็นการจำเป็นเพื่อบรรลุวัตถุประสงค์เกี่ยวกับเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ หรือประโยชน์ด้านสาธารณสุข

9.5 สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคล (“Right to Restriction of Processing”)

เจ้าของข้อมูลส่วนบุคคล มีสิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคลของตน เมื่อเข้าเงื่อนไขดังต่อไปนี้

- เมื่อท่านอยู่ในระหว่างการตรวจสอบข้อมูล ตามคำร้องขอใช้สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง
- เมื่อเป็นข้อมูลที่ต้องทำการลบหรือทำลาย เนื่องจากการประมวลผลข้อมูลส่วนบุคคลอันมิชอบด้วยกฎหมาย แต่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิในการขอให้ระงับการใช้แทนการลบหรือทำลายข้อมูลส่วนบุคคลของตน

- เมื่อข้อมูลส่วนบุคคลไม่จำเป็นในการเก็บรักษาไว้ ตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลอีกต่อไป แต่เจ้าของข้อมูลมีความจำเป็นที่ต้องขอให้การเก็บรักษาไว้ เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
- เมื่อท่านอยู่ในระหว่างการพิสูจน์ข้ออ้างที่ว่าการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลนั้นมีเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่าประโยชน์ สิทธิ เสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล
- ท่านอยู่ในระหว่างการตรวจสอบเพื่อดำเนินการปฏิเสธการคัดค้านการประมวลผลของเจ้าของข้อมูลส่วนบุคคล ในกรณีที่ท่านเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ว่าเป็นไปข้อยกเว้นที่ท่านสามารถประมวลผลได้เนื่องจากเป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะของท่าน

หากท่านปฏิเสธไม่ดำเนินการตามคำร้องขอใช้สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามสิทธิได้

ท่านควรจัดให้มีมาตรการที่เหมาะสม ในการระงับการประมวลผลข้อมูลในระบบของท่าน เช่น การระงับการให้ผู้ใช้ข้อมูลเข้าถึงข้อมูลชั่วคราว หรือการแยกส่วนข้อมูลที่ถูกระงับออกจากข้อมูลอื่นชั่วคราว เพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลนั้นถูกดำเนินการตามคำร้องขอ

9.6 สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล (“Right to Object”)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการคัดค้านการประมวลผลข้อมูลของตนเมื่อใดก็ได้ เมื่อเข้าเงื่อนไขดังต่อไปนี้

1. กรณีที่ข้อมูลส่วนบุคคลที่ท่านทำการเก็บรวบรวมได้รับยกเว้นไม่ต้องขอความยินยอม เฉพาะในกรณีดังนี้
    I. เพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะ หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ท่าน
    II. เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของท่านหรือของบุคคลอื่น

    <u>สามารถปฏิเสธคำร้องขอได้หาก</u> ท่านสามารถพิสูจน์ได้ว่าการประมวลผลข้อมูลนั้นแสดงให้เห็นถึงเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่าผลประโยชน์ สิทธิ เสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล หรือการประมวลข้อมูลส่วนบุคคล

นั้นทำเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

2. กรณีที่ ท่านทำการประมวลผลข้อมูลส่วนบุคคล เพื่อวัตถุประสงค์ที่เกี่ยวข้องกับการตลาดแบบตรง (Direct marketing) ในกรณีนี้ท่านจะ*ไม่สามารถปฏิเสธคำร้องขอ*ในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลได้
3. กรณีที่เป็นการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ
   สามารถปฏิเสธคำร้องขอได้หาก เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะของท่าน

หากท่านอ้างเหตุแห่งการปฏิเสธการคัดค้านการประมวลผลดังที่กล่าวมา ท่านจะต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคล พร้อมด้วยเหตุผลตามที่ระบุในหัวข้อ 10.2.10

ในกรณีที่เจ้าของข้อมูลส่วนบุคคล ใช้สิทธิคัดค้านการประมวลผลข้อมูลส่วนบุคคล และท่านสามารถอ้างเหตุแห่งการปฏิเสธ ท่านจะไม่สามารถเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลต่อไปได้ และท่านจะต้องดำเนินการตามคำร้องขอ ซึ่งจะต้องปฏิบัติโดยแยกส่วนออกจากข้อมูลอื่นอย่างชัดเจนในทันทีเมื่อเจ้าของข้อมูลส่วนบุคคลได้แจ้งการคัดค้านให้ทราบ

9.7 สิทธิในการขอรับหรือโอนย้ายข้อมูลส่วนบุคคล (“Right to Data Portability”)

ลูกค้ามีสิทธิขอรับข้อมูลที่เกี่ยวกับลูกค้าจากท่าน ในกรณีที่ท่านได้ทำให้ข้อมูลนั้นอยู่ในรูปแบบที่สามารถอ่าน หรือ ใช้งานโดยทั่วไปได้ด้วยเครื่องมือ หรือ อุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้หรือเปิดเผยได้ด้วยวิธีการอัตโนมัติ รวมทั้ง

9.7.1 มีสิทธิขอให้ท่านส่งหรือโอนข้อมูลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น เมื่อสามารถทำได้ด้วยวิธีการอัตโนมัติ
สามารถปฏิเสธคำร้องขอได้หาก การประมวลผลข้อมูลส่วนบุคคลนั้นเป็นการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะหรือเป็นการปฏิบัติหน้าที่ตามกฎหมาย หรือการใช้สิทธินั้นเป็นการละเมิดสิทธิเสรีภาพของบุคคลอื่น และท่านจะต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคล พร้อมด้วยเหตุผลตามที่ระบุในหัวข้อ 10.2.10

9.7.2 ขอรับข้อมูลที่ท่านส่งหรือโอนข้อมูลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยตรง เว้นแต่สภาพทางเทคนิคไม่สามารถทำได้

ดังนั้น เพื่อประโยชน์ของทั้งเจ้าของข้อมูลส่วนบุคคลและประโยชน์แก่ท่านเอง ท่านจึงควรมีนโยบายและกระบวนการจัดการที่ชัดเจนในกรณีที่เจ้าของข้อมูลส่วนบุคคลมาขอใช้สิทธิของเจ้าของ

ข้อมูลส่วนบุคคล ยกตัวอย่างเช่น ท่านอาจมอบหมายงานหรือจัดตั้งหน่วยงานภายใน ในการดูแล รับเรื่องร้องขอดังกล่าว แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) เป็นผู้รับผิดชอบและพิจารณาการใช้สิทธิว่าสามารถดำเนินการให้ได้หรือไม่ และจัดให้มีช่องทางที่เหมาะสมในการยื่นคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

9.8 สิทธิในการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ (“Right to Lodge a Complaint”)

ในกรณีที่ท่าน รวมทั้งลูกจ้างหรือผู้รับจ้างของท่าน ฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ลูกค้ามีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญได้

9.9 ตัวอย่างแบบคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

ตัวอย่าง แบบคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้ให้สิทธิแก่เจ้าของข้อมูลในการร้องขอให้ผู้ควบคุมข้อมูลดำเนินการตามสิทธิที่ร้องขอ (เลือกระบุ (1) นักวางแผนการเงินไทย CFP / ระบุชื่อบริษัทของนักวางแผนการเงิน CFP (“นักวางแผนการเงิน CFP”) หรือ (2) ที่ปรึกษาการเงิน AFPT / ระบุชื่อบริษัทของนักวางแผนการเงินไทยที่ปรึกษาการเงิน AFPT (“ที่ปรึกษาการเงิน AFPT”)) ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลของท่านจึงขอข้อมูลท่านเพิ่มเติมจากท่านเพื่อดำเนินการตามความประสงค์จะใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล โดยโปรดกรอกรายละเอียดในแบบฟอร์มนี้และดำเนินการตามที่ (เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) กำหนด

ข้อมูลของผู้ยื่นคำร้อง

<u>รายละเอียดผู้ยื่นคำร้อง</u>

ชื่อ: [ชื่อภาษาไทย และอังกฤษ (ถ้ามี)].....

ที่อยู่: [ที่อยู่] .....

เบอร์ติดต่อ: [โทรศัพท์] .....

Email: [email] .....

ท่านเป็นเจ้าของข้อมูลหรือไม่?

❒ **ผู้ยื่นคำร้องเป็นบุคคลเดียวกับเจ้าของข้อมูล** ทั้งนี้ ข้าพเจ้าได้แนบเอกสารดังต่อไปนี้ เพื่อการตรวจสอบตัวตน และถิ่นที่อยู่ของผู้ยื่นคำร้อง เพื่อให้ (เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) สามารถดำเนินการตามสิทธิที่ร้องขอได้อย่างถูกต้อง

<u>เอกสารพิสูจน์ตัวตนและ/หรือพิสูจน์ถิ่นที่อยู่</u>

❒ สำเนาบัตรประจำตัวประชาชน (กรณีสัญชาติไทย)

❒ สำเนา Passport (กรณีต่างชาติ)

❒ สำเนาทะเบียนบ้าน

❒ อื่น ๆ (ถ้ามี).....

❒ **ผู้ยื่นคำร้องเป็นตัวแทนของเจ้าของข้อมูล**

<u>รายละเอียดเจ้าของข้อมูล</u>

ชื่อ: [ชื่อภาษาไทย และอังกฤษ (ถ้ามี)]

ที่อยู่: [ที่อยู่]

เบอร์ติดต่อ: [โทรศัพท์]

Email: [email]

ทั้งนี้ ข้าพเจ้าได้แนบเอกสารดังต่อไปนี้ เพื่อการตรวจสอบอำนาจ ตัวตน และถิ่นที่อยู่ของผู้ยื่นคำร้องและเจ้าของข้อมูล เพื่อให้ (เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) สามารถดำเนินการตามสิทธิที่ร้องขอได้อย่างถูกต้อง

<u>เอกสารพิสูจน์อำนาจดำเนินการแทน</u>

❒ หนังสือมอบอำนาจ

<u>เอกสารพิสูจน์ตัวตนและ/หรือถิ่นที่อยู่</u>

❒ สำเนาบัตรประจำตัวประชาชนของ**ท่านและเจ้าของข้อมูล** (กรณีสัญชาติไทย)

❒ สำเนา Passport ของ**ท่านและเจ้าของข้อมูล** (กรณีต่างชาติ)

❒ สำเนาทะเบียนบ้านของ**เจ้าของข้อมูล**

❒ อื่น ๆ (ถ้ามี).....

(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) ขอสงวนสิทธิในการสอบถามข้อมูล หรือเรียกเอกสารเพิ่มเติมจากผู้ยื่นคำร้อง หากข้อมูลที่ได้รับไม่สามารถแสดงให้เห็นอย่างชัดเจนได้ว่าผู้ยื่นคำร้องเป็นเจ้าของข้อมูลหรือมีอำนาจในการยื่นคำร้องขอดังกล่าว (เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) ขอสงวนสิทธิในการปฏิเสธคำร้องขอของท่าน

รายละเอียดคำขอ

1. ความสัมพันธ์ของเจ้าของข้อมูลส่วนบุคคลกับ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)

   ❒ ผู้สมัครงาน

   ❒ พนักงาน

   ❒ ลูกค้า

   ❒ ผู้ให้บริการภายนอก / พันธมิตรทางธุรกิจ

   ❒ อื่นๆ (โปรดระบุ) .....

2. สิทธิที่เจ้าของข้อมูลส่วนบุคคลต้องการให้ดำเนินการ **(**โปรดเลือกประเภทของสิทธิที่ต้องการดำเนินการ)

   ❒ สิทธิในการเพิกถอนการให้ความยินยอม (Right to Withdraw of Consent)

   ❒ สิทธิในการขอเข้าถึงข้อมูลส่วนบุคคล (Right to Access)

   ❒ สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (Right to Rectification)

❒ สิทธิในการลบข้อมูลส่วนบุคคล (Right to Deletion)

❒ สิทธิในการห้ามมิให้ประมวลผลข้อมูลส่วนบุคคล (Right to Restriction of Processing)

❒ สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล (Right to Object)

❒ สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล (Right to Data Portability)

ข้อมูลส่วนบุคคลที่ต้องการดำเนินการ.....

.....

.....

แหล่งที่พบ (ถ้ามี) .....

.....

.....

เหตุผลประกอบคำร้องขอ.....

.....

.....

ข้อสงวนสิทธิของ(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT)

(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) ขอแจ้งให้ท่านทราบว่า (เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) อาจมีความจำเป็นต้องปฏิเสธคำร้องขอของท่านได้ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และ/หรือ กฎหมาย แนวปฏิบัติ หรือ หลักเกณฑ์ที่เกี่ยวข้องอื่น ๆ

การรับทราบและยินยอม

ท่านได้อ่านและเข้าใจเนื้อหาของคำร้องขอฉบับนี้อย่างละเอียดแล้ว และยืนยันว่าข้อมูลต่าง ๆ ที่ได้แจ้งให้แก่(เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) ทราบนั้นเป็นความจริง ถูกต้อง ท่านเข้าใจดีว่าการตรวจสอบเพื่อยืนยันอำนาจ ตัวตน และถิ่นที่อยู่นั้นเป็นการจำเป็นอย่างยิ่งเพื่อพิจารณาดำเนินการตามสิทธิที่ท่านร้องขอ หากท่านให้ข้อมูลที่ผิดพลาดด้วยเจตนาทุจริต ท่านอาจถูกดำเนินคดีตามกฎหมายได้ และ (เลือกระบุ (1) นักวางแผนการเงิน CFP หรือ (2) ที่ปรึกษาการเงิน AFPT) อาจขอข้อมูลเพิ่มเติมจากท่านเพื่อการตรวจสอบดังกล่าวเพื่อให้การดำเนินการอนุญาตให้เข้าถึง การทำสำเนา หรือการเปิดเผยการได้มาของข้อมูลเป็นไปได้อย่างถูกต้องครบถ้วนต่อไป

ในการนี้ ท่านจึงได้ลงนามไว้เพื่อเป็นหลักฐาน

ลงชื่อ.....ผู้ยื่นคำร้อง

(.....)

วันที่.....

10. แนวปฏิบัติเกี่ยวกับหน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (Guideline on Data Controller and Data Processor Roles and Responsibilities)

10.1 การระบุสถานะในการคุ้มครองข้อมูลส่วนบุคคลของท่าน

ท่านอาจทำหน้าที่เป็นทั้งผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) และผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ซึ่งขึ้นอยู่กับแต่ละกรณี อย่างไรก็ตามท่านจะต้องสามารถระบุสถานะให้ได้ว่า สำหรับชุดข้อมูลใดท่านเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือเป็นผู้ประมวลผลข้อมูลส่วนบุคคล โดยสามารถพิจารณาจากการที่ท่านเป็นผู้ที่กำหนดวัตถุประสงค์และสามารถตัดสินใจในเรื่องของการประมวลผลข้อมูลส่วนบุคคลได้เองหรือไม่ หรือท่านทำหน้าที่เป็นผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคลอื่น เนื่องจากการระบุสถานะเป็นสิ่งสำคัญพื้นฐานในการกำหนดหน้าที่ต่อไป โดยท่านสามารถพิจารณาได้ตามรายละเอียดใน Checklist ด้านล่างดังต่อไปนี้

<u>รายการตรวจสอบว่าท่านเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือไม่ (Data Controller Checklist)</u>

- ❒ ท่านเป็นผู้ตัดสินใจในเรื่องของการเก็บรวบรวมหรือประมวลผลข้อมูลส่วนบุคคลได้
- ❒ ท่านสามารถกำหนดวัตถุประสงค์หรือผลลัพธ์จากการประมวลผลข้อมูลส่วนบุคคลที่ควรจะเป็นได้
- ❒ ท่านเป็นผู้ตัดสินใจได้ว่าควรเก็บรวบรวมข้อมูลส่วนบุคคลใดบ้าง
- ❒ ท่านเป็นผู้ตัดสินใจได้ว่าจะเก็บรวบรวมข้อมูลส่วนบุคคลของใครบ้าง
- ❒ ท่านเป็นผู้ที่ได้รับประโยชน์เชิงเศรษฐกิจหรือประโยชน์อื่นจากการประมวลผลข้อมูล
- ❒ ท่านกระทำการประมวลผลข้อมูลภายใต้ข้อตกลงหรือสัญญาที่ได้ทำไว้กับเจ้าของข้อมูลส่วนบุคคล
- ❒ ท่านทำการเก็บรวบรวมข้อมูลส่วนบุคคลของพนักงานท่าน
- ❒ ท่านเป็นผู้พิจารณาเกี่ยวกับผลกระทบที่อาจเกิดขึ้นต่อเจ้าของข้อมูลส่วนบุคคลจากการประมวลผลข้อมูลส่วนบุคคลของท่าน

❒ ท่านใช้ดุลยพินิจอย่างมืออาชีพในการประมวลผลข้อมูลส่วนบุคคล

❒ ท่านเป็นผู้ที่มีความสัมพันธ์เชิงธุรกิจโดยตรงกับเจ้าของข้อมูลส่วนบุคคล

❒ ท่านมีอิสระในการตัดสินใจเกี่ยวกับวิธีการประมวลผลข้อมูลส่วนบุคคล

❒ ท่านทำการแต่งตั้งผู้ประมวลผลข้อมูลเพื่อทำการประมวลผลข้อมูลส่วนบุคคลในนามของท่าน

<u>รายการตรวจสอบว่าท่านเป็นผู้ประมวลผลข้อมูลส่วนบุคคลหรือไม่ (Data Processor Checklist)</u>

❒ ท่านเป็นผู้ประมวลผลข้อมูลส่วนบุคคลตามคำแนะนำเกี่ยวกับการประมวลผลจากบุคคลอื่นหรือไม่

❒ ท่านได้รับข้อมูลส่วนบุคคลจากบุคคลที่สามหรือโดยผู้ที่กำหนดว่าท่านจะเก็บรวบรวมข้อมูลใดบ้าง

❒ ท่านไม่ได้เป็นผู้ตัดสินใจได้ว่าควรเก็บรวบรวมข้อมูลส่วนบุคคลใดบ้าง

❒ ท่านไม่ได้เป็นผู้ตัดสินใจได้ว่าจะเก็บรวบรวมข้อมูลส่วนบุคคลของใครบ้าง

❒ ท่านไม่ได้เป็นผู้ที่กำหนดฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล

❒ ท่านไม่ได้เป็นผู้กำหนดวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล

❒ ท่านไม่ได้เป็นผู้ตัดสินใจว่าข้อมูลส่วนบุคคลจะถูกเปิดเผยให้แก่ใคร

❒ ท่านไม่ได้เป็นผู้กำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

❒ ท่านอาจทำการตัดสินใจในเรื่องของการประมวลผลข้อมูลอย่างไรแต่เป็นการทำภายใต้ข้อตกลงในสัญญาที่ได้ทำกับผู้อื่น

❒ ท่านไม่มีหน้าที่ทำการประเมินผลกระทบจากการประมวลผลข้อมูลส่วนบุคคลที่อาจเกิดขึ้นแก่เจ้าของข้อมูลส่วนบุคคล

10.2 หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller Roles and Responsibilities)

10.2.1 เมื่อท่านเป็นผู้ควบคุมข้อมูลส่วนบุคคล ท่านจะทำการประมวลผลข้อมูลส่วนบุคคลได้ตามวัตถุประสงค์อันชอบด้วยกฎหมาย นอกจากนั้นท่าน จะต้องจัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสม ทั้งมาตรการเชิงเทคนิค (Technical Measure) เช่น ใช้วิธีการทางเทคนิคที่เหมาะสมด้วยการเข้ารหัส (Encryption) การแฝงข้อมูล (Pseudonymization) หรือการทำข้อมูลให้เป็นนิรนาม (Anonymization) การควบคุมการเข้าถึง (Access Control) รวมถึงการตรวจสอบติดตามกิจกรรมเกี่ยวกับข้อมูลส่วนบุคคลที่เกิดขึ้น (Log) และมาตรการเชิงบริหารจัดการ (Organizational Measure) เช่น จัดทำนโยบายความมั่นคงปลอดภัยภายใน (Internal Security Policy) เพื่อให้พนักงานหรือลูกจ้างปฏิบัติตาม รวมถึงการสร้างความรับรู้ (Awareness) เรื่องการคุ้มครองข้อมูลส่วนบุคคลแก่บุคลากรเหล่านั้น เพื่อป้องกันการสูญหาย เข้าถึง ใช้ หรือเปลี่ยนแปลงแก้ไขหรือเปิดเผยข้อมูลโดยมิชอบ และจะต้องมีการทบทวนมาตรการในการรักษาความปลอดภัยของข้อมูลเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงและปลอดภัยอย่างเหมาะสมอยู่เสมอ

10.2.2 ในกรณีที่ท่านต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่น ท่านจะต้องดำเนินการป้องกัน ไม่ให้ผู้นั้นนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยโดยมิชอบ

10.2.3 ท่านจะต้องจัดให้มีระบบในการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้ เมื่อพ้นกำหนดระยะเวลาในการเก็บรักษาหรือที่ไม่เกี่ยวข้องเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่จะทำการเก็บรักษาไว้ภายใต้ข้อยกเว้นตามกฎหมาย

10.2.4 หากเกิดเหตุการณ์ละเมิดขึ้น ท่านจะต้องแจ้งแก่สำนักงานคุ้มครองข้อมูลส่วนบุคคล โดยไม่ชักช้าภายใน 72 ชั่วโมง นับจากที่ได้รับทราบเหตุ เว้นแต่การละเมิดนั้นไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล หากเหตุการณ์ละเมิดนั้นมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ให้ท่านรีบแจ้งเหตุละเมิดนั้นแก่เจ้าของข้อมูลส่วนบุคคลทราบด้วย รวมถึงแนวทางในการเยียวยาโดยเร็วที่สุด

10.2.5 ท่านต้องทำการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) หากมีการประมวลผลข้อมูลส่วนบุคคล มีความจำเป็นที่ต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการกำหนด หรือกิจกรรมหลักของท่านเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว นอกจากนั้นท่านจะต้องให้ข้อมูลการติดต่อ DPO ไว้ใน Privacy Notice/ Privacy Policy ของท่านด้วย เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถติดต่อ DPO ได้ หากมีความประสงค์จะใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

ตัวอย่าง ข้อมูลการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ในส่วนของ Privacy Notice/ Privacy Policy “หากมีข้อสงสัยเกี่ยวกับข้อมูลส่วนบุคคลหรือมีความประสงค์ที่จะใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล ท่านสามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของเราได้ตามรายละเอียดการติดต่อด้านล่างนี้ *เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)* : นาย ข. *อีเมล*: dataprotectionofficer@ABCbank.com *โทร*: 1234”

ท่านสามารถดูรายละเอียดเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้ในหัวข้อ “เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO)”

10.2.6 ท่านจะต้องทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment : DPIA) ในกรณีที่การประมวลผลข้อมูลมีความเสี่ยงที่จะเกิดผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ท่านจะต้องมีการจัดทำ DPIA สามารถดูรายละเอียดเกี่ยวกับการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลได้ในหัวข้อ “แนวปฏิบัติเกี่ยวกับการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA)”

10.2.7 ท่านมีหน้าที่ในการดำเนินการให้เป็นไปตามสิทธิของเจ้าของข้อมูลส่วนบุคคล หากเจ้าของข้อมูลส่วนบุคคลมีการร้องขอใช้สิทธิ ในการรับเรื่องร้องขอจากเจ้าของข้อมูลส่วนบุคคล ท่านอาจกำหนดให้มีผู้ที่รับผิดชอบในเรื่องดังกล่าวอย่างชัดเจน เช่น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หน่วยงานรับเรื่อง

ร้องเรียน หน่วยงานลูกค้าสัมพันธ์ เป็นต้น เพื่อจัดให้มีการดำเนินการตามคำร้องขอของเจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า หากท่านปฏิเสธคำร้องขอตามเหตุแห่งการปฏิเสธการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลนั้น ท่านจะต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคล พร้อมด้วยเหตุผลตามที่ระบุในหัวข้อ 10.2.10

10.2.8 ท่านจะต้องทำการเลือกผู้ประมวลผลข้อมูลส่วนบุคคลที่มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการที่เหมาะสมในการประมวลผลและการรักษาความมั่นคงปลอดภัยของข้อมูล

10.2.9 ท่านจะต้องจัดให้มีการทำข้อตกลงกันระหว่างท่าน (ผู้ควบคุมข้อมูลส่วนบุคคล) และผู้ประมวลผลข้อมูลส่วนบุคคล หรือที่เรียกว่า Data Processing Agreement เพื่อให้ผู้ประมวลผลข้อมูลดำเนินการให้เป็นไปตามกฎหมาย

10.2.10 ท่านจะต้องทำการจัดให้มีการเก็บบันทึกข้อมูลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการบันทึกข้อมูลที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้ตามหลักการ หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้ ท่านจะต้องทำการบันทึกรายการอย่างน้อยดังต่อไปนี้

1) ข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวม
2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคล
6) การใช้หรือเปิดเผย
7) การปฏิเสธคำขอหรือการคัดค้านตามข้อกำหนดของกฎหมาย
8) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย

สำหรับกิจการขนาดเล็ก หากการประมวลผลข้อมูลนั้นอาจก่อให้เกิดความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลหรือมีการประมวลผลข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว หรือเป็นการประมวลผล

ข้อมูลอาชญากรรม ให้ท่านทำการเก็บบันทึกการประมวลผลข้อมูลส่วนบุคคลนั้นด้วย

10.2.11 ท่านมีหน้าที่ในการให้ความร่วมมือกับองค์กรกำกับดูแล หรือทำหน้าที่ตามกฎหมาย ตามคำสั่งของหน่วยงานรัฐหรืออำนาจโดยชอบในการเข้าถึงข้อมูล

10.2.12 กรณีท่านได้มีการเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลภายนอกอื่นใด แต่ละฝ่ายจะมีหน้าที่และความรับผิดชอบในฐานะผู้ควบคุมข้อมูลส่วนบุคคลแยกต่างหากจากกันตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

10.3 หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor Roles and Responsibilities)

ในกรณีที่ท่านทำหน้าที่ในการประมวลผลข้อมูลส่วนบุคคล ในนามของผู้ควบคุมข้อมูลส่วนบุคคลอื่น ซึ่งท่านจะต้องทำการประมวลผลข้อมูลตามที่ได้ตกลงกับผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น ซึ่งผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีข้อตกลงหรือสัญญาในการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) หากท่านทำการประมวลผลนอกเหนือหรือขัดต่อคำสั่งของผู้ควบคุมข้อมูล การกระทำดังกล่าวให้ถือว่าท่านทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลสำหรับการประมวลผลข้อมูลนั้น ซึ่งท่านก็จะต้องปฏิบัติตามหน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคลตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลสำหรับกรณีดังกล่าวด้วย

ในกรณีที่ท่านมีสถานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ท่านจะต้องปฏิบัติตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามแนวปฏิบัติดังต่อไปนี้

10.3.1 ท่านจะต้องดำเนินการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น ไม่ทำการประมวลผลข้อมูลส่วนบุคคลนอกเหนือจากที่ตกลงกับผู้ควบคุมข้อมูลส่วนบุคคลหากไม่ได้รับอนุญาตเป็นลายลักษณ์อักษร เว้นแต่คำสั่งดังกล่าวนั้นขัดต่อกฎหมาย

10.3.2 ท่านจะต้องจัดให้มีมาตรการในการรักษาความมั่นคงและปลอดภัยที่เหมาะสม มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อรักษาความมั่นคงปลอดภัยในการประมวลผลที่เหมาะสมกับความเสี่ยง เพื่อป้องกันการสูญหาย การใช้ เปลี่ยนแปลง แก้ไข หรือการเปิดเผยข้อมูลโดยมิชอบ

10.3.3 ท่านจะต้องจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ หากการประมวลผลข้อมูลนั้นอาจก่อให้เกิดความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลหรือมีการประมวลผลข้อมูลส่วน

บุคคลที่เป็นข้อมูลอ่อนไหวหรือเป็นการประมวลผลข้อมูลอาชญากรรม ให้ท่านทำการเก็บบันทึกการประมวลผลข้อมูลส่วนบุคคล ท่านจะต้องจัดให้มีรายละเอียดการเก็บบันทึกรายการประมวลผลข้อมูลส่วนบุคคลจะต้องมีดังต่อไปนี้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้

1. ชื่อและข้อมูลการติดต่อท่าน ตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของท่าน
2. ชื่อและข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลที่ท่านดำเนินการ ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลนั้น และตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคล
3. ชื่อและข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล รวมถึงสถานที่ติดต่อและวิธีการ ติดต่อ ในกรณีที่ท่านจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
4. ประเภทหรือลักษณะของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ที่ท่านดำเนินการตามคาสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งรวมถึงข้อมูลส่วนบุคคลและวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล
5. ประเภทของบุคคลหรือหน่วยงานที่ได้รับข้อมูลส่วนบุคคล ในกรณีที่มีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ (หากมี)
6. คำอธิบายเกี่ยวกับมาตรการเชิงเทคนิคและเชิงบริหารจัดการเกี่ยวกับการรักษาความมั่นคงและปลอดภัยของข้อมูลส่วนบุคคล

10.3.4 ท่านต้องทำการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) หากมีการประมวลผลข้อมูลส่วนบุคคล มีความจำเป็นที่ต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการกำหนด หรือกิจกรรมหลักของท่านเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว

10.3.5 ท่านจะต้องทำการแจ้งเหตุแก่ผู้ควบคุมข้อมูลกรณีข้อมูลส่วนบุคคลเกิดการรั่วไหล (Data Breach) ท่านจะต้องทำการแจ้งโดยไม่ชักช้าหลังจากทราบเหตุ และท่านไม่มีหน้าที่ต้องแจ้งแก่สำนักงานคุ้มครองข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล

11. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)

ท่านจะต้องมีบุคลากรที่ทำหน้าที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) เพื่อการคุ้มครองสิทธิประโยชน์ของท่านและเพื่อคุ้มครองสิทธิประโยชน์ของเจ้าของข้อมูลส่วนบุคคล นอกจากนั้นการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะช่วยให้องค์กรสามารถบริหารความเสี่ยงและจัดการข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพและประสิทธิผล

11.1 การแต่งตั้งและคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ท่านสามารถที่จะจัดแต่งตั้งบุคคลหรือคณะทำงานจากบุคลากรของท่านเอง หรือจัดจ้างบุคคลภายนอกก็ได้ ซึ่งบุคคล/คณะทำงานดังกล่าวจะต้องมีความรู้ความเข้าใจในด้านกฎหมายการคุ้มครองข้อมูลส่วนบุคคล มีความเข้าใจกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของท่าน การรักษาความปลอดภัยของข้อมูลส่วนบุคคล งานด้านเทคโนโลยีสารสนเทศ อีกทั้งเข้าใจถึงภาพรวมธุรกิจของท่านและมีความสามารถในการสร้างวัฒนธรรมขององค์กรในการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม

หากท่านมีความประสงค์ที่จะแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลร่วมกันกับกลุ่มเครือกิจการ นั้นสามารถทำได้ โดยท่านหรือกลุ่มเครือกิจการจะต้องสามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้โดยง่าย

11.2 หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Responsibility of DPO)

ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนดให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลนั้นมีหน้าที่ดังต่อไปนี้

1) ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล (ซึ่งหมายถึงเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ควรให้คำแนะนำแก่พนักงานทุกคนของท่าน รวมถึงผู้รับจ้างให้ทำการประมวลผลข้อมูลส่วนบุคคลของท่าน) เกี่ยวกับการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
2) ทำการตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลเพื่อให้เป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

3) ประสานงานและให้ความร่วมมือกับสำนักงานคุ้มครองข้อมูลส่วนบุคคล ในกรณีที่มีปัญหาเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
4) รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

นอกจากนั้นเพื่อให้การปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เป็นไปได้อย่างมีประสิทธิภาพเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลควรได้รับการสนับสนุนการปฏิบัติงานจากท่าน โดยการให้อำนาจหน้าที่ และมีความเป็นอิสระในการทำงาน มีสายการรายงานที่ตรงไปยังผู้บริหารสูงสุดของท่านได้ อีกทั้ง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจมีความจำเป็นที่จะต้องได้รับสิทธิในเข้าถึงข้อมูลส่วนบุคคลที่จำเป็นเพื่อการปฏิบัติหน้าที่ ท่านจึงควรแสดงให้เห็นถึงความสำคัญของหน้าที่ดังกล่าว เพื่อให้พนักงานทุกคนตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล และให้ความร่วมมือในการปฏิบัติหน้าที่กับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล โดยการให้ข้อมูลหรือแจ้งเหตุความเป็นไปได้ที่จะเกิดการละเมิดของข้อมูลส่วนบุคคล หรือปัญหาต่าง ๆ ที่เกี่ยวข้องกับการประมวลผลข้อมูล ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทราบและเพื่อหาแนวทางการแก้ไขต่อไป

12. แนวปฏิบัติเกี่ยวกับการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA)

การประมวลผลข้อมูลส่วนบุคคลผู้ควบคุมข้อมูลส่วนบุคคลจะต้องคำนึงถึงความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล และจะต้องจัดให้มีมาตรการในการรักษาความมั่นคงและปลอดภัยที่เหมาะสมกับความเสี่ยง ดังนั้นการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลหรือ Data Protection Impact Assessment (DPIA) นั้นเป็นหนึ่งในกระบวนการที่ท่านต้องจัดให้มีสำหรับการประมวลผลที่มีความเสี่ยงสูง เพื่อเป็นการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

การจัดทำ DPIA ที่มีประสิทธิภาพนั้นจะช่วยให้ท่านสามารถกำกับการปฏิบัติตามกฎเกณฑ์ในเรื่องของการคุ้มครองข้อมูลส่วนบุคคลได้ดียิ่งขึ้น อีกทั้งยังเป็นการสร้างความเชื่อมั่นและความไว้วางใจให้กับเจ้าของข้อมูลส่วนบุคคลและส่วนรวมมากขึ้น ช่วยลดความเสี่ยงในการประมวลผลข้อมูลส่วนบุคคลที่ไม่เหมาะสม ลดความเสี่ยงที่จะเกิดผลกระทบต่อชื่อเสียงของท่าน ซึ่งจะเป็นผลดีแก่ท่านเอง

12.1 ความแตกต่างระหว่าง Data Protection Impact Assessment (DPIA) กับ Privacy Impact Assessment (PIA)

- **Data Protection Impact Assessment (DPIA)** เป็นกระบวนการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล สำหรับกิจกรรมประมวลผลข้อมูลส่วนบุคคลต่าง ๆ ซึ่งตามกฎหมายกำหนดให้ทำเฉพาะกับความเสี่ยงสูง นั่นก็คือมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ซึ่งท่านสามารถขอคำปรึกษาจาก DPO ในขั้นตอนการออกแบบและการจัดทำ DPIA กระบวนการในจัดทำ DPIA ได้แก่ การระบุความเสี่ยงและผลกระทบที่อาจเกิดขึ้น (สำหรับการระบุความเสี่ยงและประเมินผลกระทบที่อาจเกิดขึ้น โปรดดูรายละเอียดในหัวข้อ แนวปฏิบัติเกี่ยวกับการจำแนกข้อมูล) รวมถึงแนวทางการลดความเสี่ยงที่อาจเกิดขึ้นจากกิจกรรมการประมวลผลนั้น การทำ DPIA ไม่ใช่กระบวนการที่ทำเพียงครั้งเดียวแต่จะต้องมีการทบทวนความเหมาะสมอยู่เสมอ เนื่องจากความเสี่ยงอาจเปลี่ยนแปลงได้จากปัจจัยหลายอย่าง เช่น การเปลี่ยนแปลงของเทคโนโลยีอย่างรวดเร็วอาจทำให้ความเสี่ยงที่จะเกิดผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลสูงขึ้น เป็นต้น
- **Privacy Impact Assessment (PIA)** เป็นกระบวนการที่เกี่ยวข้องกับการวิเคราะห์ การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลว่าจะทำอย่างไร โดยที่ PIA เป็นกระบวนการที่ใช้ในการป้องกันในเรื่องของการจัดทำ Privacy by Design นั่นก็คือ การที่ท่านจะต้องคำนึงถึงสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลตั้งแต่ขั้นตอนการออกแบบ ซึ่ง

มักทำเมื่อมีการเริ่มหรือเข้าควบรวมกิจการอื่น มีการใช้กระบวนการใหม่ หรือออกผลิตภัณฑ์/บริการใหม่

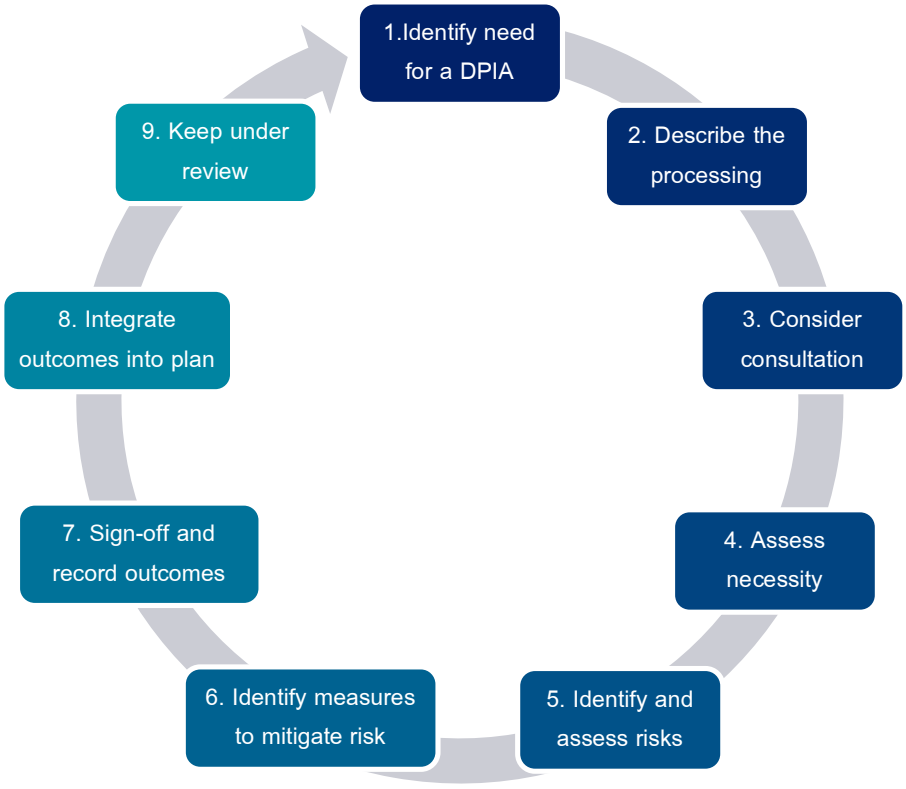
ท่านอาจทำ DPIA เพียงอย่างเดียวก็ได้หรืออาจจัดทำ PIA เข้ากับ DPIA ก็ได้เนื่องจากแนวทางในการจัดทำนั้นมีความคล้ายคลึงกัน อย่างไรก็ตาม ท่านอาจพิจารณาการทำ PIA เพิ่มเติมเมื่อเห็นว่ามีความจำเป็น

12.2 แนวปฏิบัติเกี่ยวกับการจัดทำ DPIA

แนวปฏิบัติฉบับนี้ได้ อ้างอิงหลักการจาก GDPR ในการจัดทำ DPIA ซึ่งกำหนดให้กระบวนการจัดทำจะต้องปฏิบัติตาม 4 ขั้นตอนต่อไปนี้เป็นอย่างน้อย

1. ท่านจะต้องทำการระบุรายละเอียดของกิจกรรมการประมวลผลอย่างเป็นระบบ อันได้แก่ กระบวนการหรือวิธีการประมวลผลข้อมูล วัตถุประสงค์ในการประมวลผลข้อมูลและประโยชน์อันชอบด้วยกฎหมายของท่าน
2. การประเมินความจำเป็นและสัดส่วนในการใช้ข้อมูลอย่างเหมาะสม ที่เกี่ยวข้องกับการประมวลผลตามวัตถุประสงค์
3. การประเมินความเสี่ยงที่อาจเกิดผลกระทบกับความเป็นส่วนตัว สิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
4. แนวทางในการจัดการกับความเสี่ยงที่อาจเกิดขึ้น รวมถึงมาตรการในการรักษาความปลอดภัยของข้อมูลที่เหมาะสมเพื่อให้แน่ใจว่าท่านมีการคุ้มครองสิทธิเสรีภาพและประโยชน์อันของธรรมของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่นที่มีความเสี่ยงที่จะได้รับผลกระทบ หากท่านพิจารณาแล้วว่าระดับของความเสี่ยงนั้นสูงเกินกว่าที่ท่านสามารถจัดให้มีมาตรการในการลดความเสี่ยงนั้นได้ ท่านควรพิจารณาไม่กระทำการประมวลผลข้อมูลส่วนบุคคลหรือปรึกษาคณะกรรมคุ้มครองข้อมูลส่วนบุคคลก่อน

การจัดทำ DPIA เป็นกระบวนการที่ท่านควรเริ่มจัดทำก่อนการทำการประมวลผลข้อมูลและดำเนินการควบคู่ไปกับกระบวนการวางแผนและพัฒนา และทำอย่างต่อเนื่อง หากขั้นตอนในการจัดทำ DPIA มีความละเอียดและชัดเจน ก็จะเป็นการเพิ่มประสิทธิภาพและประสิทธิผลในการประมวลผลข้อมูลอย่างเหมาะสม ท่านอาจพิจารณาขั้นตอนในการจัดทำ DPIA เพิ่มเติมตามดังภาพด้านล่าง เพื่อใช้ในการจัดทำ DPIA ได้อย่างครอบคลุมยิ่งขึ้น



ขั้นตอนในการจัดทำ DPIA (Steps carry out a DPIA)

ในการพิจารณาการจัดทำ DPIA นั้นได้กำหนดให้จำเป็นต้องทำเมื่อมีกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ซึ่งท่านสามารถพิจารณากิจกรรมการประมวลผลที่เข้าข่ายเป็นกิจกรรมที่มีความเสี่ยงสูงได้ ตามหลักการของ GDPR ดังต่อไปนี้

- Systematic and Extensive Profiling with Significant Effects การประมวลผลข้อมูลด้วยระบบอัตโนมัติ หรือ การทำ Profiling ที่อาจมีผลกระทบอย่างมีนัยสำคัญ
- Process Special Category or Criminal Offence Data on a Large Scale การประมวลผลข้อมูลที่มีความอ่อนไหว เช่น ข้อมูลประวัติอาชญากรรม ข้อมูลพฤติกรรมทางเพศ เป็นจำนวนมาก
- Systematically Monitor Publicly Accessible Places on a Large Scale ระบบการตรวจตราที่ใช้เฝ้าดูพื้นที่สาธารณะเป็นจำนวนมาก เช่น ศูนย์การค้า ห้องสมุด

กรอบในการพิจารณาที่จะช่วยในการตัดสินใจของท่านว่าในกรณีใดท่านมีความจำเป็นที่ต้องทำ DPIA สามารถทำตามมาตรฐานสากลของ GDPR กำหนดให้หากกิจกรรมการประมวลผลข้อมูลส่วนบุคคลเข้าข่ายตามเกณฑ์ที่ระบุตั้งแต่ 2 ข้อขึ้นไป

1. (Evaluation or Scoring) เป็นกระบวนการทำโปรไฟลิ่งหรือการประเมินผลหรือให้คะแนนโดยระบบอัตโนมัติ และการใช้ข้อมูลส่วนบุคคลเพื่อการคาดการณ์ (prediction) โดยเฉพาะเมื่อการประมวลผลนั้นมีความเกี่ยวข้องกับข้อมูลส่วนบุคคลเชิงลึก เช่น พฤติกรรม, ความชอบ, สุขภาพ, หรือ ตำแหน่งที่ตั้ง เป็นต้น
2. (Automated-Decision Making with Legal or Similar Significant Effect) หากกิจกรรมการประมวลผลข้อมูลส่วนบุคคลมีการใช้เทคโนโลยีเพื่อทำการตัดสินใจอัตโนมัติ ในเรื่องที่ส่งผลกระทบกับกฎหมายหรือในเรื่องที่ส่งผลกระทบกับบุคคลอย่างมีนัยสำคัญ เช่น อาจทำให้ถูกเลือกปฏิบัติ
3. (Systematic Monitoring) ระบบการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องกับ การติดตาม การสังเกต สอดส่อง หรือควบคุมบุคคล โดยเฉพาะในพื้นที่ที่บุคคลสาธารณะสามารถเข้าถึงได้ (Public Accessible Area) เช่น ระบบเฝ้าระวังหรือตรวจตราในพื้นที่สาธารณะ โดยที่บุคคลไม่อาจทราบถึงหรือไม่รู้ล่วงหน้าว่ามีกิจกรรมการประมวลผลนี้ หรือไม่ทราบว่ามีผู้ควบคุมข้อมูลส่วนบุคคลเป็นใครและกำลังทำอะไรอยู่ ส่งผลให้เป็นการยากที่เจ้าของข้อมูลส่วนบุคคลจะสามารถหลีกเลี่ยง หรือ ปฏิเสธการมีส่วนร่วมได้
4. (Sensitive Data) เมื่อกิจกรรมการประมวลผลข้อมูลส่วนบุคคลนั้นเกี่ยวข้องกับข้อมูลอ่อนไหว เช่น เชื้อชาติ, เผ่าพันธุ์, ประวัติอาชญากรรม, ความเห็นทางการเมือง เป็นต้น (โปรดดูรายละเอียดเพิ่มเติมในหัวข้อ 5.4 ข้อมูลอ่อนไหว) เนื่องจากการประมวลผลข้อมูลดังกล่าว
5. (Data Processed on a Large Scale) หากการประมวลผลข้อมูลส่วนบุคคลนั้นเป็นการประมวลผลข้อมูลส่วนบุคคลจำนวนมาก โดยพิจารณาจากจำนวนเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง, ปริมาณข้อมูลหรือเนื้อหาของข้อมูลส่วนบุคคล, ระยะเวลาของกิจกรรมประมวลผล, และ ขอบเขตทางภูมิศาสตร์ของกิจกรรมการประมวลผล
6. (Datasets That Have Been Matched or Combined) ชุดข้อมูลที่เกิดจากการรวบรวมหรือเปรียบเทียบข้อมูลส่วนบุคคลที่มาจากแหล่งข้อมูลหลายแหล่ง ที่มีวัตถุประสงค์ในการประมวลผลข้อมูลต่างกัน ข้อมูลที่ถูกนำมารวมหรือเปรียบเทียบไม่จำกัดว่าเป็นข้อมูลที่ถูกประมวลผลแล้ว และไม่จำกัดว่าแหล่งข้อมูลมาจากท่านเองแต่อาจมาจากผู้ควบคุมข้อมูลอื่นก็ได้ ซึ่งการทำเช่นนี้อาจทำให้การประมวลผลข้อมูลส่วนบุคคลนั้นผิดจากวัตถุประสงค์ที่ได้มีการแจ้งเจ้าของข้อมูลส่วนบุคคลไว้ในตอนแรก อีกทั้งอาจไม่เป็นไปตามความคาดหมายอย่างสมเหตุสมผลของเจ้าของข้อมูลส่วนบุคคลได้
7. (Data Concerning Vulnerable Data Subjects) หากองค์กรมีการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับผู้เปราะบาง (Vulnerable Person) เช่น ผู้เยาว์ ผู้อพยพ ผู้ป่วยทางจิต หรือ

ผู้สูงวัย GDPR ให้จัดว่ากิจกรรมการประมวลผลนั้นมีความเสี่ยงที่จะทำให้เกิดผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล เนื่องจากผู้เปราะบางอาจไม่อยู่ในสภาพที่สามารถให้ความยินยอมหรือปฏิเสธการประมวลผลข้อมูลส่วนบุคคลได้ รวมถึงการทำโปรไฟลิ่งข้อมูลของผู้เยาว์หรือการให้บริการออนไลน์แก่ผู้เยาว์โดยเฉพาะเพื่อวัตถุประสงค์การทำการตลาดแบบตรง

8. (Innovative Use or Applying Technological or Organizational Solutions) เมื่อมีการประมวลผลข้อมูลส่วนบุคคลซึ่งเกิดจากเทคโนโลยีใหม่ที่มีการใช้อย่างกว้างขวางในชีวิตประจำวันของเจ้าของข้อมูลส่วนบุคคล เช่น การ สแกนลายนิ้วมือ และใบหน้า ซึ่งอาจจะนำไปสู่ความเสี่ยงที่นอกเหนือความคาดหมายได้ เนื่องด้วยเทคโนโลยีดังกล่าวยังไม่เคยปรากฏหรือใช้มาก่อน ท่านจึงอาจไม่มีข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นได้ต่อเจ้าของข้อมูลส่วนบุคคล
9. (Data Transfer Across Borders) หากมีการโอนข้อมูลไปยังต่างประเทศ สามารถดูรายละเอียดเพิ่มเติมได้ที่หัวข้อ “6.1 การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ” นอกจากท่านจะต้องพิจารณากฎหมายและมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทางแล้ว ยังต้องพิจารณาถึงความเป็นไปได้ที่ข้อมูลนั้นอาจถูกส่งต่อด้วย
10. (Prevents Data Subjects from Exercising a Right or Using a Service or a Contract) หากกิจกรรมการประมวลผลนั้นอาจส่งผลให้เกิดการเปลี่ยนแปลงหรืออาจถูกปฏิเสธสิทธิของเจ้าของข้อมูล หรืออาจถูกปฏิเสธการได้รับบริการหรือการเข้าทำสัญญาของเจ้าของข้อมูล เช่น ท่านมีกระบวนการคัดกรองลูกค้า จากการประมวลผลข้อมูลของลูกค้ากับฐานข้อมูลของท่าน เพื่อตรวจสอบข้อมูลเครดิตและตัดสินใจว่าจะให้ลูกค้าเข้าทำสัญญาเงินกู้กับท่านหรือไม่

อย่างไรก็ตามในกรณีที่กิจกรรมประมวลผลข้อมูลนั้นเข้าข่ายตามเกณฑ์ที่ได้ระบุไว้มากกว่าสองข้อ ท่านสามารถเลือกที่จะไม่ทำ DPIA ได้ หากพิจารณาแล้วว่าการประมวลผลข้อมูลส่วนบุคคลนั้นจะไม่ส่งผลกระทบที่ทำให้เกิดความเสี่ยงสูงต่อเจ้าของข้อมูลส่วนบุคคล โดยท่านควรที่จะทำการปรึกษากับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลก่อนเพื่อพิจารณาถึงความเหมาะสม รวมถึงทำการจดบันทึกถึงเหตุผลที่ท่านใช้ในการตัดสินใจไม่ทำ DPIA หรือกรณีที่แม้เข้าข่ายเพียงหนึ่งข้อแต่อาจส่งผลกระทบที่ทำให้เกิดความเสี่ยงสูงกับเจ้าของข้อมูลส่วนบุคคล ท่านก็จำเป็นจะต้องจัดทำ DPIA

ตัวอย่าง แบบฟอร์มการทำ DPIA

1. จุดประสงค์ในการจัดทำ DPIA

อธิบายอย่างละเอียดถึงกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้อง วัตถุประสงค์ และประเภทของการประมวลผลข้อมูล และระบุเหตุผลที่ในการจัดทำ DPIA สำหรับกิจกรรมการประมวลผลนั้น และหากมีเอกสารที่เกี่ยวข้องโปรดแนบมาพร้อมแบบฟอร์มนี้ :

……

……

……

2. รายละเอียดของกิจกรรมการประมวลผล

(Nature of data processing) ระบุรูปแบบของกิจกรรมการประมวลผลที่เกี่ยวข้อง โดยอธิบายถึงรายละเอียดหากคุณจะมีการเก็บรวบรวม ใช้ เปิดเผย หรือ ทำลายข้อมูลส่วนบุคคล และโปรดระบุหากมีการส่งต่อข้อมูลส่วนบุคคลไปยังองค์กรอื่น และส่วนไหนของกิจกรรมการประมวลผลข้อมูล นั้นพิจารณาแล้วว่ามีความเสี่ยงสูง

……

……

……

(Scope) ขอบเขตของกิจกรรมการประมวลผลข้อมูล อธิบายถึงรูปแบบในการประมวลผลข้อมูลส่วนบุคคลที่มีความเกี่ยวข้อง โดยระบุหากข้อมูลส่วนบุคคลนั้นนับว่าเป็นข้อมูลอ่อนไหว เช่น ประวัติอาชญากรรมหรือ ข้อมูลทางด้านสุขภาพ และโปรดระบุถึงรายละเอียดการเก็บรวบรวมหรือใช้ของข้อมูลที่เกี่ยวข้องในแง่ของปริมาณ ความถี่ในการเก็บรวบรวม ระยะเวลาในการจัดเก็บ และมีเจ้าของข้อมูลส่วนบุคคลกี่คนที่อาจจะได้รับผลกระทบ

……

……

……

(Context) ระบุถึงบริบทของกิจกรรมการประมวลผล โดยอธิบายถึงความสัมพันธ์ระหว่างองค์กรและเจ้าของข้อมูลส่วนบุคคล ขอบเขตของการควบคุมที่เจ้าของข้อมูลส่วนบุคคลมีความคาดหมายของเจ้าของข้อมูลส่วนบุคคลต่อกิจกรรมการประมวลผลนี้ เจ้าของข้อมูลส่วนบุคคลนั้นมีกลุ่มของเยาวชน

หรือบุคคลอ่อนไหวหรือไม่ และโปรดระบุหากมีเคยมีการแจ้งองค์กรถึงความเสี่ยงต่อกิจกรรมการประมวลผลนี้

……

……

……

(Purpose) อธิบายถึงจุดประสงค์ของกิจกรรมการประมวลผลข้อมูลนี้ จุดมุ่งหมายของคุณคืออะไร, ผลกระทบที่น่าจะเกิดต่อเจ้าของข้อมูลส่วนบุคคล, และ ผลประโยชน์ที่องค์กรจะได้รับจากกิจกรรมการประมวลผลนี้

……

……

……

3. การพิจารณาความจำเป็นและสัดส่วนของกิจกรรมการประมวลผลที่เหมาะสม

(Nature) ระบุถึงมาตรการ และ ฐานกฎหมายที่ใช้ในกิจกรรมการประมวลผล โดยอธิบายถึงความเกี่ยวข้องระหว่างกิจกรรมการประมวลผลและเป้าหมายของกิจกรรมการประมวลนั้น และโปรดระบุหากมีวิธีการอื่นที่จะช่วยให้องค์กรบรรลุจุดมุ่งหมายดังกล่าวได้นอกเหนือจากกิจกรรมการประมวลผลนั้น คุณมีมาตรการอย่างไรในการแจ้งและการสนับสนุนการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

……

……

……

4. การพิจารณาและประเมินความเสี่ยง

อธิบายถึงที่มาของความเสี่ยงและผลกระทบที่น่าจะเกิดขึ้นต่อเจ้าของข้อมูลส่วนบุคคล

……

……

……

<u>ความน่าจะเป็นที่ผลกระทบจะเกิดขึ้น (Likelihood)</u>

❒ โอกาสต่ำ ❒ โอกาสปานกลาง ❒ โอกาสสูง

ความร้ายแรงของผลกระทบ (Severity)

❒ ไม่ร้ายแรง ❒ ร้ายแรงปานกลาง ❒ ร้ายแรงมาก

ความเสี่ยงโดยรวม (Overall Risk)

ความเสี่ยงต่ำ	ความเสี่ยงสูง	ความเสี่ยงสูง
ความเสี่ยงต่ำ	ความเสี่ยงปานกลาง	ความเสี่ยงสูง
ความเสี่ยงต่ำ	ความเสี่ยงต่ำ	ความเสี่ยงต่ำ

13. เหตุการณ์การรั่วไหลของข้อมูลส่วนบุคคล (Personal Data Breach)

การรั่วไหลของข้อมูลส่วนบุคคล หมายถึง การที่ข้อมูลส่วนบุคคลถูกทำลาย การสูญหาย การแก้ไขเปลี่ยนแปลง การเปิดเผย หรือการเข้าถึง ส่งต่อ เก็บ รักษาหรือถูกประมวลผลอย่างอื่นไม่ว่าจะเกิดจากการกระทำอันมิชอบด้วยกฎหมายหรือโดยอุบัติเหตุ

ในกรณีที่มีการรั่วไหลของข้อมูลส่วนบุคคลเกิดขึ้น ผู้ที่ทราบเหตุจะต้องมีการแจ้งไปยังเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยเร็วที่สุด เพื่อที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะทำการตรวจสอบถึงสาเหตุที่มาและระบุจุดต้นเหตุของการรั่วไหล รวมทั้งออกมาตรการเยียวยาเหตุการณ์รั่วไหลของข้อมูล พร้อมทั้งแจ้งแก่เจ้าของข้อมูลส่วนบุคคลและ/หรือสำนักงานคุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายกำหนดโดยไม่ชักช้า

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่จดบันทึกการรั่วไหลของข้อมูลส่วนบุคคล และประเมินความเสี่ยงเมื่อเกิดการรั่วไหลของข้อมูลส่วนบุคคลขึ้น ในการประเมินความเสี่ยงจากการรั่วไหลของข้อมูลนั้น อาจพิจารณาถึงผลกระทบต่อสิทธิและเสรีภาพขั้นพื้นฐาน ผลกระทบต่อชีวิตและทรัพย์สินของเจ้าของข้อมูลส่วนบุคคล เนื่องจากหากพิจารณาแล้วว่า ไม่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสามารถทำการจดบันทึกไว้และอาจไม่จำเป็นต้องมีการแจ้งแก่เจ้าของข้อมูลส่วนบุคคลหรือแจ้งต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคลถึงเหตุการณ์การรั่วไหลที่เกิดขึ้น แต่หากผลของการประเมินแสดงให้เห็นว่าการรั่วไหลของข้อมูลอาจจะทำให้เกิดความเสี่ยงสูง ซึ่งมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องมีการดำเนินการแจ้งแก่เจ้าของข้อมูลส่วนบุคคลรวมทั้งแนวทางในการเยียวยาอีกทั้งแจ้งเหตุละเมิดของข้อมูลส่วนบุคคลแก่สำนักงานคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายในระยะเวลา 72 ชั่วโมง นับจากทราบเหตุการณ์การรั่วไหลของข้อมูลส่วนบุคคล

ท่านควรมีการจัดทำแบบฟอร์มบันทึกการรั่วไหลของข้อมูลส่วนบุคคล ขึ้นเพื่อเป็นแนวทางในการจดบันทึกอย่างถูกต้องและครบถ้วน สำหรับหน้าที่ในการจดบันทึกควรกำหนดให้เป็นหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือในกรณีที่พนักงานผู้พบเหตุการณ์รั่วไหลของข้อมูลอาจให้พนักงานผู้พบเหตุการณ์เป็นผู้ทำการบันทึกแทนเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลก็ได้แล้วแต่กรณี และแจ้งแก่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทราบถึงเหตุการณ์การรั่วไหลของข้อมูลที่เกิดขึ้นด้วย เพื่อให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลดำเนินการหาสาเหตุและมาตรการเยียวยา รวมถึงติดตามผลการดำเนินงานการแก้ไขปัญหาการรั่วไหลของข้อมูล

ตัวอย่าง แบบฟอร์มการบันทึกการรั่วไหลของข้อมูลส่วนบุคคล

โปรดระบุรายละเอียดเหตุการณ์การรั่วไหลของข้อมูลส่วนบุคคล

วันและเวลาที่คุณพบการรั่วไหล : .....

โปรดอธิบายอย่างละเอียดถึงเหตุการณ์ที่เกิดขึ้น :

.....

.....

.....

คุณพบการรั่วไหลได้อย่างไร :

.....

.....

วันและเวลาที่การรั่วไหลเกิดขึ้น : .....

ประเภทของเจ้าของข้อมูลส่วนบุคคล (เลือกทุกข้อที่มีความเกี่ยวข้อง)

❒ ลูกค้า ❒ พนักงาน

❒ ผู้เยาว์ ❒ ไม่ทราบแน่ชัด

❒ อื่น ๆ (โปรดระบุ) .....

ประเภทของข้อมูลที่เกิดการรั่วไหล (เลือกทุกข้อที่มีความเกี่ยวข้อง)

❒ ข้อมูลทั่วไป เช่น ชื่อ ข้อมูลติดต่อ ❒ เอกสารทางการ เช่น บัตรประชาชน

❒ Usernames, Passwords ❒ ข้อมูลด้านการเงิน เช่น เลขบัตรเครดิต

❒ ข้อมูล GPS locations ❒ ข้อมูลเกี่ยวกับเชื้อชาติ หรือ สัญชาติ

❒ ข้อมูลด้านความคิดเห็นทางการเมือง ❒ ข้อมูลเกี่ยวกับศาสนา

❒ ข้อมูลเกี่ยวกับเพศ ❒ ข้อมูลเรื่องสุขภาพ

❒ ข้อมูลทางชีวภาพ ❒ ประวัติอาชญากรรม

❒ ยังไม่ทราบ ❒ อื่น ๆ (โปรดระบุ) .....

ปริมาณโดยสังเขปของข้อมูลที่รั่วไหล : .....

ปริมาณโดยสังเขปของเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ : .....

.....

โปรดอธิบายอย่างละเอียดถึงผลกระทบที่น่าจะเกิดจากการรั่วไหล : .....

.....

ความน่าจะเป็นที่การรั่วไหลของข้อมูลส่วนบุคคลจะส่งผลกระทบที่เป็นการคุกคามต่อเจ้าของข้อมูลส่วนบุคคล :

❒ เป็นไปได้สูง

❒ เป็นไปได้

❒ เป็นกลาง

❒ เป็นไปได้ต่ำ

❒ เป็นไปไม่ได้

❒ ไม่ทราบแน่ชัด

โปรดอธิบายอย่างละเอียดถึงผลกระทบที่อาจจะเกิด หรือ เกิดไปแล้วต่อเจ้าของข้อมูลส่วนบุคคล

.....

.....

หากมีการล่าช้าในการแจ้งเหตุการณ์การรั่วไหลเกิดขึ้นโปรดชี้แจงเหตุผล

.....

.....

จงอธิบายมาตรการที่ได้บังคับใช้ในการควบคุมการรั่วไหลที่เกิดขึ้น

……

……

ได้มีการแจ้งเจ้าของข้อมูลส่วนบุคคลถึงเหตุการณ์การรั่วไหลหรือไม่

❒ มีการแจ้งเจ้าของข้อมูลส่วนบุคคลเรียบร้อยแล้ว

❒ อยู่ในระหว่างการดำเนินการแจ้งเจ้าของข้อมูลส่วนบุคคล

❒ มีการตัดสินใจที่จะไม่แจ้งเจ้าของข้อมูลส่วนบุคคล

❒ อยู่ในระหว่างการตัดสินใจขององค์กร

❒ อื่น ๆ (โปรดระบุ) ……

ได้มีการแจ้งคณะกรรมการหรือองค์กรที่เกี่ยวข้องถึงเหตุการณ์การรั่วไหลหรือไม่

❒ มีการแจ้ง

❒ ไม่มีการแจ้ง

❒ ยังไม่ทราบแน่ชัด

หากตอบว่ามีการแจ้ง โปรดชี้แจงรายละเอียด

……

……

……

14. Q&A

คำถาม	คำตอบ
การเก็บข้อมูลส่วนบุคคลของคู่สมรส และบุตรของผู้เข้ารับบริการวางแผนทางการเงิน เช่น อายุ เพศ รายได้ การศึกษา สุขภาพ เพื่อวัตถุประสงค์ในการวางแผนการเกษียณ การศึกษาบุตร สามารถพิจารณาใช้ฐานผลประโยชน์อันชอบธรรมได้หรือไม่	เนื่องด้วยข้อมูลสุขภาพเป็นข้อมูลอ่อนไหว (sensitive data) ของเจ้าของข้อมูลส่วนบุคคล ท่านไม่สามารถพิจารณาใช้ฐานผลประโยชน์อันชอบธรรมสำหรับกรณีดังกล่าวได้ หากท่านมีความจำเป็นต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (ประมวลผลข้อมูลส่วนบุคคล) ดังกล่าว ท่านต้องพิจารณาขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลให้ชัดแจ้งก่อนหรือในขณะที่ทำการประมวลผลข้อมูลส่วนบุคคล
การระบุผู้รับผลประโยชน์ในกรมธรรม์ กองทุนสำรองเลี้ยงชีพ (PVD) หรือการระบุทายาทในพินัยกรรม สามารถใช้ฐานผลประโยชน์อันชอบธรรมได้หรือไม่	ประเด็นดังกล่าวท่านสามารถนำหลักการผลประโยชน์อันชอบธรรม (Legitimate Interest) มาปรับใช้ ทั้งนี้ ท่านต้องมีการพิจารณา 3 part test ก่อนที่จะนำหลักผลประโยชน์อันชอบธรรมมาปรับใช้
การเปิดเผยข้อมูลของผู้รับคำปรึกษาให้แก่สำนักงานบัญชี สำนักงานกฎหมาย ตัวแทนประกันชีวิต เพื่อนำเสนอผลิตภัณฑ์หรือบริการ ต้องพิจารณาใช้ฐานใด	การเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลภายนอกเพื่อวัตถุประสงค์ในการนำเสนอผลิตภัณฑ์หรือบริการ กรณีนี้ท่านต้องขอความยินยอมจากผู้รับคำปรึกษาให้ชัดแจ้งก่อนหรือในขณะที่ทำการประมวลผลข้อมูลส่วนบุคคล
การขอความยินยอมโดยชัดแจ้งทำโดยวิธีตามข้อ 5.3.6 เลยได้หรือไม่ หากได้ ตัวอย่างแบบฟอร์มการขอความยินยอมในข้อดังกล่าว สามารถใช้ขอความยินยอมรวมกันระหว่างข้อมูลส่วนบุคคลกับข้อมูลอ่อนไหวเลยได้หรือไม่	สามารถขอความยินยอมตามข้อดังกล่าวได้ ทั้งนี้รายละเอียดเรื่องความชัดแจ้งขอให้พิจารณาเพิ่มเติมจากกฎหมายลำดับรอง แนวปฏิบัติ/คู่มือของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หรือกฎหมายอื่น ๆ ที่เกี่ยวข้องซึ่งอาจประกาศเพิ่มเติมในภายหลัง ท่านสามารถพิจารณาใช้แบบฟอร์มดังกล่าวสำหรับการขอความยินยอมจากเจ้าของข้อมูล

คำถาม	คำตอบ
	ส่วนบุคคล ทั้งในกรณีข้อมูลส่วนบุคคล และข้อมูลส่วนบุคคลอ่อนไหว โดยควรระบุประเภท และตัวอย่างของข้อมูลส่วนบุคคลที่ท่านเก็บรวบรวมให้ชัดเจน เช่น - ข้อมูลส่วนบุคคล เช่น ชื่อ นามสกุล หมายเลขโทรศัพท์ อีเมล - ข้อมูลส่วนบุคคลอ่อนไหว เช่น ข้อมูลสุขภาพ
ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมก่อนวันที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มีผลใช้บังคับ ต้องดำเนินการอย่างไร	ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลได้เก็บรวบรวมไว้ก่อนวันที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมีผลใช้บังคับ ให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิม ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย (มาตรา 95)

เอกสารอ้างอิง

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. 2565
- คู่มือการให้คำปรึกษาการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ฉบับลงวันที่ 30 พฤษภาคม 2565
- คู่มือ PDPA สำหรับประชาชน ฉบับลงวันที่ 23 มิถุนายน 2565
- แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคาร สมาคมธนาคารไทย (Guideline on Personal Data Protection for Thai Banks)
- Thailand Data Protection Guidelines 1.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล กันยายน 2561 ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
- Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ตุลาคม 2562 ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
- Thailand Data Protection Guidelines 3.0 Extension แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เมษายน 2564 ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

Deloitte.